Assessment Report

Internal Network Penetration Test

For: SAMPLE

Date: Dec 11th 2024

Assessment Information

Assessor:
ECR Security
5501A Balcones Dr
Suite 186

Austin, Texas 78731
(512) 861-9399
https://www.ecrsecurity.com
info@ecrsecurity.com

Assessor Name:
Brian Milliron

Client:
SAMPLE
123 Contoso Rd

Point of Contact:
John Doe
IT Director
555-555-1212
jdoe@contoso.com

Assessment Scope Summary

Engagement Timeframe: November 27th to December 9th, 2024
Engagement Type: Internal Network Penetration Test
Engagement Scope: 300 internal IPs
Report Date: December 11th 2024

Revision History

Date	Version	Description	Author
12/11/2024	1	Final report	Brian Milliron

Table of Contents

Engagement Overview

ECR Security is a professional penetration testing firm. Penetration testing is the process of simulating real-world attacks with the objective of identifying security vulnerabilities that could negatively affect the organization's IT systems, the data they handle, and consequently the business.

Internal network testing assesses the organization's security from the perspective of an inside attacker. This can be a disgruntled employee, external attacker which has breached the network perimeter, wireless network, or gained access to the physical facilities to attach a malicious device to the internal network. In addition to testing for vulnerabilities, this assessment tests the organization's detection and response capabilities, confirming the effectiveness of SIEM and log aggregation technologies.

For each vulnerability discovered during the assessment, ECR Security attributed a risk severity rating and, whenever possible, validated the existence of the vulnerability with working exploit code. The issues' severity classification is based on the potential it presents to provide means for fraud, data leakage, and other harmful events that may bring a direct adverse impact to the business.

As a time-boxed and best-effort exercise, the nature of penetration testing does not guarantee there are no other security issues in the scope under assessment, or that computer intrusion will not happen in the future. This assessment report should be considered a point in time snapshot of the organization's security posture, which may no longer be valid if changes to the infrastructure, application code, configuration and architecture have occurred.

Business Risk Summary

Financial Loss: If a business's IT security is breached, it can result in financial losses due to theft, fraud, or the cost of remedying the issue. This can include direct costs such as fines, legal fees, and compensation, as well as indirect costs such as reputation damage, loss of customer trust, and loss of revenue.

Operational Disruption: If a business's systems are compromised, it can disrupt their operations, leading to downtime, loss of productivity, and inability to provide services to customers. This can also result in reputation damage, as customers may become frustrated with the lack of service.

Regulatory Compliance: Depending on the industry, businesses may be subject to various regulatory requirements related to data security. If they fail to comply with these requirements, they may face penalties or fines.

Data Breaches: A security vulnerability can lead to data breaches, which can result in sensitive information being exposed or stolen. This can include personal information of customers or employees, financial information, trade secrets, and other confidential information. Data breaches can result in significant legal and financial consequences, as well as reputation damage.

Damage to Reputation: A security breach can damage a business's reputation, especially if sensitive information is exposed. Customers may lose trust in the business, which can result in a loss of revenue and difficulty in acquiring new customers.

Summary of Findings

ECR Security reviewed the security of SAMPLE's infrastructure and has determined a **Critical** risk of compromise from internal attackers, as shown by the presence of the vulnerabilities detailed in this report. The detailed findings and remediation recommendations for these assessments may be found later in the report.

Overall Severity Rating	
Overall Technical Severity Score	**Critical Risk**
*Remediation of the Critical and High findings would reduce the overall severity rating to **Medium Risk**.*	

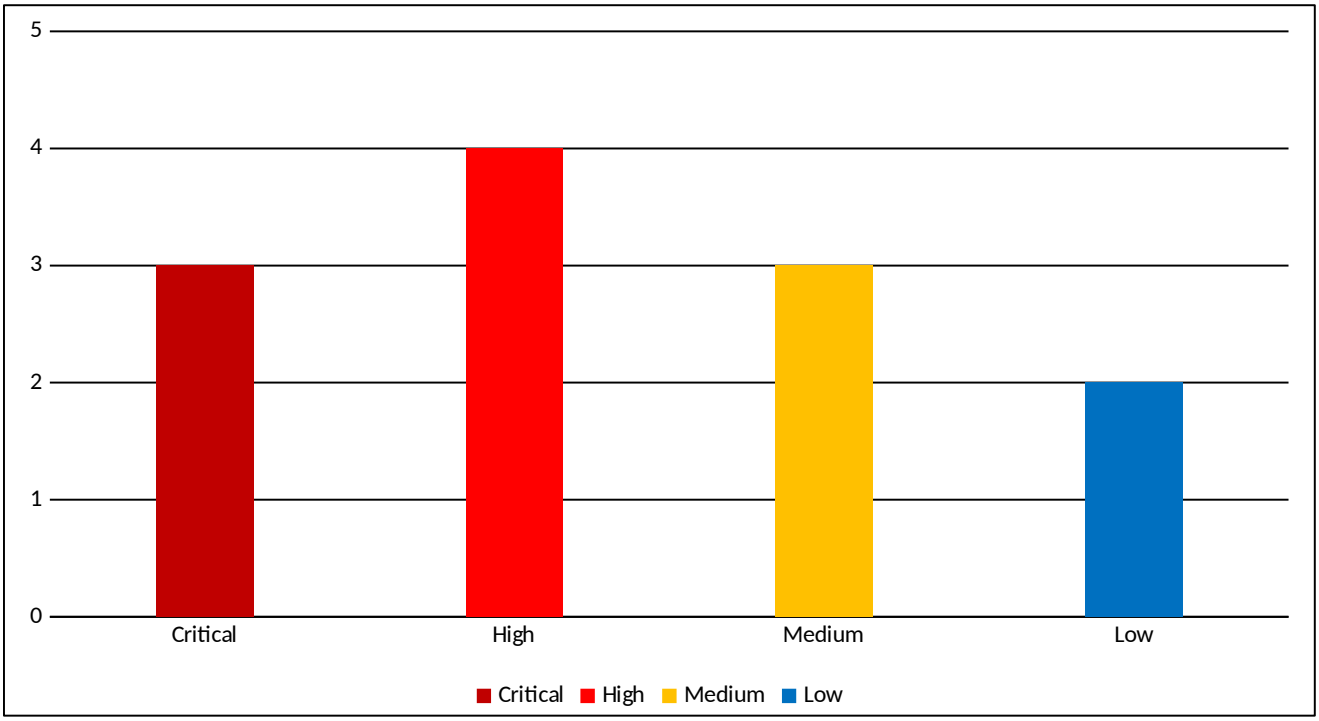


Table 1 – Vulnerabilities validated

Severity Rating	ID	Issue Name	Staus
Critical	C1	Log4jShell RCE	Open
Critical	C2	MS17-010: EternalBlue Vulnerability	Open
Critical	C3	Cisco DCNM Authentication Bypass	Open
High	H1	Default Password	Open
High	H2	IPMI Password Hashes Exposed	Open
High	H3	Kerberos Pre-Authentication Not Required	Open
High	H4	Local Admin Password Reuse	Open
Medium	M1	Plaintext Authentication	Open
Medium	M2	Unrestricted NFS Share	Open
Medium	M3	End of Life/Unsupported Software	Open
Low	L1	Information Disclosure	Open
Low	L2	SNMP Default Community String	Open

Table 2 – Listing of Vulnerabilities

Summary of Strengths

While ECR Security was tasked with finding issues and vulnerabilities dealing with the current environment, it is useful to know when positive findings appear. Understanding the strengths of the current environment can reinforce security best practices and provide strategy and direction toward a robust defensive posture. The following traits were identified as strengths in SAMPLE's environment.

1. Strong inbound firewall rules for database services, restricting access to only a select few trusted machines.
2. Excellent group management that restricted which users are local administrators to domain joined machines, as well as which users are allowed to Remote Desktop in.
3. Strong NTLM relay protections. SMB signing was required on all tested machines. Additionally broadcast name resolution such as LLMNR and mDNS was not found to be in use.

Summary of Weaknesses

ECR Security discovered and investigated many vulnerabilities during the course of its assessments for SAMPLE. We have categorized these vulnerabilities into general weaknesses across the current environment, and provide direction toward remediation for a more secure enterprise.

1. Three tested devices were found to be running out of date software with known critical vulnerabilities that can lead to system compromise and, combined with the weaknesses listed below, full compromise of both the Active Directory domain and the network infrastructure.
2. Best practices regarding secure Active Directory account creation were not followed. In particular, Kerberos pre-authentication is not required on Domain Administrator accounts. Additionally Domain Administrator accounts are not required to use passwords of a sufficient strength to resist password cracking attempts.
3. Local Administrator passwords are shared across a large number of tested machines. This facilitates easy lateral movement across the network once a single machine is breached and the shared password recovered.
4. IPMI devices were not properly segmented from the network, allowing any connected client to retrieve the password hash of the ADMIN user.
5. Default passwords were found to be in use on two devices, allowing anyone connected to the internal network to gain administrative access to those devices and possibly to disrupt the services they provide or use them as a staging point to launch attacks on other devices.

Strategic Recommendations

Review the organization’s patch management process in order to determine how and why critical vulnerabilities such as C1, C2, and C3 have gone unpatched. It could be those devices have been overlooked, are on subnets which are not scanned, are not domain joined, or have been excluded from scans. Examine whether there are patch management exemptions in place and whether the reasons for those exemptions are still valid.

Review the organization’s technical process and procedure documentation regarding creation and management of administrative accounts, changing default passwords, setting up file shares, and securely setting up web pages for internal company use. Ensure process and procedure guidelines are up to date and reflect the organization’s security goals. Also ensure that IT personnel know about the process and procedure documentation and where to access it.

Review the organization’s policies for handling unsupported and end of life software. Ensure that these policies reflect the organization’s security goals as well as the pragmatic realities of IT operational needs.

Rules of Engagement

The assessment did not include the following mechanisms:

- Intrusive tests or exploits that intentionally crash or disable a service.
- Brute forcing of passwords likely to lock out accounts.
- Denial of Service (DoS)
- Test cases that could result in damage to systems or data

Internal Penetration Testing

SAMPLE approved the following engagement rules:

Internal Testing Activities		
Is ECR Security approved to perform validation of vulnerabilities that may lead to system access?	☒ Yes	☐ No
Is ECR Security approved to perform web application attacks that may include execution of system commands on the affected systems?	☒ Yes	☐ No
Are all in-scope systems available from a single network segment?	☒ Yes	☐ No
Is ECR Security approved to perform ARP poisoning attacks	☒ Yes	☐ No
Is ECR Security approved to perform other man-in-the-middle attacks	☒ Yes	☐ No
Are all internal parties notified of ECR Security testing activities?	☒ Yes	☐ No
In the event that ECR Security is able to penetrate a system, is ECR Security approved to perform the following:		
Perform privilege escalation attacks (if needed)?	☒ Yes	☐ No
Obtain local password hashes and perform attempts to crack passwords	☒ Yes	☐ No
Leverage the system to pivot within the organization	☒ Yes	☐ No
Utilize information from the compromised system against other devices	☒ Yes	☐ No
If ECR Security is able to gain access to privileged accounts, does ECR Security have permission to attempt access to sensitive devices?	☒ Yes	☐ No
If ECR Security is able to gain access to the domain controller, does ECR Security have permission to attempt to create accounts?	☒ Yes	☐ No
If ECR Security is able to gain access to the domain controller, does ECR Security have permission to recover password hashes?	☒ Yes	☐ No
Is ECR Security authorized to use any collected data in other services being delivered?	☒ Yes	☐ No

Internal Penetration Testing Scope

SAMPLE identified the following internal IP addresses as being in scope for the engagement:

In-Scope IP Addresses		
10.180.150.0/24	10.182.66.0/24	10.120.98.0/24
10.195.101.0/24	10.208.180.0/24	10.180.6.0/24
192.168.5.0/24	192.168.6.0/24	10.0.0.0/24
192.168.55.0/24	192.168.88.0/24	192.168.0.0/24

Methodology

Test cases were limited to issues that would identify deficiencies in leading practices, regulatory and industry standards, including:

Leading Security Practices
• Industry best practices
• OWASP Top 10
• NIST SP 800-115
• Penetration Testing Execution Standard (PTES)
• Open Source Security Testing Methodology Manual (OSSTMM)

Step 1: Reconnaissance

Testing begins with enumeration of live hosts and research into the architecture and environment.

