TCM SECURITY

Demo Corportation

Security Assessment Findings Report

Date: April 29, 2025
Project: Democorp-2025-001
Version: 1.0

BUSINESS CONFIDENTIAL

Table of Contents

Confidentiality Statement

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

DemoCorp 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. 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.

Contact Information

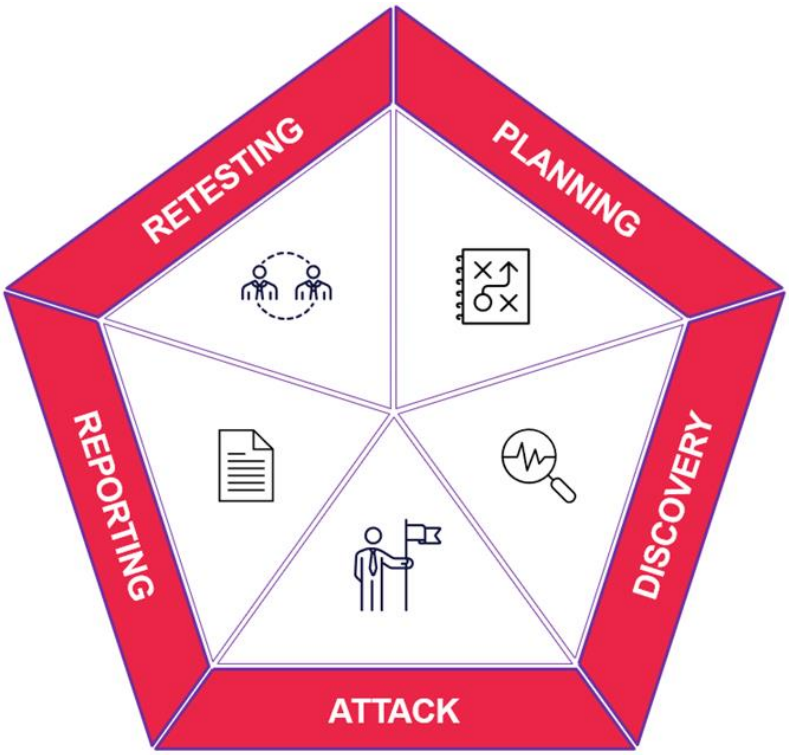
Name	Title	Contact Information
DemoCorp		
Hedy Lamarr	Sr. Manager of Cybersecurity	h.lamarr@democorp.com
TCM Security		
Aaron Wilson	Red Team Lead	awilson@tcm-sec.com

Assessment Overview

From May 9, 2025, to May 20, 2025, DemoCorp engaged TCMS to evaluate the security posture of its infrastructure compared to current industry best practices that included Internal penetration testing. 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*.

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered, and rules of engagement are obtained.
- 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.



Assessment Components

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.

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
Internal Penetration Test	<Scope Details>

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 DemoCorp.

Client Allowances

DemoCorp provided TCMS no allowances.

Executive Summary

TCMS evaluated DemoCorp's security posture through Internal penetration testing from May 9, 2025, to May 20, 2025. The following sections provide a high-level overview of vulnerabilities discovered, successful and unsuccessful attempts, and strengths and weaknesses.

Scoping and Time Limitations

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

Testing was subject to time limitations, internal penetration testing for ten (10) business days. The TCMS team accounted for these constraints when assessing the overall risk and severity of the findings.

Internal Testing Summary

The Internal Penetration Test evaluated the security posture of DemoCorp's internal networks. From an internal perspective TCMS performed vulnerability scanning and testing against the IP addresses provided by DemoCorp. This includes individual vulnerability exploitation, as well as Active Directory and network-level attacks.

The domain is vulnerable to Active Directory Certificate Services (ADCS) exploitation, which allowed trivial compromise of the domain (see IPT-001). Several internal web servers and services use default passwords (see IPT-002). Users and computers can create and delegate computer accounts (IPT-003). Command Prompt restrictions can be bypassed; PowerShell is unrestricted via GPO (see IPT-004). There are Active Directory security misconfigurations (see IPT-005). 4.4% of domain passwords were cracked (see IPT-006). Hashes are disclosed via IPMI (see IPT-007). There are Kerberoastable accounts (see IPT-008). SMB signing is not required on hosts in the network (see IPT-009). Domain usernames can be enumerated from a web application (see IPT-010). There is unpatched software and operating systems (see IPT-011 and IPT-013). There are overly permissive Active Directory user accounts (see IPT-0012). Unencrypted Telnet services are in use (see IPT-014). There are Domain Admin logins to non-privileged systems (see IPT-015). SNMP is deployed with default community string names (see IPT-016).

For further information on findings, please review the Technical Findings section of the report.

Key Strengths and Weaknesses

The following identifies the key strengths identified during the assessment:

- Network restrictions are in place for certain actions (e.g. downloading Kali Linux).
- Network security and monitoring solutions prevented several attacks.

The following identifies the key weaknesses identified during the assessment:

- Active Directory Certificate Services (ADCS) are vulnerable.
- Default credentials were found on web applications.
- Users can create computer accounts.
- There are Active Directory security misconfigurations and overly permissive accounts.

Vulnerability Summary & Report Card

The following tables illustrate the vulnerabilities found by impact and recommended remediations:

Internal Penetration Test Findings

6	5	5	0	0
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Internal Penetration Test		
IPT-001: Domain Misconfiguration – Active Directory Certificate Services	Critical	Inventory and practice least privilege for all certificate templates.
IPT-002: Account Misconfiguration – Default Credentials on Web Services	Critical	Change default credentials or disable unused accounts.
IPT-003: Domain Misconfiguration – Users and Computers Can Create and Delegate Computer Accounts	Critical	Audit the necessity of permitting user and computer accounts to create new computer accounts within the domain.
IPT-004: Security Misconfiguration – Command Prompt and PowerShell Restrictions	Critical	Fully restrict access to the command prompt and PowerShell.
IPT-005: Insufficient Hardening – Active Directory Security Misconfigurations	Critical	Configure Active Directory settings in accordance with best practices.
IPT-006: Insufficient Authentication Controls – Domain Password Policies	Critical	Implement CIS benchmark password requirements or a PAM solution.
IPT-007: Insufficient Hardening – IPMI Hash Disclosure	High	Disable IPMI if not needed or enforce password complexity requirements.
IPT-008: Insufficient Hardening – Kerberoasting	High	Use Group Managed Service Accounts for privileged services.
IPT-009: Insufficient Hardening – SMB Signing Not Required	High	Enable SMB signing on all domain computers.
IPT-010: Security Misconfiguration – Username Enumeration	High	Synchronize error messaging within application responses.
IPT-011: Insufficient Patch Management – Software	High	Update software to the latest stable versions.
IPT-012: Account Misconfiguration – Overly Permissive AD User Accounts	Moderate	Audit the permissions identified and remove or modify should the settings not reflect a need for the organization.

Finding	Severity	Recommendation
IPT-013: Insufficient Patch Management – Operating Systems	Moderate	Update vulnerable operating systems to the latest stable versions.
IPT-014: Insufficient Data in Transit Encryption – Telnet	Moderate	Migrate to TLS supported protocols.
IPT-015: Privilege Management – Domain Admin Logins on Non-Privileged Systems	Moderate	Restrict domain admin access to domain controllers only.
IPT-016: Insufficient SNMP Community String Complexity	Moderate	Disable SNMP if not required.

Technical Findings

Internal Penetration Test Findings

Finding IPT-001: Domain Misconfiguration – Active Directory Certificate Services (Critical)

Description:	The DemoCorp domain is vulnerable to Active Directory Certificate Services exploitation. The following templates were identified as vulnerable and exploited: • AMTClientConfigurationCertificate – ESC1 TCMS recommends verifying the following templates are not able to be exploited: • DemoCorpWebServer • DemoCorpWebServerRequest • AMTProvisioningCertificate
Risk:	**Likelihood:** High – Authenticated accounts in the domain can exploit this attack path. **Impact:** Very High – Exploitation allows an attacker to obtain hashes and access as privileged accounts, such as domain administrators and domain controllers.
System(s):	DemoCorp domain
Tools Used:	Certify; Certipy; PingCastle
References:	Mandiant – ADCS Hardening SpectorOps – Certified Pre-Owned

