Marvel Corp

Security Assessment Findings Report

May 26– May 30, 2025

Training Lab/Report Example

Table of Contents

Portfolio Statement

This report documents a penetration test conducted against a personally owned Active Directory lab created for cybersecurity training and penetration testing practice.

Marvel Corp is a fictional organization created solely for the lab environment. No production systems, customer environments, or third-party infrastructure were tested during this assessment.

This report was originally created in May 2025 while preparing for TCM Security's Practical Junior Penetration Tester (PJPT) certification. It has been sanitized for public release and is being published as a portfolio example of penetration testing and technical reporting.

Disclaimer

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

Time-limited engagements do not allow for a complete evaluation of all security controls. Testing was prioritized to identify weaknesses that could reasonably be leveraged by an attacker and to demonstrate their potential impact.

The findings contained in this report are specific to the intentionally vulnerable training environment assessed at the time of testing.

Contact Information

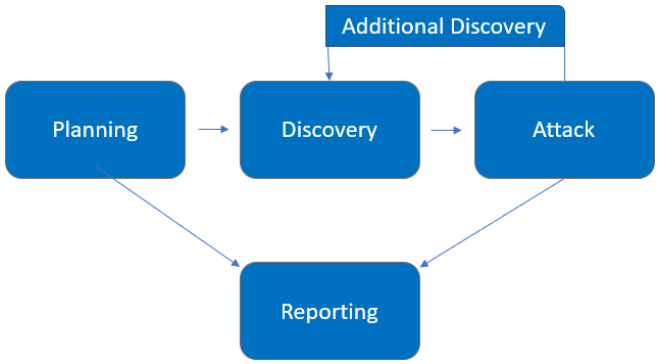
Name	Title	Contact Information
Marvel Corp		
MidwestSec		
Zach Davis	Junior Penetration Tester	

Assessment Overview

From May 26, 2025, to May 30, 2025, MDWS conducted a simulated internal penetration test against the Marvel Corp Active Directory lab to evaluate its security posture against common attack techniques and industry security practices. 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 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 tester 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	10.x.x.x/24

Scope Exclusions

Per client request, MDWS 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 Marvel Corp.

Client Allowances

Marvel Corp provided MDWS the following allowances:

- Direct access to the internal network
- Credentials to a low-level account

Executive Summary

MDWS evaluated Marvel's internal security posture through penetration testing from May 26, 2025, to May 30, 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.

Time limitations were in place for testing. Internal network penetration testing was permitted for five (5) business days.

Testing Summary

MDWS performed an internal assessment of Marvel Corp's internal network security posture. From an internal perspective, this was done via the assumption of a compromised internal user. A device provided by MDWS was allowed direct access to the internal network.

From a testing standpoint, several common Active Directory attacks were attempted and successful against Marvel Corps' network. This included Link-Local Multicast Name Resolution (LLMNR) Poisoning, SMB relaying, IPv6 man-in-the-middle-relaying, and Kerberoasting. These were tested to gain a complete picture of the network's security posture.

The MDWS team discovered that LLMNR was enabled in the network (Finding IPT-001), 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 IPT-004).

Ultimately, the MDWS team was able to leverage account passwords captured through hash dumps to move laterally through the network. This allowed for MDWS to capture and crack the hash of a user whose account was a domain administrator (IPT-003). From there, the domain was fully compromised. MDWS created their own domain administrator account for persistence.

Once fully compromised, continued testing was done to see what other weaknesses existed. These weaknesses included the ability for users to be impersonated through delegation attacks (Finding IPT-003), SMB relay attacks were possible due to SMB signing being disabled (Finding IPT-006), and IPv6 traffic was not restricted, which could lead to LDAPS relaying and domain compromise (Finding IPT-005), and plaintext passwords stored in active directory objects (Finding IPT-009). For a full breakdown of the entire attack chain, see IPT-012.

Tester Notes and Recommendations

Testing results of the Marvel 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, one constant stood out: a weak password policy. 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 60% of the password hashes through basic dictionary attacks.

We recommended that Marvel 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 Marvel 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.

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

Key Strengths and Weaknesses

The following identifies the key strengths identified during the assessment:

1. All systems were up to date running Windows 10 and Server 2022.
2. Some attacks were caught by the Marvel Security Operations Center (SOC).