Step 2: Automated Testing

An automated vulnerability scan is conducted to identify software packages installed on hosts in the environment and the version or patch level. These are compared to a database of known vulnerabilities to identify potential vulnerabilities which may exist in the target environment.

Step 3: Vulnerability Verification

Potential vulnerabilities are researched and manually verified using test scripts and other technical methods to determine if the conditions for successful exploitation exist.

Step 4: Exploitation

A review of all previous data is conducted to determine if the previously identified vulnerabilities can be safely exploited and whether publicly available exploits exist. If both conditions are met, an exploitation attempt is conducted to prove exploitability under current conditions. In cases where the vulnerability poses a serious and immediate risk to the organization, the assessor will reach out to notify the point of contact by email and/or phone depending on severity.

Step 5: Privilege Escalation

Once a vulnerability has been successfully exploited, a discovery process is undertaken to determine additional business risk by searching the vulnerable asset for sensitive information. If possible, privilege escalation and/or lateral movement are conducted to discover how deep into the environment an attacker could potentially move using the previously exploited vulnerability.

Step 6: Reporting

Once the engagement is complete, a report is compiled including detailed analysis of each vulnerability and overall threat assessment. The report also includes proof of exploitability and technical data necessary for remediation.

Step 5: Retest (Optional)

After the client has finished remediating the discovered vulnerabilities, ECR Security offers optional retesting for all vulnerabilities listed in the report to verify whether the remediation effort was successful. At the conclusion of the remediation testing the report will be updated with a new risk level determination and vulnerabilities which have been closed will be marked as such.

C1: Log4jShell RCE

```
[+] The target is vulnerable.
[+] Delivering the serialized Java object to execute the payload...
[*] Client sent unexpected request 2
[!] http://10.180.138.22:443 handling request from 10.180.150.30; (UUID: 0nifgco
g) Without a database connected that payload UUID tracking will not work!
[*] http://10.180.138.22:443 handling request from 10.180.150.30; (UUID: 0nifgco
g) Staging python payload (40280 bytes) ...
[!] http://10.180.138.22:443 handling request from 10.180.150.30; (UUID: 0nifgco
g) Without a database connected that payload UUID tracking will not work!
[*] Meterpreter session 1 opened (10.180.138.22:443 -> 127.0.0.1 ) at 2022-04-21
 11:49:54 -0500
```

Figure 1 – Metasploit Log4shell scanner output

Description: One (1) ESXi server was observed to be vulnerable to the Log4jShell vulnerability (CVE-2021-44228). Apache Log4j2 versions 2.0-beta7 through 2.17.0 (excluding security fix releases 2.3.2 and 2.12.4) are vulnerable to a remote code execution (RCE) attack where an attacker with permission to modify the logging configuration file can construct a malicious configuration using a JDBC Appender with a data source referencing a JNDI URI which can execute remote code. This issue is fixed by limiting JNDI data source names to the Java protocol in Log4j2 versions 2.17.1, 2.12.4, and 2.3.2.

Impact: Because the java instance is running as root, exploiting the vulnerability grants instant root access to the underlying OS, and since the root password is weak and easily cracked this enables interactive logon as root, further expanding the scope of action a malicious actor can take. As root, a malicious actor can change any OS settings, including the password for the default vSphere admin account. Using this access, an attacker can gain control of VMs hosted by vSphere, possibly gaining additional user accounts and privileges in the process.

Recommendations:

- Apply vendor patches to remediate the Log4j vulnerability.
- Require root passwords to meet password complexity requirements.
- Create a non-root service account to run java instances.

Affected Host: 10.180.150.30

References:

https://kb.vmware.com/s/article/87068

https://www.vmware.com/security/advisories/VMSA-2021-0028.html

C2: MS17-010: EternalBlue Vulnerability

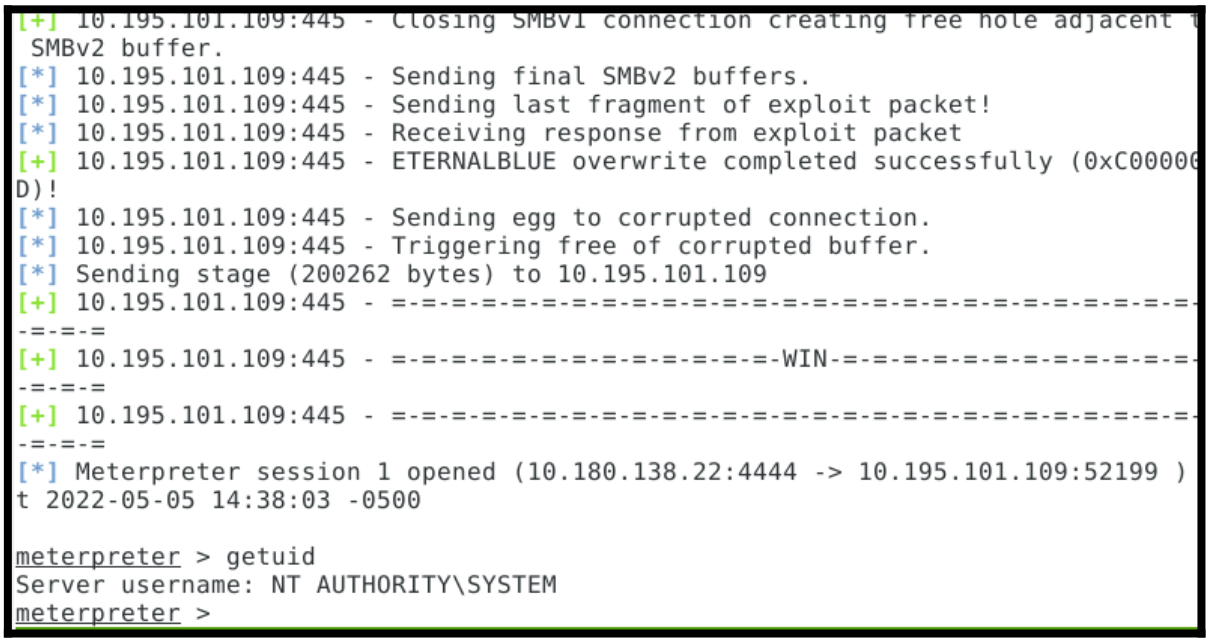


Figure 2 – EternalBlue exploit

Description: Two (2) hosts were observed to be vulnerable to MS17-10 EternalBlue vulnerability. 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.

Impact: An attacker can exploit EternalBlue to get SYSTEM privileges on the vulnerable host, gaining access to any cached credentials or password hashes on the machine, which can then be used for lateral movement or privilege escalation.

Recommendations: Windows 7 is End of Life and will be unsupported by Microsoft going forward. ECR Security recommends upgrading to a newer version of Windows still in the support window. If this is not possible then install security patch MS17-10 and/or disable SMBv1.

Affected Hosts:
10.120.98.36, 10.195.101.109

References:

https://www.sentinelone.com/blog/eternalblue-nsa-developed-exploit-just-wont-die/

https://www.hypr.com/security-encyclopedia/eternalblue

https://research.checkpoint.com/2017/eternalblue-everything-know/

C3: Cisco DCNM Authentication Bypass

Individual Issues Identified	Severity Rating
Cisco Data Center Network Manager < 11.1(1) Authentication Bypass Vulnerability (CVE-2017-6640)	**Critical**
Cisco Data Center Network Manager Command Injection Vulnerability (CVE-2019-15978)	**Critical**

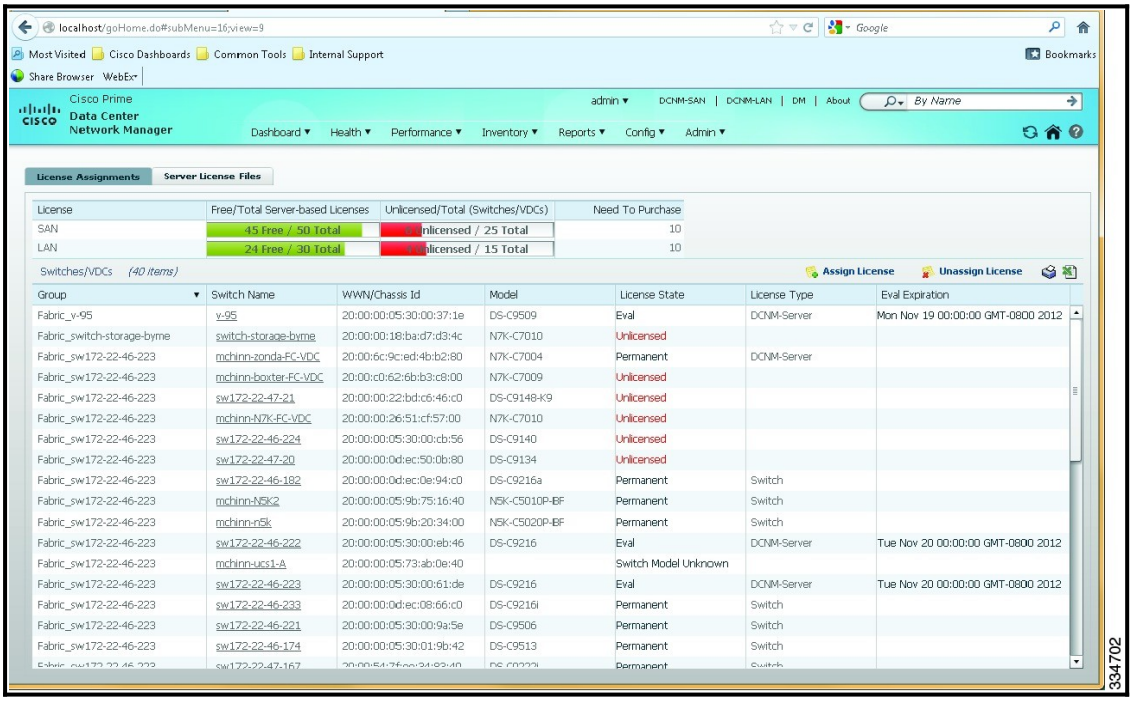


Figure 3 - Cisco Data Center Network Manager < 11.1(1) Authentication Bypass Vulnerability

Description: The Cisco Prime Data Center Network Manager (DCNM) running on the remote host is affected by multiple vulnerabilities, including an authentication bypass vulnerability (CVE-2017-6640), and a command injection vulnerability (CVE-2019-15978).

- The authentication bypass vulnerability is due to the presence of a default user account with a static password that is not automatically removed post-installation. An unauthenticated, remote attacker can exploit this to login and gain root or system-level privileges.
- The command injection vulnerability exists in the REST API and SOAP API due to insufficient validation of user-supplied input. A successful exploit could allow the attacker to gain administrative access on the affected device.

Impact: The vulnerability allows an attacker to gain administrative access to the web interface without needing any user credentials. Because the device is used to manage network switches, access to the web interface gives access to all the switches and

other devices that are managed by the DCNM server. This would allow an attacker to change configuration settings on any switch in the network, including the ability to add span ports and monitor traffic or access protected VLANS.

Recommendation: Update the device to version 11.3(1) or later. If it cannot be updated, it should be retired.

