FortifyTech
Security Assessment Findings Report

Business Confidential

Date: May 8th, 202

Confidentiality Statement

This document is the exclusive property of FortifyTech and CyberShield This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both FortifyTech and CyberShield.

FortifyTech may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. CyberShield prioritized the assessment to identify the weakest security controls an attacker would exploit. CyberShield recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Assessment Overview

From May 5th, 2021 to May 8th, 2024, FortifyTech engaged CyberShield to evaluate the security posture of its infrastructure on their IP of 10.15.42.36 and 10.15.42.7. The application that we use are WPScan, Nuclei, GoBuster, and Nmap Scan.

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Risk Factors

Risk is measured by two factors: Likelihood and Impact:

Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, attacker skill level, and client environment.

Impact

Impact measures the potential vulnerability's effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm, and financial loss.

Scope

Assessment	Details
Penetration Test	10.15.42.36, 10.15.42.7

Executive Summary

This report presents the findings of the penetration test conducted on the target network. The objective of the test was to identify potential vulnerabilities and assess the security posture of the network.

1. **Network Scanning (Nmap)** The network scan did not reveal any apparent vulnerabilities. All 1000 scanned ports on the IP address 10.15.42.36 were in ignored states, indicating that these ports are likely closed or filtered by a firewall, thus reducing their vulnerability to attacks.

2. **Directory Enumeration (GoBuster)** The GoBuster scan identified potential directories on the target IP address 10.15.42.7. Notably, the /admin and /login directories could be potential login pages, as indicated by the server's 302 status code responses. Further scanning of the /admin directory revealed several directories and files, most of which redirect to other URLs.

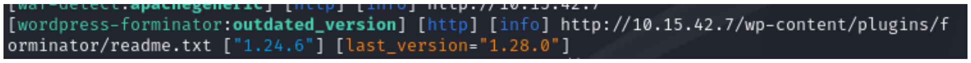
3. **WordPress Vulnerability Scanning (WPScan)** The WordPress site at http://10.15.42.7123 is running on an Apache/2.4.59 (Debian) server with PHP/8.2.181. The site is using the twentytwentyfour theme, version 1.11. No plugins were detected during the scan.

4. **Plugin Vulnerability (Nuclei)** The WordPress Forminator plugin (version 1.24.6) is outdated, with the latest version being 1.28.0. This outdated version could potentially introduce vulnerabilities to the site.

5. **Identified Vulnerabilities** The site was found to be vulnerable to Terrapin (CVE-2023-48795). Additionally, another vulnerability (CVE-2023-4596) was identified during the test.

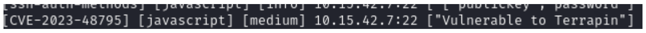
This summary provides an overview of the potential vulnerabilities identified during the penetration test. It is recommended to address these findings promptly to enhance the security posture of the network. Further investigation and remediation efforts may be required based on these results.

Evidence



```
[waf-detect:apachegeneric] [http] [info] http://10.15.42.7
[wordpress-forminator:outdated_version] [http] [info] http://10.15.42.7/wp-content/plugins/f
orminator/readme.txt ["1.24.6"] [last_version="1.28.0"]
```

Figure 1: the wordpress forminator plugin version 1.24.6 which is already outdated



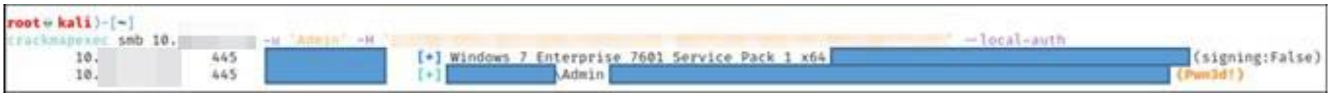
```
[ssh-auth-methods] [javascript] [info] 10.15.42.7:22 ["["publickey","password"]"]
[CVE-2023-48795] [javascript] [medium] 10.15.42.7:22 ["Vulnerable to Terrapin"]
```

Figure 2: vulnerable to Terrapin

Finding IPT-002: Security Misconfiguration – Local Admin Password Reuse (Critical)

Description:	TCMS utilized local administrator hashes to gain access to other machines in the network via a 'pass-the-hash' attack. The local administrator hashes were obtained via machine access provided by the cracked account in IPT-001. Pass-the-hash attacks do not require knowing the account password to successfully log into a machine. Thus, reusing the same local admin password (and therefore the same hash) on multiple machines will permit system access to those computers. TCMS leveraged this attack to gain access to ~50 machines within the main office. This led to further account access and the eventual compromise of the domain controller.
Risk:	Likelihood: High – This attack is effective in large networks with local admin password reuse. Impact: Very High – Pass-the-hash permits an attacker to move laterally and vertically throughout the network.
System:	All
Tools Used:	Impacket, Crackmapexec
References:	https://capec.mitre.org/data/definitions/644.html https://tcm-sec.com/pentest-tales-001-you-spent-how-much-on-security/

Evidence



```
root㉿kali)-[~]
crackmapexec smb 10.[redacted]  -u 'Admin' -H [redacted] --local-auth
      10.[redacted]      445   [redacted]    [+] Windows 7 Enterprise 7601 Service Pack 1 x64 [redacted](signing:False)
      10.[redacted]      445   [redacted]    [+] [redacted]\Admin [redacted] (Pwn3d!)
```

Figure 3: Local admin hash used to gain access to machine

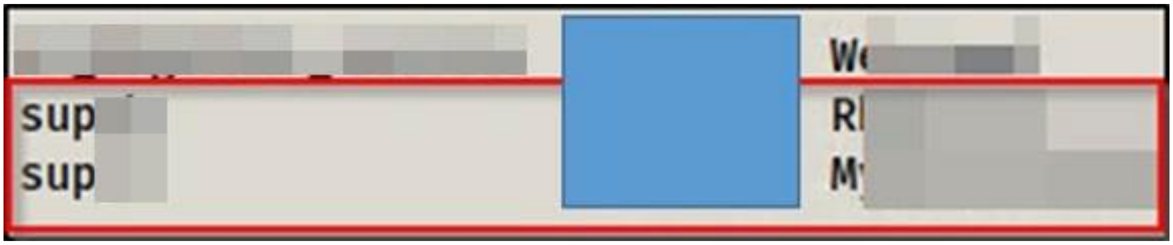
Remediation

Utilize unique local admin passwords. Limit local admin users via least privilege. Consider implementing a PAM solution. For full mitigation and detection guidance, please reference the MITRE guidance here.

Finding IPT-003: Security Misconfiguration – WDigest (Critical)

Description:	Demo Corp permitted out-of-date operating systems within their network, including Windows 7, 8, Server 2008, and Server 2012. These operating systems, by default, permit WDigest, which stores all current logged-in user's passwords in clear-text. TCMS leveraged machine access gained in IPT-001 and IPT-002 to move laterally throughout the network until uncovering a machine with Domain Admin credentials stored in WDigest.
Risk:	Likelihood: Moderate – This attack is effective in networks with older operating systems. Impact: Very High – WDigests credentials are stored in clear text, which can permit the theft of sensitive accounts, such as Domain Administrators.
System:	All systems older than Windows 10 and Server 2016
Tools Used:	Metasploit, Kiwi
References:	https://stealthbits.com/blog/wdigest-clear-text-passwords-stealing-more-than-a-hash/

Evidence



```
[redacted] [redacted] W[redacted]
sup[redacted] [redacted] R[redacted]
sup[redacted] M[redacted]
```

Figure 4: Cleartext passwords of Domain Administrators

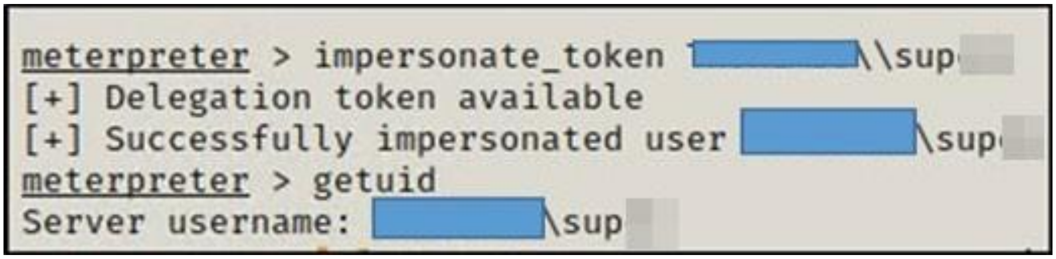
Remediation

Disable WDigest via GPO. For full mitigation and detection guidance, please reference the guidance here.

