IronShield Cyber Defense

Empire Company
Security Assessment Findings Report

Business Confidential

Date: December 20th, 2024
Project: EC-001
Version 1.0

Table of Contents

Confidentiality Statement

This document is the exclusive property of Empire Company (EC) and IronShield Cyber Defense. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or part, in any form, requires consent of both EC and IronShield Cyber Defense.

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

Contact Information

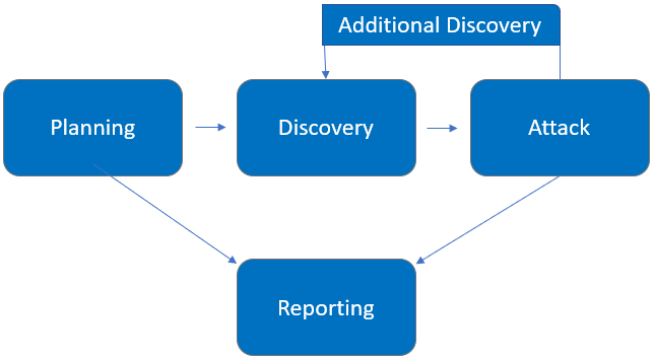
Name	Title	Contact Information
Empire Company		
John Smith	VP, Information Security (CISO)	Office: (555) 555-5555 Email: john.smith@demo.com
Jim Smith	IT Manager	Office: (555) 555-5555 Email: jim.smith@demo.com
Joe Smith	Network Engineer	Office: (555) 555-5555 Email: joe.smith@demo.com
IronShield Cyber Defense		
Bryan Vega	Lead Penetration Tester	Office: (555) 555-5555 Email: b.vega@gmail.com

Assessment Overview

From December 20th, 2024 to December 22nd, 2024, EC engaged IronShield Cyber Defense 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.

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 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.

Scope

Assessment	Details
Internal Penetration Test	10.25.25.0/24

Scope Exclusions

Per client request, IronShield 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 Empire Company.

Client Allowances

Empire Company granted access to the internal network in order to perform the assessment.

Executive Summary

IronShield evaluated Empire Company internal security posture through penetration testing from December 20th, 2024, to December 22nd, 2024. 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 three business days

Testing Summary

The network assessment evaluated Empire Company's internal network security posture. From an internal perspective, the IronShield team performed vulnerability scanning against all IPs provided by Empire Company to evaluate the overall patching health of the network. Key findings included insufficient LLMNR configuration, reused local administrator passwords, and weak password policies, which allowed IronShield to capture and crack credentials, enabling lateral movement and domain controller compromise. Additional issues, such as disabled SMB signing, insecure IPv6 configurations, and plaintext passwords in Active Directory, further exposed the environment to exploitation.

The risks identified were highly likely to be exploited due to the ease of access and misconfigurations, with impacts rated as very high for critical findings. Attack methods included LLMNR poisoning, pass-the-hash, Kerberoasting, and token impersonation, demonstrating how attackers could pivot across systems and escalate privileges. These vulnerabilities highlight a lack of hardening and insufficient privileged account management, leaving the network open to advanced threats.

The assessment began with LLMNR poisoning to capture a NetNTLMv2 hash of a regular network user, which was cracked offline to obtain plaintext credentials. These credentials provided access to a machine in the network, where IronShield dumped local administrator hashes to escalate privileges. The reused local administrator password enabled lateral movement to additional machines, further expanding access. Using Mimikatz, IronShield extracted the domain administrator's plaintext password from memory, leveraging it to gain full control of the domain controller. This sequence of attacks revealed critical weaknesses in credential management, privilege escalation, and lateral movement defenses within Empire Company's network.

These findings emphasize the ease with which attackers can exploit misconfigurations and weak practices to compromise critical systems. IronShield's testing highlights the importance of implementing robust security measures to mitigate such risks effectively. For further information on findings, please review the Internal Penetration Test Findings section.

Tester Notes and Recommendations

IronShield conducted a comprehensive penetration test of Empire Company's network, identifying critical vulnerabilities that facilitated a full domain compromise. The attack chain began with LLMNR poisoning, which exposed NetNTLMv2 hashes of regular users. These were cracked offline, allowing initial access to the network. Privilege escalation was achieved through the reuse of local administrator passwords and extracting plaintext domain administrator credentials using tools like Mimikatz. The reuse of credentials, lack of hardening, and insufficient password policies significantly increased the attack's success.