The following identifies the key weaknesses identified during the assessment:

1. Password policy found to be insufficient
2. LLMNR is enabled within the network
3. SMB signing is disabled on all non-server devices in the work
4. IPv6 is improperly managed within the network
5. User accounts can be impersonated through token delegation
6. Service accounts utilized weak passwords
7. Domain administrator utilized weak passwords

Vulnerability Summary and Report Card - Internal

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

9	1	0	0	2
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Internal Penetration Test		
IPT-001: Insufficient LLMNR Configuration	Critical	Disable multicast name resolution via GPO.
IPT-002: Security Misconfiguration – Local Admin Password Reuse	Critical	Utilize unique local admin passwords and limit local admin users via least privilege.
IPT-003: Insufficient Hardening – Token Impersonation	Critical	Restrict token delegation.
IPT-004: Insufficient Password Complexity	Critical	Implement CIS Benchmark password requirements / PAM solution.
IPT-005: Security Misconfiguration – IPv6	Critical	Restrict DHCPv6 traffic and incoming router advertisements in Windows Firewall via GPO.
IPT-006: Insufficient Hardening – SMB Signing Disabled	Critical	Enable SMB signing on all Marvel Corp domain computers.
IPT-007: Security Misconfiguration – AV Deactivated	Critical	Ensure that AV is activated.
IPT-008: Insufficient Hardening – Golden Ticket Attack	Critical	Regularly rotate the KRBTGT account password and monitor for abnormal Kerberos ticket usage
IPT-009: Insufficient Privileged Account Management – Plaintext Password	Critical	Remove and audit accounts for similar misconfigurations
IPT-010: Insufficient Privileged Account Management – Kerberoasting	High	Use Group Managed Service Accounts (GMSA) for privileged services.
IPT-011: Proof of Domain Compromise	Informational	
IPT-012: Path to Domain Admin	Informational	Review action and remediation steps.

Technical Findings

Internal Penetration Test Findings

Finding IPT-001: Insufficient LLMNR Configuration (Critical)

Description:	Marvel Corp allows multicast name resolution on their end-user networks. MDWS captured 5 user account hashes by poisoning LLMNR traffic. MDWS cracked 2 hashes with commodity cracking software. Marvel Corp was able to relay the hash from the original machine to other machines on the network, gaining access to the password hashes on those machines.
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.
System:	All
Tools Used:	Responder, Hashcat
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

Evidence

Remediation

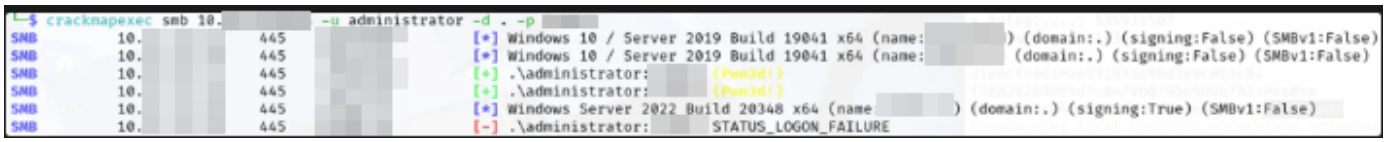
Disable multicast name resolution via GPO. For full mitigation and detection guidance, please reference the MITRE guidance here.

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.

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

Description:	MDWS utilized the cracked hash to gain access to other machines in the network via a 'pass-the-password' attack. The local administrator hash was obtained via machine access provided by the cracked account in IPT-001. Reusing the same local admin password on multiple machines will permit system access to those computers. MDWS leveraged this attack to gain access to 2 machines. 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 – This 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

Evidence



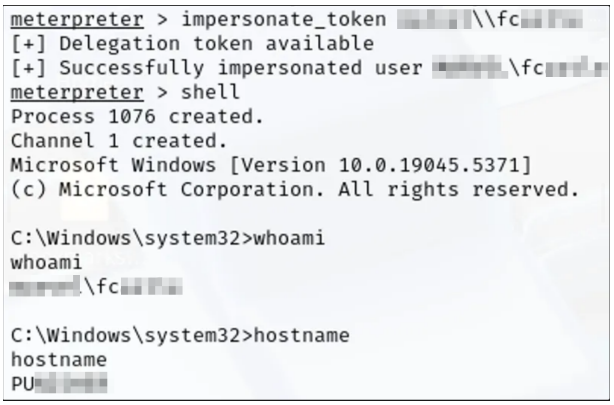
Remediation

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: Insufficient Hardening – Token Impersonation (Critical)

Description:	Due to the password reuse (IPT-002), MDWS was able to impersonate the fc***** account. The fc***** account is a domain administrator. This led to complete domain compromise.
Risk:	Likelihood: High – The penetration tester viewed and impersonated tokens with the use of open-source tools. Impact: Very High - If exploited, an attacker can gain 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



