Active Directory Security Assessment

Prepared for **Rhackgondins Corp**

Assessment Period: February 24, 2026 — February 27, 2026
Report Date: March 09, 2026

Version 1.0.0 | System Administrator

2. Document Control

2.1. Confidentiality Statement

This document is the property of **Rhackgondins Corp** and contains confidential information. This report is provided on a need-to-know basis and must not be disclosed, copied, or distributed to any third party without prior written consent from both parties.

The information contained in this report is based on observations made during the assessment period. The findings and recommendations are valid as of the assessment date and may not reflect subsequent changes to the environment.

2.2. Document History

Version	Date	Author	Description
1.0	2026-02-27	System Administrator	Initial release

2.3. Distribution List

Name	Role	Distribution
Julian Francisco	Primary Contact	Full Report
IT Security Team	Remediation	Full Report
Executive Leadership	Oversight	Executive Summary Only

2. Table of Contents

3. Executive Summary

An Active Directory security assessment was conducted on the corporate environment of NovaTech Industries to evaluate the security posture of the domain infrastructure, identify potential attack paths, and provide actionable recommendations for hardening.

The assessment revealed several critical and high-severity findings that could allow an attacker with initial foothold to escalate privileges to Domain Administrator within the internal network. Key concerns include misconfigured delegation settings, weak password policies, insufficient network segmentation of Tier 0 assets, and excessive privileges granted to service accounts.

It is strongly recommended that NovaTech Industries prioritize the remediation of Critical and High severity findings immediately to reduce the risk of a domain-wide compromise.

3.1. Key Findings Overview

During the assessment period from **February 24, 2026** to **February 27, 2026**, a total of **5** vulnerabilities were identified across the Active Directory environment of Rhackgondins Corp.

Severity	Count
Critical	0
High	3
Medium	2
Low	0
Informational	0

4. Scope & Methodology

4.1. Assessment Scope

internal company AD

The following systems and components were included in the scope of this assessment:

Type	Target	Details
other	local.company.ad	company ad

4.2. Methodology

The Active Directory assessment followed a structured methodology aligned with industry best practices, including MITRE ATT&CK for Enterprise, the ANSSI Active Directory Security Guidelines, and NIST SP 800-53 controls. The assessment was conducted in the following phases:

Phase 1 — Reconnaissance & Enumeration: Comprehensive enumeration of the Active Directory environment including domain structure, trusts, Group Policy Objects, organizational units, user and group memberships, service accounts, and delegation configurations.

Phase 2 — Vulnerability Identification: Analysis of identified configurations against known attack techniques including Kerberoasting, AS-REP Roasting, DCSync, unconstrained delegation abuse, ACL-based attacks, password spraying, and credential harvesting.

Phase 3 — Attack Path Analysis: Mapping of viable attack paths from standard user accounts to Domain Administrator privileges using graph-based analysis tools to identify the shortest and most likely escalation routes.

Phase 4 — Reporting & Remediation Guidance: Documentation of all findings with detailed remediation guidance prioritized by risk severity and implementation complexity.

4.3. Tools & Techniques

The following tools were utilized during the assessment:

- **BloodHound** / **SharpHound** — Active Directory relationship and attack path mapping
- **Impacket** — Python toolkit for network protocol interaction (secretsdump, GetUserSPNs, GetNPUsers)
- **CrackMapExec** — Network-wide Active Directory assessment and credential validation
- **Rubeus** — Kerberos interaction and abuse toolkit
- **PowerView** / **SharpView** — Active Directory enumeration and reconnaissance
- **PingCastle** — Active Directory security health check and risk assessment
- **ADRecon** — Comprehensive Active Directory data collection and reporting
- **Certify** / **Certipy** — Active Directory Certificate Services (AD CS) enumeration and exploitation
- **ldapdomaindump** — LDAP-based domain information extraction
- **Hashcat** — Offline password hash cracking

5. Active Directory Environment Overview

The NovaTech Industries Active Directory environment consists of a single-forest, single-domain architecture operating at a Windows Server 2016 functional level. The environment supports approximately 1,200 user accounts, 85 servers, and 450 workstations across 3 physical locations.

