DEMO CORP

Security Assessment Findings Report

Penetration Tester: Heath Adams

Published Date: July 1, 2024

Project: TCMS PNPT Demo Report

Version: 1.0

Table of Contents

1 Confidentiality Statement

This document is the exclusive property of DEMO CORP and TCM Security (TCMS). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both DEMO CORP and TCMS.

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

2 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. TCMS prioritized the assessment to identify the weakest security controls an attacker would exploit. TCMS recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

3 Contact Information

DEMO CORP		
Name	**Title**	**Contact Email**
John Smith	Global Information Security Manager	jsmith@democorp.com

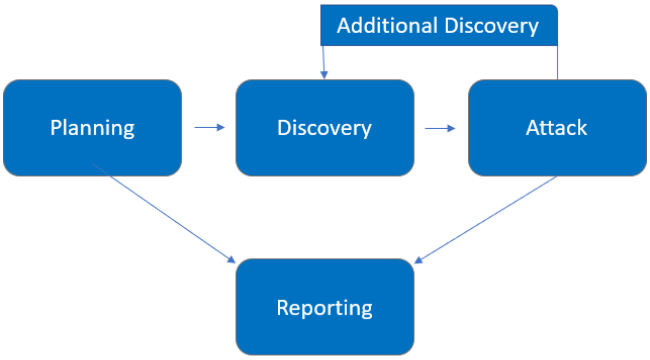
TCM Security		
Assessor Name	**Title**	**Assessor Contact Email**
Heath Adams	Lead Penetration Tester	heath@tcm-sec.com

4 Assessment Overview

From 2024-06-24 to 2024-07-01 , DEMO CORP engaged TCMS to evaluate the security posture of its infrastructure compared to current industry best practices that included an internal network penetration test. All testing performed is based on the NIST SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and customized testing frameworks.

4.1 Phases of Penetration Testing

- **Planning**: Gather customer goals and obtain rules of engagement.
- **Discovery**: Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- **Attack**: Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- **Reporting**: Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



5 Assessment Components

5.1 External Penetration Test

An external penetration test emulates the role of an attacker attempting to gain acces to an internal network without internal resources or inside knowledge. A TCMS engineer attempts to gather sensitive information through open-source intelligence (OSINT), including employee information, historical breached passwors, and more that can be leveraged against external system to gain internal network access. The engineer also performs scanning and enumeration to identify potential vulnerabilities in hopes of exploitation.

5.2 Internal Penetration Test

An internal penetration test emulates the role of an attacker from inside the network. An engineer will scan the network to identify potential host vulnerabilities and perform common and advanced internal network attacks, such as: LLMNR/NBT-NS poisoning and other man- in-the-middle attacks, token impersonation, kerberoasting, pass-the-hash, golden ticket, and more. The engineer will seek to gain access to hosts through lateral movement, compromise domain user and admin accounts, and exfiltrate sensitive data.

6 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.
Medium	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.
Info	0.0	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

7 Risk Factors

Risk is measured by two factors: Likelihood and Impact:

7.1 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.

7.2 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.

8 Scope

The scope of this assessment was one external IP address, two internal network ranges, the TODO Active Directory domain, and any other Active Directory domains owned by DEMO CORP discovered if internal network access were achieved.

In Scope Assets

Host/URL/IP Address	Description
10.x.x.x/8	DEMO CORP internal network
TODO	DEMO CORP internal AD domain
TODO	TODO
TODO other discovered internal domain(s)	TODO

8.1 Scope Exclusions

Per client request, TCMS did not perform any of the following attacks during testing:

- Denial of Service (DoS)
- Phishing/Social Engineering

All other attacks not specified above were permitted by DEMO CORP.

8.2 Client Allowances

DEMO CORP provided TCMS the following allowances:

- Internal access to network via dropbox and port allowances

9 Executive Summary

TCMS evaluated DEMO CORP internal security posture through penetration testing from 2024-06-24 to 2024-07-01. The following sections provide a high-level overview of vulnerabilities discovered, successful and unsuccessful attempts, and strengths and weaknesses.

