ACTIVE DIRECTORY SECURITY ASSESSMENT

Sample Engagement Security Report

End-to-end analysis of attack paths, privilege escalations, and compliance gaps identified during the engagement.

REPORT DATE	May 02, 2026
REPORT TYPE	Active Directory Security Assessment
PROFILE	Full
DOMAINS	9 scoped

OVERALL POSTURE **HIGH**

2	2	2	0
CRITICAL	HIGH	MEDIUM	ATTACK PATHS

SAMPLE — Generated against demo fixture north-haven.local. Your ADscan instance generates this against your real domain in 90 seconds.

EXECUTIVE SUMMARY · READ IN 30 SECONDS

Your AD posture is acceptable — harden the remaining high-severity findings to lock it in.

73 /100

POSTURE SCORE

ACCEPTABLE

0 25 50 75 100

0

PATHS TO DOMAIN ADMIN

Direct or near-direct routes to full AD takeover.

0

DOMAIN BREAKERS

Cuentas cuyo control equivale a compromiso del dominio.

2

CRITICAL FINDINGS

Issues requiring action within the next 7 days.

SEVERITY DISTRIBUTION

6 findings

Critical 2 High 2 Medium 2 Low 0

BOTTOM LINE

Score: 73/100 (acceptable). 2 critical findings require immediate action. Apply the immediate items in the remediation roadmap to clear them.

SAMPLE — Generated against demo fixture north-haven.local. Your ADscan instance generates this against your real domain in 90 seconds.

00 Contents

SAMPLE — Generated against demo fixture north-haven.local. Your ADscan instance generates this against your real domain in 90 seconds.

SECTION 01

01 Executive Summary

High-level assessment overview for senior leadership.

!

OVERALL RISK POSTURE

High risk — urgent remediation recommended

2	2	2	0	0
CRITICAL	HIGH	MEDIUM	LOW	ATTACK PATHS

SEVERITY DISTRIBUTION

Critical (2) High (2) Medium (2)

An automated Active Directory security assessment was conducted across 9 Active Directory domains. A total of 6 security findings were detected — **4 critical security gaps** were identified that represent an immediate threat to business operations and regulatory standing.

The highest-priority issues requiring management attention are *noPac/sAMAccountName Spoofing (CVE-2021-42278 + CVE-2021-42287)*, *Unsigned SMB Relay Targets Detected*, and *Sensitive Data Found in SMB Shares*. Full technical detail and step-by-step remediation guidance are provided in the Technical Findings section of this report.

The identified gaps have direct implications for compliance with PCI DSS v4.0 and ENS (Esquema Nacional de Seguridad). Regulatory frameworks in scope require effective identity and access controls — the Active Directory weaknesses documented here represent evidence of control failure that auditors and regulators would classify as significant non-conformities.

Senior management should authorise a structured remediation programme targeting the critical findings within **60 days**. Progress should be reported at the next governance review.

Compliance Snapshot

At-a-glance regulatory posture across assessed frameworks. Full control-level detail in dedicated sections.

ENS COMPLIANT
100%
controls conformant
No critical gaps identified
PCI_DSS COMPLIANT
100%
controls conformant
No critical gaps identified

SAMPLE — Generated against demo fixture north-haven.local. Your ADscan instance generates this against your real domain in 90 seconds.

Critical Findings

Top critical and high-severity issues driving the risk posture. Full details in Technical Findings.

CRITICAL · 9.8

noPac/sAMAccountName Spoofing (CVE-2021-42278 + CVE-2021-42287)

NoPac chains two Active Directory vulnerabilities to achieve domain compromise from any standard domain user account. CVE-2021-42278 permits creating machine accounts with a...

Domain: **example.local** CWE: **CWE-290**

CRITICAL · 9.0

Unsigned SMB Relay Targets Detected

SMB signing is a security mechanism that cryptographically signs SMB packets to prevent tampering and relay attacks. When SMB signing is not required on a host, that host is...