5.1. Domain Information

Forest Name	novatech.local
Domain Name	novatech.local
Forest Functional Level	Windows Server 2016
Domain Functional Level	Windows Server 2016
Domain Controllers	3 (DC01, DC02, DC03)
Total Users	1,247 (1,089 enabled)
Service Accounts	34
Domain Admins	8
Group Policy Objects	127
Trusts	1 external trust (partner.novatech.local — bidirectional)
AD CS (Certificate Services)	Enterprise CA deployed (CA01.novatech.local)

5.2. Tiering Model

NovaTech Industries has a partially implemented tiering model. Tier 0 assets (Domain Controllers, AD CS) are logically separated but lack dedicated administrative workstations (PAWs). Administrative accounts are shared across tiers, significantly increasing the attack surface.

6. Findings Summary

The following table provides a summary of all identified vulnerabilities, sorted by severity. Each finding is detailed in the subsequent section of this report.

#	Finding	Severity	CVSS
1	Kerberoasting	High	8.8
2	Unconstrained Kerberos Delegation	High	8.2
3	NTLM Relay Attack	High	8.1
4	Weak Group Policy Password Settings	Medium	6.5
5	Weak Group Policy Password Settings	Medium	6.5

6.1. Kerberoasting

Severity	High	CVSS Score	8.8 (High)
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H		

6.2. Description

Kerberoasting is an attack technique that targets Active Directory service accounts by requesting Kerberos Ticket Granting Service (TGS) tickets for Service Principal Names (SPNs) associated with domain user accounts. Any authenticated domain user can request these tickets, which are encrypted using the service account's NTLM password hash. The attacker then extracts the tickets and attempts to crack them offline to recover the plaintext password.

During the assessment, multiple service accounts with SPNs were identified using standard LDAP queries. TGS tickets were requested for these accounts and successfully cracked offline using hashcat with a wordlist attack, revealing weak passwords that had not been rotated in over 12 months.

The attack is difficult to detect because requesting TGS tickets is a normal Kerberos operation. No special privileges are needed beyond standard domain user authentication, making this one of the most accessible post-compromise escalation paths in Active Directory environments.

6.3. Exploitation

The following steps were taken to exploit this vulnerability:

1. Enumerated SPNs associated with user accounts using `GetUserSPNs.py` from Impacket:

```
GetUserSPNs.py domain.local/user:password -dc-ip 10.10.10.1 -request
```

2. Multiple service accounts were identified with SPNs, including `svc_sqlserver`, `svc_backup`, and `svc_web`.
3. Exported the TGS tickets in hashcat format and cracked them offline:

```
hashcat -m 13100 tgs_hashes.txt /usr/share/wordlists/rockyou.txt --rules-file best64.rule
```

4. Successfully recovered passwords for 2 out of 3 service accounts within 15 minutes. The `svc_sqlserver` account had Domain Admin equivalent privileges via group membership.

6.4. Impact

Successful Kerberoasting allowed recovery of service account passwords that provided elevated access to critical infrastructure. The compromised `svc_sqlserver` account was a member of the Domain Admins group, granting full control over the entire Active Directory domain including all user accounts, group policies, and domain-joined systems.

With Domain Admin access, an attacker could create backdoor accounts, extract all domain password hashes via DCSync, deploy ransomware across the domain, access sensitive file shares, and modify security policies to maintain persistence.

6.5. Remediation

Implement the following measures to mitigate Kerberoasting:

Use strong passwords for service accounts: All accounts with SPNs should use passwords of at least 25 characters, randomly generated. Consider using Group Managed Service Accounts (gMSA) which automatically rotate 120-character passwords.

```
# Create a Group Managed Service Account
New-ADServiceAccount -Name "svc_sqlserver"   -DNSHostName "svc_sqlserver.domain.local"   -
PrincipalsAllowedToRetrieveManagedPassword "SQLServers"
```

Apply least privilege: Remove service accounts from privileged groups like Domain Admins. Grant only the specific permissions required for the service to function.

Monitor for anomalous TGS requests: Enable Kerberos service ticket request auditing (Event ID 4769) and alert on unusual volumes of TGS requests from a single source, particularly for RC4-encrypted tickets.

6.6. References

MITRE ATT&CK - Kerberoasting (T1558.003)
AD Security - Cracking Kerberos TGS Tickets

6.7. Unconstrained Kerberos Delegation

Severity	High	CVSS Score	8.2 (High)
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:N		

6.8. Description

Unconstrained Kerberos delegation is a configuration on Active Directory computer or service accounts that allows the account to impersonate any user to any service. When a user authenticates to a server configured with unconstrained delegation, a copy of their Ticket Granting Ticket (TGT) is stored in the server's memory. The server can then use this TGT to request service tickets on behalf of the user to any service in the domain.
During the assessment, two servers were found configured with unconstrained delegation that are not domain controllers. An attacker who compromises one of these servers can extract cached TGTs from memory and use them to impersonate any user who has recently authenticated to the server, including domain administrators.