9.1 Scoping and Time Limitations

Scoping during the engagement did not permit denial of service or social engineering across all testing components.

Time limitations were in place for testing. Internal network penetration testing was permitted for TODO (TODO) business days.

9.2 Testing Summary

The network assessment evaluated DEMO CORP internal network security posture. From an internal perspective, the TCMS team performed vulnerability scanning against all IPs provided by DEMO CORP to evaluate the overall patching health of the network. The team also performed common Active Directory based attacks, such as Link-Local Multicast Name Resolution (LLMNR) Poisoning, SMB relaying, IPv6 man-in-the-middle relaying, and Kerberoasting. Beyond vulnerability scanning and Active Directory attacks, the TCMS evaluated other potential risks, such as open file shares, default credentials on servers/devices, and sensitive information disclosure to gain a complete picture of the network’s security posture.

The TCMS team discovered that LLMNR was enabled in the network (Finding TODO), which permitted the interception of user hashes via LLMNR poisoning. These hashes were taken offline and cracked via dictionary attacks, which signals a weak password policy (Finding TODO). Utilizing the cracked passwords, the TCMS team gained access to several machines within the network, which indicates overly permissive user accounts.

With machine access, and the use of older operating systems in the network (Finding TODO), the team was able to leverage WDigest (Finding TODO) to recover cleartext credentials to accounts. The team was also able to dump local account hashes on each machine accessed. The TCMS team discovered that the local account hashes were being re-used across devices (Finding TODO), which lead to additional machine access through pass-the-hash attacks.

Ultimately, the TCMS team was able to leverage accounts captured through WDigest and hash dumps to move laterally throughout the network until landing on a machine that had a Domain Administrator credential in cleartext via WDigest. The testing team was able to use this credential to log into the domain controller and compromise the entire domain. For a full walkthrough of the path to Domain Admin, please see Finding TODO.

In addition to the compromise listed above, the TCMS team found that users could be impersonated through delegation attacks (Finding TODO), SMB relay attacks were possible due to SMB signing being disabled (Finding TODO), and IPv6 traffic was not restricted, which could lead to LDAPS relaying and domain compromise (Finding TODO).

The remainder of critical findings relate to patch management as devices with critical out-of-date software (Finding TODO), operating systems (Finding TODO), and Microsoft RCE vulnerabilities (Findings TODO, TODO, TODO, TODO), were found to be present within the network.

The remainder of the findings were high, moderate, low, or informational. For further information on findings, please review the Technical Findings section.

9.3 Tester Notes and Recommendations

Testing results of the DEMO CORP network are indicative of an organization undergoing its first penetration test, which is the case here. Many of the findings discovered are vulnerabilities within Active Directory that come enabled by default, such as LLMNR, IPv6, and Kerberoasting.

During testing, two constants stood out: a weak password policy and weak patching. The weak password policy led to the initial compromise of accounts and is usually one of the first footholds an attacker attempts to use in a network. The presence of a weak password policy is backed up by the evidence of our testing team cracking over 2,200 user account passwords, including a majority of the Domain Administrator accounts, through basic dictionary attacks.

We recommended that DEMO CORP re-evaluates their current password policy and considers a policy of 15 characters or more for their regular user accounts and 30 characters or more for their Domain Administrator accounts. We also recommend that Demo Corp explore password blacklisting and will be supplying a list of cracked user passwords for the team to evaluate. Finally, a Privilege Access Management solution should be considered.

Weak patching and dated operating systems led to the compromise of dozens of machines within the network. We believe the number of compromised machines would have been significantly larger, however the TCMS and DEMO CORP teams agreed it was not necessary to attempt to exploit any remote code execution (RCE) based vulnerabilities, such as MS17-010 (Finding TODO), as the domain controller had already been compromised and the teams did not want to risk any denial of service through failed attacks.

We recommend that the DEMO CORP team review the patching recommendations made in the Technical Findings section of the report along with reviewing the provided Nessus scans for a full overview of items to be patched. We also recommend that DEMO CORP improve their patch management policies and procedures to help prevent potential attacks within their network.