To mitigate these vulnerabilities, Empire Company should immediately disable LLMNR and NBNS through Group Policy Objects (GPO) to prevent credential theft via poisoning attacks. Enforcing strong password policies is critical, including requiring complex passwords resistant to offline cracking and implementing multi-factor authentication (MFA) to strengthen authentication security.

Additionally, implementing a Local Administrator Password Solution (LAPS) will ensure unique local administrator passwords across all machines, effectively mitigating pass-the-hash attacks. Users should be educated on the risks of enabling "Remember my credentials" during drive mapping, and policies should be enforced to disable credential caching where feasible. Finally, privileged accounts should be hardened by restricting administrative privileges to essential accounts, enforcing the principle of least privilege, and actively monitoring privileged account activity for anomalies.

By addressing these recommendations, Empire Company can significantly enhance its security posture and reduce the likelihood of similar attacks in the future.

Key Strengths and Weaknesses

The following identifies the key strengths identified during the assessment:

1. N/A

The following identifies the key weaknesses identified during the assessment:

1. Password policy found to be insufficient
2. Passwords were observed in cleartext due to Network Map Drive
3. LLMNR is enabled within the network

4. SMB signing is disabled on all non-server devices in the work
5. IPv6 is improperly managed within the network
6. User accounts can be impersonated through token delegation
7. Local admin accounts had password re-use and were overly permissive
8. Service account was running as domain administrator
9. Service account utilized weak passwords
10. Domain administrator utilized weak password

Vulnerabilities by Impact

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

Internal Penetration Test Findings

6	3	0	0	1
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 Password Complexity	Critical	Implement CIS Benchmark password requirements / PAM solution.
IPT-004: Security Misconfiguration – IPv6	Critical	Restrict DHCPv6 traffic and incoming router advertisements in Windows Firewall via GPO.
IPT-005: Insufficient Hardening – SMB Signing Disabled	Critical	Enable SMB signing on all Empire Company domain computers.
Finding IPT-009: Insufficient Hardening – Token Impersonation	Critical	Restrict token delegation.
IPT-006: Insufficient Privileged Account Management – Kerberoasting	High	Use Group Managed Service Accounts (GMSA) for privileged services.

Finding IPT-007: Plaintext Password Exposure in Active Directory Service Account Description	High	Remove the plaintext password from the service account's description field.
Finding IPT-008: Insecure Network Drive Mapping Using Administrator Credentials	High	Avoid using the "Remember me" option when mapping network drives.
IPT-010: Steps to Domain Admin	Informational	Review action and remediation steps.

Internal Penetration Test Findings

Finding IPT-001: Insufficient LLMNR Configuration (Critical)

Description:	Empire Company allows multicast name resolution on their end-user networks. IronShield captured 1 user account hashes by poisoning LLMNR traffic and cracked the password with commodity cracking software. The cracked account was 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
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

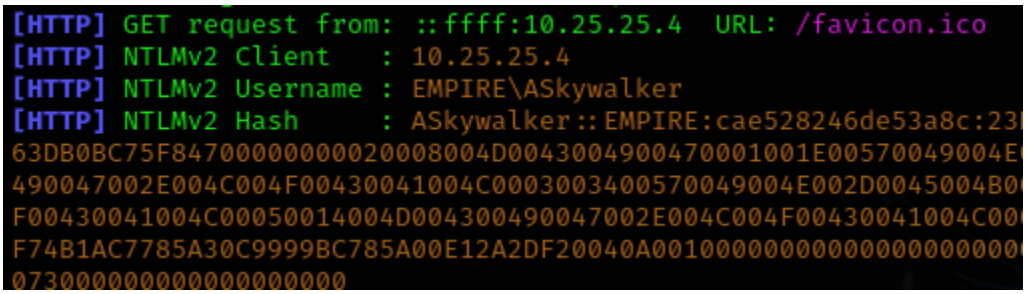


Figure 1: Captured hash of "ASKywalker"

Figure 2: Cracked hash of "ASkywalker"