Evidence

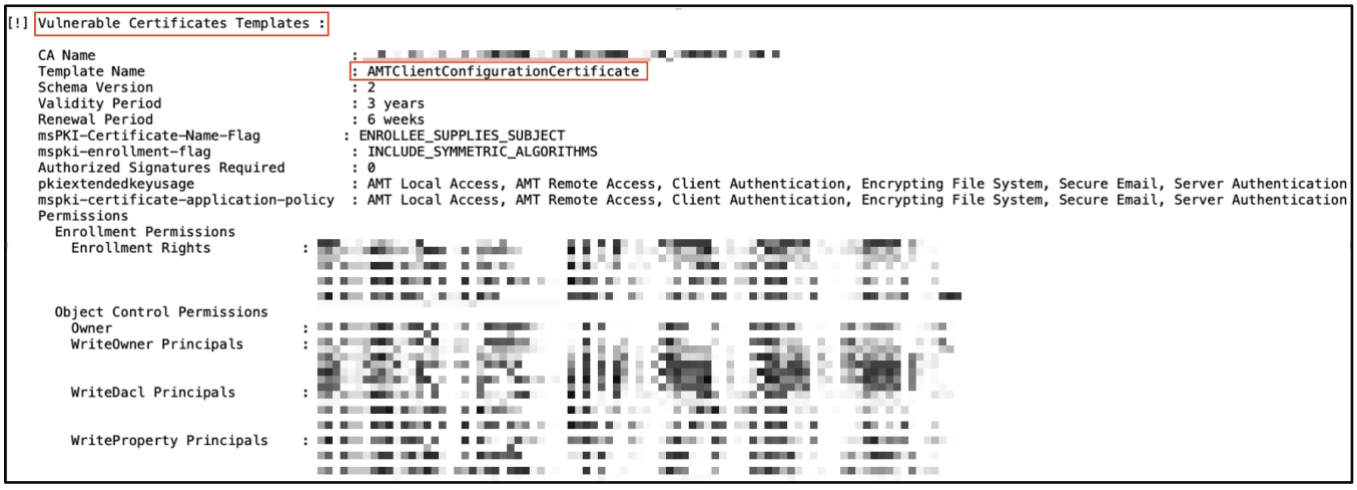


Figure 1 - Vulnerable Certificate Found

Figure 2 - Certificate Issued

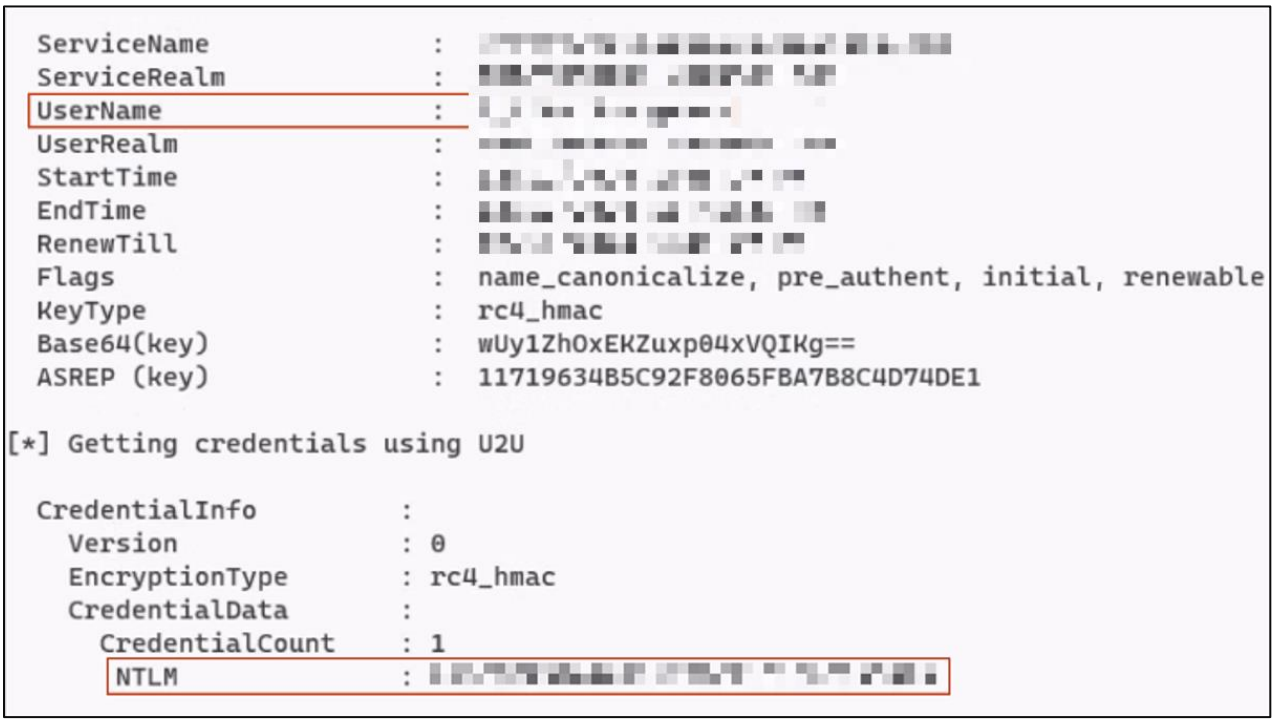


Figure 3 - Retrieving Domain Admin NTLM Hash

Figure 4 - Dumping the Domain Controller with NTLM Hash

Remediation

Regularly inventory and practice least privilege for all certificate templates within the environment. Audit and/or configure the environment for the following settings:

- Disable all templates that are not needed.
- Restrict enrollment permissions to only users or groups required.
- Enforce manual issuance approval where possible.
- Disable “Enrollee Supplies Subject” where possible.
- Restrict “Client Authentication” only where it’s required.
- Setup advance detections for events such as certificate requests, certificate issuance, and Kerberos ticket requests.
- Implement additional monitoring or configurations as required for the environment.

Finding IPT-002: Account Misconfiguration – Default Credentials on Web Services (Critical)

Description:	TCMS validated default credentials on web applications in the DemoCorp environment. TCMS successfully relayed a printer password which was automatically logged into a Guest account to gain an initial foothold during the engagement. This significantly elevated the criticality of the finding, as domain compromise was possible through this account. Note: TCMS may not have been able to identify and verify all default credentials during the engagement. It is recommended that DemoCorp audit all web services for this type of access.
Risk:	**Likelihood:** High – Credentials are published for these devices and are an attacker's first authentication attempt. **Impact:** High – Attackers can control devices, destroy data, or shut down systems.
System(s):	See default_creds.txt in "Additional Scans and Reports"
Tools Used:	Manual Review; EyeWitness
References:	NIST SP800-53r5 IA-5 – Authenticator Management