On a positive note, our testing team triggered several alerts during the engagement. The DEMO CORP Security Operations team discovered our vulnerability scanning and was alerted when we attempted to use noisy attacks on a compromised machine. While not all attacks were discovered during testing, these alerts are a positive start. Additional guidance on alerting and detection has been provided for findings, when necessary, in the Technical Findings section.

Overall, the DEMO CORP network performed as expected for a first-time penetration test. We recommend that the DEMO CORP team thoroughly review the recommendations made in this report, patch the findings, and re-test annually to improve their overall internal security posture.

9.4 Key Strengths and Weaknesses

The following identifies the key strengths identified during the assessment:

1. Observed some scanning of common enumeration tools (Nessus)

2. Mimikatz detected on some machines
3. Service accounts were not running as domain administrators
4. DEMO CORP local administrator account password was unique to each device

The following identifies the key weaknesses identified during the assessment:

1. Password policy found to be insufficient
2. Critically out-of-date operating systems and weak patching exist within the network
3. Passwords were observed in cleartext due to WDigest
4. LLMNR is enabled within the network
5. SMB signing is disabled on all non-server devices in the work
6. IPv6 is improperly managed within the network
7. User accounts can be impersonated through token delegation
8. Local admin accounts had password re-use and were overly permissive
9. Default credentials were discovered on critical infrastructure, such as iDRACs
10. Unauthenticated share access was permitted
11. User accounts were found to be running as service accounts
12. Service accounts utilized weak passwords
13. Domain administrator utilized weak passwords

10 Vulnerability Summary & Report Card

During the course of testing, Heath Adams uncovered a total of 7 findings that pose a material risk to DEMO CORP's information systems. Heath Adams also identified 1 informational finding that, if addressed, could further strengthen DEMO CORP's overall security posture. Informational findings are observations for areas of improvement by the organization and do not represent security vulnerabilities on their own. The below chart provides a summary of the findings by severity level.

In the course of this penetration test **3 Critical**, **1 High**, **1 Medium**, **1 Low** and **1 Info** vulnerabilities were identified:

Finding Severity	Number of Findings
Critical	3
High	1
Medium	1
Low	1
Informational	1