> **ADSCAN ANALYSIS**
> DCs are relayable SMB targets — relay to DC meaningfully raises privilege-escalation potential

Domain: **corp.local** CWE: **CWE-287**

HIGH · 7.5

Sensitive Data Found in SMB Shares

Files accessible over SMB shares were found to contain sensitive data such as plaintext credentials, API keys, private keys, or configuration artifacts that include...

Domain: **example.local** CWE: **CWE-200**

SECTION 02

02 Attack Path Analysis

End-to-end attack chains identified in the Active Directory environment.

Attack path classification. EXPLOITED Successfully validated during active testing. ATTEMPTED Probed but not fully completed. THEORETICAL Mapped from configuration analysis; not actively exploited.

SAMPLE — Generated against demo fixture north-haven.local. Your ADscan instance generates this against your real domain in 90 seconds.

SECTION 03

03 Technical Findings

Detailed vulnerability breakdown with remediation guidance.

ADSCAN SCORING METHODOLOGY

Three categories, two scores. Honest by design.

Each finding is classified into one of three categories — visible as a coloured badge — so the reader can separate *what kind of finding it is* from *how severe*: ● VULNERABILITY is a real exploit (formal CVSS Base applies); ● CHAIN PREREQUISITE is a primitive that enables an attack chain (no CVSS Base — Critical only when the chain is confirmed); ● POSTURE documents the absence of a control (hygiene gap, capped at High even on Tier-0).

Two scores are reported per finding. **CVSS Base** is the FIRST.org-aligned, environment-agnostic score for compliance and comparability. **ADscan Priority** overlays environmental signals observed in this assessment to surface what to fix first. When they differ, the finding was elevated by one of the conditions below.

`Tier-0 exposure` — affected principal or attack-path target is Domain Admin / KRBTGT / DC. **`DC targeting`** — at least one Domain Controller is in scope of the issue.

`Relay confirmed` — a vulnerable relay target (ADCS Web Enrollment without EPA, LDAP without signing/CB) was identified in this workspace.

`Exploitation confirmed` — concrete evidence captured (cracked hash, working PoC, full chain executed).

F-001 ●

noPac/sAMAccountName Spoofing (CVE-2021-42278 + CVE-2021-42287)

CRITICAL

ADscan Priority 9.8 Critical CVSS Base 9.8 CVE ● VULNERABILITY

CWE-290 example.local

METHODOLOGY *Posture finding — measured by ADscan methodology (no CVSS Base applies).*

DESCRIPTION

NoPac chains two Active Directory vulnerabilities to achieve domain compromise from any standard domain user account. CVE-2021-42278 permits creating machine accounts with a sAMAccountName that does not end in the required dollar sign ($), meaning the account name can be set to match a Domain Controller's name exactly (e.g. 'DC01' instead of the legitimate 'DC01$'). CVE-2021-42287 exploits a Kerberos PAC validation bug: when a service ticket is requested for a principal that no longer exists, the KDC falls back to searching with a trailing '$' appended. An attacker exploits this combination by creating a machine account named 'DC01', requesting a TGT for it, renaming the account back to its original name so 'DC01' no longer exists, and then requesting a service ticket for 'DC01'. The KDC falls back to 'DC01$', finds the legitimate Domain Controller, and issues a service ticket with DC-level privileges. The resulting ticket can be used for a full DCSync.

IMPACT

Any domain user can escalate to Domain Controller-level privileges within minutes and perform a full DCSync to extract every domain credential including KRBTGT. The attack requires only default permissions (ms-DS-MachineAccountQuota > 0, the default value is 10) and produces a Domain Admin-equivalent Kerberos ticket without interacting with any privileged account. The low barrier makes this exploitable by any attacker with a single valid domain credential.