Affected Host:
10.208.180.235

References:

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-dcnm2

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200102-dcnm-comm-inject

H1: Default Password

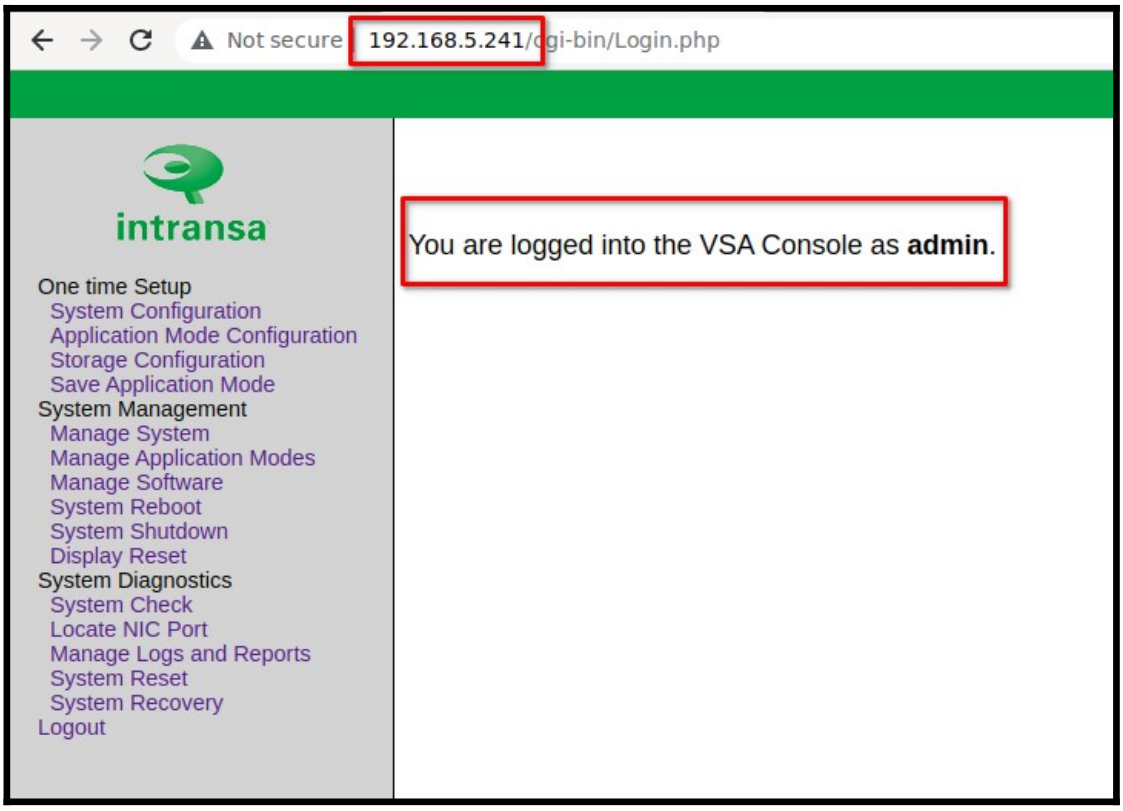


Figure 4 - Intransa VSA with Default Credentials

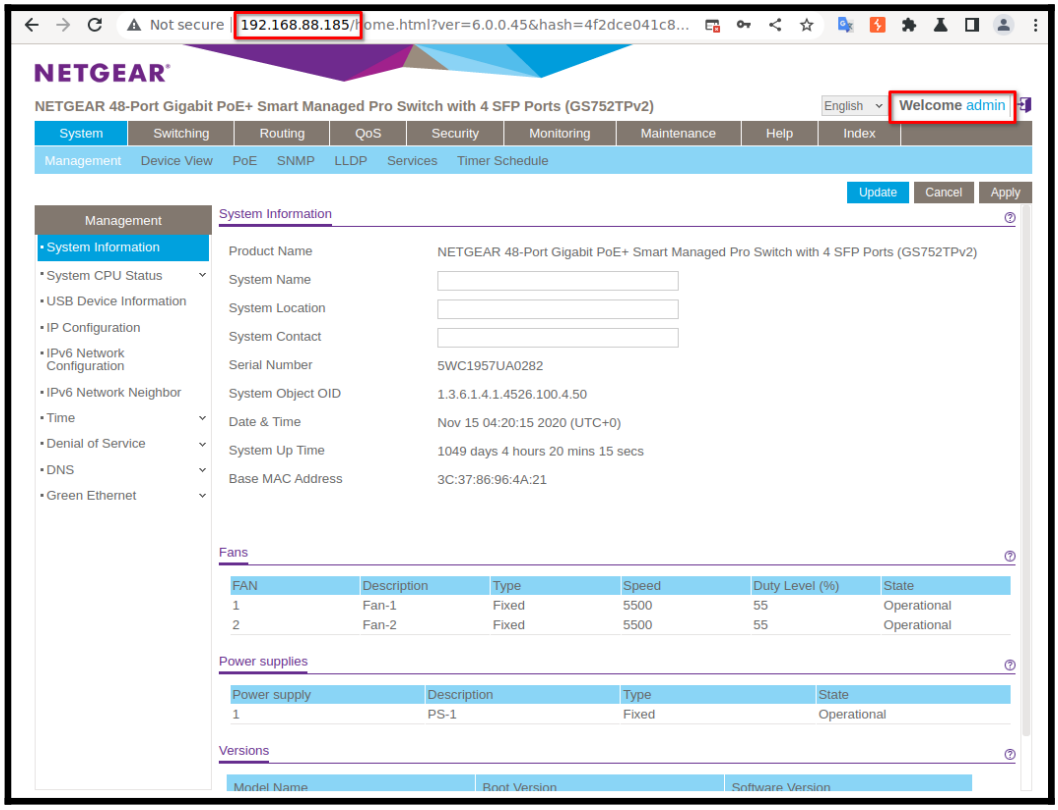


Figure 5 - Network Switch with Default Credentials

Description: Two (2) of the analyzed devices have applications running which were found to have the default accounts in use, allowing assessors to log in with administrative privileges.

Impact: Having an account with a default password could allow an attacker to cause a Denial of Service (DoS) condition. Additionally, it may be possible for an attacker to use the device as a platform for further attacks on other devices. In the case of the switch, an attacker could change the configuration to allow a man-in-the-middle (MITM) attack on users who are connected to the switch.

Recommendation: Change the admin password and, if possible, the default admin account name.

Affected Hosts:
192.168.88.185, 192.168.5.241

References: https://datarecovery.com/rd/default-passwords/

H2: IPMI Password Hashes Exposed

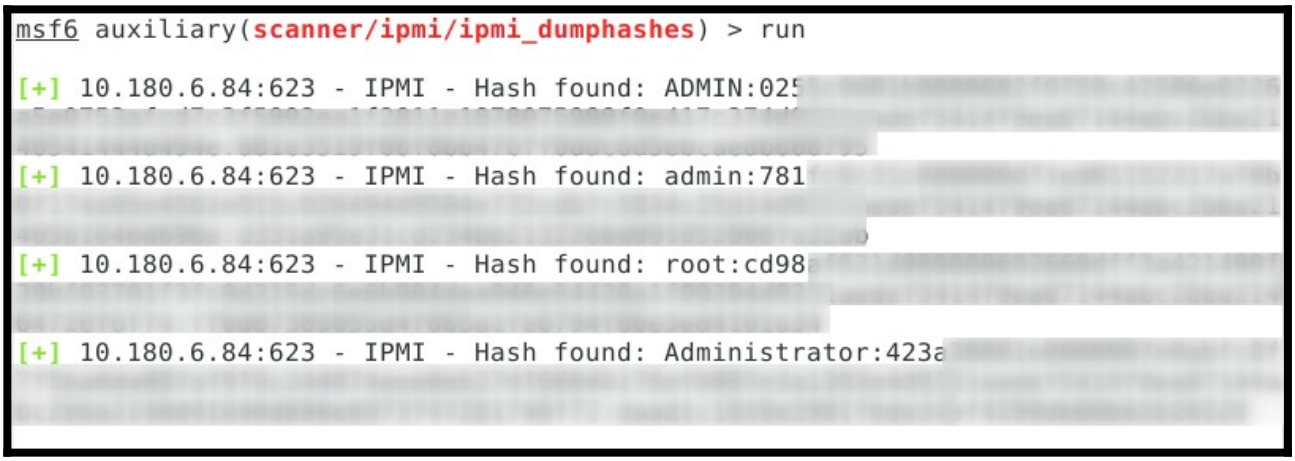


Figure 6 – Exposed password hashes

Description: One (1) server was observed to divulge IPMI password hashes to a remote unauthenticated attacker by setting the encryption cipher to zero. All the attacker needs is the ability to initiate the handshake with the controller to gain the hash information.

Impact: If an attacker gains access to the baseband management or iLO Administrator password, he can take control of the server hardware. This can result in Denial of Service (DoS) condition or possibly escalation to control of the OS.

Recommendations:

- Apply vendor firmware patches to affected systems.
- Isolate the iLO interface on a protected management VLAN
- Use strong passwords to limit the success of off-line bruteforce attacks.

Affected Host:
10.180.6.84

References:

https://www.dell.com/support/kbdoc/en-us/000222162/data-domain-ipmi-v2-0-password-hash-disclosure

H3: Kerberos Pre-Authentication Not Required

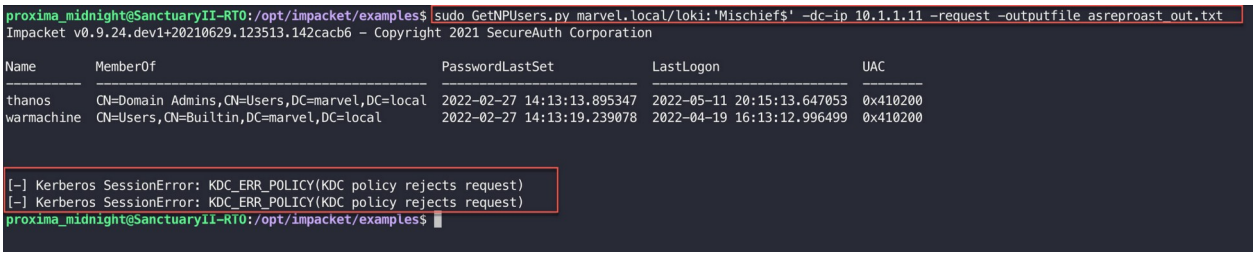


Figure 7 – Listing of users without pre-authentication

Description: Two (2) Active Directory user accounts were observed to not require Kerberos Pre-Authentication prior to issuing an AS-REP containing a Kerberos TGT. One of the accounts belongs to a Domain Administrator.

Impact: The AS-REP is encrypted with the user's Active Directory password, so cracking the encryption on the ticket provides the plaintext user password. One of the affected user accounts is an administrative user, so gaining this user password allows for lateral movement and the possibility to gain additional passwords and password hashes.

Recommendation: Require Kerberos Pre-Authentication for all Active Directory users. This may not be possible for service accounts, in which case remove the service accounts from the Domain Administrators group and make sure they are using long complex passwords of at least 20 characters to resist password cracking.

Affected User Accounts:
thanos, warmachine

References: https://www.ibm.com/think/topics/kerberoasting

H4: Local Admin Password Reuse

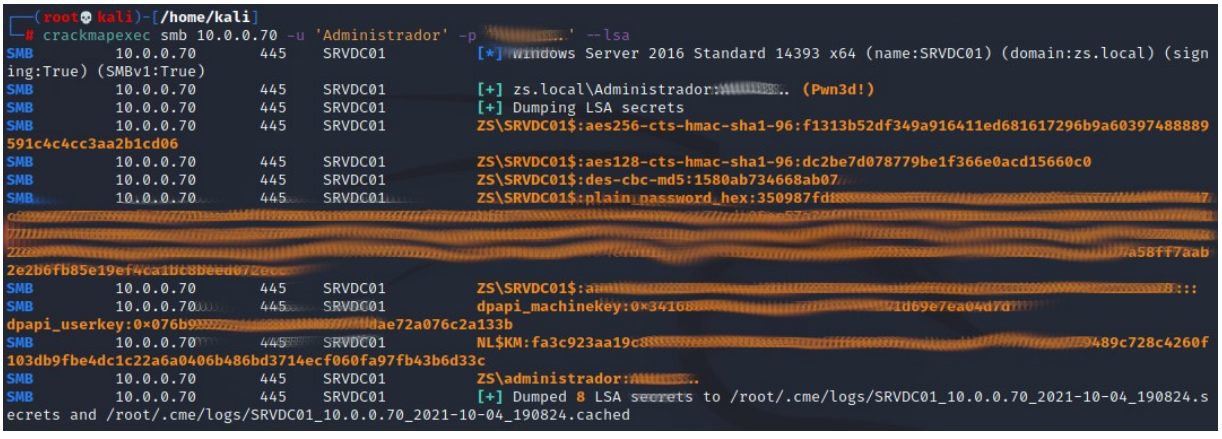


Figure 8 – Local Administrator password compromised

Description: The Local Administrator built in Windows account was found to be active and using a shared password across multiple tested machines.