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:	IronShield utilized local administrator hashes to gain access to other machines in the network via a 'pass-the-hash' attack. The local administrator hashes were obtained via machine access provided by the cracked account in IPT-001. Pass-the-hash attacks do not require knowing the account password to successfully log into a machine. Thus, reusing the same local admin password (and therefore the same hash) on multiple machines will permit system access to those computers. IronShield leveraged this attack to gain access to 2 machines within the main office. This led to further account access and the eventual compromise of the domain controller.
Risk:	Likelihood: High – This attack is effective in large networks with local admin password reuse. Impact: Very High – Pass-the-hash permits an attacker to move laterally and vertically throughout the network.
System:	All
Tools Used:	Impacket, Netexec
References:	https://capec.mitre.org/data/definitions/644.html https://tcm-sec.com/pentest-tales-001-you-spent-how-much-on-security/

Evidence

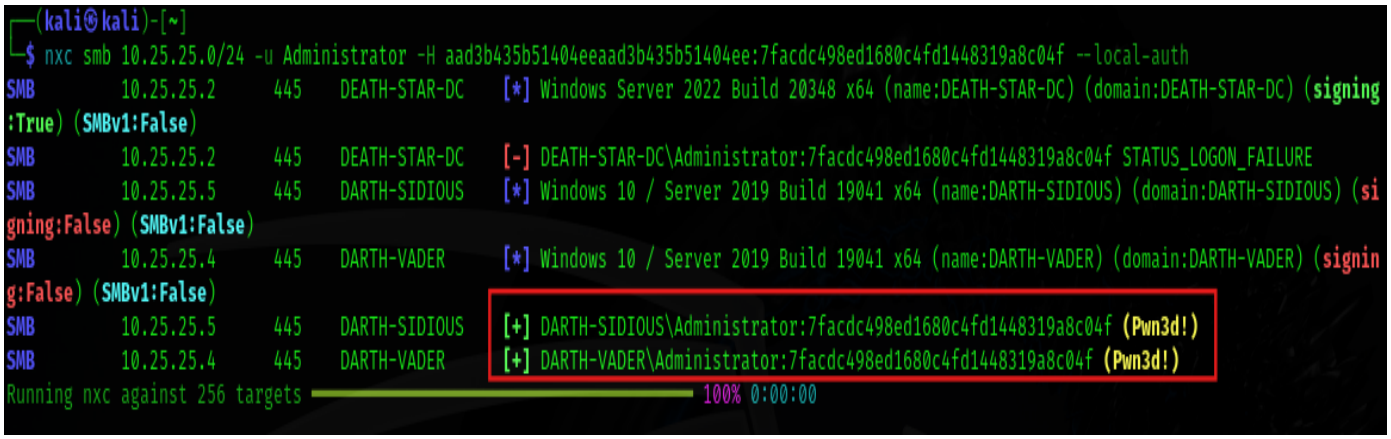


Figure 3: Local admin hash used to gain access to machine

Remediation

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

Finding IPT-003: Insufficient Password Complexity (Critical)

Description:	IronShield dumped hashes from the domain controller and proceeded to attempt common password guessing attacks against all users. IronShield cracked [Amount] passwords using basic password list guessing attacks and low effort brute forcing attacks. [amount] 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 Empire Company ability to operate.
System:	All
Tools Used:	Manual Review
References:	NIST SP800-53 IA-5(1) - Authenticator Management https://www.cisecurity.org/white-papers/cis-password-policy-guide/

Evidence

Account	Password
Administrator	P@$$w0rd!
Empire.local\SQLService	MyPassword123
Empire.local\ASkywalker	Password1
Empire.local\SPalpatine	Password2
DARTH-VADER\Administrator	Password1!
DARTH- SIDIOUS\Administrator	Password1!

Figure 4: Cracked account hashes

Remediation

Implement CIS Benchmark password requirements / PAM solution. IronShield recommends that Empire Company 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, IronShield recommends that Empire Company enforce stricter password requirements for Domain Administrator and other sensitive accounts.