Finding IPT-004: Insufficient Hardening – Token Impersonation (Critical)

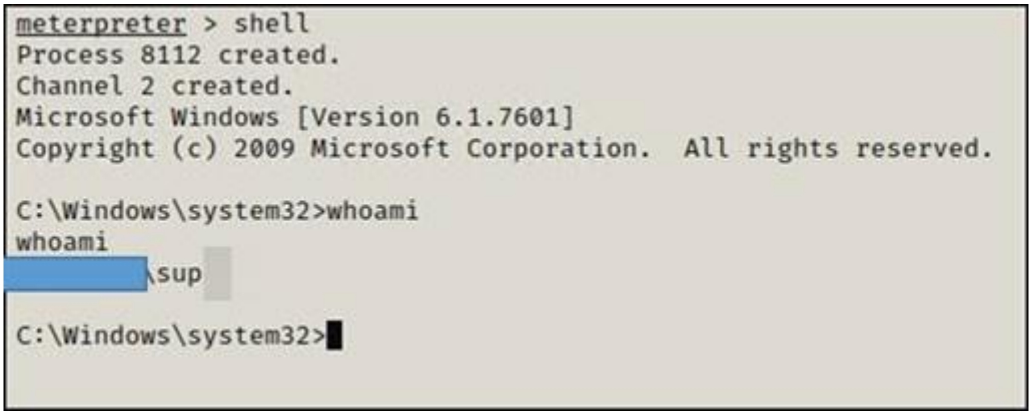
Description:	TCMS impersonated the token of “supcb” to obtain Domain Administrator privileges.
Risk:	Likelihood: High – The penetration tester viewed and impersonated tokens with the use of open-source tools. Impact: Very High - If exploited, an attacker gains domain administrator access.
System:	All
Tools Used:	Metasploit, Incognito
References:	NIST SP800-53 r4 CM-7 - Least Functionality NIST SP800-53 r4 AC-6 - Least Privilege https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/how-to-configure- protected-accounts

Evidence



```
meterpreter > impersonate_token [redacted]\\sup[redacted]
[+] Delegation token available
[+] Successfully impersonated user [redacted]\sup[redacted]
meterpreter > getuid
Server username: [redacted]\sup[redacted]
```

Figure 5: Impersonation of “sup”



```
meterpreter > shell
Process 8112 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
[redacted]\sup[redacted]

C:\Windows\system32>
```

Figure 6: Shell access as Domain Admin “sup”

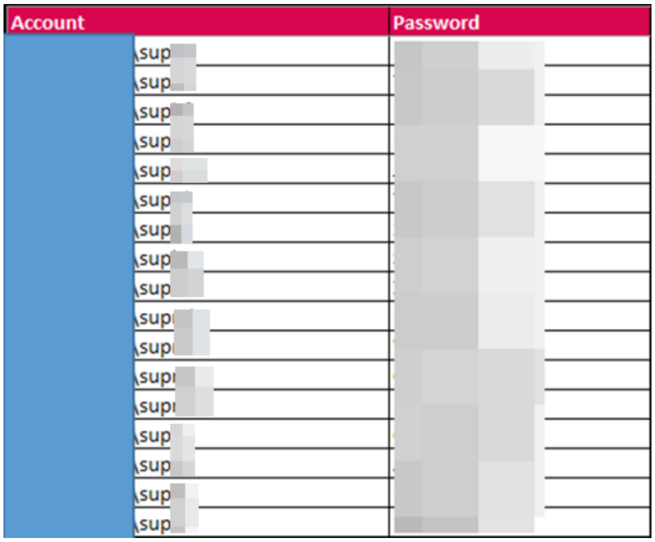
Remediation

Restrict token delegation. For full mitigation and detection guidance, please reference the MITRE guidance here.

Finding IPT-005: Insufficient Password Complexity (Critical)

Description:	TCMS dumped hashes from the domain controller and proceeded to attempt common password guessing attacks against all users. TCMS cracked 2,226 passwords using basic password list guessing attacks and low effort brute forcing attacks. 17 cracked accounts had domain administrator rights.
Risk:	Likelihood: High - Simple passwords are susceptible to password cracking attacks. Encryption provides some protection, but dictionary attacks base on common word lists often crack weak passwords. Impact: Very High - Domain admin accounts with weak passwords could lead to an adversary critically impacting Demo Corp ability to operate.
System:	All
Tools Used:	Manual Review
References:	NIST SP800-53 IA-5(1) - Authenticator Management https://www.cisecurity.org/white-papers/cis-password-policy-guide/

Evidence



Account	Password
[redacted]\sup[redacted]	[redacted]
[redacted]\sup[redacted]	[redacted]
[redacted]\sup[redacted]	[redacted]
[redacted]\sup[redacted]	[redacted]
[redacted]\sup[redacted]	[redacted]
[redacted]\sup[redacted]	[redacted]
[redacted]\sup[redacted]	[redacted]
[redacted]\sup[redacted]	[redacted]
[redacted]\sup[redacted]	[redacted]
[redacted]\sup[redacted]	[redacted]
[redacted]\sup[redacted]	[redacted]
[redacted]\sup[redacted]	[redacted]
[redacted]\sup[redacted]	[redacted]
[redacted]\sup[redacted]	[redacted]
[redacted]\sup[redacted]	[redacted]
[redacted]\sup[redacted]	[redacted]
[redacted]\sup[redacted]	[redacted]

Figure 7: Excerpt of cracked domain hashes

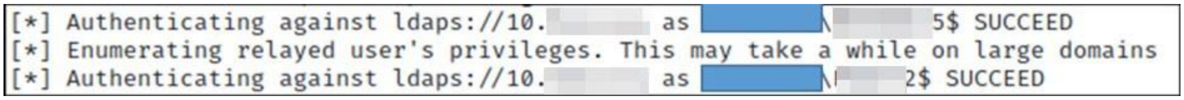
Remediation

Implement CIS Benchmark password requirements / PAM solution. TCMS recommends that Demo Corp enforce industry best practices around password complexity and management. A password filter to prevent users from using common and easily guessable passwords is also recommended. Additionally, TCMS recommends that Demo Corp enforce stricter password requirements for Domain Administrator and other sensitive accounts.

Finding IPT-006: Security Misconfiguration – IPv6 (Critical)

Description:	Through IPv6 DNS poisoning, the TCMS team was able to successfully relay credentials to the Demo Corp domain controller.
Risk:	Likelihood: High – IPv6 is enabled by default on Windows networks. The tools and techniques required to perform this task are trivial. Impact: Very High - If exploited, an attacker can gain domain administrator access.
System:	All
Tools Used:	Mitm6, Impacket
References:	https://blog.fox-it.com/2018/01/11/mitm6-compromising-ipv4-networks-via-ipv6/

Evidence



```
[*] Authenticating against ldaps://10.[redacted] as [redacted]\[redacted]5$ SUCCEED
[*] Enumerating relayed user's privileges. This may take a while on large domains
[*] Authenticating against ldaps://10.[redacted] as [redacted]\[redacted]2$ SUCCEED
```

Figure 8: Successfully relayed LDAP credentials via mitm6

Remediation

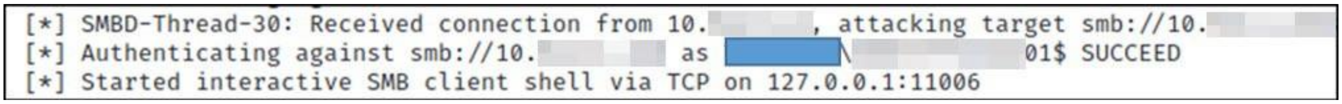
1. IPv6 poisoning abuses the fact that Windows queries for an IPv6 address even in IPv4-only environments. If you do not use IPv6 internally, the safest way to prevent mitm6 is to block DHCPv6 traffic and incoming router advertisements in Windows Firewall via Group Policy. Disabling IPv6 entirely may have unwanted side effects. Setting the following predefined rules to Block instead of Allow prevents the attack from working:
    a. (Inbound) Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCPV6-In)
    b. (Inbound) Core Networking - Router Advertisement (ICMPv6-In)
    c. (Outbound) Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCPV6-Out)
2. If WPAD is not in use internally, disable it via Group Policy and by disabling the WinHttpAutoProxySvc service.
3. Relaying to LDAP and LDAPS can only be mitigated by enabling both LDAP signing and LDAP channel binding.

Consider Administrative users to the Protected Users group or marking them as Account is sensitive and cannot be delegated, which will prevent any impersonation of that user via delegation.

Finding IPT-007: Insufficient Hardening – SMB Signing Disabled (Critical)

Description:	Demo Corp failed to implement SMB signing on multiple devices. The absence of SMB signing could lead to SMB relay attacks, yielding system-level shells without requiring a user password.
Risk:	Likelihood: High – Relaying password hashes is a basic technique not requiring offline cracking. Impact: High – If exploited, an adversary gains code execution, leading to lateral movement across the network.
System:	Identified 709 machines, please see the below file for listing. [file removed]
Tools Used:	Nessus, Nmap, MultiRelay, Responder
References:	CIS Microsoft Windows Server 2012 R2 v2.2.0 (Page 180) https://github.com/lgandx/Responder/blob/master/tools/MultiRelay.py

Evidence



```
[*] SMBD-Thread-30: Received connection from 10.[redacted], attacking target smb://10.[redacted]
[*] Authenticating against smb://10.[redacted] as [redacted]\[redacted]01$ SUCCEED
[*] Started interactive SMB client shell via TCP on 127.0.0.1:11006
```

Figure 9: Successful SMB relay

Remediation

Enable SMB signing on all Demo Corp domain computers. Alternatively, as SMB signing can cause performance issues, disabling NTLM authentication, enforcing account tiering, and limiting local admin users can effectively help mitigate attacks. For full mitigation and detection guidance, please reference the MITRE guidance here.