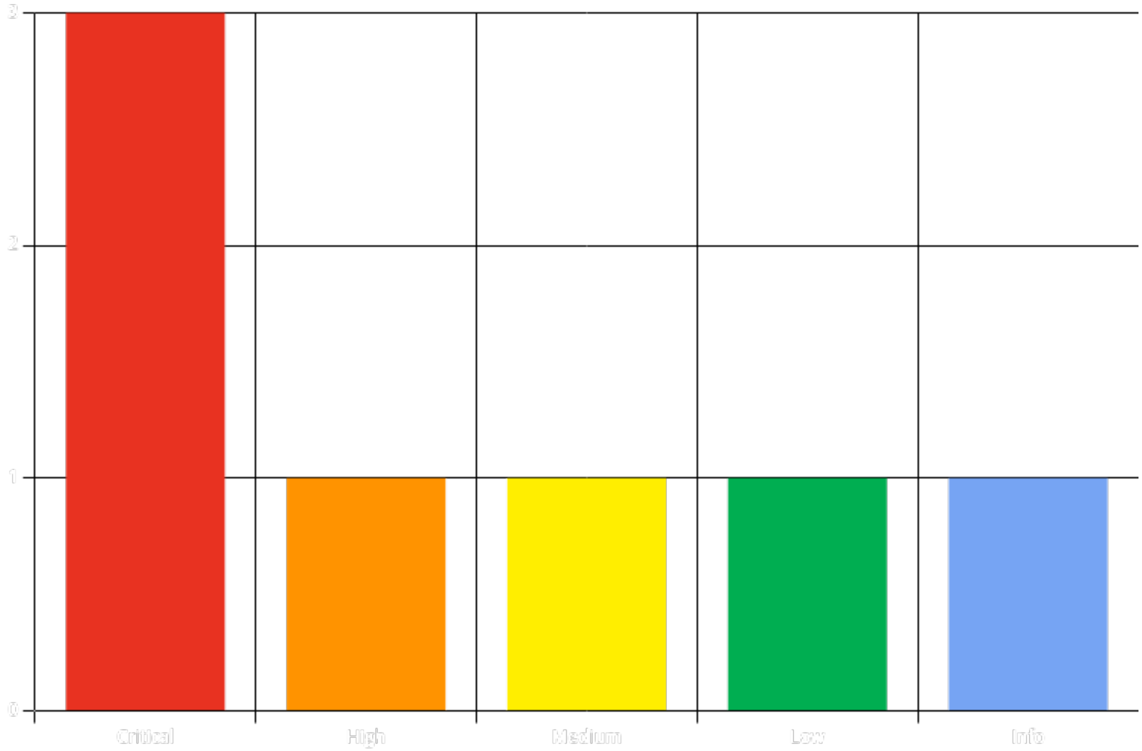


Figure 1 - Distribution of identified vulnerabilities

10.1 External Penetration Test Findings

Below is a high-level overview of each external finding identified during testing. The following table illustrates the vulnerabilities found by impact and recommended remediations. These findings are covered in depth in the Technical Findings Details section of this report.

ID	Severity	Finding Name	Recommendation
EPT-1	9.9 (Critical)	Sample External Finding	See Page 15

10.2 Internal Penetration Test Findings

Below is a high-level overview of each internal finding identified during testing. The following table illustrates the vulnerabilities found by impact and recommended remediations. These findings are covered in depth in the Technical Findings Details section of this report.

ID	Severity	Finding Name	Recommendation
IPT-2	9.9 (Critical)	Insufficient Hardening – SMB Signing Disabled	See Page 17
IPT-3	9.9 (Critical)	Insufficient LLMNR Configuration	See Page 19
IPT-4	8.1 (High)	Default Credentials on Web Services	See Page 21
IPT-5	5.5 (Medium)	IPMI Hash Disclosure	See Page 23
IPT-6	1.8 (Low)	Sample Low Severity Finding	See Page 25
IPT-7	0.0 (Info)	Steps to Domain Admin	See Page 26

11 Technical Findings

11.1 External Penetration Test Findings

1. Sample External Finding - Critical

CWE	N/A
CVSS 3.1	9.9 / CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Description	A description of the finding.
Risk	**Likelihood**: TODO **Impact**: TODO
Affected Systems	TODO AFFECTED COMPONENT
Tools Used	TODO TOOLS USED
Remediation	TODO REMEDIATION
References	TODO REFERENCES

Detailed Walkthrough

Heath Adamsperformed the following to fully compromise the TODO INSERT DOMAIN NAME domain.

1. TODO LIST HIGH LEVEL STEPS
2. ...

Detailed reproduction steps for this attack chain are as follows: TODO FILL IN DETAILED ATTACK CHAIN STEPS

Heath Adamsthen performed the following to fully compromise the TODO INSERT OTHER INTERNAL DOMAIN NAME(S) domain.

1. TODO LIST HIGH LEVEL STEPS
2. ...

Detailed reproduction steps for this attack chain are as follows: TODO FILL IN DETAILED ATTACK CHAIN STEPS

Evidence

```
ADD COMMAND OUTPUT AS APPROPRIATE
```

TODO ADD SCREENSHOTS AS APPROPRIATE

Screenshot

Figure 2 - Screenshot

Screenshot

Figure 3 - Screenshot

11.3 Internal Penetration Test Findings

2. Insufficient Hardening – SMB Signing Disabled - Critical

CWE	N/A
CVSS 3.1	9.9 / CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
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.
Affected Systems	Identified 709 machines, please see the below file for listing.
Tools Used	• Nessus • Nmap • MultiRelay • Responder
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.
References	• CIS Microsoft Windows Server 2012 R2 v2.2.0 (Page 180) • https://github.com/lgandx/Responder/blob/master/tools/MultiRelay.py

Detailed Walkthrough

Heath Adamsperformed the following to fully compromise the TODO INSERT DOMAIN NAME domain.