Finding IPT-004: Security Misconfiguration – IPv6 (Critical)

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

Evidence

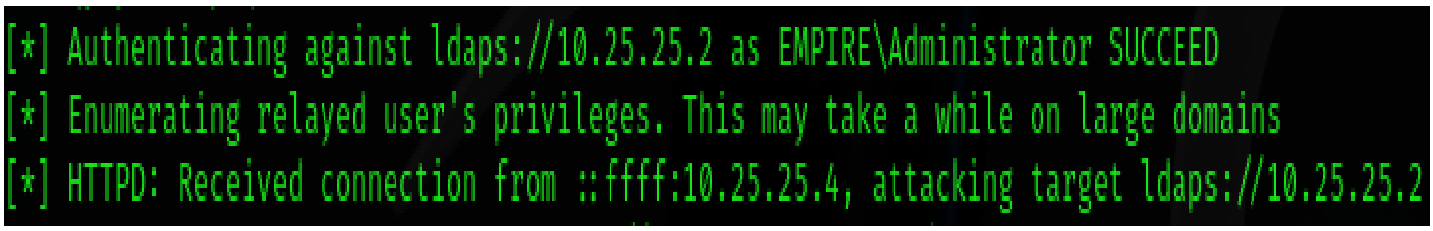


Figure 8: Successfully relayed LDAP credentials via mitm6

Remediation

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

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

Finding IPT-005: Insufficient Hardening – SMB Signing Disabled (Critical)

Description:	Empire Company 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:	10.25.25.4 and 10.25.25.5
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

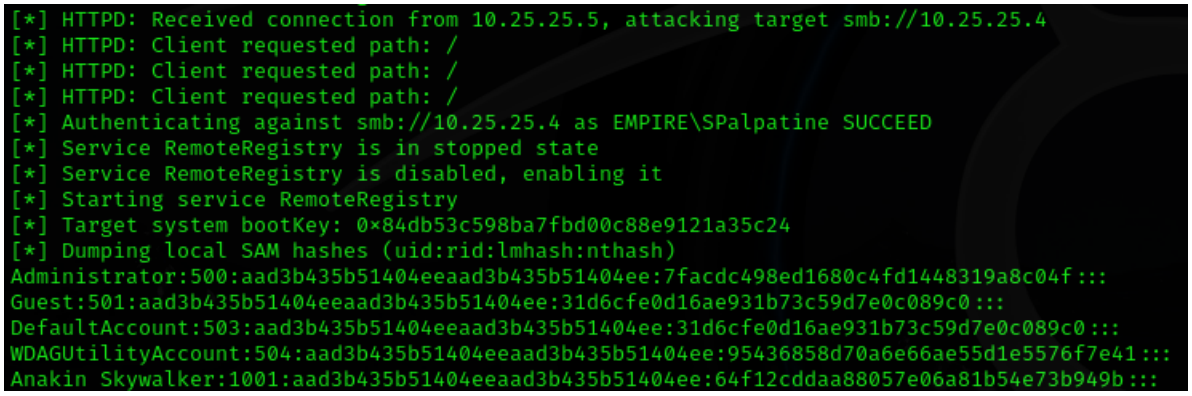


Figure 9: Successful SMB relay from Darth-Sidious machine

Remediation

Enable SMB signing on all Empire Company domain computers. Alternatively, 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-006: Insufficient Privileged Account Management – Kerberoasting (High)

Description:	IronShield retrieved a user service principal name (SPNs) from the Empire Company domain controller using a domain user-level account (IPT-001) in a Kerberoasting attack. Retrieving these user SPNs permitted IronShield to crack 1 account password. Service account SQLService was observed running as domain administrator.
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:	All
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㉿kali)-[~]
└─$ sudo GetUserSPNs.py EMPIRE.local/ASkywalker:Password1 -dc-ip 10.25.25.2 -request
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/crypto.py:12: CryptographyDeprecationWarning: Python 2 is no longer
supported by the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

ServicePrincipalName                          Name        MemberOf                                                    PasswordLastSet      LastL
ogon
--------------------------------------------  ----------  ----------------------------------------------------------  -------------------  -----
Death-Star-DC/SQLService.Empire.local:60111   SQLService  CN=Group Policy Creator Owners,OU=Groups,DC=Empire,DC=local  2025-01-09 17:01:50  <neve
r>