6.9. Exploitation

1. Enumerated accounts with unconstrained delegation:

```
Get-ADComputer -Filter {TrustedForDelegation -eq $true} -Properties TrustedForDelegation
# Results: FILESRV01, WEBSRV02
```

2. After gaining administrative access to FILESRV01, used Rubeus to monitor for incoming TGTs:

```
Rubeus.exe monitor /interval:5 /nowrap
```

3. Coerced authentication from a domain controller using the PrinterBug (SpoolSample), causing the DC machine account's TGT to be cached on FILESRV01.
4. Used the captured DC TGT to perform a DCSync attack, extracting all domain password hashes.

6.10. Impact

Unconstrained delegation provides a direct escalation path to Domain Admin when combined with authentication coercion techniques. Any server with unconstrained delegation that is compromised gives the attacker the ability to impersonate any domain user or computer that authenticates to it, including domain controllers. This effectively turns a single server compromise into complete domain compromise.

6.11. Remediation

Remove unconstrained delegation: Replace with constrained delegation or resource-based constrained delegation, which limits the services the account can delegate to:

```
# Remove unconstrained delegation
Set-ADComputer -Identity "FILESRV01" -TrustedForDelegation $false

# Configure constrained delegation instead
Set-ADComputer -Identity "FILESRV01"   -Add @{'msDS-
AllowedToDelegateTo'='MSSQLSvc/sqlserver.domain.local:1433'}
```

Add sensitive accounts to Protected Users group: Members of the Protected Users group cannot be delegated, preventing their TGTs from being cached on delegation-enabled servers.
Monitor delegation changes: Alert on modifications to the `TrustedForDelegation` attribute (Event ID 4742) to detect unauthorized delegation configurations.

6.12. References

MITRE ATT&CK - Steal or Forge Kerberos Tickets (T1558)
SpecterOps - Hunting Unconstrained Delegation

6.13. NTLM Relay Attack

Severity	High	CVSS Score	8.1 (High)
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N		

6.14. Description

NTLM relay is an attack where an attacker intercepts NTLM authentication attempts and forwards them to a target server, authenticating as the victim without knowing their password. This is possible when NTLM authentication is used without proper protections such as SMB signing or Extended Protection for Authentication (EPA).
During the assessment, SMB signing was found to be disabled or not required on multiple servers, including domain controllers. By poisoning LLMNR/NBT-NS responses on the network, NTLM authentication attempts from privileged users were captured and relayed to servers where SMB signing was not enforced, gaining authenticated access.

6.15. Exploitation

1. Identified servers with SMB signing not required using CrackMapExec:

```
crackmapexec smb 10.10.10.0/24 --gen-relay-list targets.txt
```

2. Started Responder in analyze mode to capture NTLM authentications via LLMNR/NBT-NS poisoning:

```
responder -I eth0 -A
```

3. Used ntlmrelayx to relay captured authentications to target servers:

```
ntlmrelayx.py -tf targets.txt -smb2support -socks
```

4. Successfully relayed an authentication from a Domain Admin account to a file server, gaining administrative access.

6.16. Impact

NTLM relay attacks allow an attacker to impersonate any user whose authentication can be intercepted. When combined with LLMNR/NBT-NS poisoning on the local network, this provides a reliable path to capturing and relaying privileged credentials. The relayed session grants the same access as the victim user, potentially including administrative access to servers, domain controllers, and sensitive file shares.

6.17. Remediation

Enable SMB signing on all systems: Configure Group Policy to require SMB signing for both clients and servers across the domain:

```
# Group Policy: Computer Configuration > Policies > Windows Settings >
# Security Settings > Local Policies > Security Options
# "Microsoft network server: Digitally sign communications (always)" = Enabled
# "Microsoft network client: Digitally sign communications (always)" = Enabled
```

Disable LLMNR and NBT-NS: These legacy name resolution protocols are commonly abused. Disable them via Group Policy and ensure DNS is properly configured as the sole name resolution method.

Enable Extended Protection for Authentication (EPA): Configure EPA on all web services and LDAP to prevent cross-protocol relay attacks.

6.18. References

MITRE ATT&CK - LLMNR/NBT-NS Poisoning and SMB Relay (T1557.001)
The Hacker Recipes - NTLM Relay

6.19. Weak Group Policy Password Settings

Severity	Medium	CVSS Score	6.5 (Medium)
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N		

6.20. Description

The domain password policy, configured through the Default Domain Policy GPO, defines minimum requirements for user account passwords. During the assessment, the password policy was found to have insufficient settings that allow users to set weak, easily guessable passwords.