1. TODO LIST HIGH LEVEL STEPS
2. ...

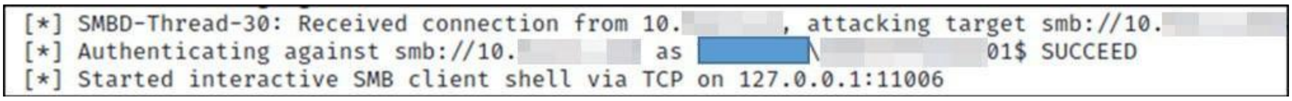
Detailed reproduction steps for this attack chain are as follows: TODO FILL IN DETAILED ATTACK CHAIN STEPS

Heath Adamsthen performed the following to fully compromise the TODO INSERT OTHER INTERNAL DOMAIN NAME(S) domain.

1. TODO LIST HIGH LEVEL STEPS
2. ...

Detailed reproduction steps for this attack chain are as follows: TODO FILL IN DETAILED ATTACK CHAIN STEPS

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
```

3. Insufficient LLMNR Configuration - Critical

CWE	N/A
CVSS 3.1	9.9 / CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Description	DEMO CORP allows multicast name resolution on their end-user networks. TCMS captured 20 user account hashes by poisoning LLMNR traffic and cracked 2 with commodity cracking software. The cracked accounts were used to leverage further access that led to the compromise of the Domain Controller.
Risk	**Likelihood**: High – This attack is effective in environments allowing multicast name resolution. **Impact**: Very High – LLMNR poisoning permits attackers to capture password hashes to either crack offline or relay in real-time and pivot laterally in the environment.
Affected Systems	All
Tools Used	• Responder • Hashcat
Remediation	Disable multicast name resolution via GPO. For full mitigation and detection guidance, please reference the MITRE guidance here. The cracked hashes demonstrate a deficient password complexity policy. If multicast name resolution is required, Network Access Control (NAC) combined with application whitelisting can limit these attacks.
References	• Stern Security - Local Network Attacks: LLMNR and NBT-NS Poisoning • NIST SP800-53 r4 IA-3 - Device Identification and Authentication • NIST SP800-53 r4 CM-6(1) - Configuration Settings

Detailed Walkthrough

Heath Adamsperformed the following to fully compromise the TODO INSERT DOMAIN NAME domain.

1. TODO LIST HIGH LEVEL STEPS
2. ...

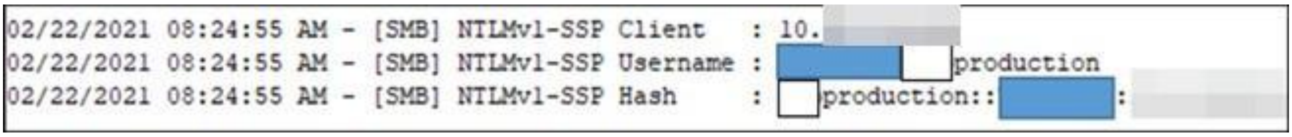
Detailed reproduction steps for this attack chain are as follows: TODO FILL IN DETAILED ATTACK CHAIN STEPS

Heath Adamsthen performed the following to fully compromise the TODO INSERT OTHER INTERNAL DOMAIN NAME(S) domain.

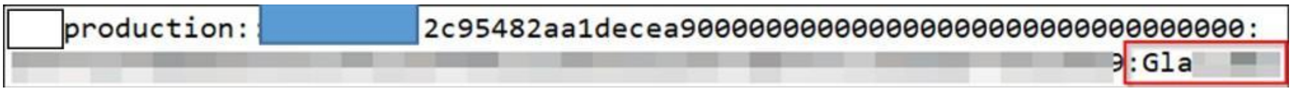
1. TODO LIST HIGH LEVEL STEPS
2. ...

Detailed reproduction steps for this attack chain are as follows: TODO FILL IN DETAILED ATTACK CHAIN STEPS

Evidence



```
02/22/2021 08:24:55 AM - [SMB] NTLMv1-SSP Client   : 10.[redacted]
02/22/2021 08:24:55 AM - [SMB] NTLMv1-SSP Username : [redacted][redacted]production
02/22/2021 08:24:55 AM - [SMB] NTLMv1-SSP Hash     : [redacted]production::[redacted]:[redacted]
```