Evidence

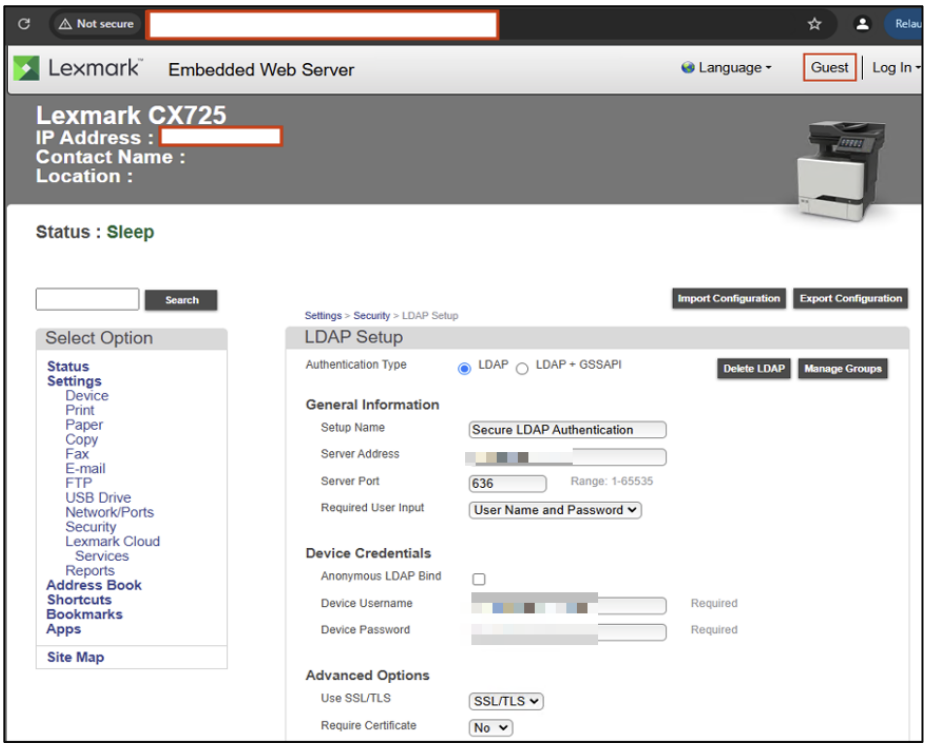


Figure 5 - LDAP Settings Accessible Via Guest Account

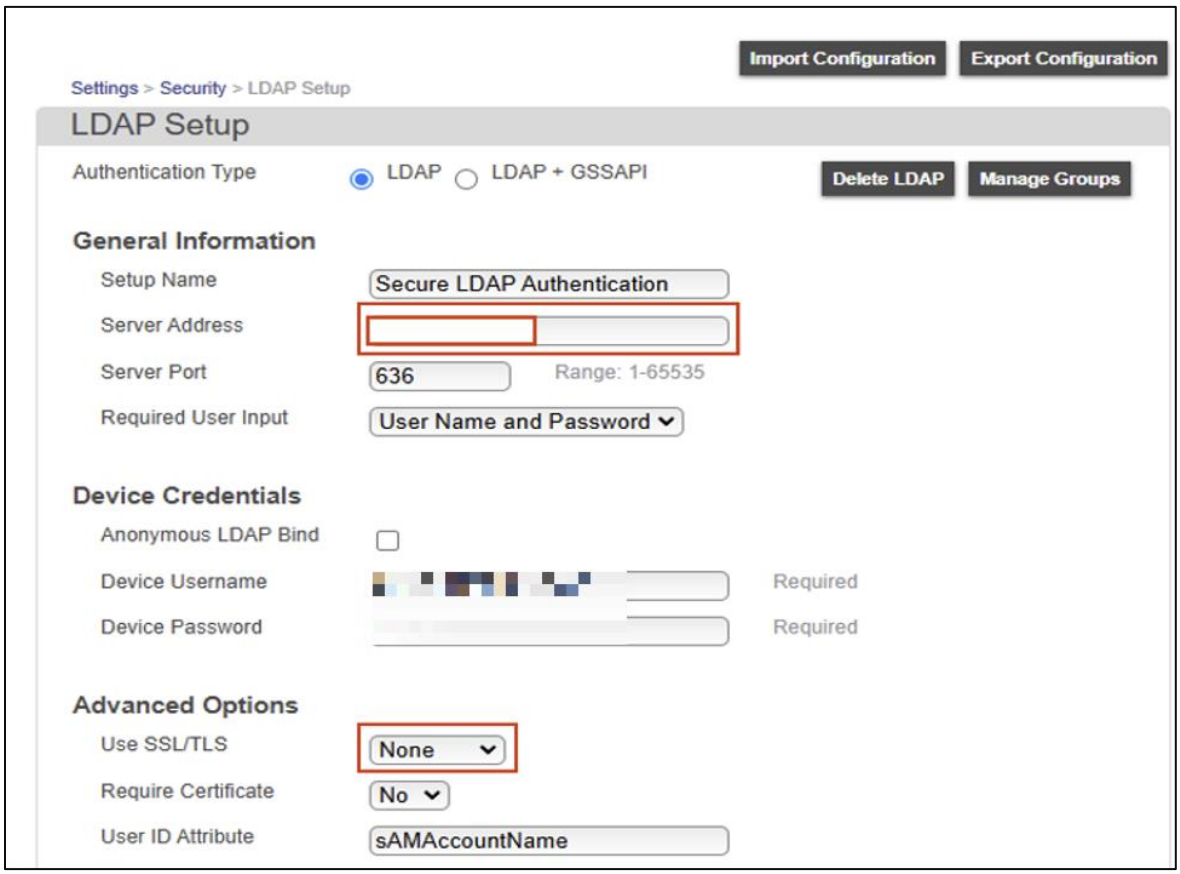


Figure 6 - Modification Allowed Via Guest Access

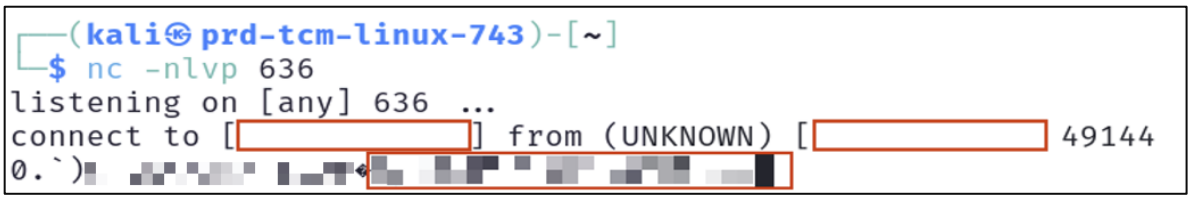


Figure 7 - Cleartext Credentials Received for Domain Account

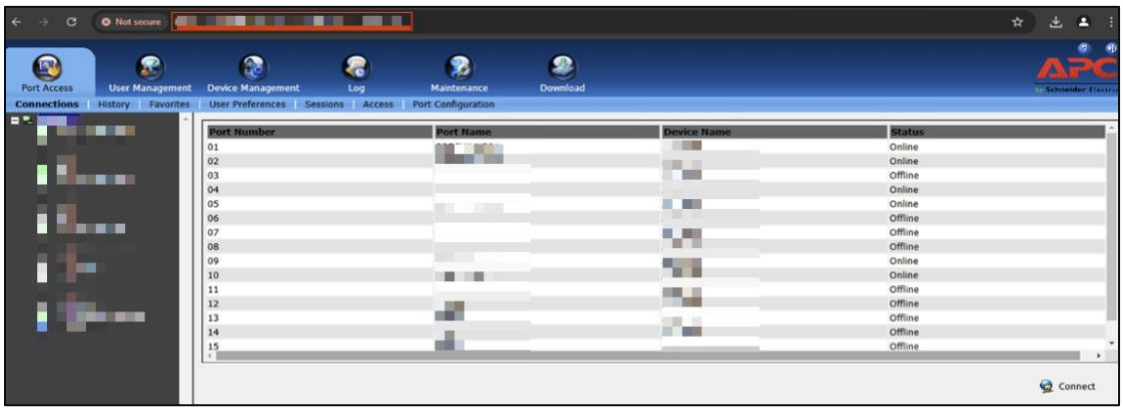


Figure 8 - Access and Control to Schneider Electric Service

Remediation

Change default credentials or disable unused accounts.

Finding IPT-003: Domain Misconfiguration – Users and Computers Can Create and Delegate Computer Accounts (Critical)

Description:	DemoCorp allows user and computer accounts to create computer accounts in the domain, following Microsoft's default policy. Utilizing this, TCMS joined a TCMS-controlled computer to the domain via a compromised user and executed malicious code without restriction or detection.
Risk:	**Likelihood:** Very High – Any attacker with access to the network can execute IPv6 delegation attacks in the network. **Impact:** Very High – Compromised accounts can be used to create new computers with delegation rights, allowing for an attacker to dump account hashes.
System(s):	DemoCorp domain
Tools Used:	PingCastle; PowerSploit; PowerMad
References:	TCM-KB-INT-001

Evidence

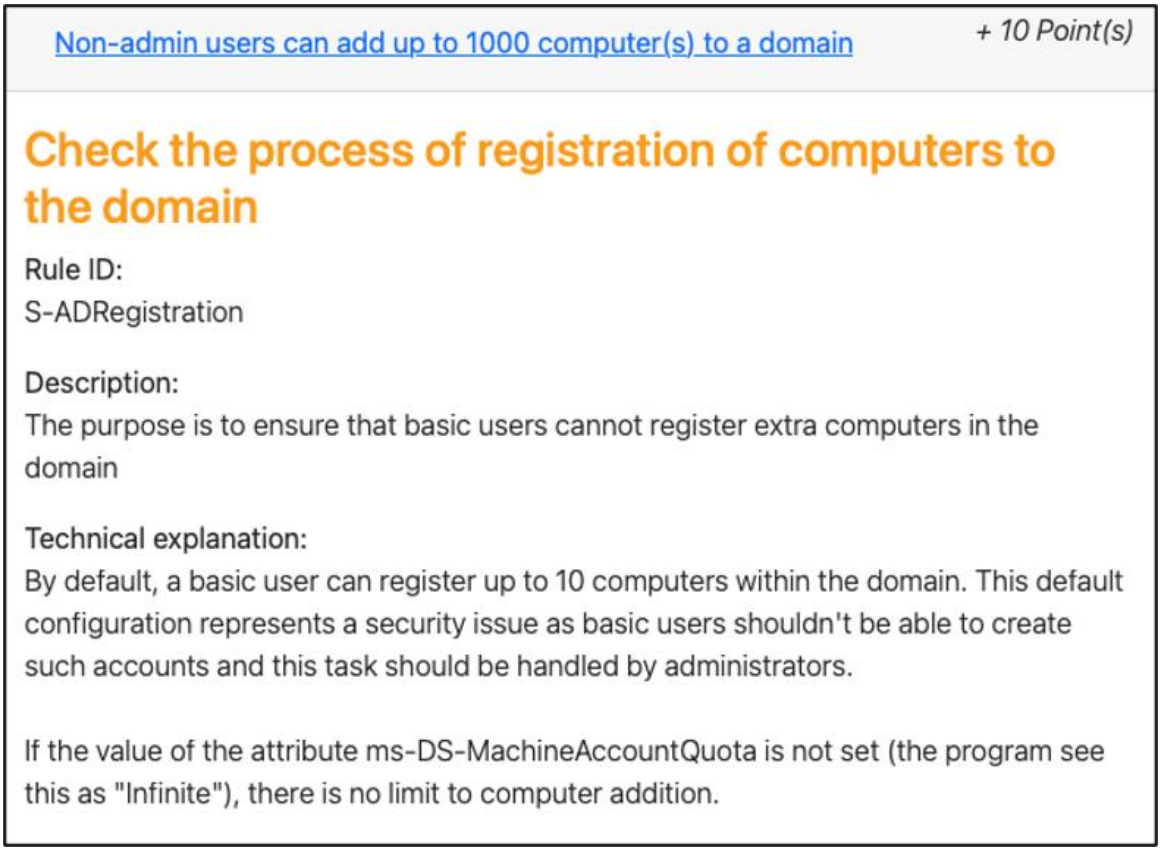


Figure 9 - ms-DS-MachineAccountQuote Discovery

```
PS C:\Users\tcms\Desktop\Tools\Powermad> New-MachineAccount -MachineAccount AngTCM
Enter a password for the new machine account: **********************
[+] Machine account AngTCM added
```

Figure 10 - Account Addition

Remediation

Audit the necessity of permitting user and computer accounts to create new computer accounts within the domain. Set the ms-ds-machineaccountquota attribute to "0" should there be no necessary business need for the configuration.

Note: The following computer and/or user accounts were created from this vulnerability and will need to be removed from the domain:

- AngTCM
- tcms

Finding IPT-004: Security Misconfiguration – Command Prompt and PowerShell Restrictions (Critical)

Description:	DemoCorp has enabled restrictions via domain group policy to prevent users from opening and running Windows Command Prompt. TCMS notes that PowerShell was not restricted via a domain group policy. TCMS bypassed policy restrictions to utilize the command prompt and PowerShell. These bypasses included: • Windows desktop shortcut TCMS was able to utilize Windows Command Prompt and PowerShell on a virtual machine joined to the domain to elevate privileges, increasing the criticality of this finding.
Risk:	**Likelihood:** High – Bypasses used are trivial and were not restricted. **Impact:** High – Users can execute commands and functions that are meant to be restricted.
System(s):	DemoCorp domain
Tools Used:	Windows Desktop Shortcut; PowerShell
References:	TCM-KB-INT-005 – Uses Can Run Command Prompt and PowerShell Terminals