Finding IPT-008: Insufficient Patch Management – Software (Critical)

Description:	Demo Corp permitted various deprecated software in their network. This includes: • Apache version < 2.4.46 • Apache Tomcat version < 7.0.100, 8.5.51, 9.0.31 • Cisoco AireOS version 8.5.151.10 • CodeMeter version 3.05 (5.21.1478.500) • Dropbear SSH Server version 2015.68 • Dell iDRAC7 version 2.63.60.62.01 • Dell iDRAC8 version 2.63.60.61.06 • Dell iDRAC9 version 3.36.36.36.21 • ESXi version 5.5 • ESXi version 6.5 build 15256549 • Flexera FlexNet Publisher version 11.16.0 • IIS version 7.5 • ISC BIND version 9.6.2-P2 • Microsoft DNS Server version 6.1.7601.24261 • Microsoft SQL Server version 11.0.6594.0 • Netatalk OpenSession version < 3.1.12 • PHP version < 7.3.11 • Rockwell Automation RSLinx Classic Above lists all critical and high-rated deprecated software, the majority of which permit serious vulnerabilities, such as remote code execution. For a full patching list, please review the provided Nessus scan documentation.
Risk:	Likelihood: High – An attacker can discover these vulnerabilities with basic tools. Impact: Very High – If exploited, an attacker could possibly gain full remote code execution on or deny service to a system.
Tools Used:	Nessus
References:	NIST SP800-53 r4 MA-6 – Timely Maintenance NIST SP800-53 r4 SI-2 – Flaw Remediation

Remediation

Update to the latest software version. For a full list of vulnerable systems, versions, and patching requirements, please see the below document.

[file removed]

Finding IPT-009: Insufficient Patch Management – Operating Systems (Critical)

Description:	Demo Corp permitted various deprecated software in their network. This includes: • Windows Server 2003 (end of life on July 14, 2015) • Windows Server 2008 R2 (end of life on January 14, 2020) • Windows XP (end of life on April 8, 2014) • Windows 7 (end of life on January 14, 2020) • Ubuntu 11 (end of life on May 9, 2013) • FreeBSD 11.0 (end of life on October, 2016) End of life systems are susceptible to a multitude of vulnerabilities. TCMS did not attempt any attacks against these servers due to the risk of a denial of service, which is out of scope.
Risk:	Likelihood: High – An attacker can discover these vulnerabilities with basic tools. Impact: High – If exploited, an attacker could possibly gain full remote code execution on or deny service to a system.
System:	Identified 139 machines, please see the below file for listing. [file removed]
Tools Used:	Nessus
References:	NIST SP800-53 r4 MA-6 – Timely Maintenance NIST SP800-53 r4 SI-2 – Flaw Remediation

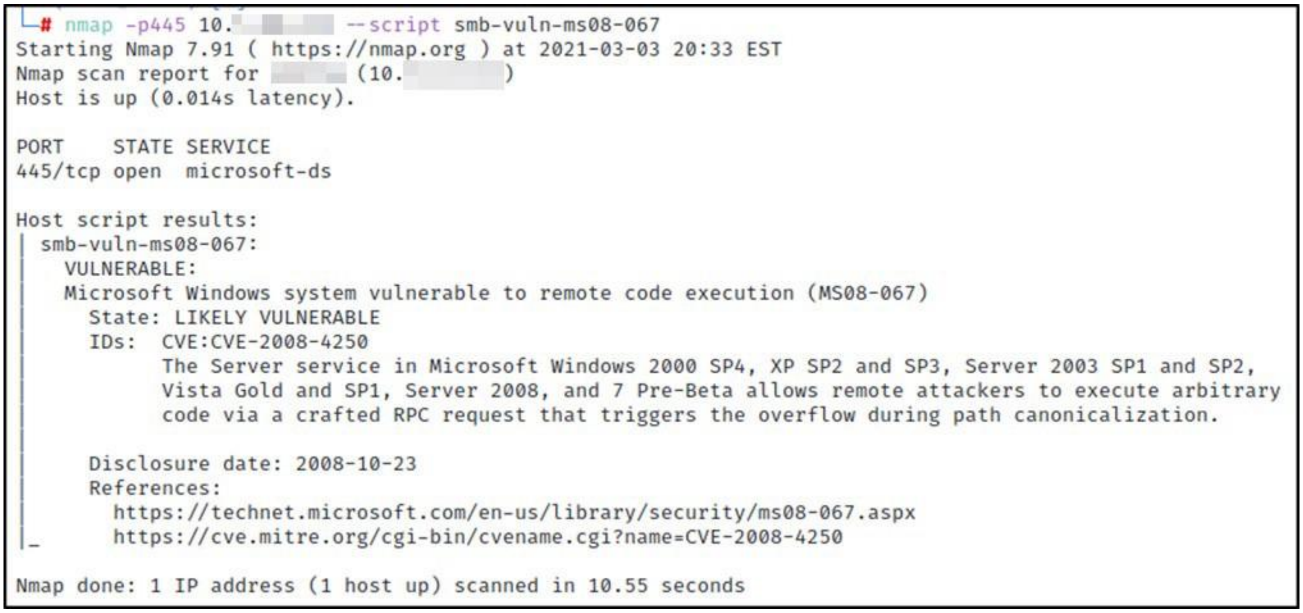
Remediation

Update Operating Systems to the latest version.

Finding IPT-010: Insufficient Patching – MS08-067 - ECLIPSEDWING/NETAPI (Critical)

Description:	Demo Corp permitted an unpatched system on the internal network that is vulnerable to MS08-067. TCM Security confirmed that the vulnerability likely exists but did not attempt the exploit to prevent any denial of service.
Risk:	Likelihood: High – Considered one of the most exploited vulnerabilities in Microsoft Windows as it ships natively with Windows XP. Impact: Very High – If exploited, an attacker gains code execution as the system user. An adversary will require additional techniques to obtain domain administrator access.
System:	10.x.x.x
Tools Used:	Nessus, Nmap
References:	NIST SP800-53 r4 MA-6 – Timely Maintenance NIST SP800-53 r4 SI-2 – Flaw Remediation

Evidence



```
└─# nmap -p445 10.[redacted] --script smb-vuln-ms08-067
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-03 20:33 EST
Nmap scan report for [redacted] (10.[redacted])
Host is up (0.014s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250

Nmap done: 1 IP address (1 host up) scanned in 10.55 seconds
```

Figure 10: Unpatched MS08-067

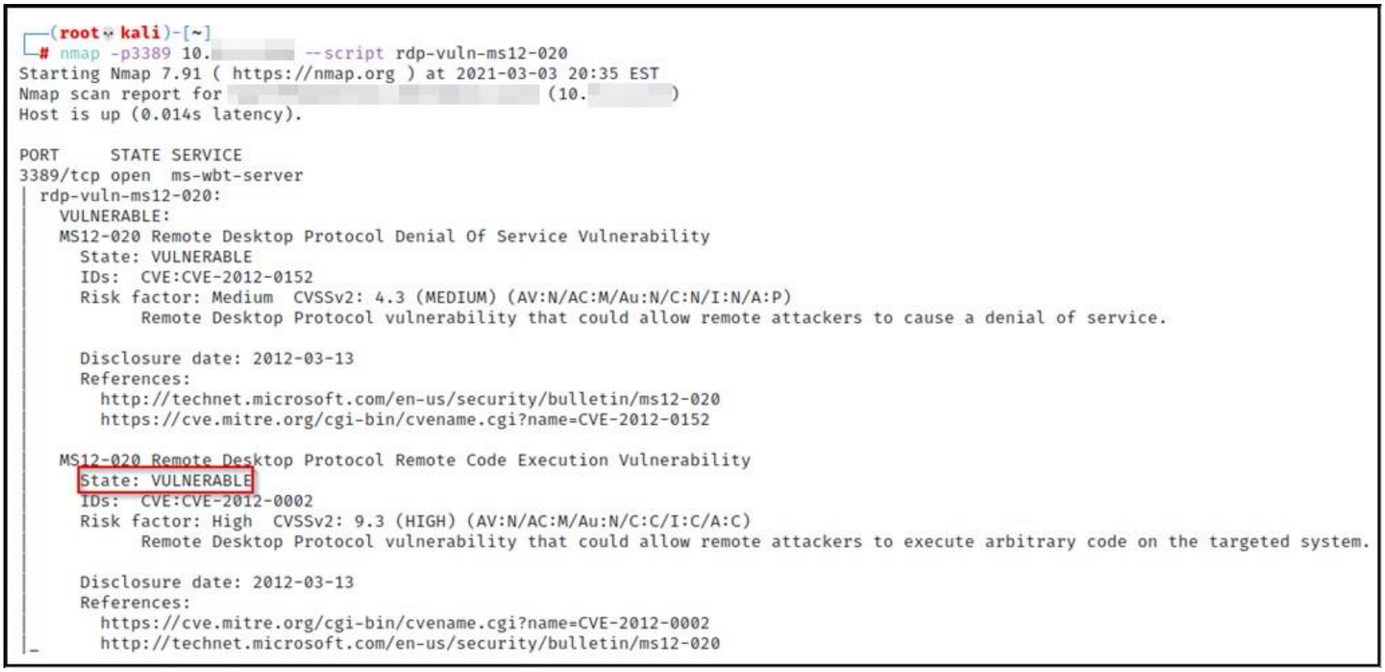
Remediation

Apply the appropriate Microsoft patches to remediate the issue. More information on patching MS08-067 can be found here: https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2008/ms08-067