Impact: An adversary who compromises a single workstation and gains access to the Local Administrator password can gain administrative access domain wide.

Recommendation: Implement Windows LAPS to manage Local Administrator passwords. LAPS will automatically set strong passwords unique to each machine so a single compromise doesn't allow for lateral movement using the Local Administrator password beyond the initial compromised host.

Affected Hosts:
Refer to the vulnerability spreadsheet for a complete list of affected assets.

References:

https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-overview

M1: Plaintext Authentication

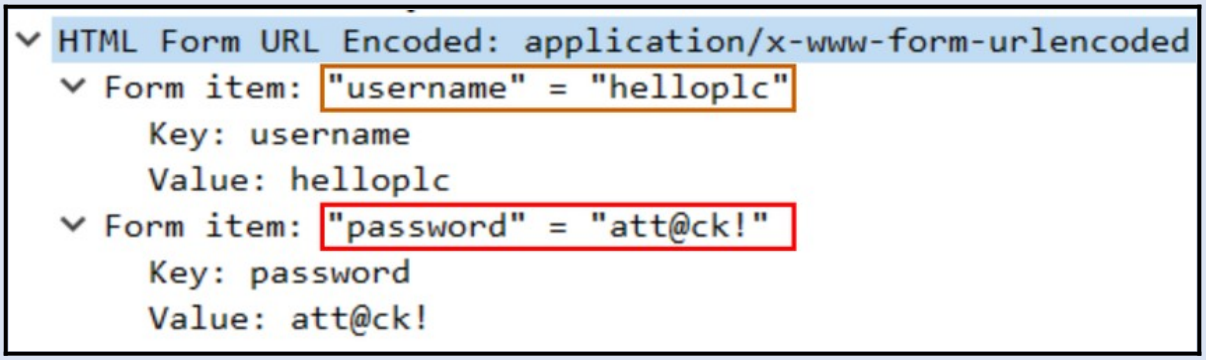


Figure 9 – HTTP Authentication

Description: One (1) webserver was observed to allow user authentication over unencrypted HTTP.

Impact: An adversary with the capability to intercept network traffic can capture the user login credentials and use them to impersonate a legitimate user, including any administrative capability possessed by the user, potentially granting full control of the server.

Recommendation: All logins should be protected by strong encryption. Require HTTPS for web logins.

Affected Host:
10.0.0.34

References:

https://www.cisa.gov/resources-tools/resources/hyper-text-transfer-protocol-secure-https

M2: Unrestricted NFS Share

Individual Issues Identified	Severity Rating
NFS Share with Anonymous Write Access	Medium
NFS Share with Anonymous Read Access	Low

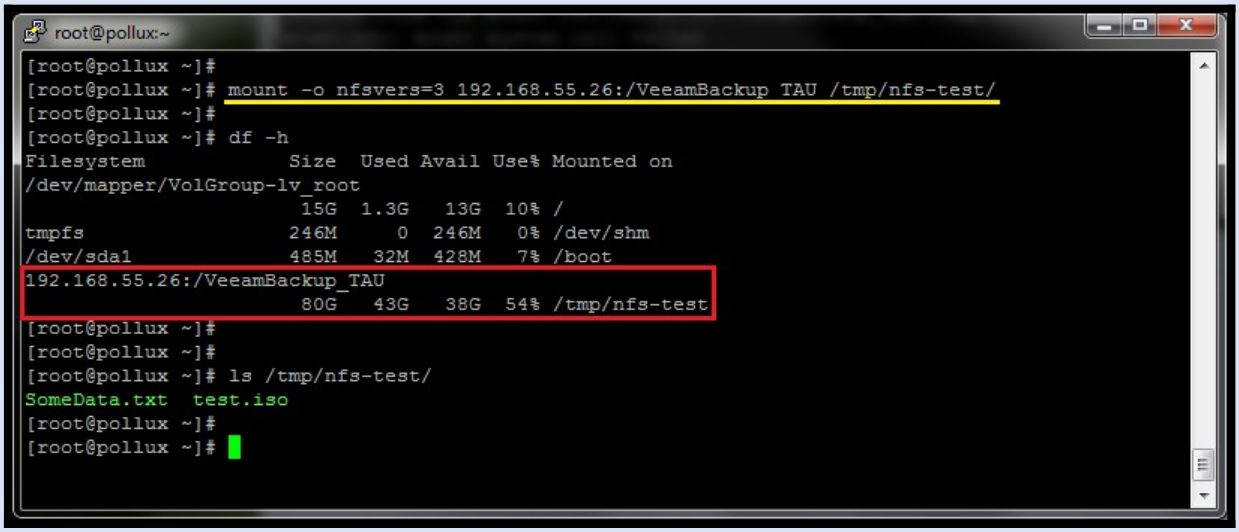


Figure 10 – Anonymous read access

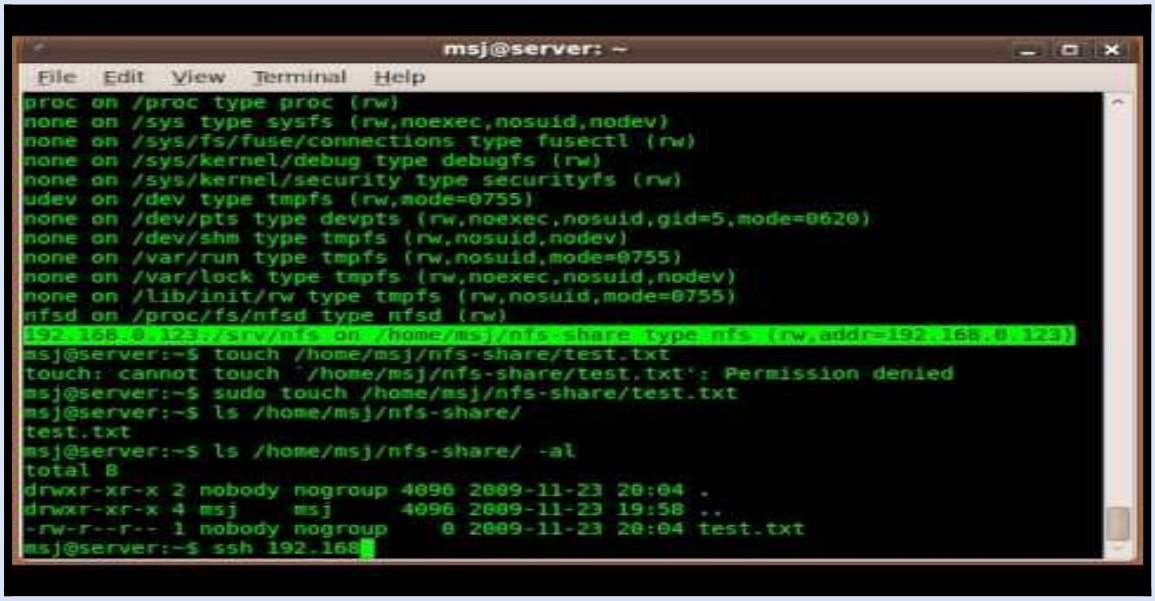


Figure 11 – Anonymous write access

Description: NFS (Network File System) is a distributed file system protocol that allows remote access to shared file systems over the network. Two (2) hosts were observed to have unrestricted NFS shares, allowing anonymous users to mount and read the share. One (1) of these hosts was configured to allow anonymous users to write to the NFS share.

Impact: Allowing anonymous users to read NFS shares can expose sensitive data to unauthorized users. Allowing anonymous write access can allow an attacker to modify important business data or plant backdoors which can grant additional access and escalate privileges.

Recommendation: Require a valid user account to access NFS shares.

Affected Hosts:
192.168.0.123, 192.168.55.26

References:

https://tldp.org/HOWTO/NFS-HOWTO/security.html

https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/7/html/storage_administration_guide/s1-nfs-security#s3-nfs-security-hosts-nfsv4

M3: End of Life/Unsupported Software

Individual Issues Identified	Severity Rating
Unpatched iLO	Medium
Unsupported IIS Version	Medium
Unsupported Windows Version	Medium
Unsupported MSSQL Server	Medium

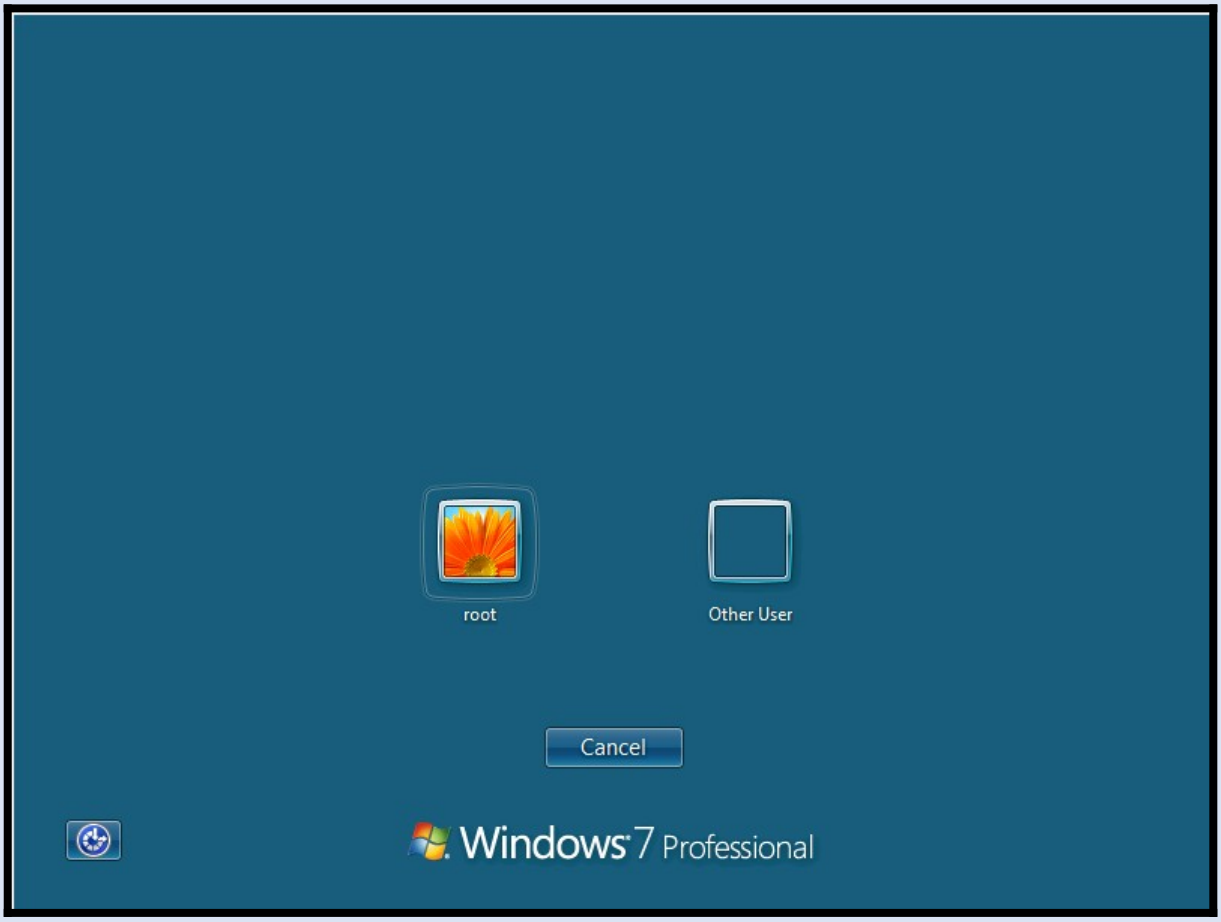


Figure 12 – Unsupported version of Windows

```
* Connected to 10.195.163.187 (10.195.163.187) port 80 (#0)
> GET / HTTP/1.1
> Host: 10.195.163.187
> User-Agent: curl/7.64.0
> Accept: */*
>
< HTTP/1.1 302 Found
< Date: Fri, 06 May 2022 18:41:53 GMT
< Server: Apache/2.2.34 (Debian)
< Access-Control-Allow-Headers: csrfpId
< Location: http://10.195.163.187/admin
< Content-Length: 291
< Connection: close
< Content-Type: text/html; charset=iso-8859-1
<
```