Evidence

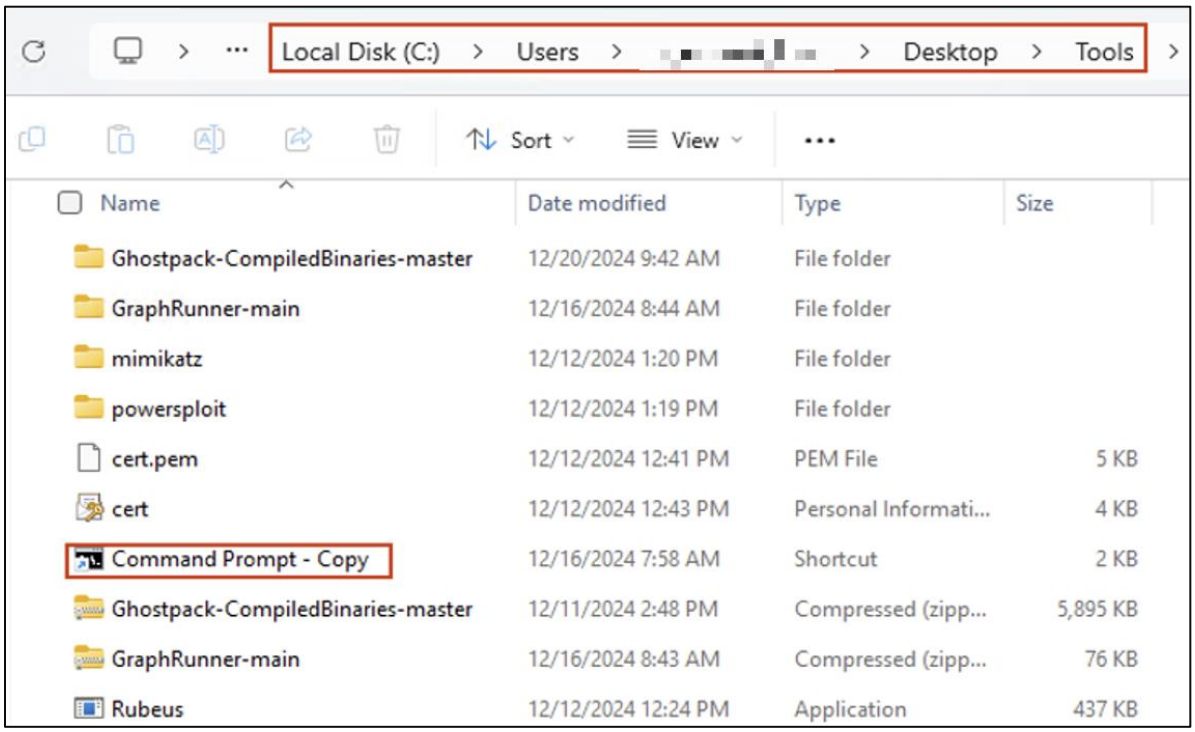


Figure 11 - Command Prompt Shortcut Created

Figure 12 - Command Prompt in Use

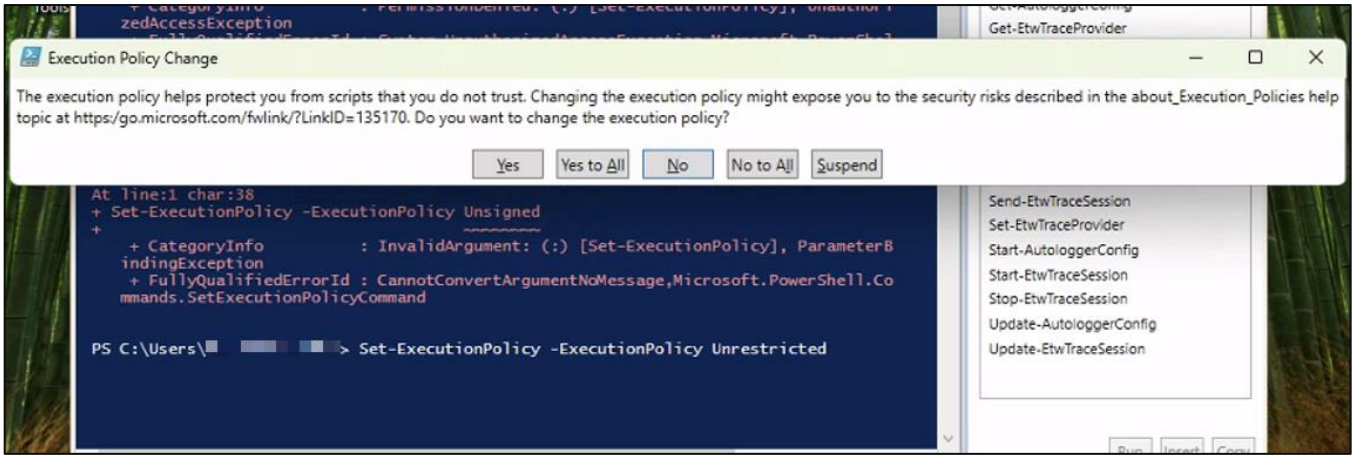


Figure 13 - PowerShell Accessible

Remediation

Fully restrict access to the Command Prompt and PowerShell. Refer to the references section for a step-by-step guide on implementation.

Finding IPT-005: Insufficient Hardening – Active Directory Security Misconfigurations (Critical)

Description:	During testing, the TCMS team ran a script to identify security misconfigurations within DemoCorp's Active Directory environment. The script identified several high-risk configurations settings. Some critical findings include: • Accounts exist which have non-expiring passwords, including domain administrators and other privileged accounts • Unconstrained delegations are configured on the domain • Objects exist that could have an empty password • The Azure AD SSO account password has not been changed since 2019 • Authenticated users can create DNS records See ad_hc_DemoCorp.com.html for more details.
Risk:	**Likelihood:** Moderate – An attacker can discover these vulnerabilities with basic tools but usually requires authentication. **Impact:** Very High – If exploited, privilege access on the domain could be achieved.
System(s):	DemoCorp domain
Tools Used:	PingCastle
References:	NIST SP800-53r5 MA-6 – Timely Maintenance NIST SP800 53r5 SI-2 – Flaw Remediation

Evidence

Group Name	Nb Admins	Nb Enabled	Nb Disabled	Nb Inactive	Nb PWd never expire
Account Operators	0	0	0	0	0
Administrators	12	11	1	1	5
Backup Operators	2	2	0	0	2
Certificate Operators	0	0	0	0	0
Certificate Publishers	0	0	0	0	0
Dns Admins	1	1	0	0	0
Domain Administrators	7	6	1	0	1
Enterprise Administrators	1	1	0	0	0
Enterprise Key Administrators	1	1	0	0	0
Key Administrators	0	0	0	0	0

Figure 14 - Privileged Accounts Where the Password Does Not Expire

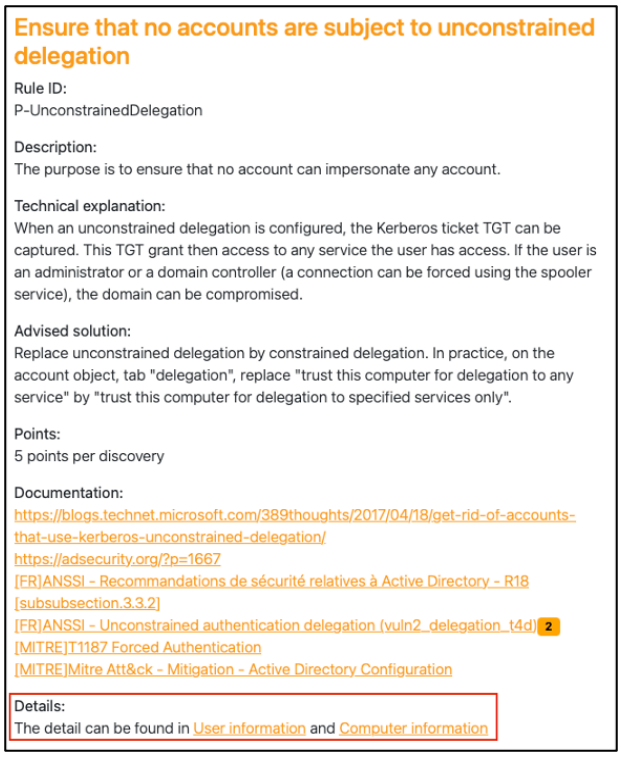


Figure 15 - Unconstrained Delegations

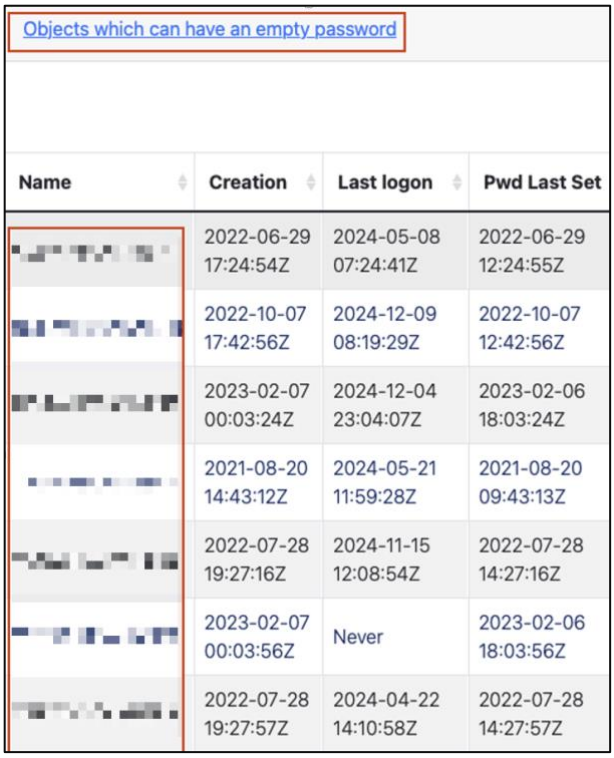


Figure 16 - Objects Which Could Have an Empty Password

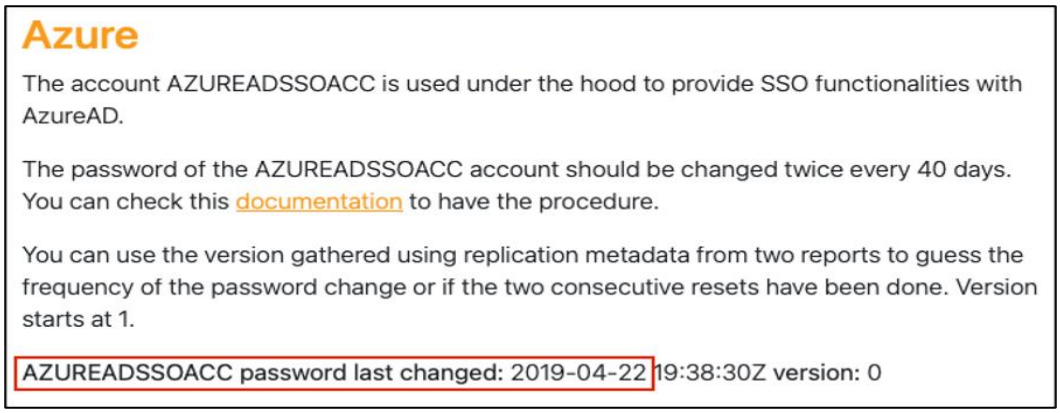


Figure 17 - AZUREADSSOACC Password Age

Remediation

Configure Active Directory settings in accordance with best practices.