Finding IPT-011: Insufficient Patching – MS12-020 – Remote Desktop RCE (Critical)

Description:	Demo Corp permitted an unpatched system on the internal network that is vulnerable to MS12-020. TCM Security confirmed that the vulnerability likely exists but did not attempt the exploit to prevent any denial of service.
Risk:	Likelihood: High – The vulnerability is easily discoverable and exploitable with open-source tools. Impact: Very High – If exploited, an attacker gains code execution as the system user. An adversary will require additional techniques to obtain domain administrator access.
System:	10.x.x.x
Tools Used:	Nessus, Nmap
References:	NIST SP800-53 r4 MA-6 – Timely Maintenance NIST SP800-53 r4 SI-2 – Flaw Remediation

Evidence



```
┌──(root㉿kali)-[~]
└─# nmap -p3389 10.[redacted] --script rdp-vuln-ms12-020
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-03 20:35 EST
Nmap scan report for [redacted] (10.[redacted])
Host is up (0.014s latency).

PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
| rdp-vuln-ms12-020:
|   VULNERABLE:
|   MS12-020 Remote Desktop Protocol Denial Of Service Vulnerability
|     State: VULNERABLE
|     IDs:  CVE:CVE-2012-0152
|     Risk factor: Medium  CVSSv2: 4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:N/A:P)
|           Remote Desktop Protocol vulnerability that could allow remote attackers to cause a denial of service.
|
|     Disclosure date: 2012-03-13
|     References:
|       http://technet.microsoft.com/en-us/security/bulletin/ms12-020
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0152
|
|   MS12-020 Remote Desktop Protocol Remote Code Execution Vulnerability
|     State: VULNERABLE
|     IDs:  CVE:CVE-2012-0002
|     Risk factor: High  CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
|           Remote Desktop Protocol vulnerability that could allow remote attackers to execute arbitrary code on the targeted system.
|
|     Disclosure date: 2012-03-13
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0002
|_      http://technet.microsoft.com/en-us/security/bulletin/ms12-020
```

Figure 11: Unpatched MS12-020

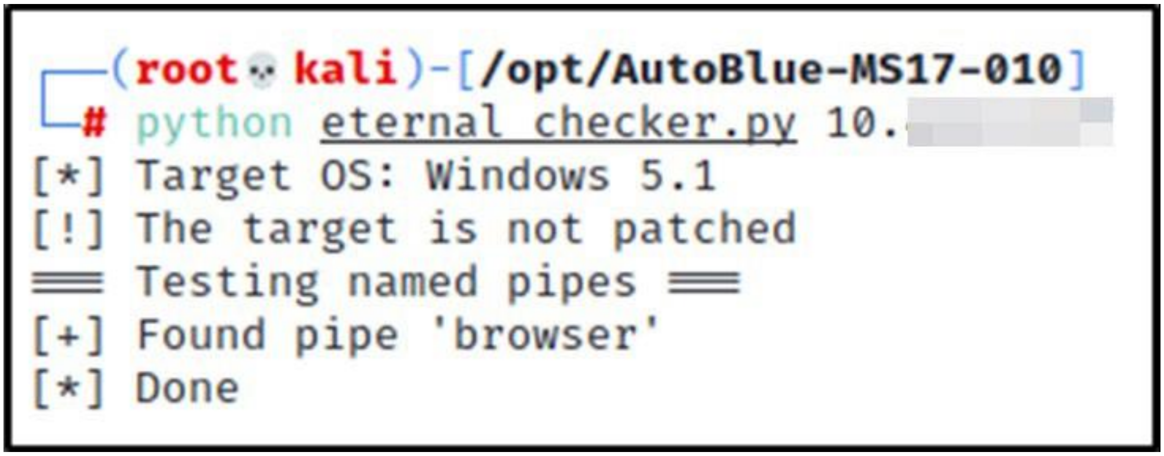
Remediation

Apply the appropriate Microsoft patches to remediate the issue. More information on patching MS12-020 can be found here: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2012/ms12-020

Finding IPT-012: Insufficient Patching – MS17-010 - EternalBlue (Critical)

Description:	Demo Corp permitted several unpatched systems on the internal network that are vulnerable to MS17-010 (EternalBlue). TCM Security confirmed that the vulnerability likely exists but did not attempt the exploit to prevent any denial of service.
Risk:	Likelihood: High – Malicious actors have used SMB exploitations like EternalBlue in recent breaches. Impact: Very High – If exploited, an attacker gains code execution as the system user. An adversary will require additional techniques to obtain domain administrator access.
System:	10.x.x.x
Tools Used:	Nessus, Metasploit, AutoBlue
References:	[NIST SP800-53 r4 MA-6](#) – Timely Maintenance [NIST SP800-53 r4 SI-2](#) – Flaw Remediation

Evidence



```
┌──(root💀kali)-[/opt/AutoBlue-MS17-010]
└─# python eternal_checker.py 10.[redacted]
[*] Target OS: Windows 5.1
[!] The target is not patched
═══ Testing named pipes ═══
[+] Found pipe 'browser'
[*] Done
```

Figure 12: Unpatched MS17-010

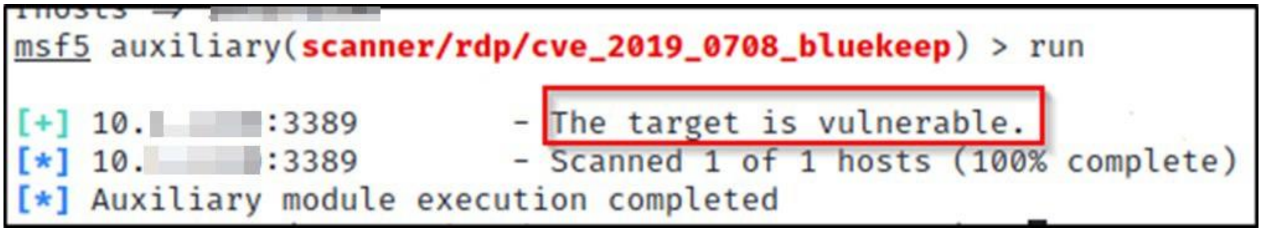
Remediation

Apply the appropriate Microsoft patches to remediate the issue. More information on patching MS17-010 can be found here: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

Finding IPT-013: Insufficient Patching – CVE-2019-0708 - BlueKeep (Critical)

Description:	Demo Corp permitted several unpatched systems on the internal network that are vulnerable to CVE-2019-0708 (BlueKeep). TCM Security confirmed that the vulnerability likely exists but did not attempt the exploit to prevent any denial of service.
Risk:	Likelihood: High – The vulnerability is easily discoverable and exploitable with open-source tools. Impact: Very High – If exploited, an attacker gains code execution as the system user. An adversary will require additional techniques to obtain domain administrator access.
System:	10.x.x.x
Tools Used:	Nessus, Nmap
References:	NIST SP800-53 r4 MA-6 – Timely Maintenance NIST SP800-53 r4 SI-2 – Flaw Remediation