$krb5tgs$23$*SQLService$EMPIRE.LOCAL$Death-Star-DC/SQLService.Empire.local~60111*$e0f81a8b1f5d2b773b80cd754c5c49c7$5e1229c20cf930c7219c07df45efe
e48de952112d2e569db7ccf59084e70d588ed2d7fef07af6e5a81f421013b3369cea8ba1bc27c69e8a61db48f3fe699f4fc9599b00a6eb5da9da2a3f8a6ee4130979d14d2e1f4092
ad5074582df64ede2aa086351f1aa64a7513cae1c1108889ffb4f6a4f53debb7c22deb1ebc87a5e65e873e6ad48a433381e39f95377d02fa9099bc7d51b6f70ee33cb0b9485ddf27
4126e243b2ede6549e4fd92d8f470c0ee42090ac4ca5343a273a4398569b20647fda153f532d0df7af7ceb864df8a4e238047bdb2be2ac8d27a963ea2bf66fa54a2384d327cd1fc2
ddd8eac3c2bafb4d8e4ad2ee9e67201cebc0be7981adbf4c3faaede9939b6766957f6c62b85d45b3c20584d0e4794fe61b15c56dcbde7fe9e5596ab4f4e70e797079e9488b011064
d3cd9b3809c6f1e5f1a57698021fccb78307db09bc3ae119bacf100526a40d1ba1ee7b8c687fb967176f4af6e0e5fcd6591f2deb95cb759727e26ea0305181f9453c75b6f66761bf
0cea82d13e5a3306e51c9399aee1c906f261fedf888789d4f4bb05c28641c553c9463d40d009b885ad2dcf10fb27c4d83c3458ce6ee1a6a761fa5bbbf8c97a707c08d422f8d92c22
dce4b2c934d6d3f42a4c4918c39d91ed1f1e789d11a495cbe56592c487ceb390ddf149365c53269a1210ebfa45e474254163cf98afdf6dd115ae23a0f0a39f27fa3e5d3763bd4d65
1feef3ad095de0d5265a7ece22ac683e62585b36df611b2c56c005a08e5f1f51978b9d090b49e3f85360b97742a0a835e7c9941410a4507721ab28d4c588df39168a4003e848d923
2288a371df724f387eab3eb9704a3949437f99d2fe5f1361bfc9e74eb40449e4e6d9e21e77ffd71b5a91b7f72d1a2d8a877b08c44f126e6b7329f71b40bec0e4ef2df90a6067fca1
4a534048d922dcc3391a148a1193ce8ce542fc5c5b355f61177c9a57e587784d635ae4f8dd9757e22716868985ab4fa2cb713042d5642b761f22534956d4a2276cdba09fab13057a
b6e7f9a78c8a8ff74ecd2d2082c4efc17624aab42505cfa8e363e0874355adca8f90de75fa512f438f70848218471 9c8da45aead900dc991e0120795657cd72a4394cb466194ce4a
08723241bd01721f4747197692604eb6a435d57ebe6df44749926a8d3cb2361c47e2dd4776b462fddba657b7cb5020b30a34fadebd1d1d06cd82585063641f51fcf992b6c43f995a
f59afc002feade39f20932f6a973650fc4631f69d3d47a421321e1d56d5e66a5f1a5f53b7bbb4abad685585bc0efb078e2cb7c5fc081ce8ee3046bf47d3c06fa9d3feaea2fea5def
8c3b05110ecbb69490411a2fd6c2437d467155993517629449 0ac5775b7aadc2d7d1b664b572eb2b0fb7883306e21c76b095ac85bd482af1d2db832a32907eafd6b8ee25290669eb
7f47ea620de2adeca598c9fbd08c1cf380643dfb60ba055c3095639d7a3010adc182ebb0fbc765efeb9338654ff62c71d
```

Figure 10: Kerberoasting Attack

Service Account	Password
SQLService	MyPassword123

Figure 11: Cracked Service Account

Domain users

CN	name	SAM Name	Member of groups	Primary group
Sheev Palpatine	Sheev Palpatine	SPalpatine		Domain Users
Anakin Skywalker	Anakin Skywalker	ASkywalker		Domain Users
SQL Service	SQL Service	SQLService	Group Policy Creator Owners, Domain Admins, Enterprise Admins, Schema Admins, Administrators	Domain Users

Figure 12: SQL Service running as Domain Admin

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.

IronShield 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-007: Plaintext Password Exposure in Active Directory Service Account Description (High)

Description:	IronShield discovered a plaintext password stored in the description field of a service account during Active Directory enumeration. The exposed password allows unauthorized access to the service account, potentially enabling lateral movement, privilege escalation, and access to sensitive systems or data.
Risk:	Likelihood: High – Any domain-authenticated user with read access to Active Directory can enumerate this information using common tools or PowerShell commands. Impact: High – If the service account has elevated permissions, an attacker could gain administrative control over critical systems or the entire domain. Attackers could leverage the account to move laterally within the network, increasing the scope of compromise.
System:	All
Tools Used:	BloodHound, PowerShell Commands and LDAP Query tools
References:	Microsoft Security Best Practices for Active Directory: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices NIST SP 800-53: Security and Privacy Controls for Information Systems: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Evidence