Finding IPT-006: Insufficient Authentication Controls – Domain Password Policies (Critical)

Description:	TCMS obtained password hashes from the DemoCorp domain and conducted dictionary and brute force attacks against the identified users. TCMS notes the domain password policy is fourteen (14) characters with complexity. TCMS cracked 1,500 passwords out of 5,000 unique accounts with commodity cracking tools which equates to a 30% crack rate.
Risk:	**Likelihood:** High – Simple passwords are susceptible to password cracking attacks. Encryption provides some protection, but dictionary attacks based on common word lists often crack weak passwords. **Impact:** Very High – Accounts with weak passwords could lead to an adversary critically impacting DemoCorp's ability to operate.
System(s):	DemoCorp domain
Tools Used:	Hashcat; DPAT
References:	NIST SP800-53r5 IA-5 – Authenticator Management https://www.cisecurity.org/white-papers/cis-password-policy-guide/

Evidence

Count	Description	More Info
	Password Hashes	Details
	Unique Password Hashes	
	Passwords Discovered Through Cracking	
	Unique Passwords Discovered Through Cracking	
	Percent of Current Passwords Cracked	Details
	Percent of Unique Passwords Cracked	Details
	LM Hashes (Non-blank)	
	Unique LM Hashes (Non-blank)	
	Passwords Only Cracked via LM Hash	Details
	Unique LM Hashes Cracked Where NT Hash was Not Cracked	
	Password Length Stats	Details
	Top Password Use Stats	Details
	Password Reuse Stats	Details
	Password History	Details

Figure 18 - Password Cracking Statistics

Remediation

Enable complexity in the domain password policy. Implement CIS benchmark password requirements or a PAM solution. A copy of the cracked passwords (DPAT Report) can be found in the "Additional scans and files" folder for further insights.

Finding IPT-007: Insufficient Hardening – IPMI Hash Disclosure (High)

Description:	DemoCorp 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. Hashes were cracked for XClarity Controller, allowing TCMS access to those platforms.
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(s):	See IPMI_hashes.txt in "Additional Scans and Reports"
Tools Used:	Metasploit; Hashcat
References:	Rapid 7 – A Penetration Tester's Guide to IPMI

Evidence

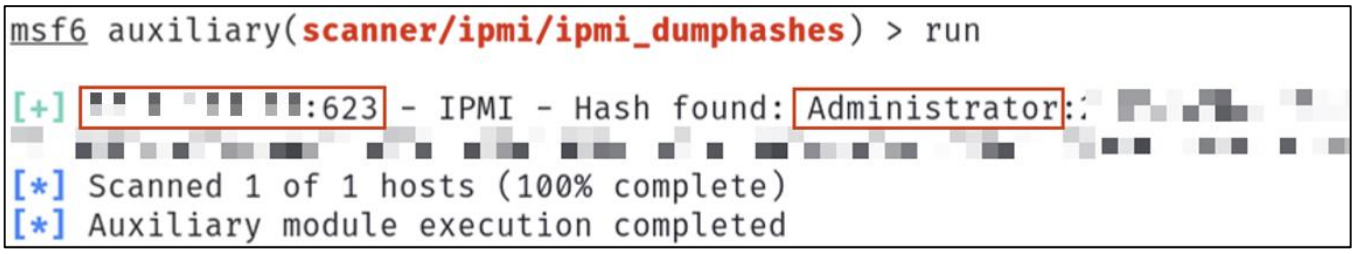


Figure 19 - Administrator Hash Dumped

Figure 20 - Hashes Which Cracked Automatically via Metasploit

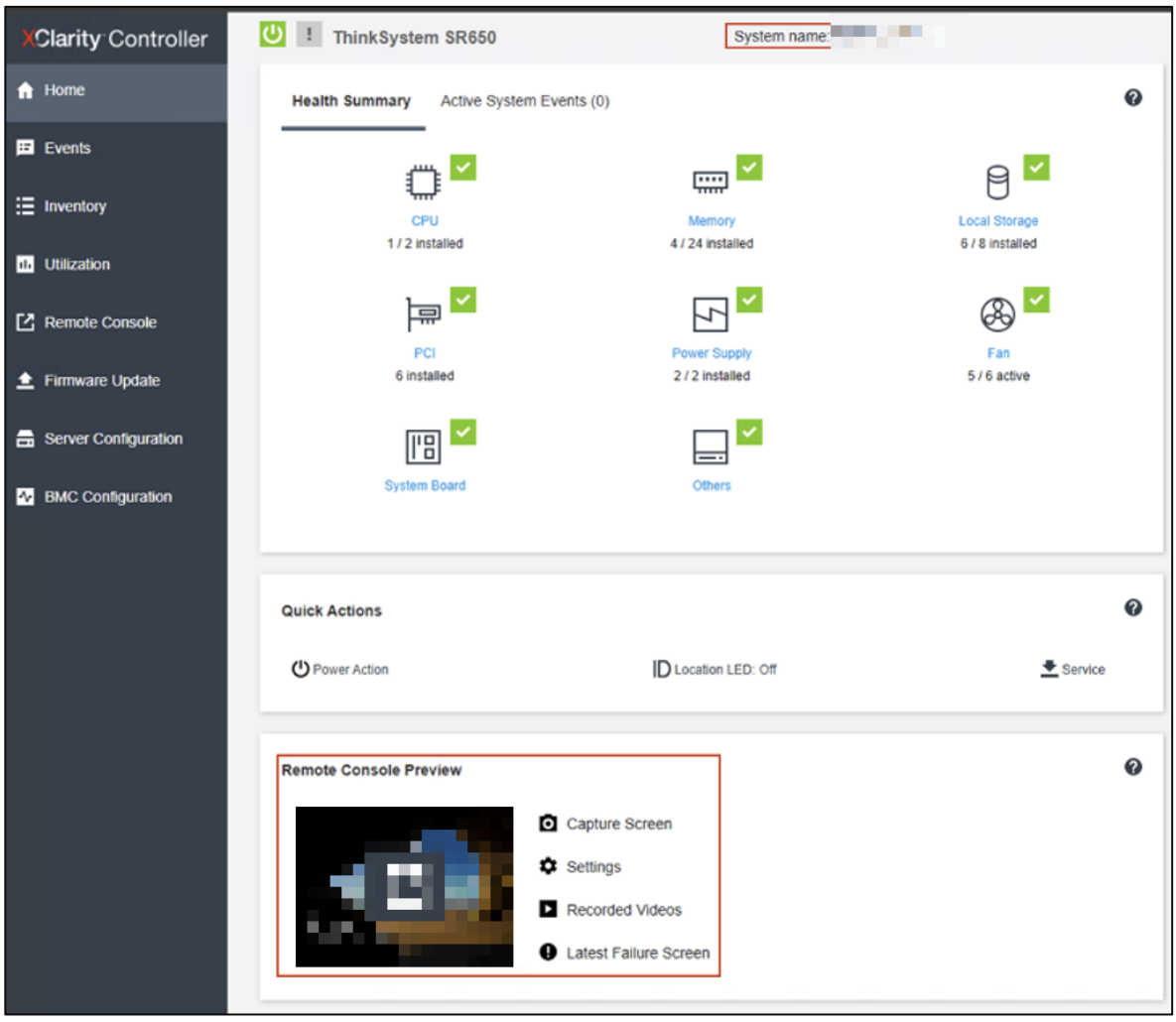


Figure 21 - Access and Enumeration Possible Via XClarity Controller

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-008: Insufficient Hardening – Kerberoasting (High)

Description:	TCMS retrieved all user service principal names (SPNs) from the DemoCorp domain controller using a domain user-level account in a Kerberoasting attack. Retrieving these user SPNs permitted TCMS the ability to crack account hashes offline. Note: TCMS was unable to crack any of the accounts during the testing period, reducing the criticality of the finding.
Risk:	**Likelihood:** High – Any account joined to the domain can request user SPN's. **Impact:** Very High – Using SPNs, it is possible to retrieve domain administrators' password hashes and crack them offline.
System(s):	DemoCorp domain
Tools Used:	Rubeus; Hashcat
References:	NIST SP800-53r5 IA-5 – Authenticator Management