Figure 13 – Out of date Apache version

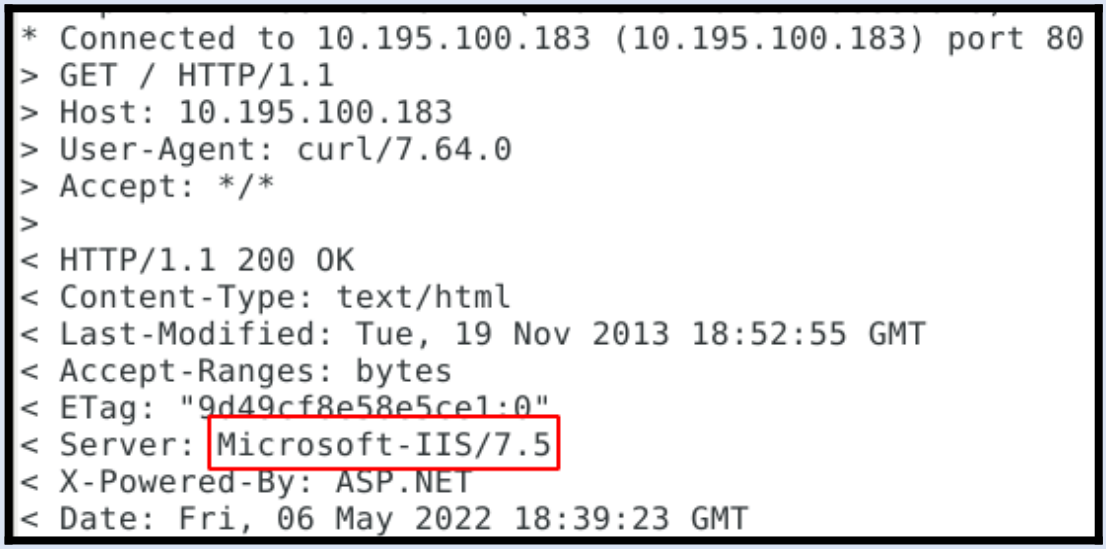


Figure 14 – Unsupported IIS

Description: Several hosts were observed to be using out of date and unsupported firmware, software and Operating Systems. Seven (7) hosts are using unpatched iLO firmware. One (1) host is running an unsupported version of Microsoft IIS. Eleven (11) hosts are running an unsupported version of Windows. Fourteen (14) hosts are running an unsupported version of Microsoft SQL Server. Two (2) hosts are running an out-of-date version of Apache.

Impact: There are multiple known vulnerabilities in the observed software.

iLO version 2.30

CVE-2018-7117 - A cross-site scripting (XSS) vulnerability exists due to improper validation of user-supplied input before returning it to users. An unauthenticated, remote attacker can exploit this, by convincing a user to click a specially crafted URL, to execute arbitrary script code in a user's browser session.

CVE-2019-11983 - A buffer overflow condition exists in the command line interface component of HPE iLO. An unauthenticated, remote attacker can exploit this to cause a denial-of-service condition or the execution of arbitrary code.

CVE-2018-7105 - A remote command execution vulnerability exists in HPE Integrated Lights-Out 5 (iLO 5) for HPE Gen10 Servers prior to v1.35, HPE Integrated Lights-Out 4 (iLO 4) prior to v2.61, HPE Integrated Lights-Out 3 (iLO 3) prior to v1.90 could be remotely exploited to execute arbitrary code leading to disclosure of information. An authenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

CVE-2018-7078 - A remote command execution vulnerability exists in HP Integrated Lights-Out (iLO) server due to an unspecified reason. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands on the server.

CVE-2018-7101 - A denial of service (DoS) vulnerability exists in HP Integrated Lights-Out (iLO) server due to unspecified reason. An unauthenticated, remote attacker can exploit this issue to cause the application to stop responding.

Apache version 2.2.34

CVE-2020-11984 - Apache HTTP server 2.4.32 to 2.4.44 mod_proxy_uwsgi info disclosure and possible RCE

CVE-2020-11993 - 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-2020-9490 - 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-2019-10092 - A limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.

CVE-2019-10081 - 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-2019-9517 - 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.

Microsoft announced the end of support for Windows 7, Windows Server 2008, and IIS 7.5 on Jan 14th, 2020, and for SQL Server 2014 on July 9th 2019. Vulnerabilities which are discovered after these dates will not be patched by the vendor.

Recommendation: Upgrade the affected software to the latest version supported by the vendor. If this is not possible, the affected devices should be placed on an isolated subnet separated from other subnets by a restrictive firewall and IPS.

Affected Hosts:
Refer to the vulnerability spreadsheet for a complete list of affected assets.

References:

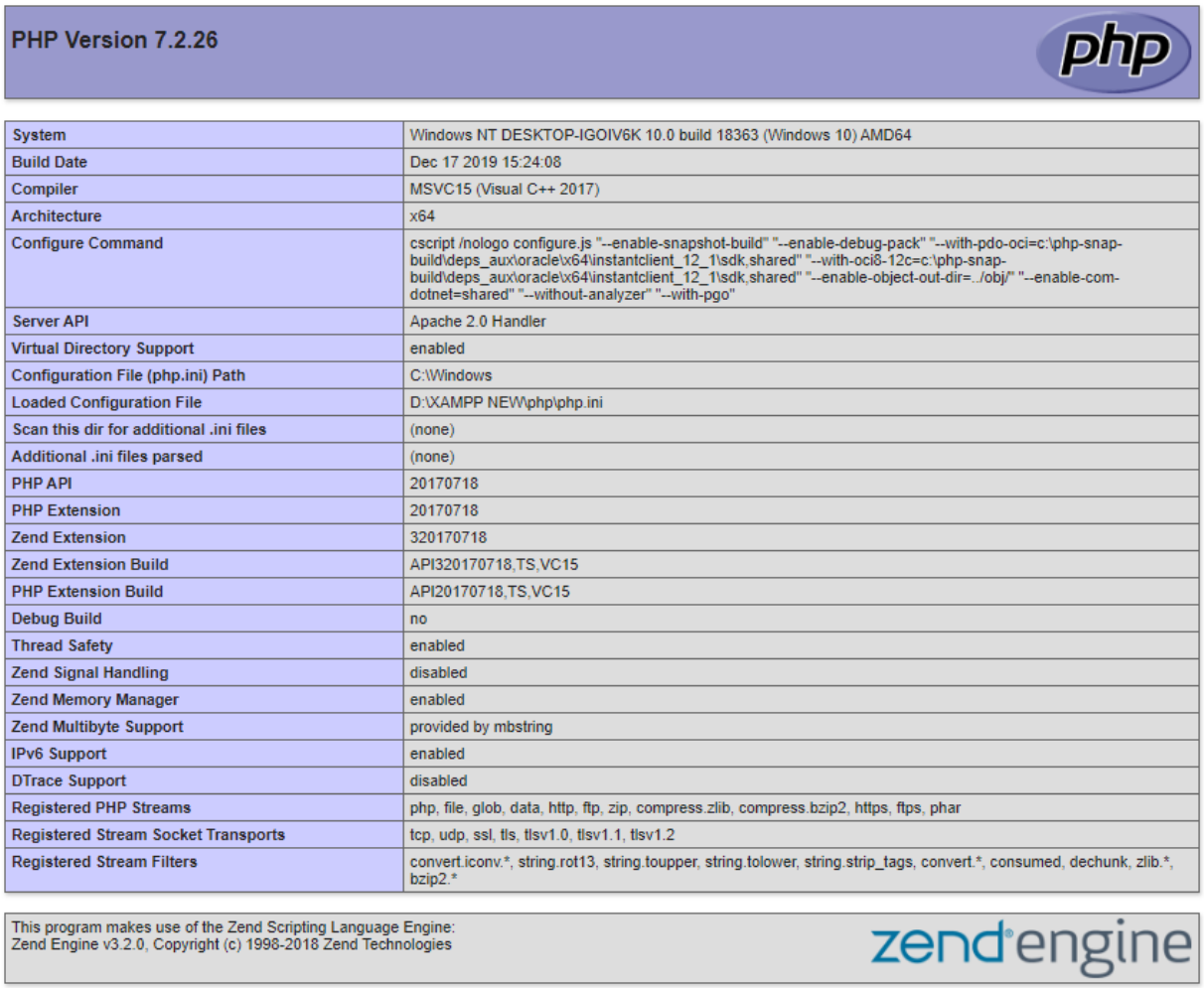
https://docs.microsoft.com/en-us/lifecycle/products/internet-information-services-iis

https://docs.microsoft.com/en-us/lifecycle/products/sql-server-2014

https://www.microsoft.com/en-US/windows/windows-7-end-of-life-support-information

https://docs.microsoft.com/en-us/troubleshoot/windows-server/windows-server-eos-faq/end-of-

L1: Information Disclosure



PHP Version 7.2.26

System	Windows NT DESKTOP-IGOIV6K 10.0 build 18363 (Windows 10) AMD64
Build Date	Dec 17 2019 15:24:08
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	D:\XAMPP NEW\php\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20170718
PHP Extension	20170718
Zend Extension	320170718
Zend Extension Build	API320170718,TS,VC15
PHP Extension Build	API20170718,TS,VC15
Debug Build	no
Thread Safety	enabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	php, file, glob, data, http, ftp, zip, compress.zlib, compress.bzip2, https, ftps, phar
Registered Stream Socket Transports	tcp, udp, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, zlib.*, bzip2.*

This program makes use of the Zend Scripting Language Engine:
Zend Engine v3.2.0, Copyright (c) 1998-2018 Zend Technologies

Figure 15 – Php(info) page

Description: One (1) web server was observed to expose sensitive configuration data to unauthorized users

Impact: Knowing the application configuration can be useful to an attacker in targeting other attacks.

Recommendations: Disable the phpinfo in the php.ini configuration file or use .htaccess to restrict acccess to it to IPs reserved for administrative workstations.

Affected Host:
10.0.0.56

References:
https://cheatsheetseries.owasp.org/cheatsheets/PHP_Configuration_Cheat_Sheet.html

L2: SNMP Default Community String

```
[*] Listening TCP ports and connections
-------------------------------------------------------------------------
---------------

  Local Address   Port      Remote Address   Port       State

        0.0.0.0    111             0.0.0.0      -       Listening
        0.0.0.0    161             0.0.0.0      -       Listening
      10.16.2.6     22        20.150.86.68    443       Time wait
      10.16.2.6  54424        20.150.86.68    443       Time wait
      10.16.2.6  54472        20.150.86.68    443       Time wait
      10.16.2.6  54474        20.150.86.68    443       Time wait
      10.16.2.6  54476        20.150.86.68      -       Listening
      10.16.2.6  54488        20.150.86.68  39162     Established
      10.16.2.6   3006             0.0.0.0      -       Listening
      10.16.2.6   3006           127.0.0.1      -       Listening
      10.16.2.6   3007             0.0.0.0  33098     Established
      10.16.2.6   3012             0.0.0.0  33628     Established
      10.16.2.6   3012           127.0.0.1  33648     Established
```

Figure 16 – Anonymous SNMP read access.