The current policy requires a minimum password length of only 8 characters with no complexity requirements enforced. Password history is set to remember only 3 passwords, and the maximum password age is 365 days. No fine-grained password policies exist for privileged accounts. Additionally, no mechanism is in place to prevent the use of commonly breached passwords.

6.21. Exploitation

1. Extracted the domain password policy using `Get-ADDefaultDomainPasswordPolicy`:

```
MinPasswordLength: 8
PasswordHistoryCount: 3
MaxPasswordAge: 365 days
ComplexityEnabled: False
LockoutThreshold: 0 (no lockout)
```

2. Performed a targeted password spray using common weak passwords against all domain accounts:

```
crackmapexec smb 10.10.10.1 -u users.txt -p 'Company2024!' --no-bruteforce
```

3. Successfully authenticated with 47 out of 312 domain accounts (15%) using a list of only 10 common passwords.

6.22. Impact

Weak password policies dramatically increase the success rate of password guessing attacks. The combination of short minimum length, no complexity requirements, and no account lockout policy allows attackers to systematically test passwords against all domain accounts with no risk of detection or lockout. The 15% success rate observed during this assessment is consistent with environments using weak password policies.

Compromised accounts provide authenticated access to domain resources including file shares, internal applications, email, and potentially administrative interfaces depending on the accounts' group memberships.

6.23. Remediation

Strengthen the Default Domain Policy:

```
# Recommended password policy settings
Set-ADDefaultDomainPasswordPolicy -Identity domain.local   -MinPasswordLength 14   -
PasswordHistoryCount 24   -MaxPasswordAge "90.00:00:00"   -ComplexityEnabled $true   -
LockoutThreshold 5   -LockoutDuration "00:30:00"   -LockoutObservationWindow "00:30:00"
```

Implement Fine-Grained Password Policies: Create stricter policies for privileged accounts (administrators, service accounts) requiring 20+ character passwords with 30-day rotation.
Deploy breached password detection: Integrate a solution that checks new passwords against known breached password databases to prevent users from selecting commonly compromised credentials.

6.24. References

Microsoft - Password Policy Settings
NIST SP 800-63B - Digital Identity Guidelines

6.25. Weak Group Policy Password Settings

Severity	Medium	CVSS Score	6.5 (Medium)
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N		

6.26. Description

The domain password policy, configured through the Default Domain Policy GPO, defines minimum requirements for user account passwords. During the assessment, the password policy was found to have insufficient settings that allow users to set weak, easily guessable passwords.

The current policy requires a minimum password length of only 8 characters with no complexity requirements enforced. Password history is set to remember only 3 passwords, and the maximum password age is 365 days. No fine-grained password policies exist for privileged accounts. Additionally, no mechanism is in place to prevent the use of commonly breached passwords.

6.27. Exploitation

1. Extracted the domain password policy using `Get-ADDefaultDomainPasswordPolicy`:

```
MinPasswordLength: 8
PasswordHistoryCount: 3
MaxPasswordAge: 365 days
ComplexityEnabled: False
LockoutThreshold: 0 (no lockout)
```

2. Performed a targeted password spray using common weak passwords against all domain accounts:

```
crackmapexec smb 10.10.10.1 -u users.txt -p 'Company2024!' --no-bruteforce
```

3. Successfully authenticated with 47 out of 312 domain accounts (15%) using a list of only 10 common passwords.

6.28. Impact

Weak password policies dramatically increase the success rate of password guessing attacks. The combination of short minimum length, no complexity requirements, and no account lockout policy allows attackers to systematically test passwords against all domain accounts with no risk of detection or lockout. The 15% success rate observed during this assessment is consistent with environments using weak password policies.

Compromised accounts provide authenticated access to domain resources including file shares, internal applications, email, and potentially administrative interfaces depending on the accounts' group memberships.

6.29. Remediation

Strengthen the Default Domain Policy:

```
# Recommended password policy settings
Set-ADDefaultDomainPasswordPolicy -Identity domain.local   -MinPasswordLength 14   -
PasswordHistoryCount 24   -MaxPasswordAge "90.00:00:00"   -ComplexityEnabled $true   -
LockoutThreshold 5   -LockoutDuration "00:30:00"   -LockoutObservationWindow "00:30:00"
```

Implement Fine-Grained Password Policies: Create stricter policies for privileged accounts (administrators, service accounts) requiring 20+ character passwords with 30-day rotation.
Deploy breached password detection: Integrate a solution that checks new passwords against known breached password databases to prevent users from selecting commonly compromised credentials.