Evidence



```
rhosts => [redacted]
msf5 auxiliary(scanner/rdp/cve_2019_0708_bluekeep) > run

[+] 10.[redacted]:3389        - The target is vulnerable.
[*] 10.[redacted]:3389        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Figure 13: Unpatched CVE-2019-0708

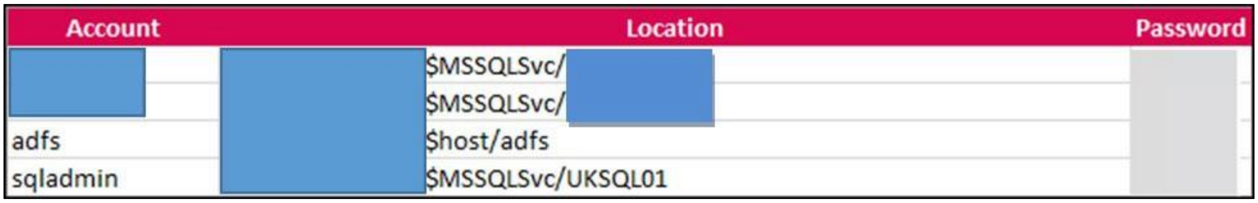
Remediation

Apply the appropriate Microsoft patches to remediate the issue. More information on patching CVE-2019-0708 can be found here: https://support.microsoft.com/en-us/topic/customer-guidance-for-cve-2019-0708-remote-desktop-services-remote-code-execution-vulnerability-may-14-2019-0624e35b-5f5d-6da7-632c-27066a79262e

Finding IPT-014: Insufficient Privileged Account Management – Kerberoasting (High)

Description:	TCMS retrieved all user service principal names (SPNs) from the Demo Corp domain controller using a domain user-level account (IPT-001) in a Kerberoasting attack. Retrieving these user SPNs permitted TCMS to crack 4 account passwords. No service accounts were observed running as domain administrators. User accounts were observed running as a service, which is not best practice.
Risk:	Likelihood: High – Any account joined to the domain can request user SPNs. Impact: High – Using SPNs, it is possible to retrieve sensitive account password hashes and crack them offline.
Tools Used:	Impacket, Hashcat
References:	Kerberoasting details: https://adsecurity.org/?p=2293 Group Managed Service Accounts Overview

Evidence



Account	Location	Password
[redacted]	[redacted] $MSSQLSvc/[redacted]	[redacted]
	$MSSQLSvc/	[redacted]
adfs	$host/adfs	[redacted]
sqladmin	$MSSQLSvc/UKSQL01	[redacted]

Figure 14: Cracked service accounts

Remediation

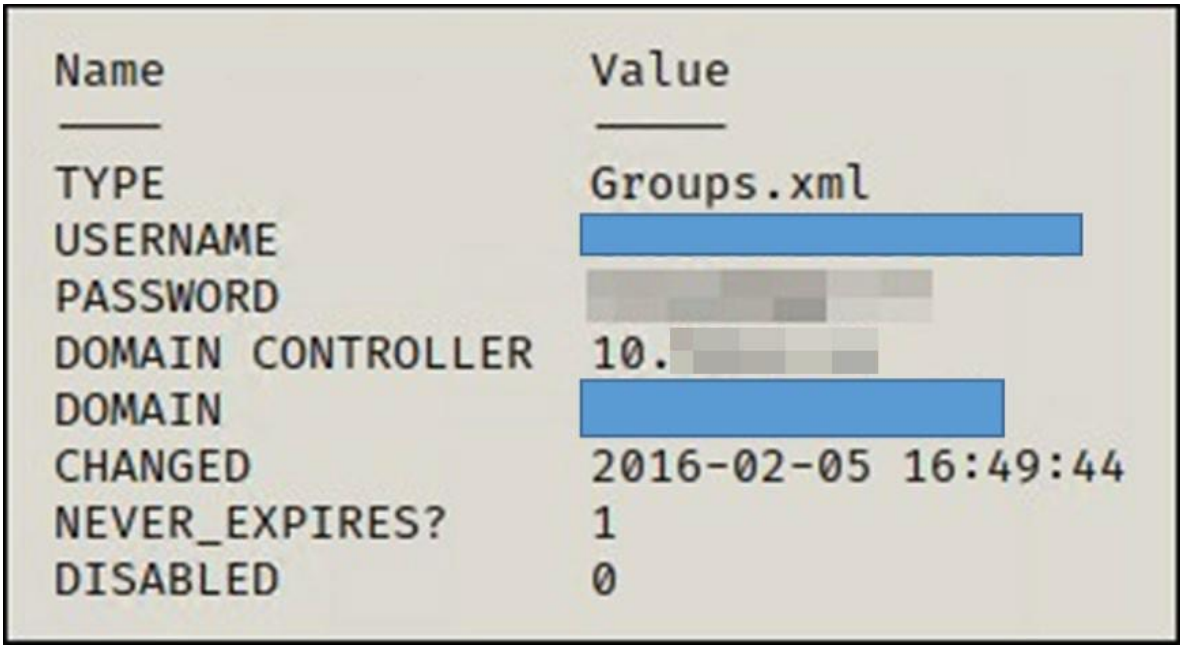
Use Group Managed Service Accounts (GMSA) for privileged services. GMSA accounts can be used to ensure passwords are long, complex, and change frequently. Where GMSA is not applicable, protect accounts by utilizing a password vaulting solution.

TCMS recommends configuring alert logging on domain controllers for Windows event ID 4769 whenever requesting a Kerberos service ticket. These alerts are prone to high false-positive rates but are a supplementary detective control. Tailor a security information and event management tool (SIEM) to alert on excessive user SPN requests.

Finding IPT-015: Security Misconfiguration – GPP Credentials (High)

Description:	Demo Corp utilized “cpasswords” in Group Policy Preference (GPP) which any domain user can query from a domain controller’s SYSVOL folder. Microsoft published the key to decrypt these passwords.
Risk:	Likelihood: High – Any authenticated user can obtain this information and decrypt the password with open source tools. Impact: High – An adversary can use these credentials to move laterally within the network.
Tools Used:	Metasploit
References:	NIST SP800-53 IA-5(1) - Authenticator Management

Evidence