```
[redacted]production:[redacted]2c95482aa1decea900000000000000000000000000000000:
[redacted]9:Gla[redacted]
```

4. Default Credentials on Web Services - High

CWE	N/A
CVSS 3.1	8.1 / CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
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.
Affected Systems	Default credentials were tested on a sample set of web applications, but suggests checking the following addresses at a minimum.
Tools Used	Manual Review
Remediation	Change default credentials or disable unused accounts.
References	NIST SP800-53 IA-5(1) - Authenticator Management

Detailed Walkthrough

Heath Adamsperformed the following to fully compromise the TODO INSERT DOMAIN NAME domain.

1. TODO LIST HIGH LEVEL STEPS
2. ...

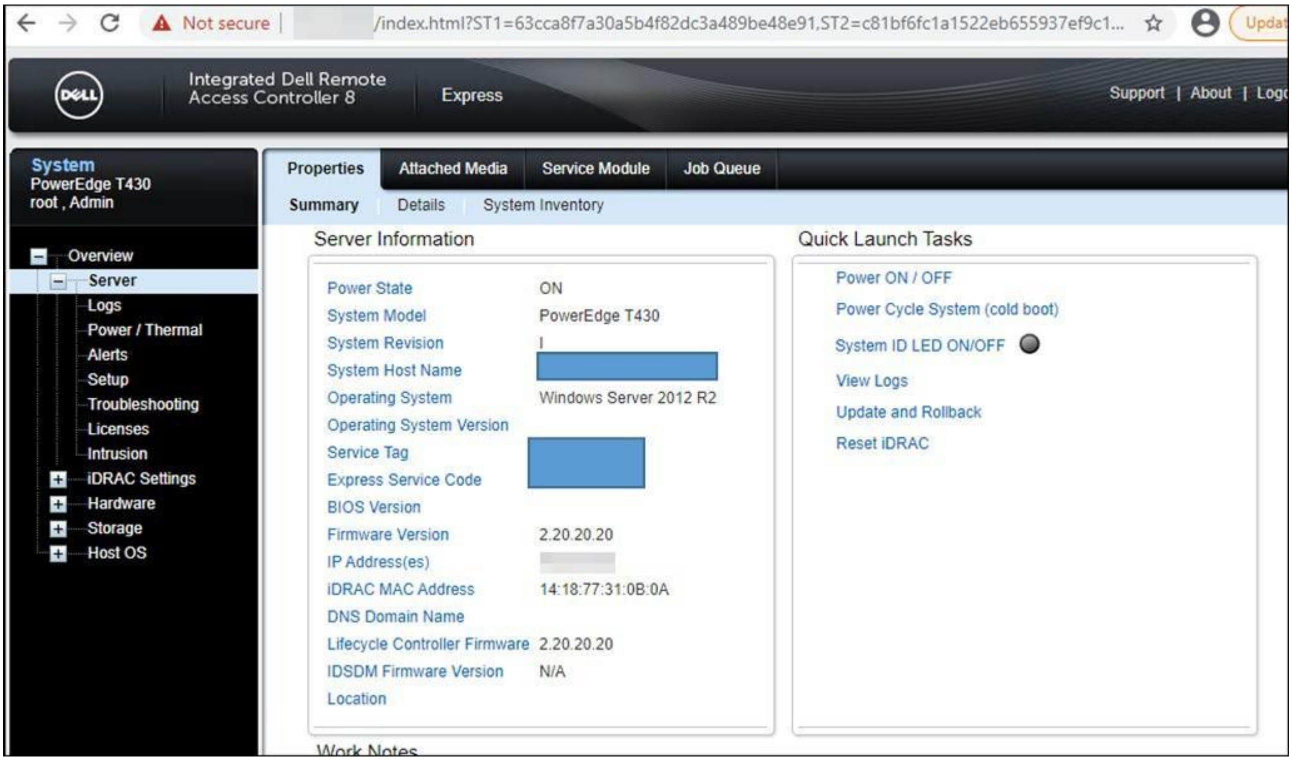
Detailed reproduction steps for this attack chain are as follows: TODO FILL IN DETAILED ATTACK CHAIN STEPS

Heath Adamsthen performed the following to fully compromise the TODO INSERT OTHER INTERNAL DOMAIN NAME(S) domain.

1. TODO LIST HIGH LEVEL STEPS
2. ...

Detailed reproduction steps for this attack chain are as follows: TODO FILL IN DETAILED ATTACK CHAIN STEPS

Evidence



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	[redacted]
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

5. IPMI Hash Disclosure - Medium

CWE	N/A
CVSS 3.1	5.5 / CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L
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.
Affected Systems	Identified 34 machines, please see the below file for listing.
Tools Used	Metasploit
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.
References	https://blog.rapid7.com/2013/07/02/a-penetration-testers-guide-to-ipmi/

Detailed Walkthrough

Heath Adamsperformed the following to fully compromise the TODO INSERT DOMAIN NAME domain.

1. TODO LIST HIGH LEVEL STEPS
2. ...

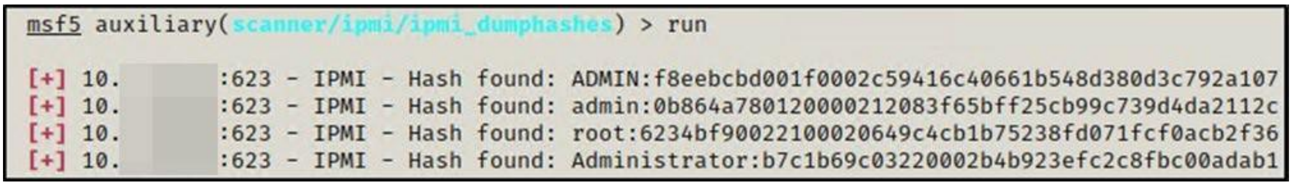
Detailed reproduction steps for this attack chain are as follows: TODO FILL IN DETAILED ATTACK CHAIN STEPS

Heath Adamsthen performed the following to fully compromise the TODO INSERT OTHER INTERNAL DOMAIN NAME(S) domain.

1. TODO LIST HIGH LEVEL STEPS
2. ...

Detailed reproduction steps for this attack chain are as follows: TODO FILL IN DETAILED ATTACK CHAIN STEPS

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
```