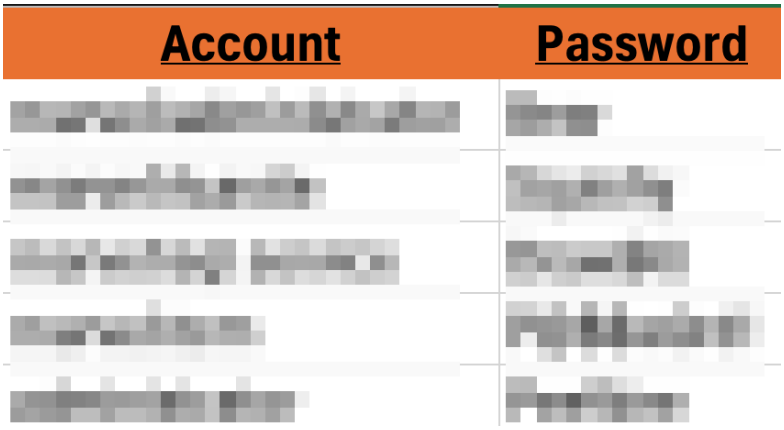
Remediation

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

Finding IPT-004: Insufficient Password Complexity (Critical)

Description:	MDWS dumped hashes from the domain controller and proceeded to attempt common password guessing attacks against all users. MDWS cracked 5 passwords (60%) using basic password list guessing attacks and low effort brute forcing attacks. 3 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 Marvel 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



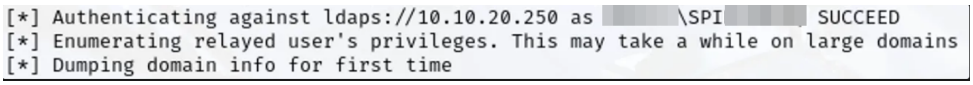
Remediation

Implement CIS Benchmark password requirements / PAM solution. MDWS recommends that Marvel 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, MDWS recommends that Marvel Corp enforce stricter password requirements for Domain Administrator and other sensitive accounts.

Finding IPT-005: Security Misconfiguration – IPv6 (Critical)

Description:	Through IPv6 DNS poisoning, the MDWS team was able to successfully relay credentials to the Marvel Corp domain controller. All details regarding the domain were dumped.
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



Remediation

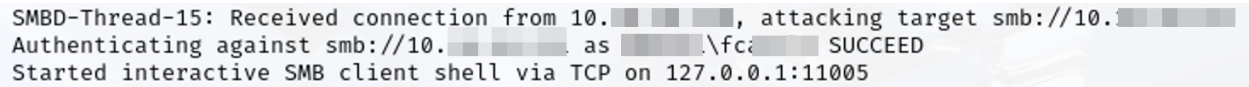
1. IPv6 poisoning abuses the fact that Windows queries for an IPv6 address even in IPv4-only environments. If you do not use IPv6 internally, the safest way to prevent mitm6 is to block DHCPv6 traffic and incoming router advertisements in Windows Firewall via Group Policy. Disabling IPv6 entirely may 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-006: Insufficient Hardening – SMB Signing Disabled (Critical)

Description:	Marvel 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 2 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



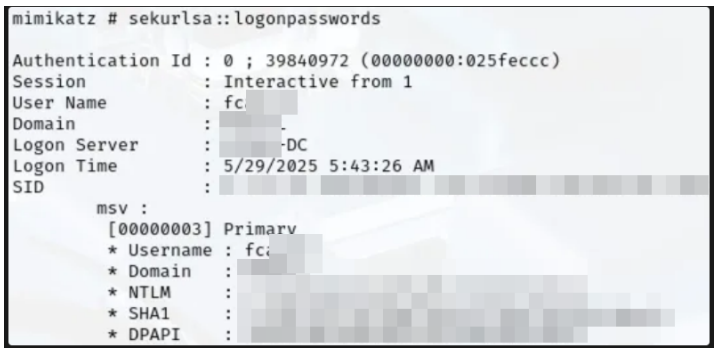
Remediation

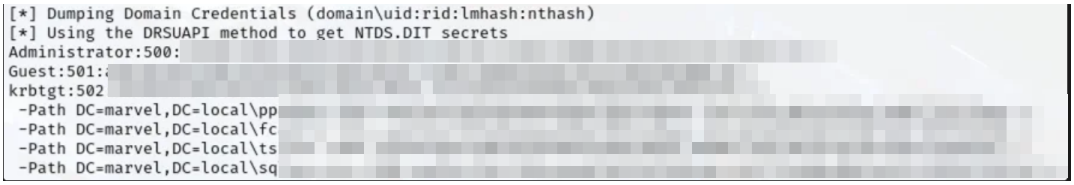
Enable SMB signing on all Marvel Corp domain computers. Alternatively, as SMB signing can cause performance issues, disabling NTLM authentication, enforcing account tiering, and limiting local admin users can effectively help mitigate attacks. For full mitigation and detection guidance, please reference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