```
Name                 Value
----                 -----
TYPE                 Groups.xml
USERNAME             [redacted]
PASSWORD             [redacted]
DOMAIN CONTROLLER    10.[redacted]
DOMAIN               [redacted]
CHANGED              2016-02-05 16:49:44
NEVER_EXPIRES?       1
DISABLED             0
```

Figure 15: Dumped GPP credentials

Remediation

Apply vendor patching. Do not use GPP cpasswords. Additionally, enabling authentication on the NFS share will protect the confidentiality of the stored information. Exporting authentication logs to a SIEM solution will give incident response teams insights to brute force login attempts.

Finding IPT-016: Insufficient Authentication - VNC (High)

Description:	Demo Corp deployed 3 servers that permitted unauthenticated access via VNC Server.
Risk:	Likelihood: High – Discovering unauthenticated VNC servers is trivial and can be done with open-source tools. Impact: High – Attackers can control industrial devices, destroy data, or shut down systems.
System:	10.x.x.x, 10.x.x.x, 10.x.x.x
Tools Used:	Nessus, VNC Viewer
References:	NIST SP800-53 IA-5(1) - Authenticator Management

Evidence

[image redacted]

Figure 16: Access to system via VNC

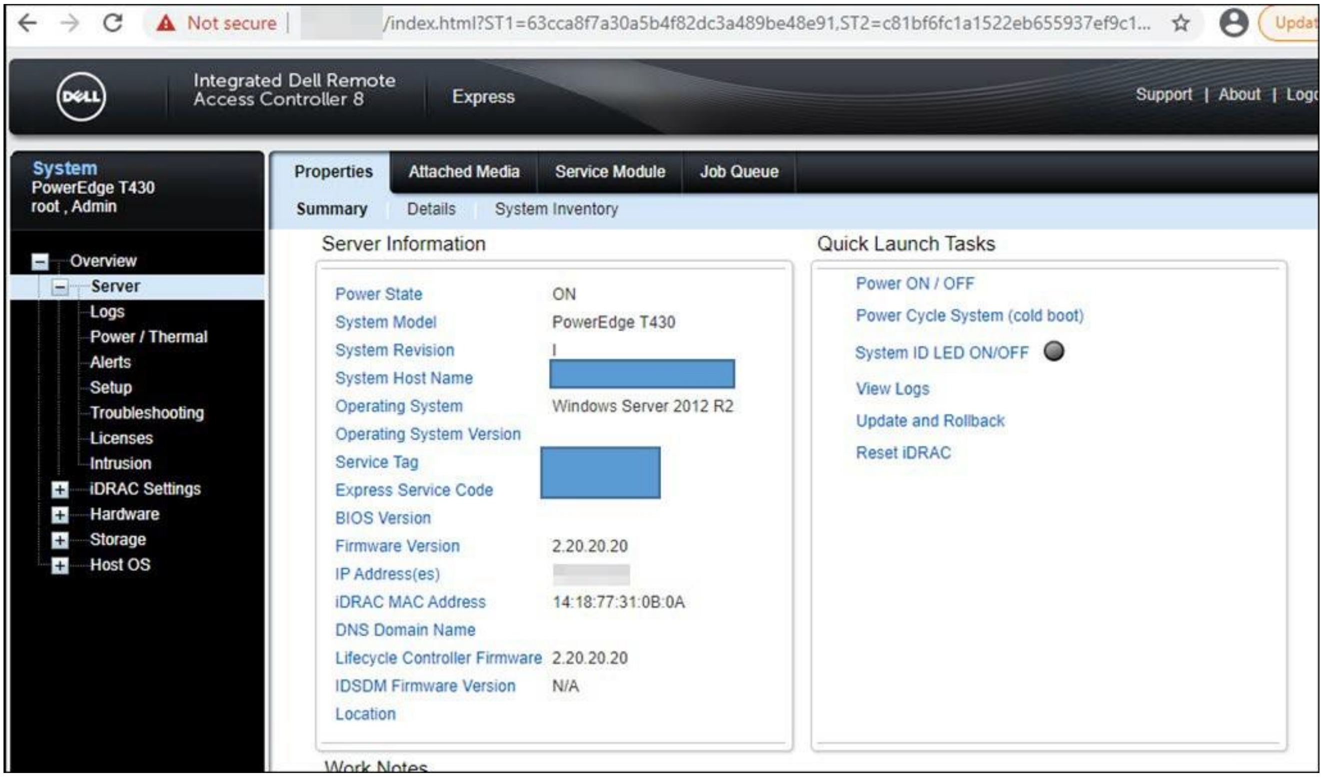
Remediation

Enable authentication on the VNC Server.

Finding IPT-017: Default Credentials on Web Services (High)

Description:	TCMS validated default credentials worked on multiple web applications within the Demo Corp environment.
Risk:	Likelihood: High – Credentials are published for these devices and an attackers first authentication attempt. Impact: High – Attackers can control devices, destroy data, or shut down systems.
System:	Default credentials were tested on a sample set of web applications, but suggests checking the following addresses at a minimum: [file removed]
Tools Used:	Manual Review
References:	NIST SP800-53 IA-5(1) - Authenticator Management

Evidence



Not secure | [redacted] /index.html?ST1=63cca8f7a30a5b4f82dc3a489be48e91,ST2=c81bf6fc1a1522eb655937ef9c1...

Integrated Dell Remote Access Controller 8 Express

Support | About | Logo

System
PowerEdge T430
root , Admin

Properties | Attached Media | Service Module | Job Queue

Summary | Details | System Inventory

Server Information

Power State ON
System Model PowerEdge T430
System Revision I
System Host Name [redacted]
Operating System Windows Server 2012 R2
Operating System Version
Service Tag [redacted]
Express Service Code
BIOS Version
Firmware Version 2.20.20.20
IP Address(es) [redacted]
iDRAC MAC Address 14:18:77:31:0B:0A
DNS Domain Name
Lifecycle Controller Firmware 2.20.20.20
IDSDM Firmware Version N/A
Location

Quick Launch Tasks

Power ON / OFF
Power Cycle System (cold boot)
System ID LED ON/OFF
View Logs
Update and Rollback
Reset iDRAC

Work Notes

Figure 17: Dell iDRAC access via default credentials

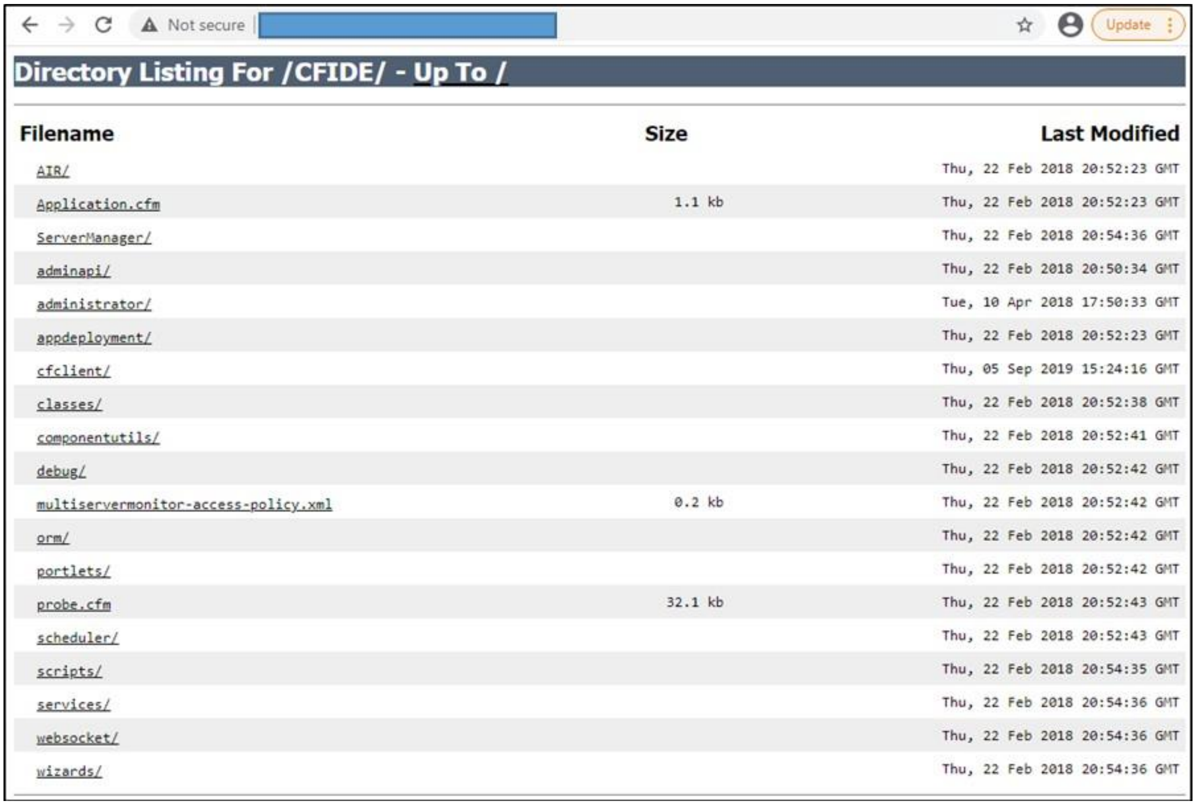
Remediation

Change default credentials or disable unused accounts.

Finding IPT-018: Insufficient Hardening – Listable Directories (High)

Description:	Demo Corp disclosed information by allowing listable directories and storing potentially critical items on web server. It is strongly recommended that Demo Corp perform a thorough web app assessment on this resource.
Risk:	Likelihood: Moderate – Adversaries will discovery content with open source tools. Impact: High – Attackers use this information in conjunction with other attacks for enumeration and cataloging for rapid attacks when vulnerabilities arise.
System:	Full list of discovered listable directories: [file removed]
Tools Used:	Manual Review
References:	NIST SP800-53r4 CM-7 - Least Functionality NIST SP800-53r4 AC-6(3) - Least Privilege

Evidence



Directory Listing For /CFIDE/ - Up To /

Filename	Size	Last Modified
AIR/		Thu, 22 Feb 2018 20:52:23 GMT
Application.cfm	1.1 kb	Thu, 22 Feb 2018 20:52:23 GMT
ServerManager/		Thu, 22 Feb 2018 20:54:36 GMT
adminapi/		Thu, 22 Feb 2018 20:50:34 GMT
administrator/		Tue, 10 Apr 2018 17:50:33 GMT
appdeployment/		Thu, 22 Feb 2018 20:52:23 GMT
cfclient/		Thu, 05 Sep 2019 15:24:16 GMT
classes/		Thu, 22 Feb 2018 20:52:38 GMT
componentutils/		Thu, 22 Feb 2018 20:52:41 GMT
debug/		Thu, 22 Feb 2018 20:52:42 GMT
multiservermonitor-access-policy.xml	0.2 kb	Thu, 22 Feb 2018 20:52:42 GMT
orm/		Thu, 22 Feb 2018 20:52:42 GMT
portlets/		Thu, 22 Feb 2018 20:52:42 GMT
probe.cfm	32.1 kb	Thu, 22 Feb 2018 20:52:43 GMT
scheduler/		Thu, 22 Feb 2018 20:52:43 GMT
scripts/		Thu, 22 Feb 2018 20:54:35 GMT
services/		Thu, 22 Feb 2018 20:54:36 GMT
websocket/		Thu, 22 Feb 2018 20:54:36 GMT
wizards/		Thu, 22 Feb 2018 20:54:36 GMT

Figure 18: Listable directory

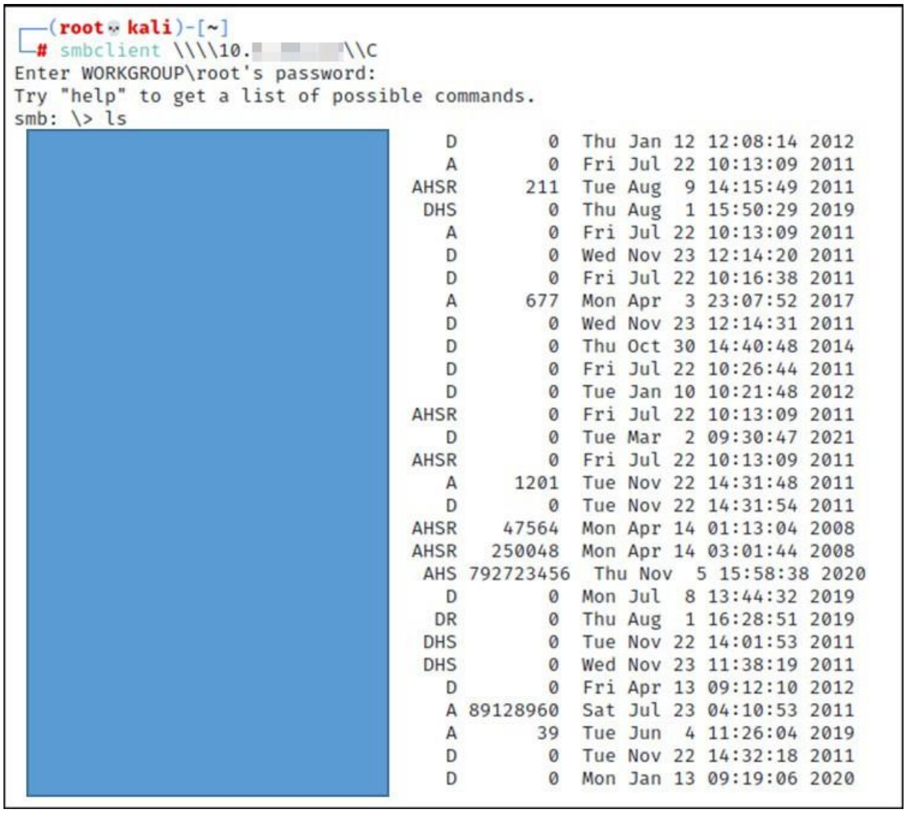
Remediation

Restrict access and conduct web app assessment.

Finding IPT-019: Unauthenticated SMB Share Access (Moderate)

Description:	Demo Corp exposed multiple servers with unauthenticated file server access.
Risk:	Likelihood: Moderate – Adversaries will discover these shares with low-noise, basic reconnaissance techniques. Impact: Moderate – Attackers learn about the environment through information leaks.
System:	10.x.x.x
Tools Used:	Nessus, smbclient
References:	NIST SP800-53r4 AC-6(3) - Least Privilege NIST SP800-53 r4 SC-4 - Information in Shared Resources

Evidence