Description: Two (2) hosts were observed to be using a default SNMP community string. The Simple Network Management Protocol (SNMP) is a commonly used network service. Its primary function is to provide network administrators with information about all kinds of network-connected devices. SNMP can be used to get and change system settings on a wide variety of devices, from network servers to routers and printers. The drawback to this service is the authentication is an unencrypted "community string". In addition, many SNMP servers provide very simple default community strings. The community string "public" is a default on a number of SNMP servers.

Impact: Read access to SNMP gives an attacker additional information about the hardware and OS to use in targeting further attacks.

Recommendations:

- Change all default community strings to a custom, hard to guess string.
- Upgrade to SNMPv3 if possible

Affected Hosts:
10.16.2.6, 10.16.2.5

References: https://www.dnsstuff.com/snmp-community-string

Attack Storyboard

Scenario 1: Log4jShell RCE Lateral Movement and Escalation

Phase: Internal Penetration Testing
Results: Full network compromise
Severity: **Critical**

Step 1: Initial Access

The ESXi server at 10.180.150.30 was observed to be vulnerable to the Log4jShell exploit. The exploit was launched and granted root access to the server.

```
[+] The target is vulnerable.
[+] Delivering the serialized Java object to execute the payload...
[*] Client sent unexpected request 2
[!] http://10.180.138.22:443 handling request from 10.180.150.30; (UUID: 0nifgco
g) Without a database connected that payload UUID tracking will not work!
[*] http://10.180.138.22:443 handling request from 10.180.150.30; (UUID: 0nifgco
g) Staging python payload (40280 bytes) ...
[!] http://10.180.138.22:443 handling request from 10.180.150.30; (UUID: 0nifgco
g) Without a database connected that payload UUID tracking will not work!
[*] Meterpreter session 1 opened (10.180.138.22:443 -> 127.0.0.1 ) at 2022-04-21
 11:49:54 -0500
```

Figure 17 – Log4Shell exploit

Step 2: Escalate to full root shell

Initially, access was limited to the meterpreter shell. However, further steps were taken to escalate access, including reading the /etc/shadow file, cracking the root password, enabling ssh access and root login. Once root ssh access had been gained, the system was examined for data which could be used for lateral movement. Binaries included in the vSphere installation would have allowed root to change the password for the Administrator@vsphere.local account, however as this account was in active use, changing the password to gain access would have created a disruption to normal business activity. As the ESXi server was joined to the safemarch.com domain, a cached Kerberos ticket was discovered in the /tmp/ directory.

Figure 19 – Captured Kerberos token

Indicators of Compromise: Monitor for user accounts logged into systems they would not normally access or access patterns to multiple systems over a relatively short period of time. Also monitor user SSH-agent socket files being used by different users.

Step 3: Lateral movement

This captured kerberos ticket was used to impersonate the computer account for the ESXi server in the domain and enumerate users vulnerable to the AS-REProast attack.

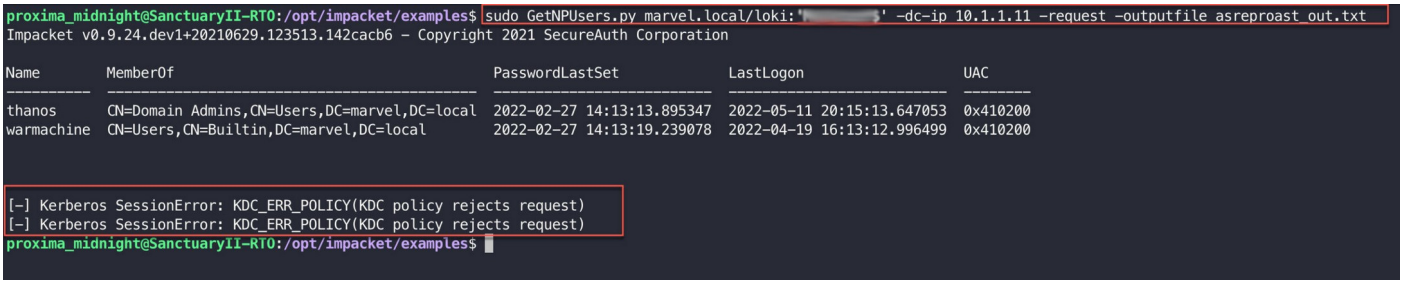


Figure 20 – Users vulnerable to AS-REP attack

A total of 2 users vulnerable to this attack were discovered, and using the ESXi computer account, their password hashes were gathered from the domain controller. One of the captured hashes belonged to a Domain Administrator, thanos, however this password hash was not cracked during the test period. The other password hash was cracked and the original password recovered within 24 hours of password cracking. This account, warmachine, was used for additional Active Directory enumeration.

This compromised account was used to gain administrative access to other computers and dump the local SAM store and LSA secrets, including additional password hashes and cached credentials.

Indicators of Compromise: Monitor for anomalous Kerberos activity, such as enabling Audit Kerberos Service Ticket Operations to log Kerberos TGS service ticket requests. Particularly investigate irregular patterns of activity (ex: accounts making numerous requests, Event ID 4769, within a small time frame, especially if they also request RC4 encryption [Type 0x17]).

Step 4: Escalate domain privileges

One of the captured NTLM password hashes was for the Administrator local account which had administrative privileges on a large number of additional machines. This led to the capture of the default Domain Administrator account NTLM password hash from the machine with IP 10.0.0.70.

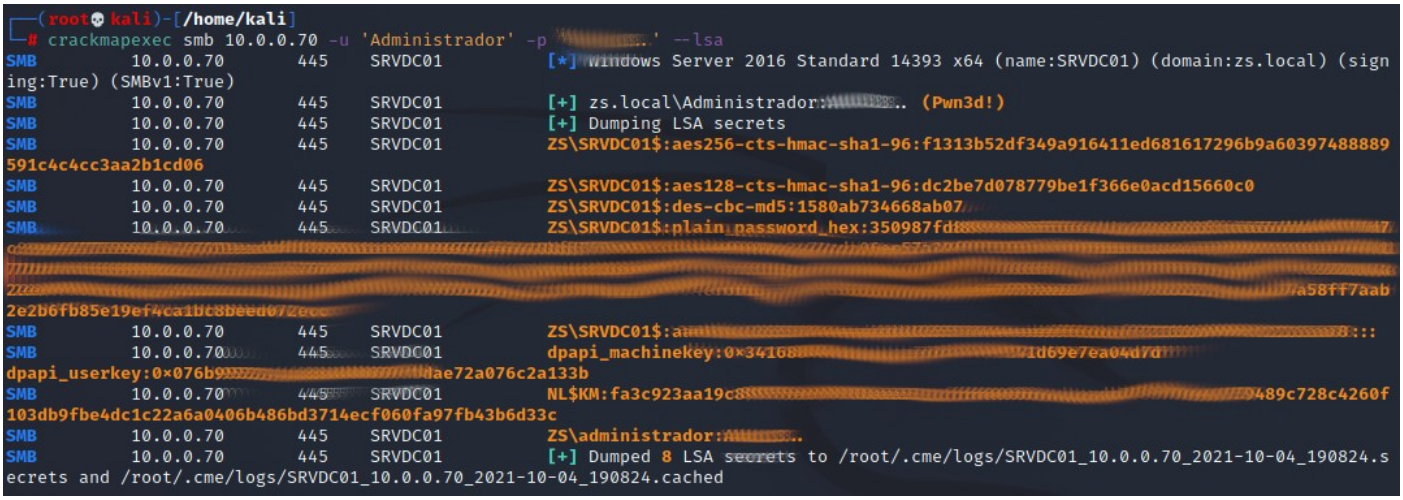


Figure 21 – Domain admin password hash captured.

Indicators of Compromise:

- *index=security (sourcetype="Powershell" EventCode=4104) Image="powershell.exe" CommandLine IN ("Invoke-Mimikatz", "Invoke-LSADump*")*
- *index=security sourcetype="WinEventLog:Security" EventCode=4663 ObjectName="\Policy\Secrets" | where ProcessName IN ("reg.exe", "powershell.exe", "wmic.exe", "schtasks.exe", "cmd.exe", "rundll32.exe", "mimikatz.exe", "procdump.exe")*

Step 5: Full domain takeover

This password hash was used to compromise the SRVDC01 domain controller and dump the ntds.dit database containing the complete list of password hashes for the entire domain. At this point the domain was fully compromised and any user account can be impersonated.

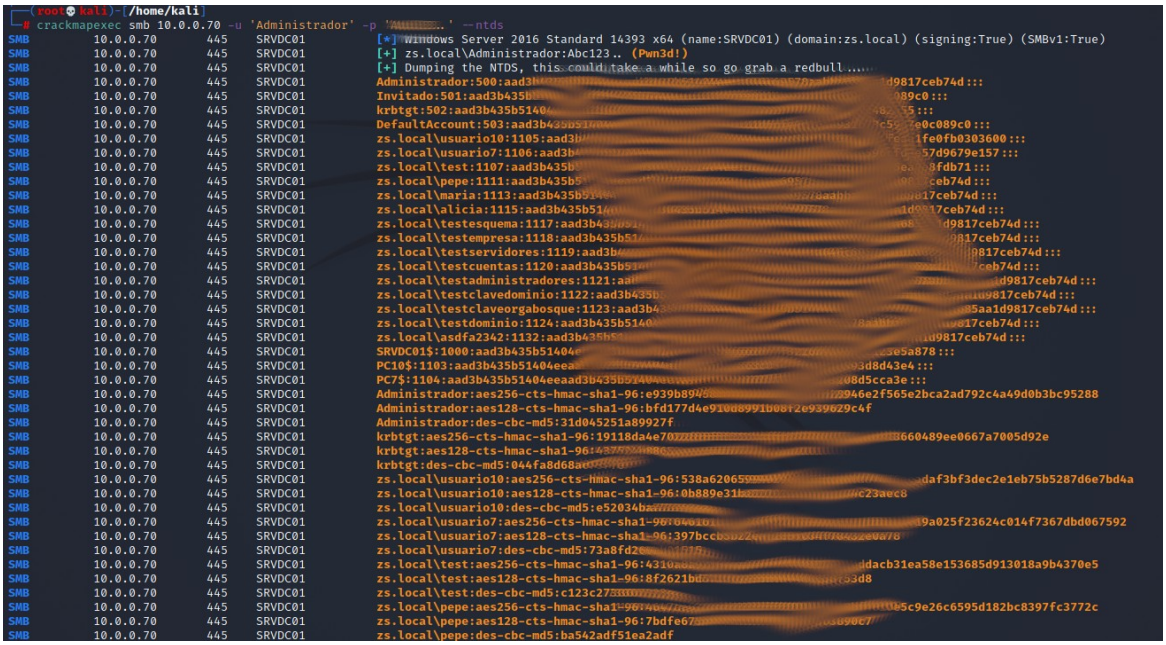


Figure 22 – NTDS.dit dumped

Indicators of Compromise:

- *((sourcetype="WinEventLog:Microsoft-Windows-Powershell/Operational" EventCode="800") AND((CommandLine LIKE "%ntds%" AND CommandLine LIKE "%ntdsutil%" AND CommandLine LIKE "%create%") OR (CommandLine LIKE "%vssadmin%" AND CommandLine LIKE "%create%" AND CommandLine LIKE "%shadow%") OR (CommandLine LIKE "%copy%" AND CommandLine LIKE "%ntds.dit%")))*
- *(sourcetype=WinEventLog:Security EventCode IN (4656, 4663)) OR (sourcetype=WinEventLog:Microsoft-Windows-Sysmon/Operational EventCode="11") ANDObjectType="File" AND TargetFilename="*ntds.dit" AND (AccessList="%%4416" OR AccessList="%%4419" OR AccessList="%%4417" OR AccessList="%%4424")*

Scenario 2: Security Station Takeover

Phase: Internal Penetration Testing
Results: Full system compromise
Severity: **Critical**