6.30. References

Microsoft - Password Policy Settings
NIST SP 800-63B - Digital Identity Guidelines

7. Remediation Roadmap

The following remediation roadmap is organized by priority based on severity, exploitability, and estimated implementation effort. NovaTech Industries should address items in the following order:

7.1. Immediate Actions (0–7 days)

- Disable or reconfigure unconstrained delegation on non-DC systems
- Rotate all service account passwords identified as Kerberoastable with weak credentials
- Disable NTLM authentication where possible, enforce NTLMv2 minimum
- Remove unnecessary Domain Admin group members

7.2. Short-term Actions (7–30 days)

- Implement LAPS (Local Administrator Password Solution) across all workstations and servers
- Enable Protected Users group for all Tier 0 administrative accounts
- Audit and remediate misconfigured ACLs on sensitive AD objects
- Enforce 15+ character password policy for service and administrative accounts
- Remediate AD CS template vulnerabilities (ESC1, ESC8)

7.3. Medium-term Actions (30–90 days)

- Deploy Privileged Access Workstations (PAWs) for Tier 0 administration
- Implement network segmentation for Domain Controllers and AD CS
- Enable SMB signing across all systems
- Deploy Microsoft Defender for Identity or equivalent AD monitoring solution
- Conduct privileged account review and implement just-in-time access

7.4. Long-term Actions (90+ days)

- Complete Active Directory tiering model implementation
- Migrate to Group Managed Service Accounts (gMSA) for all services
- Implement credential guard on all supported endpoints
- Establish recurring AD security assessment program (quarterly)

7.5. Prioritized Remediation Summary

Priority	Finding	Severity	Remediation
1	Kerberoasting	High	Implement the following measures to mitigate Kerberoasting: Use strong passwords for service accounts: All accounts w...
2	Unconstrained Kerberos Delegation	High	Remove unconstrained delegation: Replace with constrained delegation or resource-based constrained delegation, which ...

3	NTLM Relay Attack	High	Enable SMB signing on all systems: Configure Group Policy to require SMB signing for both clients and servers across ...
4	Weak Group Policy Password Settings	Medium	Strengthen the Default Domain Policy: # Recommended password policy settings Set-ADDefaultDomainPasswordPolicy -Ident...
5	Weak Group Policy Password Settings	Medium	Strengthen the Default Domain Policy: # Recommended password policy settings Set-ADDefaultDomainPasswordPolicy -Ident...

8. Appendix

8.1. Glossary

Term	Definition
AD	Active Directory — Microsoft's directory service for Windows domain networks
AD CS	Active Directory Certificate Services — PKI role for issuing and managing digital certificates
AS-REP Roasting	Attack targeting accounts that do not require Kerberos pre-authentication
CVSS	Common Vulnerability Scoring System — standardized framework for rating vulnerability severity
DCSync	Attack technique that mimics a domain controller to request password data via directory replication
GPO	Group Policy Object — AD mechanism for managing system and user configurations
gMSA	Group Managed Service Account — AD account type with automatic password management
Kerberoasting	Attack that extracts service account ticket hashes for offline cracking
LAPS	Local Administrator Password Solution — Microsoft tool for managing local admin passwords
NTLM	NT LAN Manager — legacy authentication protocol susceptible to relay and cracking attacks
PAW	Privileged Access Workstation — hardened workstation dedicated to administrative tasks
SPN	Service Principal Name — unique identifier for a service instance in Kerberos authentication
Tier 0	Highest privilege tier containing assets that control the AD forest (DCs, AD CS, etc.)

8.2. Severity Rating Scale

Severity	CVSS Range	Description
Critical	9.0 – 10.0	Vulnerabilities that can be exploited trivially and lead to complete system compromise. Immediate remediation required.
High	7.0 – 8.9	Vulnerabilities that can lead to significant data exposure or system compromise with minimal complexity. Should be addressed within 30 days.
Medium	4.0 – 6.9	Vulnerabilities that require specific conditions to exploit but could lead to moderate impact. Should be addressed within 90 days.
Low	0.1 – 3.9	Vulnerabilities with limited impact and significant exploitation barriers. Should be addressed as part of regular security maintenance.
Info	N/A	Observations and best practice recommendations that do not represent an immediate security risk but improve overall security posture.