```
┌──(root㉿kali)-[~]
└─# smbclient \\\\10.[redacted]\\C
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls
  [redacted]                             D        0  Thu Jan 12 12:08:14 2012
                                         A        0  Fri Jul 22 10:13:09 2011
                                      AHSR      211  Tue Aug  9 14:15:49 2011
                                       DHS        0  Thu Aug  1 15:50:29 2019
                                         A        0  Fri Jul 22 10:13:09 2011
                                         D        0  Wed Nov 23 12:14:20 2011
                                         D        0  Fri Jul 22 10:16:38 2011
                                         A      677  Mon Apr  3 23:07:52 2017
                                         D        0  Wed Nov 23 12:14:31 2011
                                         D        0  Thu Oct 30 14:40:48 2014
                                         D        0  Fri Jul 22 10:26:44 2011
                                         D        0  Tue Jan 10 10:21:48 2012
                                      AHSR        0  Fri Jul 22 10:13:09 2011
                                         D        0  Tue Mar  2 09:30:47 2021
                                      AHSR        0  Fri Jul 22 10:13:09 2011
                                         A     1201  Tue Nov 22 14:31:48 2011
                                         D        0  Tue Nov 22 14:31:54 2011
                                      AHSR    47564  Mon Apr 14 01:13:04 2008
                                      AHSR   250048  Mon Apr 14 03:01:44 2008
                                       AHS 792723456  Thu Nov  5 15:58:38 2020
                                         D        0  Mon Jul  8 13:44:32 2019
                                        DR        0  Thu Aug  1 16:28:51 2019
                                       DHS        0  Tue Nov 22 14:01:53 2011
                                       DHS        0  Wed Nov 23 11:38:19 2011
                                         D        0  Fri Apr 13 09:12:10 2012
                                         A 89128960  Sat Jul 23 04:10:53 2011
                                         A       39  Tue Jun  4 11:26:04 2019
                                         D        0  Tue Nov 22 14:32:18 2011
                                         D        0  Mon Jan 13 09:19:06 2020
```

Figure 19: Unauthenticated Share access

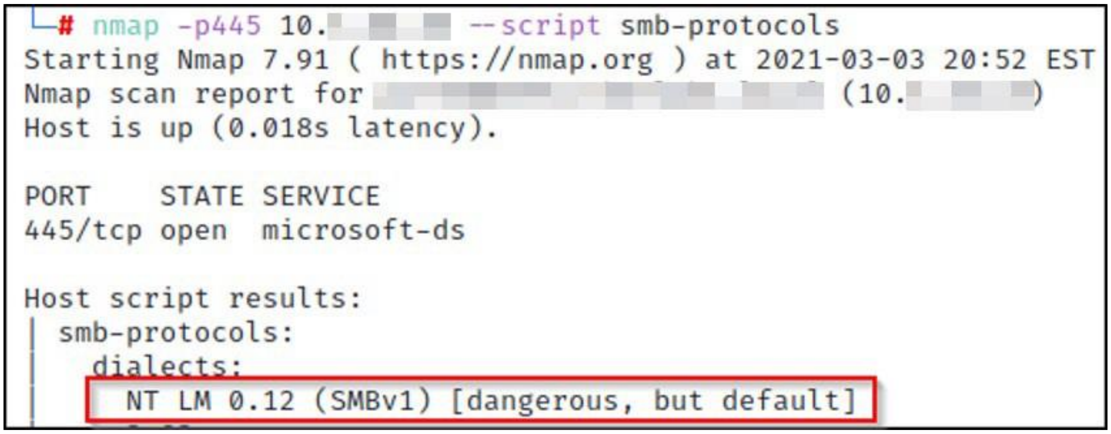
Remediation

Disable SMB share or require authentication. Enabling authentication on the share will protect the confidentiality of the stored information. Exporting authentication logs to a SIEM solution will give incident response teams insights to brute force login attempts.

Finding IPT-020: Insufficient Patch Management – SMBv1 (Moderate)

Description:	Demo Corp failed to patch SMBv1. This version is vulnerable to multiple denial of service and remote code execution attacks. TCM Security confirmed that the vulnerability likely exists but did not attempt the exploit to prevent any denial of service.
Risk:	Likelihood: Moderate – Basic scans would identify the SMB version but would require an adversary to be on the internal network and identify an exploit. Impact: Moderate – If exploited, an attacker gains denial of service and code execution capability.
System:	10.x.x.x
Tools Used:	Nessus, Nmap
References:	https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/ NIST SP800-53 r4 SI-2 - Flaw Remediation

Evidence



```
└─# nmap -p445 10.[redacted] --script smb-protocols
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-03 20:52 EST
Nmap scan report for [redacted] (10.[redacted])
Host is up (0.018s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-protocols:
|   dialects:
|     NT LM 0.12 (SMBv1) [dangerous, but default]
```

Figure 20: Unauthenticated Share access

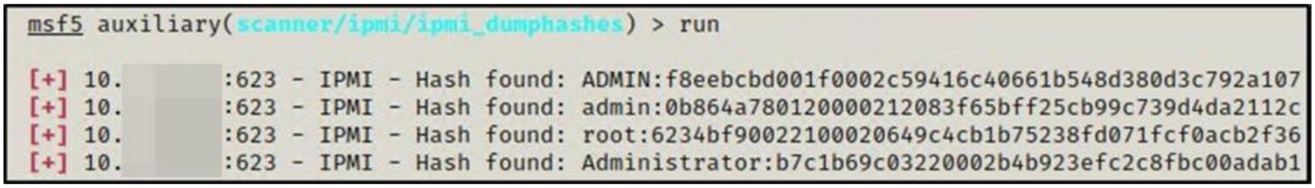
Remediation

Upgrade to SMBv3 and apply latest patching.

Finding IPT-021: IPMI Hash Disclosure (Moderate)

Description:	Demo Corp deployed remote host supporting IPMI v2.0. The (IPMI) protocol is affected by an information disclosure vulnerability due to the support of RMCP+ Authenticated Key-Exchange Protocol (RAKP) authentication. A remote attacker can obtain password hash information for valid user accounts via the HMAC from a RAKP message 2 response from a BMC.
Risk:	Likelihood: High – Basic network scans will identify this vulnerability. Impact: Moderate – If exploited, an attacker can gain access to sensitive management devices. TCMS was unable to crack any hashes during the assessment.
System:	Identified 34 machines, please see the below file for listing. [file removed]
Tools Used:	Metasploit
References:	https://blog.rapid7.com/2013/07/02/a-penetration-testers-guide-to-ipmi/

Evidence