REMEDIATION

- Apply November 2021 Patch Tuesday updates on all Domain Controllers: KB5008380 (for all supported Windows Server versions) and KB5008602 (DC-specific security fix) — both patches are required to fully close the attack chain
- Set ms-DS-MachineAccountQuota to 0 on the domain object to prevent standard domain users from creating machine accounts, eliminating the prerequisite for this attack
- If MachineAccountQuota cannot be set to 0, restrict machine account creation to designated groups only via the 'Add workstations to domain' GPO right
- Monitor for suspicious sAMAccountName changes matching DC names via Event IDs 4741 (machine account created) and 4742 (machine account changed)

F-002

Unsigned SMB Relay Targets Detected

CRITICAL

ADscan Priority 9.0 Critical CVSS Base 6.8 SMB ● CHAIN PREREQUISITE

CWE-287 corp.local

CVSS 3.1 VECTOR CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

> **ADSCAN ANALYSIS**
>
> DCs are relayable SMB targets — relay to DC meaningfully raises privilege-escalation potential

DESCRIPTION

SMB signing is a security mechanism that cryptographically signs SMB packets to prevent tampering and relay attacks. When SMB signing is not required on a host, that host is vulnerable to NTLM relay attacks. An attacker positioned on the network who captures or triggers NTLM authentication — via techniques such as LLMNR/mDNS poisoning (Responder), coercion techniques (PrinterBug, PetitPotam, DFSCoerce), or rogue network services — can relay that authentication to a signing-disabled target and authenticate with the victim's credential context. If the relayed credential belongs to a local or domain administrator, the attacker gains unrestricted access to the target system without ever cracking a password.

IMPACT

An attacker can gain authenticated access to any signing-disabled host using relayed credentials, enabling lateral movement, data exfiltration, and privilege escalation. When combined with coercion techniques targeting Domain Controllers, NTLM relay can lead to full domain compromise via ADCS certificate abuse or LDAP-based privilege escalation.

REMEDIATION

- Enforce SMB signing on all domain-joined hosts via Group Policy (Microsoft network server: Digitally sign communications always = Enabled)
- Enable SMB signing requirement on all Domain Controllers and critical servers
- Disable NTLM authentication where possible and enforce Kerberos
- Disable LLMNR and NBT-NS to prevent credential capture via poisoning

F-003

Sensitive Data Found in SMB Shares

HIGH

ADscan Priority 7.5 High CVSS Base 7.5 SMB ● VULNERABILITY

CWE-200 example.local

CVSS 3.1 VECTOR CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

DESCRIPTION

Files accessible over SMB shares were found to contain sensitive data such as plaintext credentials, API keys, private keys, or configuration artifacts that include authentication material. In enterprise environments, configuration files, deployment scripts, backup files, and legacy documentation are commonly stored on shared drives and often contain credentials used during installation, automation, or system provisioning. These files are frequently not subject to the same security controls as dedicated credential vaults, are rarely audited, and may retain credentials for accounts that have since been elevated to administrative roles. Attackers performing post-exploitation discovery systematically scan accessible shares for credential material as a high-priority reconnaissance step.

IMPACT

Exposed credentials provide direct authenticated access to systems and services without requiring any additional exploitation. Credentials found in shares frequently belong to service accounts or shared administrative accounts with elevated privileges, enabling immediate lateral movement and privilege escalation. The presence of such data also indicates a lack of secrets management hygiene that may extend to other undiscovered locations.

REMEDIATION

- Immediately rotate all exposed credentials identified during the assessment
- Remove credential material from all shared files and migrate to a secrets management solution (e.g., Azure Key Vault, HashiCorp Vault, CyberArk)
- Restrict SMB share access using least-privilege ACLs and remove broad read permissions from authenticated users or Everyone groups
- Implement automated secret scanning on file repositories and shares
- Conduct a broader audit of all accessible SMB shares for additional sensitive data

F-004

Sensitive Data Found in SMB Shares

HIGH

ADscan Priority 7.5 High CVSS Base 7.5 SMB ● VULNERABILITY

CWE-200 puppy.htb

CVSS 3.1 VECTOR CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

DESCRIPTION

Files accessible over SMB shares were found to contain sensitive data such as plaintext credentials, API keys, private keys, or configuration artifacts that include authentication material. In enterprise environments, configuration files, deployment scripts, backup files, and legacy documentation are commonly stored on shared drives and often contain credentials used during installation, automation, or system provisioning. These files are frequently not subject to the same security controls as dedicated credential vaults, are rarely audited, and may retain credentials for accounts that have since been elevated to administrative roles. Attackers performing post-exploitation discovery systematically scan accessible shares for credential material as a high-priority reconnaissance step.