Evidence

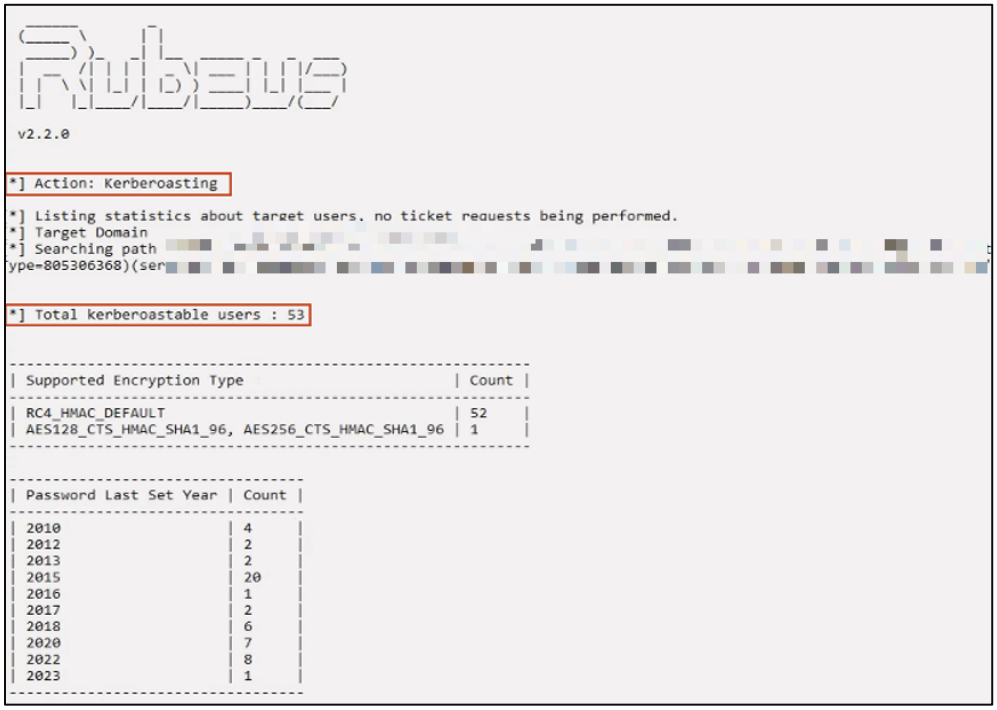


Figure 22 - Kerberoasting With Rubeus

Remediation

Use Group Managed Service Accounts for privileged services.

Finding IPT-009: Insufficient Hardening – SMB Signing Not Required (High)

Description:	DemoCorp 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(s):	<REDACTED>
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

```
┌──(kali㉿prd-tcm-linux-743)-[~]
└─$ nmap -A -Pn -p 445 [redacted]
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-20 14:37 EST
Nmap scan report for [redacted]
Host is up (0.0024s latency).

PORT    STATE SERVICE       VERSION
445/tcp open  microsoft-ds?

Host script results:
|_clock-skew: -17s
| smb2-time:
|   date: 2024-12-20T19:37:31
|_  start_date: 2024-08-21T16:06:21
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.80 seconds
```

Figure 23 – SMB Signing Enabled but Not Required

Remediation

Enable SMB signing on all DemoCorp 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-010: Security Misconfiguration – Username Enumeration (High)

Description:	A discrepancy between responses is present in the DemoCorp Aspect web application. Domain usernames can be enumerated via the application.
Risk:	**Likelihood:** High – This application is Internet accessible and in production. Attackers often look for discrepancies in responses to expand attack surfaces. **Impact:** Moderate – Discrepancies in response messages provides attackers with a mechanism for identifying valid information in the application.
System(s):	<REDACTED>
Tools Used:	Manual Review
References:	CWE-204: Observable Response Discrepancy OWASP A05:2021 - Security Misconfiguration

Evidence

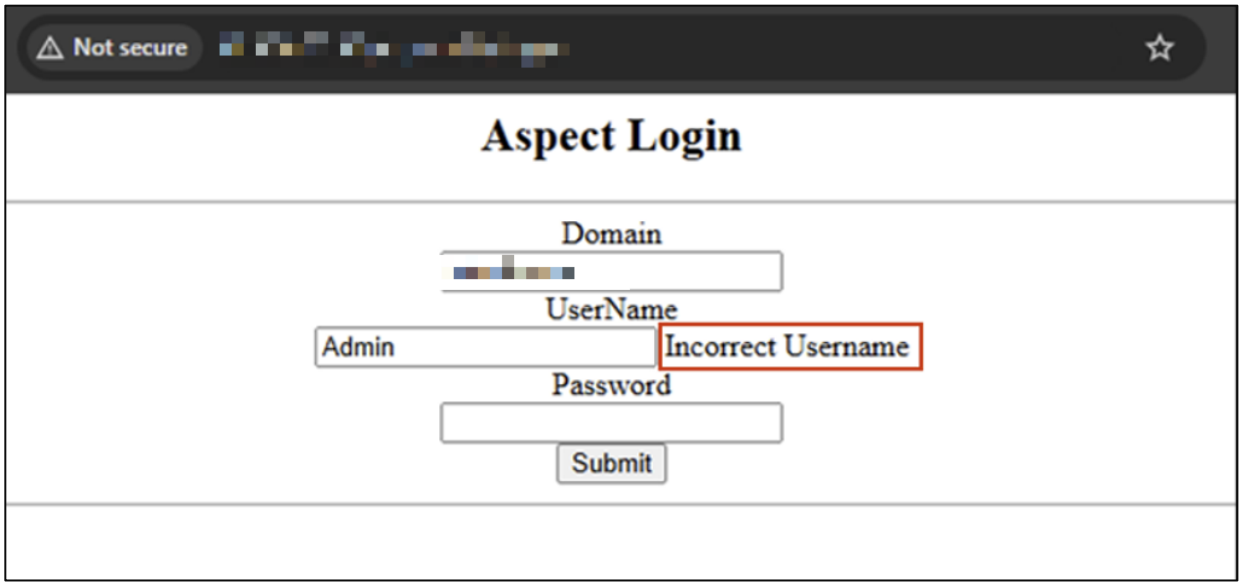


Figure 24 - Username Does Not Exist

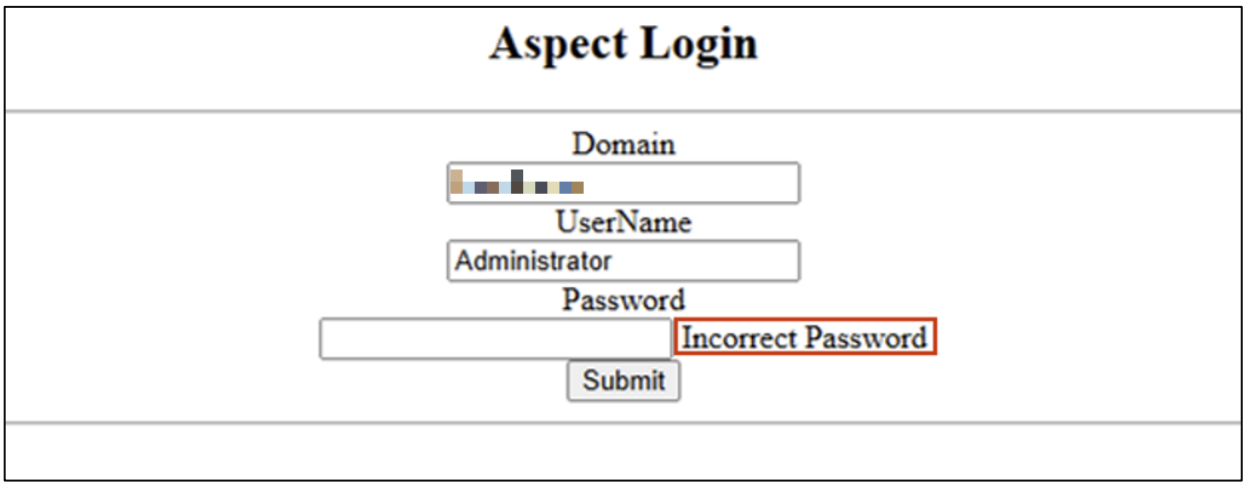


Figure 25 - Username Exists but Password Incorrect

Figure 26 - Domain Account Not Registered in Aspect

Remediation

Utilize synchronized error messaging.

Finding IPT-011: Insufficient Patch Management – Software (High)

Description:	DemoCorp deploys deprecated software in the network. This software includes the following software versions and/or vulnerabilities: • Microsoft SQL Server • Treck TCP/IP • VMware vCenter Server • Apache Struts • SSH • Dell EMC iDRAC9 • iLO 4 • Citrix ADC and Citrix NetScaler Gateway • Microsoft DirectAccess Note: The criticality of this finding was increased as multiple CVEs exist for several softwares in the environment. TCMS was not able to verify all vulnerable services within the testing window. It is recommended that DemoCorp review and audit software regularly to determine vulnerability. See the Nessus scans in "Additional Scans and Reports" as well as outdated_software.txt for more information.
Risk:	**Likelihood**: High – Attackers frequently target vulnerable software, especially when it no longer receives support and may have unpatched vulnerabilities. **Impact:** High – Should attackers gain access to vulnerable software; they can exploit these vulnerabilities to conduct further enumeration within the network and potentially achieve privilege escalation. This can lead to unauthorized access to sensitive data, system compromise, and further exploitation of the network's resources.
System(s):	See outdated_software.txt in "Additional Scans and Reports"
Tools Used:	Nessus; EyeWitness
References:	NIST SP800-53r5 MA-6 – Timely Maintenance NIST SP800 53r5 SI-2 – Flaw Remediation