Step 1: Initial Access

Two (2) security workstations at 10.120.98.36 and 10.195.101.109 were observed to be running an unpatched Windows 7 vulnerable to Eternalblue MS17-10. Both stations were successfully compromised and SYSTEM privileges gained.

```
[+] 10.195.101.109:445 - Closing SMBv1 connection creating free hole adjacent t
 SMBv2 buffer.
[*] 10.195.101.109:445 - Sending final SMBv2 buffers.
[*] 10.195.101.109:445 - Sending last fragment of exploit packet!
[*] 10.195.101.109:445 - Receiving response from exploit packet
[+] 10.195.101.109:445 - ETERNALBLUE overwrite completed successfully (0xC00000
D)!
[*] 10.195.101.109:445 - Sending egg to corrupted connection.
[*] 10.195.101.109:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 10.195.101.109
[+] 10.195.101.109:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
-=-=-=
[+] 10.195.101.109:445 - =-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-
-=-=-=
[+] 10.195.101.109:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
-=-=-=
[*] Meterpreter session 1 opened (10.180.138.22:4444 -> 10.195.101.109:52199 )
t 2022-05-05 14:38:03 -0500

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

Figure 23 – Eternalblue exploited on security workstation 1.

Step 2: Escalate Privileges

Passwords were recovered for a local administrator account on each machine. This account was used to login over RDP. One workstation was found to host control software for the security camera system and DVR. The other hosted a security badge setup and printing software.

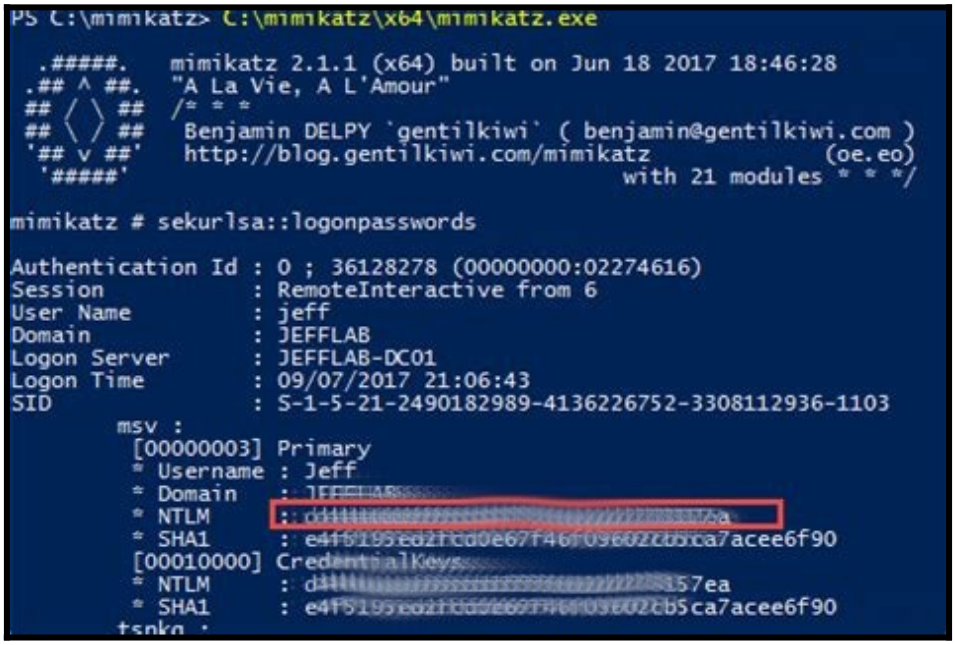


Figure 24 – Capture local admin password hash

Indicators of Compromise: Monitor for unexpected processes interacting with lsass.exe. Common credential dumpers such as Mimikatz access the LSA Subsystem Service (LSASS) process by opening the process, locating the LSA secrets key, and decrypting the sections in memory where credential details are stored. Credential dumpers may also use methods for reflective Process Injection to reduce potential indicators of malicious activity.

Step 3: Full system takeover

With access to the security camera systems, camera footage could be deleted or modified to hide a break in attempt. With access to the badge reader a new badge could be created with full access to all areas of the building. With both compromised an attacker could gain access to any part of the building, tamper or steal equipment, and have no video recording of the activity made.

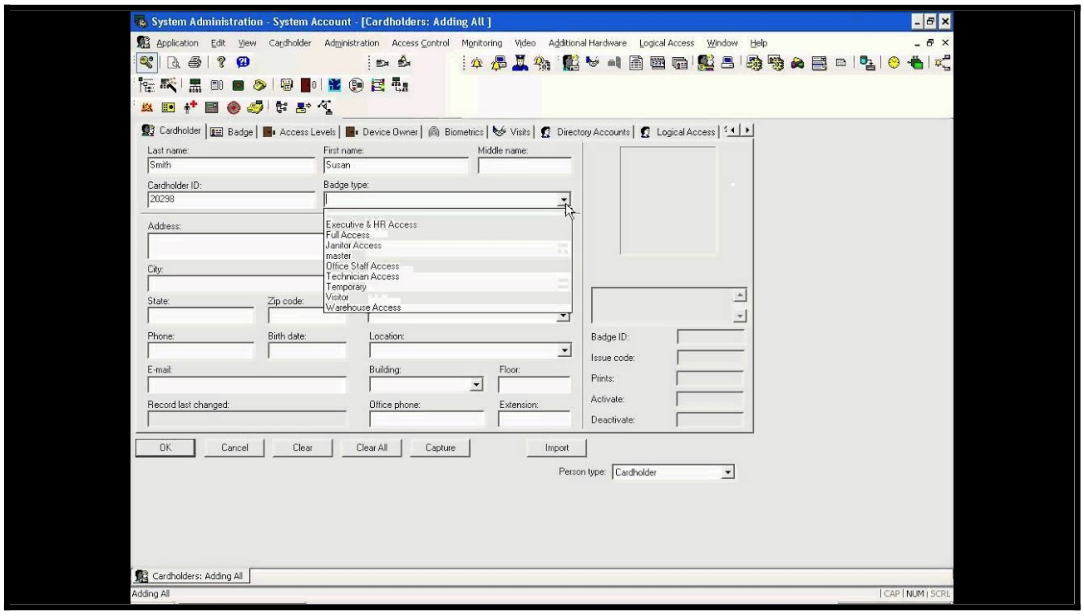


Figure 25 – Employee badge software

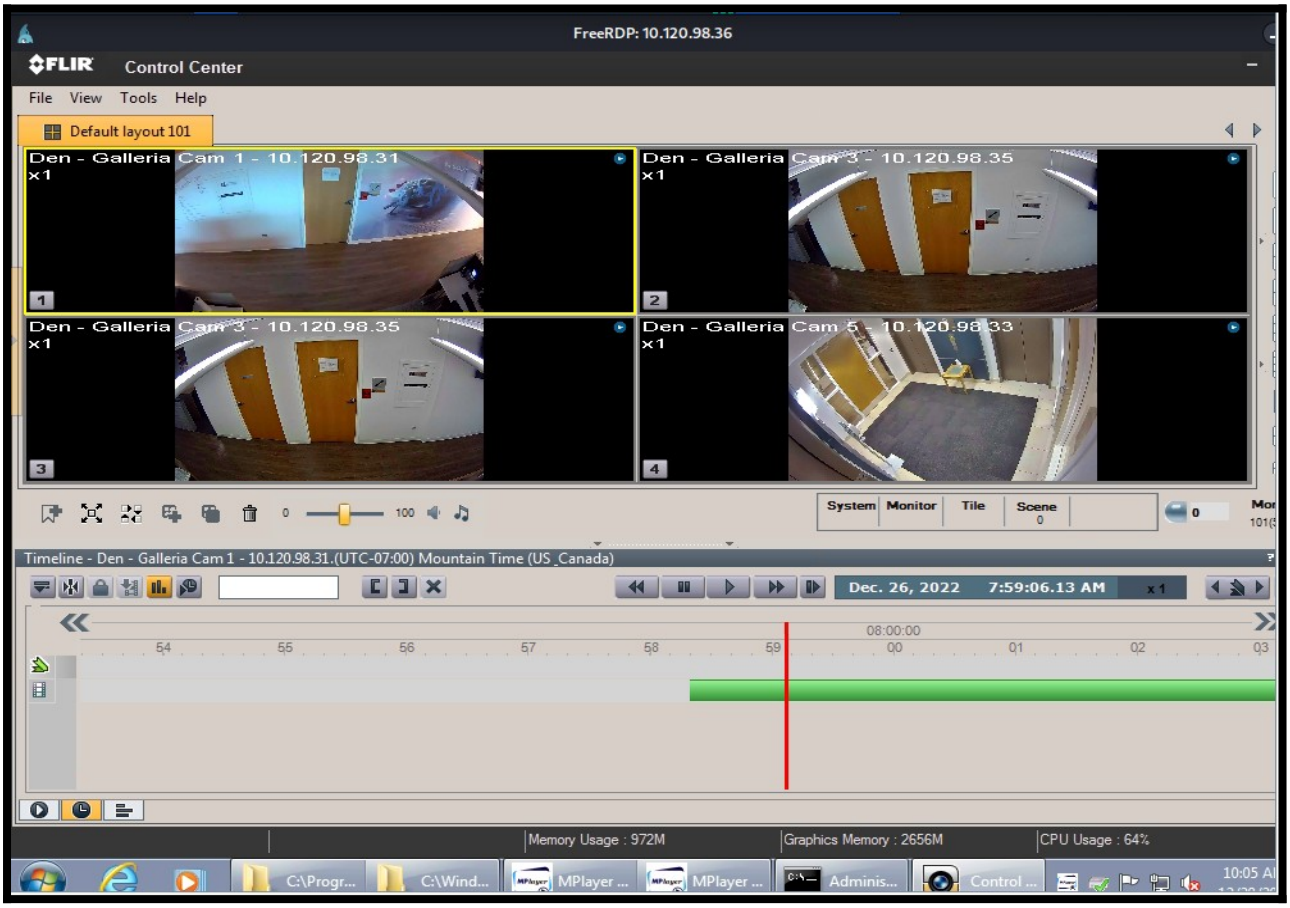


Figure 26 – Security camera DVR system

Scenario 3: *Cisco DCNM Full Takeover*

Phase: Internal Penetration Testing
Results: Full network compromise
Severity: **Critical**

Step 1: Initial Access

The Cisco Data Center Network Manager device uses a hard coded mechanism to generate authentication tokens based on a nonce provided by the server. It uses the same mechanism regardless of user credentials entered. The assessor was able to correctly encode the nonce provided by the server and gain access to the administrative interface of the jboss server running on port 9443.

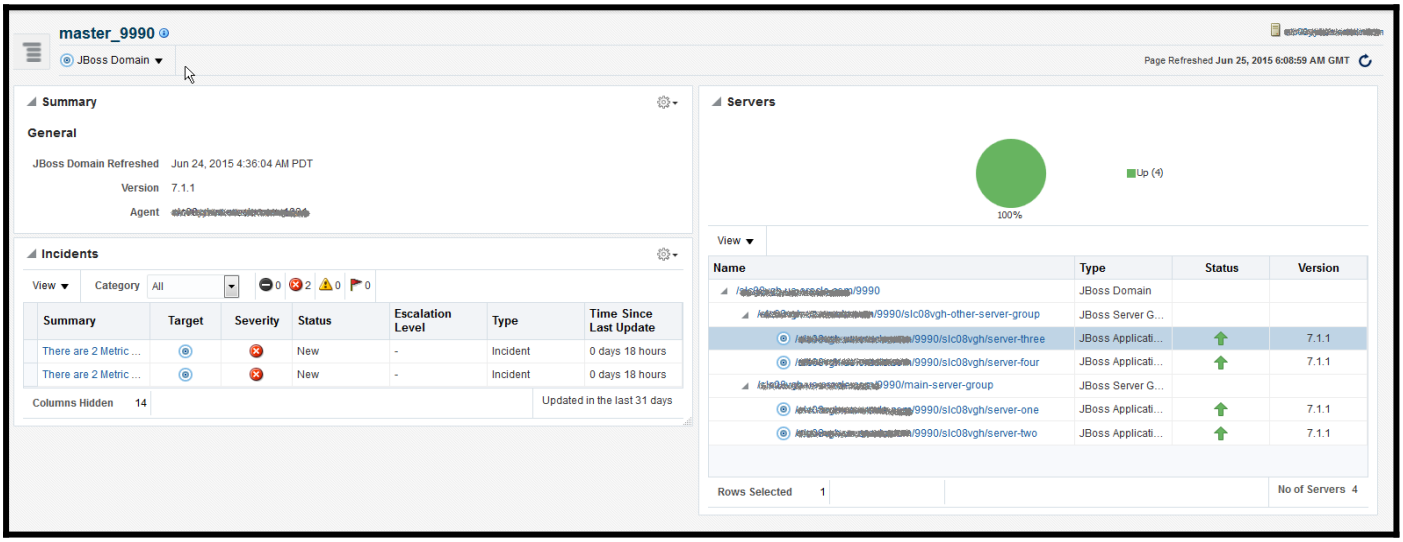


Figure 27 – Admin interface to jboss server

Step 2: Escalate privilege

After the assessor gained access to the jboss interface, the server set an authorization token, which the assessor reused to forge a SOAP request to the principal server listening on port 443 to create a new administrative user.

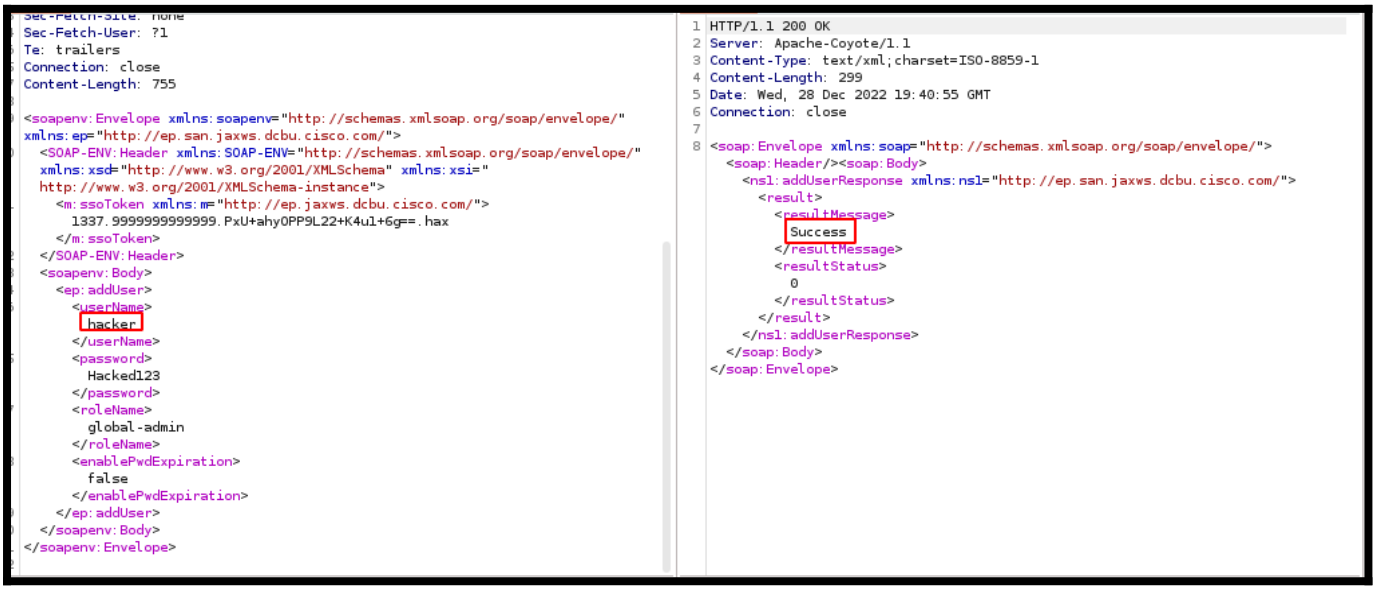


Figure 28 – Forged SOAP request creating new user.

Indicators of Compromise: Monitor for creation of new admin user accounts

Step 3: Full Access

The assessor then logged in as that user and was given access to all the switches and other devices that are managed by the DCNM server. This would allow an attacker to change configuration settings on any switch in the network, including the ability to add span ports and monitor traffic or access protected VLANS.

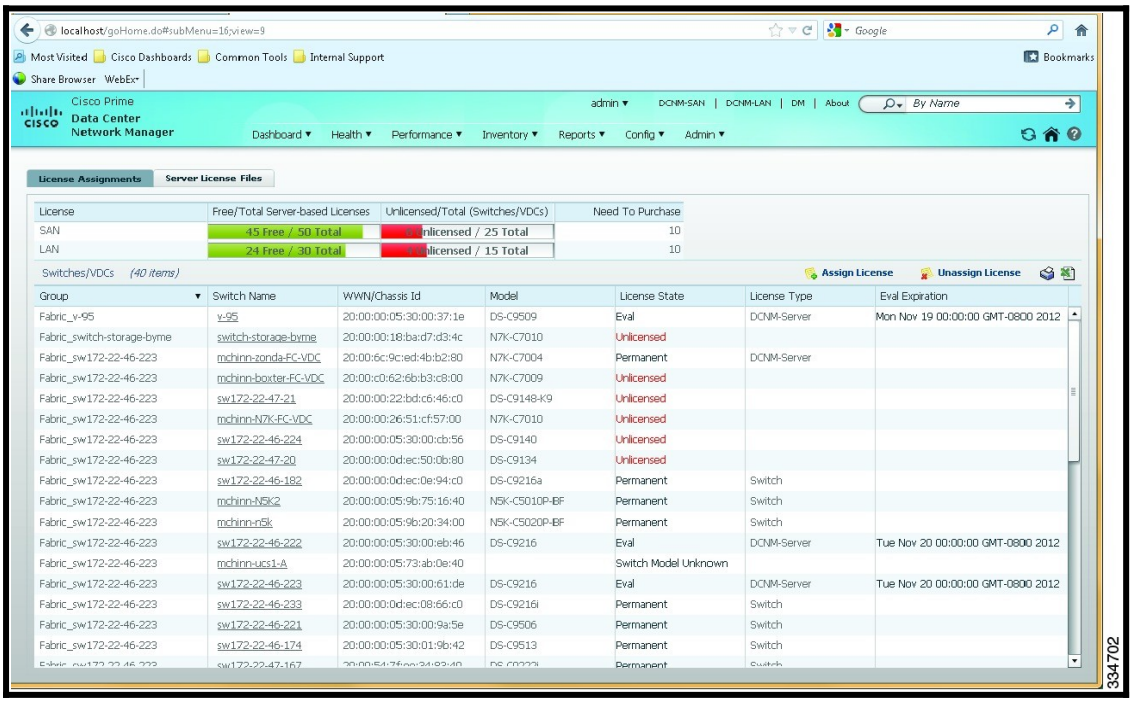


Figure 29 – DCNM interface showing managed switches.

Indicators of Compromise: Monitor for configuration changes in managed network devices.

Conclusions

Strategic Short-Term Goals

- Aim to remediate all Critical and High vulnerabilities within 30 days. Additionally M1, M2, and L1 should require only a few man hours each to remediate.

Strategic Long-Term Goals

- Review the organization's patch management process in order to determine how and why critical vulnerabilities such as C1, C2, and C3 have gone unpatched. It could be those devices have been overlooked, are on subnets which are not scanned, are not domain joined, or have been excluded from scans. Examine whether there are patch management exemptions in place and whether the reasons for those exemptions are still valid.
- Review the organization's technical process and procedure documentation regarding creation and management of administrative accounts, changing default passwords, setting up file shares, and securely setting up web pages for internal company use. Ensure process and procedure guidelines are up to date and reflect the organization's security goals. Also ensure that IT personnel know about the process and procedure documentation and where to access it.