6. Sample Low Severity Finding - Low

CWE	N/A
CVSS 3.1	1.8 / CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:N
Description	TODO DESCRIPTION
Risk	**Likelihood**: TODO **Impact**: TODO
Affected Systems	TODO AFFECTED COMPONENT
Tools Used	TODO TOOLS USED
Remediation	TODO REMEDIATION
References	TODO REFERENCES

Detailed Walkthrough

Heath Adamsperformed the following to fully compromise the TODO INSERT DOMAIN NAME domain.

1. TODO LIST HIGH LEVEL STEPS
2. ...

Detailed reproduction steps for this attack chain are as follows: TODO FILL IN DETAILED ATTACK CHAIN STEPS

Heath Adamsthen performed the following to fully compromise the TODO INSERT OTHER INTERNAL DOMAIN NAME(S) domain.

1. TODO LIST HIGH LEVEL STEPS
2. ...

Detailed reproduction steps for this attack chain are as follows: TODO FILL IN DETAILED ATTACK CHAIN STEPS

Evidence

```
ADD COMMAND OUTPUT AS APPROPRIATE
```

TODO ADD SCREENSHOTS AS APPROPRIATE

Screenshot

Figure 4 - Screenshot

Screenshot

Figure 5 - Screenshot

7. Steps to Domain Admin - Info

CWE	-
CVSS 3.1	N/A
Description	The steps below describe how the penetration tester obtained domain administrator access. Each step also provides remediation recommendations to help mitigate risk.
Risk	
Tools Used	-
Remediation	Review action and remediation steps.
References	-

Detailed Walkthrough

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.	
8	TODO ACTION	TODO REMEDIATION

Evidence

12 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