Evidence

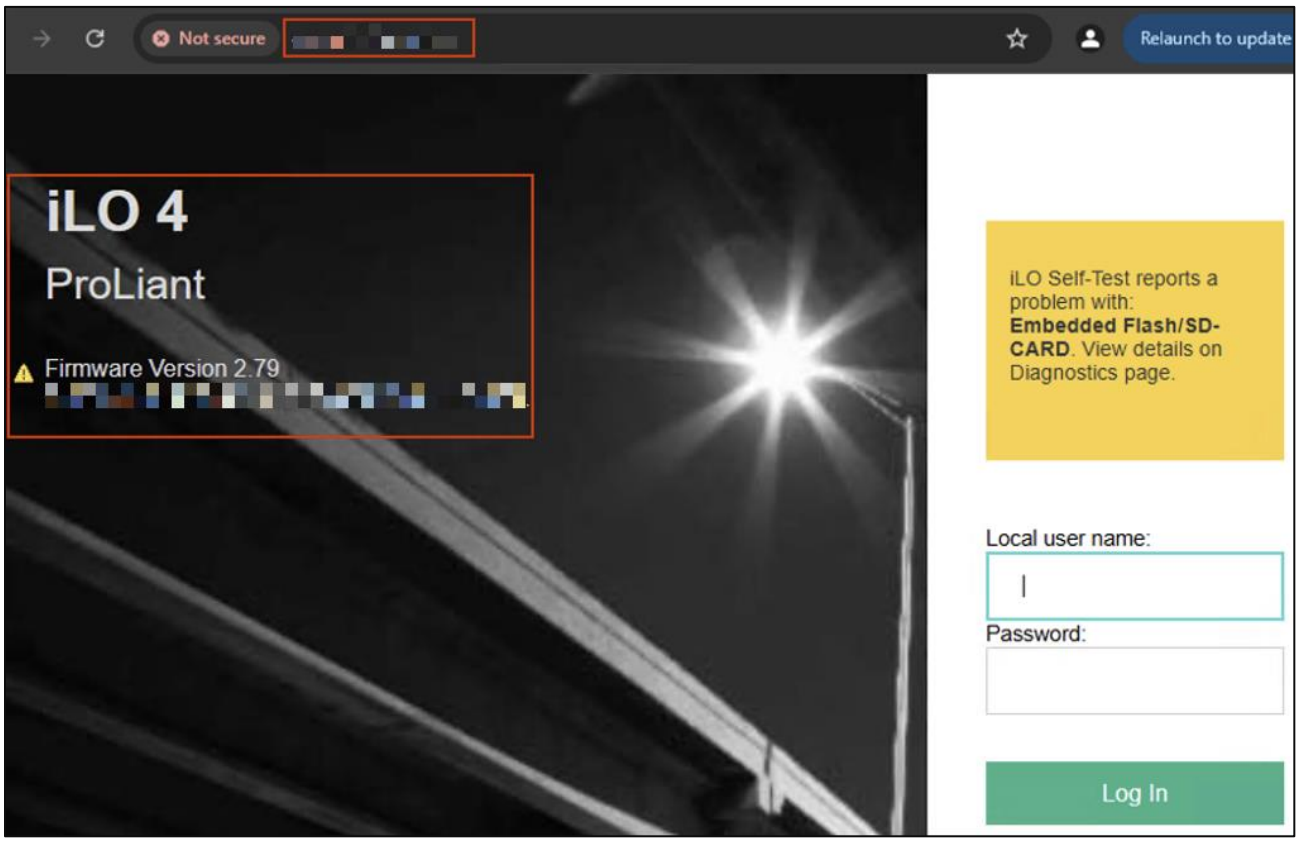


Figure 27 - iLO 4 Found

Figure 28 - Microsoft DirectAccess Found

Remediation

Update to the latest versions of software in accordance with vendor instructions.

Finding IPT-012: Account Misconfiguration – Overly Permissive AD User Accounts (Moderate)

Description:	TCMS identified that the <GROUP-REDACTED1> group has DCSYNC permissions over the domain. Further, as a member of the Administrators group, <GROUP-REDACTED1> has permissions over groups like Domain Admins. As there are members in <GROUP-REDACTED1> not in Domain Admins, it is therefore recommended to audit these group permissions for to ensure there are not overly permissive AD User Accounts. See BloodHound data uploaded in "Additional Scans and Reports" for more information.
Risk:	**Likelihood:** High – An attacker can discover these vulnerabilities with basic tools but usually requires authentication. **Impact:** Very High – If exploited, privilege access on the domain could be achieved.
System(s):	DemoCorp domain
Tools Used:	Bloodhound; Manual Review
References:	NIST SP800-53r5 AC-6(3) – Least Privilege

Evidence

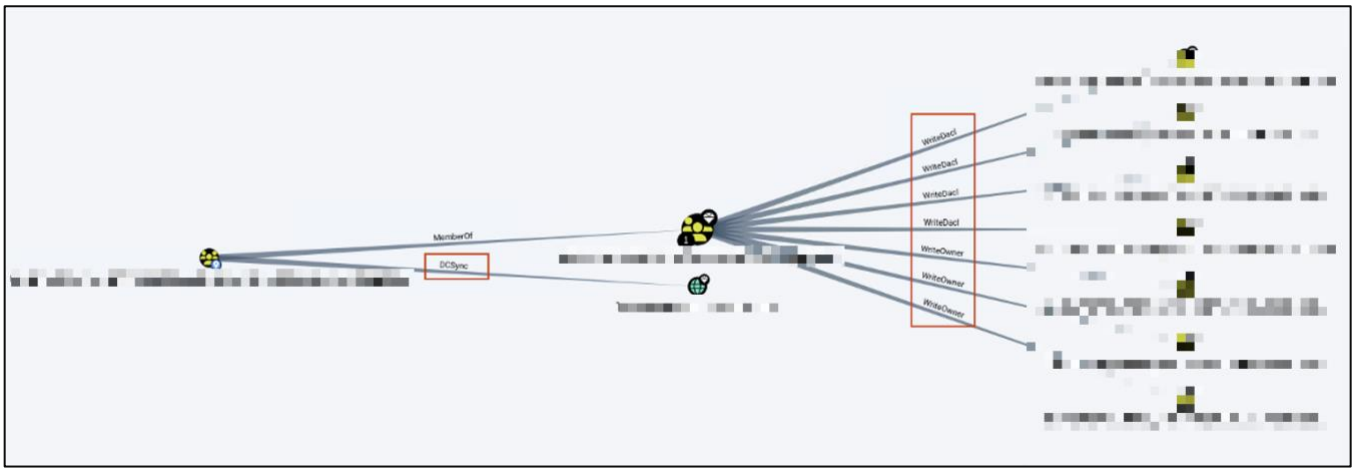


Figure 29 - <GROUP-REDACTED1> Permissions

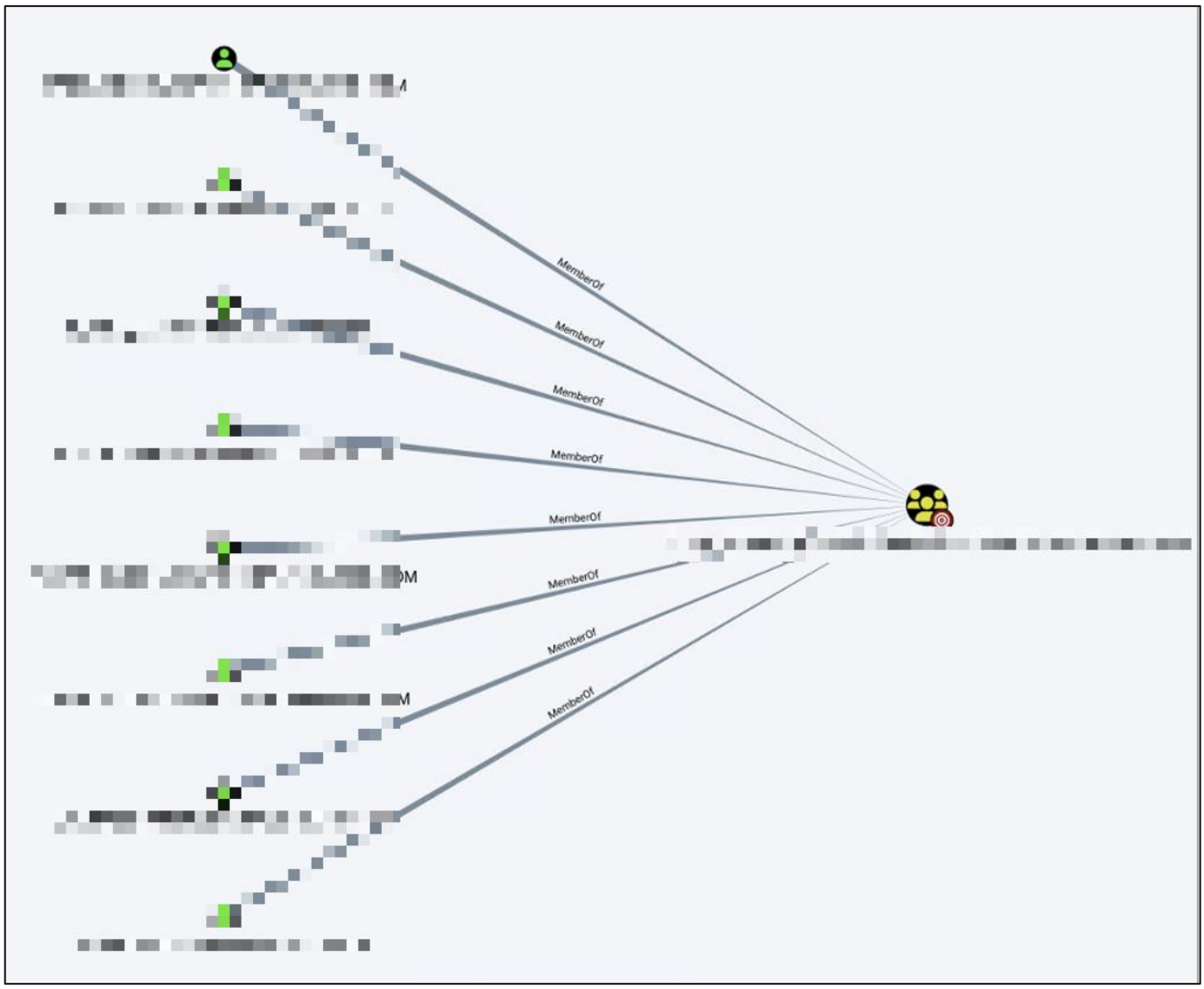


Figure 30 - Members of <GROUP-REDACTED1>

Remediation

Audit the permissions identified and remove or modify should the settings not reflect a need for the organization.