IMPACT

Exposed credentials provide direct authenticated access to systems and services without requiring any additional exploitation. Credentials found in shares frequently belong to service accounts or shared administrative accounts with elevated privileges, enabling immediate lateral movement and privilege escalation. The presence of such data also indicates a lack of secrets management hygiene that may extend to other undiscovered locations.

REMEDIATION

- Immediately rotate all exposed credentials identified during the assessment
- Remove credential material from all shared files and migrate to a secrets management solution (e.g., Azure Key Vault, HashiCorp Vault, CyberArk)
- Restrict SMB share access using least-privilege ACLs and remove broad read permissions from authenticated users or Everyone groups
- Implement automated secret scanning on file repositories and shares
- Conduct a broader audit of all accessible SMB shares for additional sensitive data

F-005

AS-REP Roasting

MEDIUM

ADscan Priority 6.9 Medium CVSS Base 6.9 KERBEROS ● VULNERABILITY

CWE-522 example.local

CVSS 3.1 VECTOR CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

DESCRIPTION

Preauthentication offers protection against offline Password Cracking. When enabled, a user requesting access to a resource initiates communication with the Domain Controller (DC) by sending an Authentication Server Request (AS-REQ) message with a timestamp that is encrypted with the hash of their password. If and only if the DC is able to successfully decrypt the timestamp with the hash of the user's password, it will then send an Authentication Server Response (AS-REP) message that contains the Ticket Granting Ticket (TGT) to the user. Part of the AS-REP message is signed with the user's password. For each account found without preauthentication, an adversary may send an AS-REQ message without the encrypted timestamp and receive an AS-REP message with TGT data which may be encrypted with an insecure algorithm such as RC4. The recovered encrypted data may be vulnerable to offline Password Cracking attacks similarly to Kerberoasting and expose plaintext credentials.

IMPACT

A successful AS-REP Roasting attack along with cracked passwords could lead to lateral movement and privilege escalation in an AD environment. If a password is cracked for a Domain Administrator account or equivalent, an attacker could gain control over most, if not all, resources in the domain.

REMEDIATION

Kerberos preauthentication is enabled by default. Older protocols might not support preauthentication therefore it is possible to have this setting disabled. Make sure that all accounts have preauthentication whenever possible and if it is not possible the following steps will help mitigate the risk of this attack:

- Enable AES Kerberos encryption instead of RC4
- Use strong 25+ character passwords for these accounts and rotate them periodically

F-006

Kerberoasting

MEDIUM

ADscan Priority 5.3 Medium CVSS Base 5.3 KERBEROS ● VULNERABILITY

CWE-522 example.local

CVSS 3.1 VECTOR CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

DESCRIPTION

In an Active Directory (AD) environment, Service Principal Names (SPNs) are used to uniquely identify instances of a Windows service. Kerberos authentication requires that each SPN be associated with one service account (Active Directory user account). Any authenticated AD user can request one or more Kerberos Ticket-Granting Service (TGS) tickets from the domain controller for any SPN accounts. These tickets are encrypted with the associated AD account's NTLM password hash. They can be brute forced offline using a password cracking tool such as Hashcat if a weak password is used along with the RC4 encryption algorithm. If AES encryption is in use, it will take more resources to crack a ticket to reveal the account's clear-text password, but it is possible if weak passwords are in use.

IMPACT

A successful Kerberoasting attack along with cracked passwords could lead to lateral movement and privilege escalation in an AD environment. If a password is cracked for a Domain Administrator account or equivalent, an attacker could gain control over most, if not all, resources in the domain.