Domain users

CN	name	SAM Name	Member of groups	Primary group	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
Sheev Palpatine	Sheev Palpatine	SPalpatine		Domain Users	11/06/24 22:13:03	01/09/25 18:35:50	01/09/25 18:35:51	DONT_EXPIRE_PASSWD, NORMAL_ACCOUNT	11/06/24 22:13:03	1106	
Anakin Skywalker	Anakin Skywalker	ASkywalker		Domain Users	11/06/24 22:11:26	01/09/25 18:33:37	01/09/25 20:14:47	DONT_EXPIRE_PASSWD, NORMAL_ACCOUNT	11/06/24 22:11:26	1105	
SQL Service	SQL Service	SQLService	Group Policy Creator Owners, Domain Admins, Enterprise Admins, Schema Admins, Administrators	Domain Users	11/06/24 22:08:16	11/06/24 23:05:31	0	DONT_EXPIRE_PASSWD, NORMAL_ACCOUNT	11/06/24 22:22:02	1104	Password is MyPassword123#
Moff Tarkin	Moff Tarkin	mtarkin	Group Policy Creator Owners, Domain Admins, Enterprise Admins, Schema Admins, Administrators	Domain Users	11/06/24 22:07:08	11/06/24 23:05:31	0	DONT_EXPIRE_PASSWD, NORMAL_ACCOUNT	11/06/24 22:07:08	1103	

Figure 13: Service Account exposing the password

Remediation

To remediate this vulnerability, immediately remove the plaintext password from the service account's description field using tools like Active Directory Users and Computers (ADUC) or PowerShell. Change the service account password to prevent unauthorized access and ensure it adheres to strong password policies.

Implement a policy prohibiting the storage of sensitive information, such as passwords, in non-secure fields like the description attribute. Regularly audit Active Directory accounts for similar misconfigurations using scripts or tools like BloodHound to identify and resolve issues proactively. Finally, apply the principle of least privilege to service accounts and enable advanced logging and monitoring to detect and respond to unauthorized access attempts.

Finding IPT-008: Insecure Network Drive Mapping Using Administrator Credentials (High)

Description:	IronShield discovered insecure network drive mapping due to credentials being saved with the "Remember my credentials" and "Reconnect at sign-in" options during drive mapping. Using Mimikatz with the credman module, the team extracted plaintext domain administrator credentials stored in memory. These credentials were used to authenticate and map the network drive, exposing the domain administrator account to potential compromise.
Risk:	Likelihood: High – Tools like Mimikatz can easily extract saved credentials from memory when the "Remember me" option is used. Impact: High – Domain administrator credentials provide full control over the Active Directory environment, enabling an attacker to compromise all systems and accounts. The attacker can use the credentials to move laterally within the network, increasing the scope of the attack.
System:	10.25.25.5
Tools Used:	Mimikatz and Lazagne
References:	Microsoft Mapping Network Drives Documentation: https://learn.microsoft.com/en-us/windows-server/storage/work-folders/work-folders-overview NIST Guidelines for Secure Authentication: https://pages.nist.gov/800-63-3/

Evidence

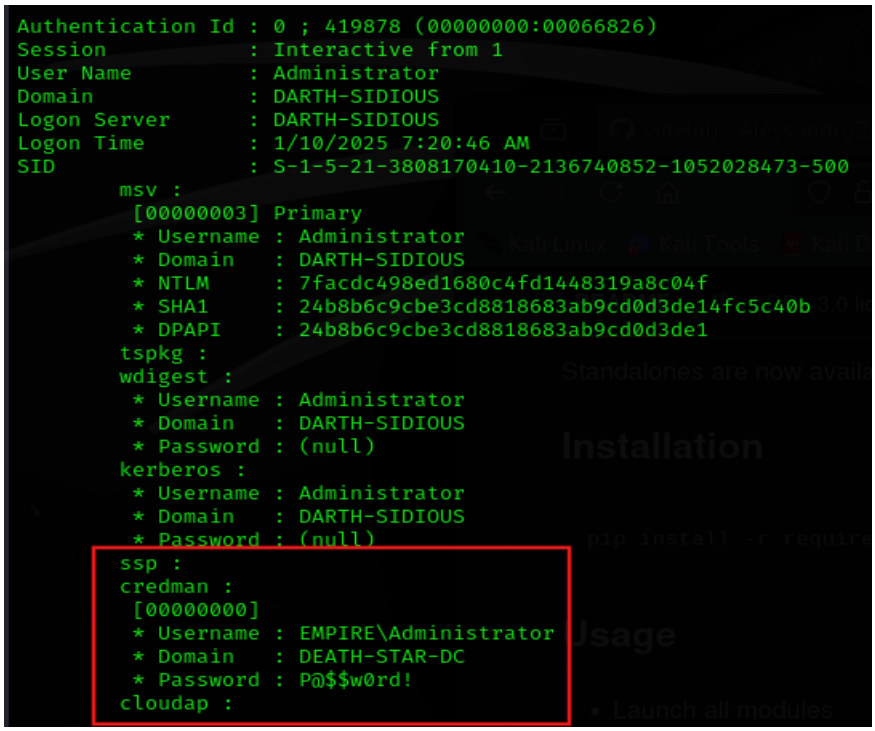


Figure 14: Domain Administrator credentials in plaintext

Remediation

To remediate this vulnerability, ensure that users and administrators avoid using the "Remember me" option when mapping network drives, as it stores credentials insecurely. Educate all personnel on secure practices for network drive mapping, including the importance of entering credentials manually for each session.

Map drives using non-administrative accounts with the least privilege necessary to perform required tasks. Regularly audit systems for stored credentials using tools like cmdkey and clear any unnecessary or insecurely stored credentials. Finally, implement security measures such as Credential Guard to protect credentials in memory from being extracted by tools like Mimikatz.

Finding IPT-009: Insufficient Hardening – Token Impersonation (Critical)

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

Evidence