Finding IPT-013: Insufficient Patch Management – Operating Systems (Moderate)

Description:	Operating systems in the DemoCorp network have met end of life support. These operating systems include: • Windows Server 2008 R2 • Windows Server 2012 R2 • Windows 8.1 • Versions of Windows 10 (20H2, 21H2, 1909, etc) Note: TCMS was potentially not able to verify all end-of-life systems within the testing window. It is recommended that DemoCorp audit operating systems across the environment to determine if they are vulnerable.
Risk:	**Likelihood:** High – Attackers target these operating systems as they no longer receive support and may have vulnerabilities that are no longer serviced. **Impact:** Very High – Attackers who gain access to these operating systems can use them for lateral movement in the domain, or to dump hashes and credentials.
System(s):	See PingCastle and BloodHound reports in "Additional Scans and Reports"
Tools Used:	Nessus; PingCastle; BloodHound
References:	NIST SP800-53r5 MA-6 – Timely Maintenance NIST SP800 53r5 SI-2 – Flaw Remediation

Evidence

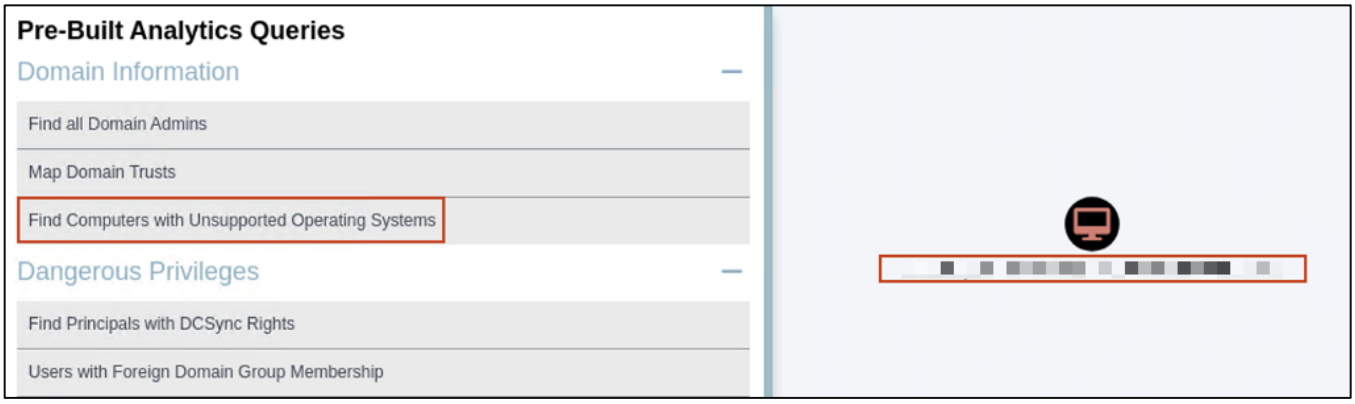


Figure 31 - Find Computers with Unsupported Operating Systems

Remediation

Update to the latest versions of Linux and Windows operating systems. Refer to the text document in the System section above for system identification.

Finding IPT-014: Insufficient Data in Transit Encryption – Telnet (Moderate)

Description:	DemoCorp deploys Telnet servers, which do not encrypt data in transit. Telnet uses plaintext authentication and passes all data, including passwords, in clear text which can be intercepted by an attacker.
Risk:	**Likelihood:** Moderate – 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(s):	<REDACTED>
Tools Used:	Telnet
References:	NIST SP800-53r5 AC-17(2) – Remote Access Protection of Confidentiality/Integrity using Encryption

Evidence

Figure 32 - Command Line Telnet Access with Default Credentials

Remediation

Migrate to TLS protected protocols.

Finding IPT-015: Privilege Management – Domain Admin Logins on Non-Privileged Systems (Moderate)

Description:	TCMS identified instances where domain admin accounts were logged into non-domain controllers, exposing administrative credentials. This misuse signifies improper handling of high-privilege accounts on non-standard systems, posing substantial security risks. Note: Criticality of this finding was reduced as network security solutions prevented TCMS from capturing credentials from these devices.
Risk:	**Likelihood:** High – Domain admin accounts are often targeted by attackers, and their use on non-domain controllers increases the chance of compromise. **Impact:** Very High – If a domain admin account is compromised on a non-domain controller, it could lead to full domain compromise, unauthorized access to sensitive data, and significant disruption of services.
System(s):	DemoCorp domain
Tools Used:	Bloodhound; PingCastle
References:	NIST SP800-53r5 AC-6(3) – Least Privilege Securing Domain Admins Groups in Active Directory

Evidence

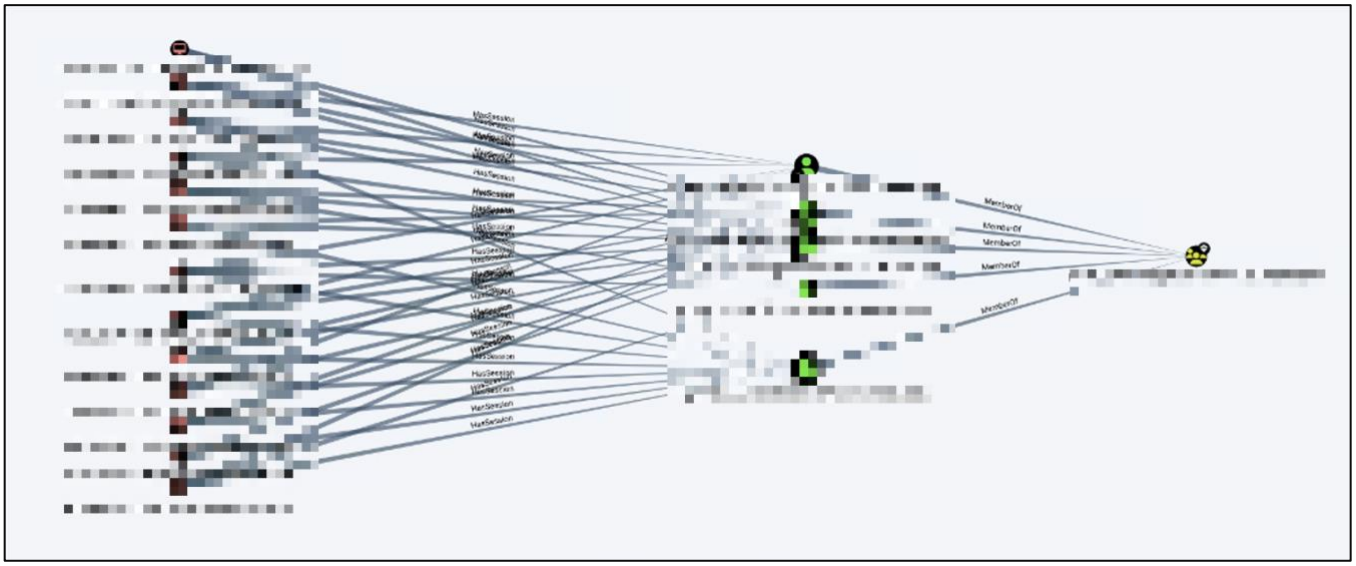


Figure 33 - Domain Admin Logins to Non-Privileged Systems

Remediation

Restrict domain admin access to domain controllers only.

Finding IPT-016: Insufficient SNMP Community String Complexity (Moderate)

Description:	DemoCorp deployed SNMP with default community string names. This configuration exposes read-only access to system management information base (MIB), including 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(s):	<REDACTED>
Tools Used:	SNMPWalk
References:	NIST SP800-53r5 AC-17(2) – Remote Access Protection of Confidentiality/Integrity using Encryption

Evidence

```
┌──(kali㉿prd-tcm-linux-743)-[~]
└─$ snmpwalk -v2c -c public [redacted]
iso.3.6.1.2.1.1.1.0 = STRING: "Source Technologies ST9717 version NF6.TL.N632 kernel 3.0.0 All-N-1"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.641.1.71107110
iso.3.6.1.2.1.1.3.0 = Timeticks: (387219846) 44 days, 19:36:38.46
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = [redacted]
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 72
iso.3.6.1.2.1.1.8.0 = Timeticks: (41) 0:00:00.41
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.2.1.31
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.2.1.4
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.2.1.49
iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.2.1.50
iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.6.3.1
iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.6.3.10.3.1.1
iso.3.6.1.2.1.1.9.1.2.7 = OID: iso.3.6.1.6.3.11.3.1.1
iso.3.6.1.2.1.1.9.1.2.8 = OID: iso.3.6.1.6.3.15.2.1.1
iso.3.6.1.2.1.1.9.1.2.9 = OID: iso.3.6.1.6.3.16.2.2.1
iso.3.6.1.2.1.1.9.1.3.1 = STRING: "The MIB module to describe generic objects for network interface sub-layers"
iso.3.6.1.2.1.1.9.1.3.2 = STRING: "The MIB module for managing IP and ICMP implementations"
```

Figure 34 - SNMP Public String

Remediation

TCMS recommends the following corrective actions:

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

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