REMEDIATION

Where possible eliminate SPNs in the environment in favor of Group Managed Service Accounts (gMSA) which are not subject to this type of attack. If migration to gMSAs is not possible the following steps will help mitigate the risk of this attack:

- Enable AES Kerberos encryption instead of RC4
- Use strong 25+ character passwords for service accounts and rotate them periodically
- Limit the privileges of service accounts and avoid creating SPNs tied to highly privileged accounts such as Domain Administrators

SECTION 04

04 MITRE ATT&CK Coverage

Techniques exercised across the identified attack surface.

TECHNIQUE	NAME	LINKED FINDINGS
T1068	**Exploitation for Privilege Escalation**	noPac/sAMAccountName Spoofing (CVE-2021-42278 + CVE-2021-42287)
T1552.001	**Unsecured Credentials: Credentials In Files**	Sensitive Data Found in SMB Shares
T1557.001	**Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay**	Unsigned SMB Relay Targets Detected
T1558	**Steal or Forge Kerberos Tickets**	noPac/sAMAccountName Spoofing (CVE-2021-42278 + CVE-2021-42287)
T1558.003	**Steal or Forge Kerberos Tickets: Kerberoasting**	Kerberoasting
T1558.004	**Steal or Forge Kerberos Tickets: AS-REP Roasting**	AS-REP Roasting

SAMPLE — Generated against demo fixture north-haven.local. Your ADscan instance generates this against your real domain in 90 seconds.

ATT&CK COVERAGE · ENTERPRISE MATRIX

6 techniques observed across 2 tactics

Density mapped to MITRE ATT&CK · darker cells indicate higher finding concentration or more severe exposure.

RECONNAISSANCE	RESOURCE DEVELOPMENT	INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND AND CONTROL	EXFILTRATION	IMPACT
		T1133 External Remote Services		T1098 Account Manipulation	T1068 (1) **Exploitation for Privilege Escalation**	T1027 Obfuscated Files or Information	T1003 OS Credential Dumping	T1018 Remote System Discovery	T1021.001 Remote Services: RDP				T1486 Data Encrypted for Impact
		T1190 Exploit Public-Facing Application		T1136 Create Account	T1078 Valid Accounts	T1070 Indicator Removal	T1003.001 LSASS Memory	T1069 Permission Groups Discovery	T1021.002 Remote Services: SMB/Windows Admin Shares				
					T1078.002 Domain Accounts	T1556.007 Hybrid Identity	T1003.006 DCSync	T1087 Account Discovery	T1550.002 Pass the Hash				
							T1110.001 Password Guessing	T1087.002 Account Discovery: Domain Account	T1550.003 Pass the Ticket				
							T1110.003 Password Spraying	T1482 Domain Trust Discovery	T1570 Lateral Tool Transfer				
							T1187 Forced Authentication						
							T1552.001 (2) **Credentials in Files**						
							T1552.006 Group Policy Preferences						
							T1555 Credentials from Password Stores						
							T1557.001 (1) **LLMNR/NBT-NS Poisoning + SMB Relay**						
							T1558 (1)						

SAMPLE — Generated against demo fixture north-haven.local. Your ADscan instance generates this against your real domain in 90 seconds.

Density none → low → moderate → high

6 techniques · 2 tactics · 6 findings

SAMPLE — Generated against demo fixture north-haven.local. Your ADscan instance generates this against your real domain in 90 seconds.

KILL CHAIN · TEMPORAL NARRATIVE

How the attack chain unfolded

Earliest tactic to most recent · severity-coded · catalog-aligned to MITRE ATT&CK.