- Review the organization's policies for handling unsupported and end of life software. Ensure that these policies reflect the organization's security goals as well as the pragmatic realities of IT operational needs.

Remediation Steps

Critical Severity Vulnerabilities

ID	Issue Name	Remediation Steps
C1	**Log4jShell RCE**	• Apply vendor patches to remediate the Log4j vulnerability. • Require root passwords to meet password complexity requirements. • Create a non-root service account to run java instances.
C2	**MS17-010: EternalBlue Vulnerability**	Upgrade to a newer version of Windows still in the support window. If this is not possible then install security patch MS17-10 and/or disable SMBv1.
C3	**Cisco DCNM Authentication Bypass**	Update the device to version 11.3(1) or later. If it cannot be updated, it should be retired.

High Severity Vulnerabilities

ID	Issue Name	Remediation Steps
H1	**Default Password**	Change the admin password and, if possible, the default admin account name.
H2	**IPMI Password Hashes Exposed**	• Apply vendor firmware patches to affected systems. • Isolate the iLO interface on a protected management VLAN • Use strong passwords to limit the success of off-line bruteforce attacks.
H3	**Kerberos Pre-Authentication Not Required**	Require Kerberos Pre-Authentication for all Active Directory users. This may not be possible for service accounts, in which case remove the service accounts from the Domain Administrators group and make sure they are using complex passwords of at least 20 characters to resist password cracking.
H4	**Local Admin Password Reuse**	Implement Windows LAPS to manage Local Administrator passwords. LAPS will automatically set strong passwords unique to each machine so a single compromise doesn't allow for lateral movement using the Local Administrator password beyond the initial compromised host.

Medium Severity Vulnerabilities

ID	Issue Name	Remediation Steps
M1	**Plaintext Authentication**	All logins should be protected by strong encryption. Require HTTPS for web logins.
M2	**Unrestricted NFS Share**	Require a valid user account to access NFS shares.
M3	**End of Life/Unsupported Software**	Upgrade the affected software to the latest version supported by the vendor. If this is not possible, the affected devices should be placed on an isolate subnet separated from other subnets by a restrictive firewall and IPS.

Low Severity Vulnerabilities

ID	Issue Name	Remediation Steps
L1	**Information Disclosure**	Disable the phpinfo in the php.ini configuration file or use .htaccess to restrict acccess to it to Ips reserved for administrative workstations.
L2	**SNMP Default Community String**	• Change all default community strings to a custom, hard to guess string. • Upgrade to SNMPv3 if possible

Appendix A: Vulnerability Ratings

ECR Security takes into account a number of factors when assigning a vulnerability rating, including: whether a vulnerability leads to partial or full system compromise, whether it can be part of an attack chain which amplifies the total impact, what user level privileges are required for exploitation, whether specific conditions or non-default configurations are required, the level of difficulty and resources required to conduct a successful attack, whether exploit code has been published, whether mitigating controls are in place, whether user interaction is required, whether the affected device is internet facing, how sensitive is the data stored on the vulnerable host, and how critical is the vulnerable device to business operations.

Rating
Critical The vulnerability has been demonstrated to be exploitable in practice in the current configuration. Exploit code is easily available. The technical skill and resources required for exploitation are well within the capability of most threat actors, and as such, the likelihood of exploitation is high. The anticipated impact on confidentiality, integrity, and/or availability is high. The combination of easy exploitability and high impact means the vulnerability should be taken extremely seriously and remediated immediately.
High The vulnerability is known to be exploitable but may require specific conditions and/or access levels. The anticipated impact on confidentiality, integrity, and/or availability is high, but the presence of mitigating factors, such as technical difficulty, reduces the likelihood of actual exploitation. Remediation should be conducted on an expedited basis.
Medium Potential impact to confidentiality, integrity, and/or availability is moderate to high, but mitigating factors, such as lack of published exploit code or uncertainty about the level of exploitability mean the likelihood of successful attack is significantly reduced. If part of an attack chain the risk could be amplified, but alone this vulnerability does not pose a serious risk. Remediation can be scheduled according to regular maintenance cycles.
Low The vulnerability is unlikely to have a significant impact on confidentiality, integrity, and/or availability either because the nature of the vulnerability is such that it cannot lead to system compromise or because the resources required to make a successful attack are so large as to be impractical. Vulnerabilities of this category may provide useful information for other attacks. Remediation can be conducted if a cost/benefit analysis finds overall benefit
Informational The vulnerability has no impact on the confidentiality, integrity, and availability of data or the network.