```
meterpreter > impersonate_token EMPIRE\\MTarkin
[+] Delegation token available
[+] Successfully impersonated user EMPIRE\MTarkin
```

Figure 15: Impersonation of "MTarkin"

```
meterpreter > shell
Process 6612 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19045.5247]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
empire\mtarkin
```

Figure 16: Shell access as Domain Admin "MTarkin"

Remediation

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

Finding IPT-010: Steps to Domain Admin (Informational)

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

Step	Action	Remediation
1	Poisoned LLMNR responses to obtain NetNTLMv2 hash of regular network user	Disable multicast name resolution via GPO.
2	Cracked NTLM hash offline of domain users 'production'	Increase password complexity. Utilize multi- factor. Implement a Privileged Account Management solution. Utilize a password filter.
3	Leveraged password of 'ASkywalker' account to gain access to one machine within the network	Limit local administrator privileges and enforce least privilege.
4	Dumped hashes on accessed machine to find hash password of 'Local Administrator' account	
5	Overly-permissive 'Local Administrator' account permitted access to a two machines within the network	Limit local administrator privileges and enforce least privilege.
6	Dumped hashes using Mimikatz from the accessed machine to find cleartext password of Domain Administrator account	Avoid using "Remember my credentials" and "Reconnect at sign-in" during drive mapping.
7	Utilized discovered credentials to log into the domain controller.	

Remediation

Review action and remediation steps.

IronShield Cyber Defense

Last Page