PRIVILEGE ESCALATION

⬢	T1068	Exploitation for Privilege Escalation	1 finding	CRITICAL

CREDENTIAL ACCESS

⬢	T1557.001	LLMNR/NBT-NS Poisoning + SMB Relay	1 finding	CRITICAL
⬢	T1558	Steal or Forge Kerberos Tickets	1 finding	CRITICAL
⬢	T1552.001	Credentials in Files	2 findings	HIGH
⬢	T1558.003	Kerberoasting	1 finding	MEDIUM
⬢	T1558.004	AS-REP Roasting	1 finding	MEDIUM

The assessment surfaced 2 critical findings mapped to 6 ATT&CK techniques across 2 tactics. While no end-to-end path to Domain Admin was validated, the highlighted techniques represent realistic stepping stones an attacker would chain in a follow-up engagement.

SECTION 05

05 ENS — Esquema Nacional de Seguridad

Medidas de seguridad del ENS afectadas por los hallazgos del análisis.

ENS — Esquema Nacional de Seguridad

El ENS establece la política de seguridad en el uso de medios electrónicos en el ámbito de las Administraciones Públicas españolas y sus proveedores. Las vulnerabilidades de Active Directory comprometen directamente los dominios de control de acceso, gestión de identidades y protección de servicios.

0	0	11	11
NON-CONFORMANT	PARTIAL	CONFORMANT	CONTROLS ASSESSED

CERTIFICATION RISK · LOW

No critical gaps detected. Maintain controls and monitor continuously.

MARCO OPERACIONAL

8 controls · **8** conformant

MEDIDAS DE PROTECCIÓN

2 controls · **2** conformant

MARCO ORGANIZATIVO

1 controls · **1** conformant

Non-conformity Summary

Gaps classified by audit severity. Major non-conformities typically trigger corrective action requests (CARs) in certification audits.

MAJOR NON-CONFORMITIES	MINOR NON-CONFORMITIES / OBSERVATIONS
✓ *No major non-conformities identified*	✓ *No minor non-conformities identified*

Major non-conformities: CVSS ≥ 7.0. Minor non-conformities: CVSS < 7.0 or attack paths only. Classification is indicative; auditor judgment may differ.

Control Assessment

Controls sorted by conformity status. Non-conformant controls carry the highest audit risk.

SAMPLE — Generated against demo fixture north-haven.local. Your ADscan instance generates this against your real domain in 90 seconds.

op.acc.1 MARCO OPERACIONAL CONFORMANT

Identificación de usuarios

Todos los usuarios con acceso al sistema deben estar identificados de forma única y no compartir identidades.

No gaps identified — control appears effective.

op.acc.2 MARCO OPERACIONAL CONFORMANT

Requisitos de acceso

Los recursos del sistema dispondrán de los controles de acceso adecuados que impidan el acceso no autorizado.

No gaps identified — control appears effective.

op.acc.3 MARCO OPERACIONAL CONFORMANT

Segregación de funciones y tareas

Los privilegios de acceso deben estar segregados para evitar concentraciones de poder que puedan ser abusadas.

No gaps identified — control appears effective.

op.acc.4 MARCO OPERACIONAL CONFORMANT

Proceso de gestión de derechos de acceso

Los derechos de acceso se gestionarán de acuerdo a las necesidades del servicio y se revisarán periódicamente.

No gaps identified — control appears effective.

op.acc.5 MARCO OPERACIONAL CONFORMANT

Mecanismo de autenticación

El sistema implementa mecanismos de autenticación robustos que impidan el acceso de usuarios no autorizados.

No gaps identified — control appears effective.

op.acc.6 MARCO OPERACIONAL CONFORMANT

Acceso local (administradores)

El acceso físico y lógico de los administradores debe ser controlado, registrado y restringido al mínimo necesario.

No gaps identified — control appears effective.

op.exp.2 MARCO OPERACIONAL CONFORMANT

Configuración de seguridad

Los sistemas deben ser configurados minimizando su exposición a amenazas, desactivando funcionalidades innecesarias.

No gaps identified — control appears effective.

op.exp.4 MARCO OPERACIONAL CONFORMANT

Mantenimiento y actualizaciones de seguridad

Se aplicarán las actualizaciones de seguridad de forma regular y oportuna, minimizando la ventana de exposición.