Finding IPT-007: Security Misconfiguration – AV Deactivated

Description:	Marvel Corp has Windows Defender installed on the workstations and server. However, it was not active and allowed for Mimikatz to run without issue. This allowed the tester to dump hashes of a local machine, which ultimately led to dumping and cracking all user hashes.
Risk:	Likelihood: Medium – Mimikatz requires that a workstation already be compromised. Impact: High – If exploited, an adversary gains full control over the endpoint and launch various attacks.
System:	All
Tools Used:	Mimikatz
References:	https://attack.mitre.org/techniques/T1003/

Evidence





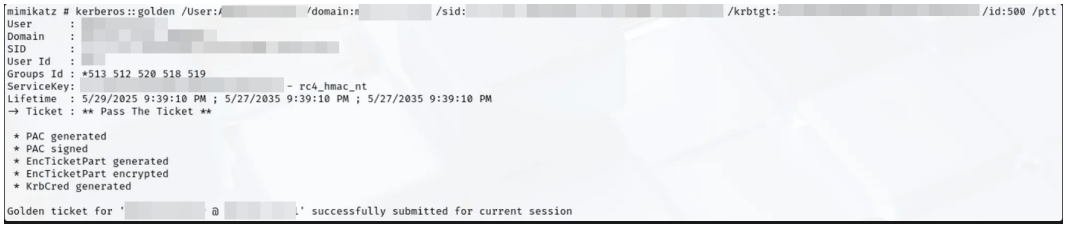
Remediation

Verify that endpoint protection is enabled and activated on all workstations.

Finding IPT-008: Insufficient Hardening – Golden Ticket Attack (Critical)

Description:	A Golden Ticket attack allows an attacker to forge Kerberos Ticket Granting Tickets (TGTs) after obtaining the krbtgt account hash. This gives the attacker the ability to impersonate any user, including domain admins. It effectively grants full access to domain resources and is a critical compromise of Active Directory.
Risk:	Likelihood: Medium – Mimikatz requires that a workstation already be compromised. Impact: High – If exploited, an adversary gains full domain access to all workstations.
System:	All
Tools Used:	Mimikatz
References:	https://attack.mitre.org/techniques/T1558/001/

Evidence



Remediation

Employ an EDR solution and monitor for Kerberos abuse. MDWS recommends configuring alert logging on domain controllers for Windows event ID 4769 whenever requesting a Kerberos service ticket. Look for unusual account names or high privilege accounts. MDWS recommends monitoring for the RC-4 HMAC encryption type.

Finding IPT-009: Insufficient Privileged Account Management – Plaintext Password in User Description (Critical)

Description:	Leveraging the IPv6 misconfiguration (IPT-005), MDWS was able to extract domain-related data, including a table of all domain user accounts. During analysis, a plaintext password was discovered in the description field of a domain administrator account. While the password was not current, its presence represents a serious security lapse.
Risk:	Likelihood: High – This attack is straightforward and feasible due to the existing IPv6 misconfiguration. Impact: Very High – The presence of a plaintext password in an account description, especially for a privileged user, could lead to full domain compromise if valid.
Tools Used:	mitm6
References:	https://blog.fox-it.com/2018/01/11/mitm6-compromising-ipv4-networks-via-ipv6/

Evidence

Domain users

CN	name	SAM Name	Member of groups	Primary group	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
[redacted]	[redacted]	[redacted]	Group Policy Creator Owners, Domain Admins, Enterprise Admins, Schema Admins, Administrators	Domain Users	01/29/25 02:56:20	05/27/25 17:24:05	0	DONT_EXPIRE_PASSWD, NORMAL_ACCOUNT	05/27/25 17:24:05	1106	Password is [redacted]

Remediation

Remove any plaintext passwords from user account description fields. Audit all accounts for similar misconfigurations and educate administrators on secure account metadata practices.