```
msf5 auxiliary(scanner/ipmi/ipmi_dumphashes) > run

[+] 10.[redacted]:623 - IPMI - Hash found: ADMIN:f8eebcbd001f0002c59416c40661b548d380d3c792a107
[+] 10.         :623 - IPMI - Hash found: admin:0b864a780120000212083f65bff25cb99c739d4da2112c
[+] 10.         :623 - IPMI - Hash found: root:6234bf90022100020649c4cb1b75238fd071fcf0acb2f36
[+] 10.         :623 - IPMI - Hash found: Administrator:b7c1b69c03220002b4b923efc2c8fbc00adab1
```

Figure 21: IPMI Hash Disclosure

Remediation

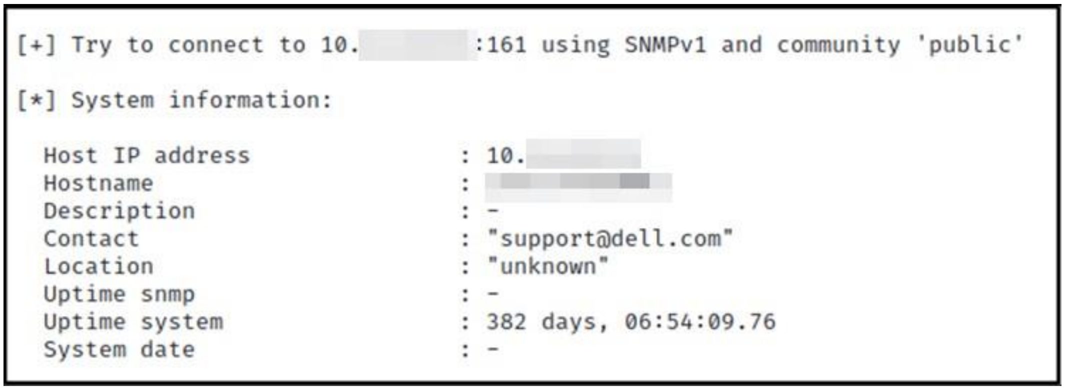
There is no patch for this vulnerability; it is an inherent problem with the specification for IPMI v2.0. Suggested mitigations include:

- Disabling IPMI over LAN if it is not needed.
- Using strong passwords to limit the successfulness of off-line dictionary attacks.
- Using Access Control Lists (ACLs) or isolated networks to limit access to your IPMI management interfaces.

Finding IPT-022: Insufficient SNMP Community String Complexity (Moderate)

Description:	Demo Corp deployed SNMP with default “public” community strings. This configuration exposed read-only access to the system’s management information base (MIB), including the network configurations.
Risk:	Likelihood: High – Basic network scans will identify this vulnerability. Impact: Moderate – If exploited, an attacker can profile the device and focus attacks.
System:	Identified 45 machines, please see the below file for listing. [file removed]
Tools Used:	Nessus, SNMP-Check, Ettercap
References:	NIST SP800-53 r4 AC-17(2) - Remote Access Protection of Confidentiality/Integrity using Encryption

Evidence

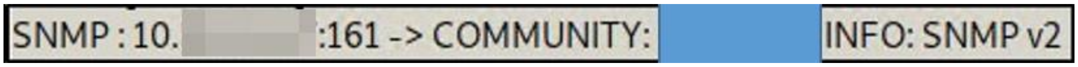


```
[+] Try to connect to 10.[redacted]:161 using SNMPv1 and community 'public'

[*] System information:

  Host IP address               : 10.[redacted]
  Hostname                      : [redacted]
  Description                   : -
  Contact                       : "support@dell.com"
  Location                      : "unknown"
  Uptime snmp                   : -
  Uptime system                 : 382 days, 06:54:09.76
  System date                   : -
```

Figure 22: Information disclosure via public SNMP community strings



```
SNMP : 10.[redacted]:161 -> COMMUNITY: [redacted] INFO: SNMP v2
```

Figure 23: Non-public SNMP string captured via Ettercap

Remediation

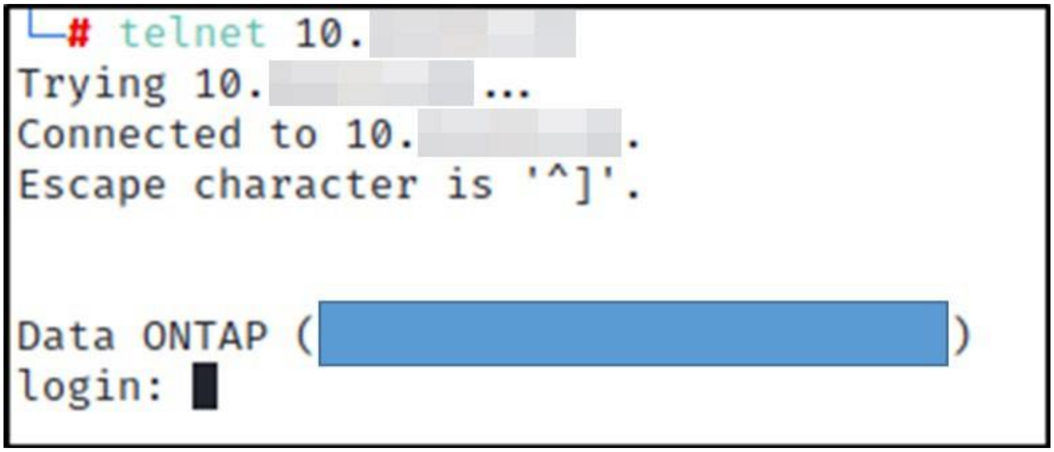
TCM Security recommends Demo Corp consider the following corrective actions:

- Disabled SNMP if not required
- Filter UDP packets going to port UDP – 161
- Evaluate migration to SNMPv3
- Use password complexity guidelines for community strings

Finding IPT-023: Insufficient Data in Transit Encryption - Telnet (Moderate)

Description:	Demo Corp permitted Telnet which does not encrypt data in transit. Telnet uses plain text authentication and passes all data (including passwords) in clear text and can be intercepted by an attacker.
Risk:	Likelihood: Low – An adversary requires a Man-in-the-Middle position between the client and server. Impact: High – If exploited an adversary may intercept administrative credentials that can be used in other attacks.
System:	Identified 53 machines, please see the below file for listing. [file removed]
Tools Used:	Telnet
References:	NIST SP800-53 r4 AC-17(2) - Remote Access |Protection of Confidentiality / Integrity Using Encryption

Evidence



```
└─# telnet 10.[redacted]
Trying 10.[redacted]...
Connected to 10.[redacted].
Escape character is '^]'.


Data ONTAP ([redacted])
login: █
```

Figure 24: Telnet login prompt

Remediation

Migrate to TLS protected protocols.

Finding IPT-024: Insufficient Terminal Services Configuration (Moderate)

Description:	The remote Terminal Services is not configured to use Network Level Authentication (NLA) only. NLA uses the Credential Security Support Provider (CredSSP) protocol to perform strong server authentication either through TLS/SSL or Kerberos mechanisms, which protect against man-in-the-middle attacks. In addition to improving authentication, NLA also helps protect the remote computer from malicious users and software by completing user authentication before a full RDP connection is established.
Risk:	Likelihood: Low – An attacker can discover these vulnerabilities with basic tools. Impact: High – If exploited, an adversary gains code execution, leading to lateral movement across the network.
System:	Identified 118 machines, please see the below file for listing. [file removed]
Tools Used:	Nessus
References:	https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v=ws.11)

Remediation

Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows.

Finding IPT-025: Steps to Domain Admin (Informational)

The steps below describe how the penetration tester obtained domain administrator access. Each step also provides remediation recommendations to help mitigate risk.

Step	Action	Remediation
1	Poisoned LLMNR responses to obtain NetNTLMv2 hash of regular network user	Disable multicast name resolution via GPO.
2	Cracked NTLM hash offline of domain administrator users ‘production’ and ‘[name removed]’	Increase password complexity. Utilize multi- factor. Implement a Privileged Account Management solution. Utilize a password filter.
3	Leveraged password of ‘production’ account to gain access to several machines within the network	Limit local administrator privileges and enforce least privilege.
4	Dumped hashes on accessed machines to find cleartext password of ‘Bartender’ account via wdigest	Disable WDigest via GPO.
5	Overly-permissive ‘Bartender’ account permitted access to a large amount of machines within the network	Limit local administrator privileges and enforce least privilege.
6	Dumped hashes on accessed machines to find cleartext password of Domain Administrator account	Disable WDigest via GPO.
7	Utilized discovered credentials to log into the domain controller.	

Remediation

Review action and remediation steps.

Additional Scans and Reports

TCMS provides all clients with all report information gathered during testing. This includes Nessus files and full vulnerability scans in detailed formats. These reports contain raw vulnerability scans and additional vulnerabilities not exploited by TCM Security.

The reports identify hygiene issues needing attention but are less likely to lead to a breach, i.e. defense-in-depth opportunities. For more information, please see the documents in your shared drive folder labeled “Additional Scans and Reports”.

Last Page