Finding IPT-010: Insufficient Privileged Account Management – Kerberoasting (High)

Description:	MDWS enumerated all user Service Principal Names (SPNs) from the Marvel Corp domain controller using a standard domain user account (see IPT-001), as part of a Kerberoasting attack. Although all user passwords had already been cracked, this step was performed to validate that Kerberoasting was a viable attack path in the environment.
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

Remediation

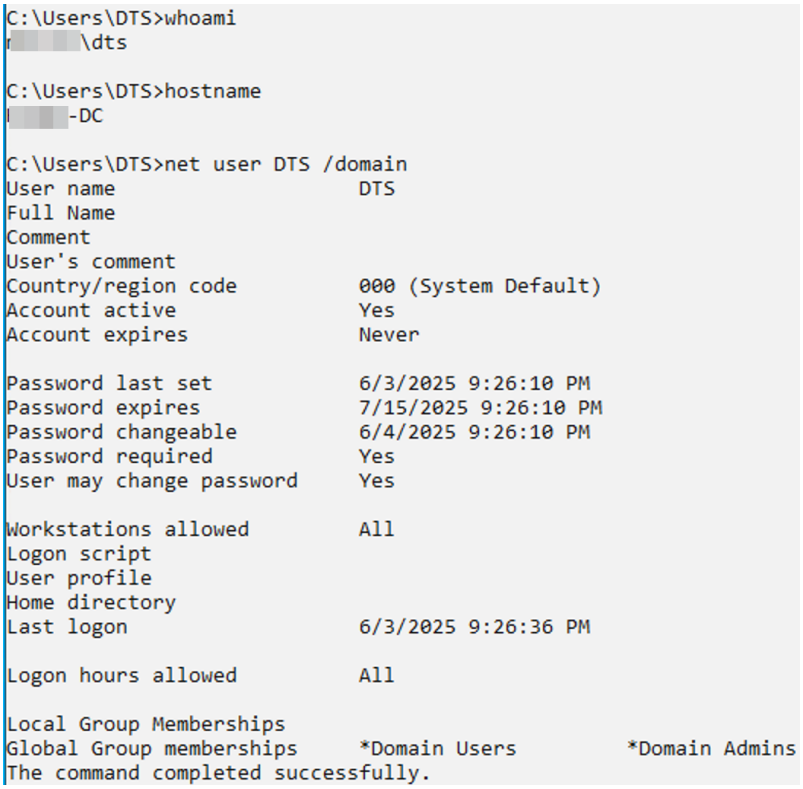
Use Group Managed Service Accounts (GMSA) for privileged services. GMSA accounts can be used to ensure passwords are long, complex, and change frequently. Where GMSA is not applicable, protect accounts by utilizing a password vaulting solution.

MDWS 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-011: Proof of Domain Compromise (Informational)

Description:	Screenshot showing the tester-created account logged in on the domain controller with Domain Administrator privileges.

Evidence



```
C:\Users\DTS>whoami
r      \dts

C:\Users\DTS>hostname
      -DC

C:\Users\DTS>net user DTS /domain
User name                    DTS
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            6/3/2025 9:26:10 PM
Password expires             7/15/2025 9:26:10 PM
Password changeable          6/4/2025 9:26:10 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   6/3/2025 9:26:36 PM

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Domain Users         *Domain Admins
The command completed successfully.
```

Finding IPT-012: 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 NetNTLM2 hash of a local administrative user	Disable multicast name resolution via GPO.
2	Cracked NTLM hash of administrative user	Increase password complexity. Utilize multi-factor.
3	Performed a “pass the password” attack and gained access to other computers	Utilize LAPS to prevent lateral movement.
4	Accessed a workstation and utilized Mimikatz to dump hashes	Ensure that AV is active. Implement an EDR.
5	Successfully cracked 3 hashes from the hash dump	Increase password complexity. Utilize multi-factor.
6	fc*****, a domain admin, was one of the cracked hashes	Utilize least privilege.
7	Used fc**** to log into the domain controller vis psexec	Utilize least privilege.
8	While logged into the domain controller, MDWS created a MDWS domain admin account	
9	MDWS logged into the domain controller as proof	

Remediation

Review action and remediation steps.

Additional Scans and Reports

MDWS 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 MidwestSec.

Cleanup

Host	Scope	Change/Cleanup Needed
10.x.x.x (PUXXXXX)	Internal	C:\mimi directory containing Mimikatz was deleted
10.x.x.x (XXXXX-DC)	Internal	MDWS domain admin account was removed

Last Page