No gaps identified — control appears effective.

mp.com.2 MEDIDAS DE PROTECCIÓN CONFORMANT

Protección de la confidencialidad

La información transmitida a través de redes o almacenada en sistemas debe protegerse contra accesos no autorizados.

No gaps identified — control appears effective.

mp.com.3 MEDIDAS DE PROTECCIÓN CONFORMANT

Protección de la autenticidad y la integridad

Se garantizará la autenticidad del origen y la integridad de la información intercambiada entre sistemas.

No gaps identified — control appears effective.

org.4 MARCO ORGANIZATIVO CONFORMANT

Proceso de autorización

Se mantendrá un proceso formal de autorización para el acceso a los sistemas y para las operaciones privilegiadas.

No gaps identified — control appears effective.

CERTIFICATION & AUDIT IMPACT

No critical gaps were identified in ENS controls assessed during this engagement. The organization demonstrates adequate control implementation for the Active Directory attack surface assessed.

SECTION 06

06 PCI DSS v4.0 Compliance

PCI DSS requirements affected by Active Directory security findings.

PCI DSS v4.0 — Payment Card Industry Data Security Standard

Active Directory security is foundational to PCI DSS because many cardholder-data systems authenticate through domain identities. Weaknesses in AD directly affect secure configuration, access control, identity, and monitoring requirements.

0	0	10	10
NON-CONFORMANT	PARTIAL	CONFORMANT	CONTROLS ASSESSED

CERTIFICATION RISK · LOW

No critical gaps detected. Maintain controls and monitor continuously.

NETWORK SECURITY

2 controls · **2** conformant

DATA PROTECTION

1 controls · **1** conformant

VULNERABILITY MANAGEMENT

2 controls · **2** conformant

ACCESS CONTROL & IDENTITY

2 controls · **2** conformant

MONITORING & TESTING

3 controls · **3** conformant

Non-conformity Summary

Gaps classified by audit severity. Major non-conformities typically trigger corrective action requests (CARs) in certification audits.

MAJOR NON-CONFORMITIES	MINOR NON-CONFORMITIES / OBSERVATIONS
✓ *No major non-conformities identified*	✓ *No minor non-conformities identified*

Major non-conformities: CVSS ≥ 7.0. Minor non-conformities: CVSS < 7.0 or attack paths only. Classification is indicative; auditor judgment may differ.

Control Assessment

Controls sorted by conformity status. Non-conformant controls carry the highest audit risk.

SAMPLE — Generated against demo fixture north-haven.local. Your ADscan instance generates this against your real domain in 90 seconds.

1 NETWORK SECURITY — CONFORMANT

Install and Maintain Network Security Controls

Network security controls must be implemented, configured, and maintained to restrict connections between trusted and untrusted networks and between different s…

No gaps identified — control appears effective.

2 NETWORK SECURITY — CONFORMANT

Apply Secure Configurations to All System Components

System components must be securely configured and hardened, including the removal of insecure defaults, legacy protocols, and unnecessary services.

No gaps identified — control appears effective.

3 DATA PROTECTION — CONFORMANT

Protect Stored Account Data

Stored account data must be minimized, protected, and rendered unreadable where retained or accessible.

No gaps identified — control appears effective.

5 VULNERABILITY MANAGEMENT — CONFORMANT

Protect All Systems and Networks from Malicious Software

Anti-malware mechanisms and related defenses must protect systems commonly affected by malicious software from compromise and credential theft.

No gaps identified — control appears effective.

6 VULNERABILITY MANAGEMENT — CONFORMANT

Develop and Maintain Secure Systems and Software

Security vulnerabilities must be identified, risk-ranked, remediated, and systems must be protected from known exploits and insecure software states.

No gaps identified — control appears effective.

7 ACCESS CONTROL & IDENTITY — CONFORMANT

Restrict Access to System Components and Cardholder Data by Business Need to Know

Access must be limited to the least privilege necessary for users, services, and administrators based on business need to know.

No gaps identified — control appears effective.

8 ACCESS CONTROL & IDENTITY — CONFORMANT

Identify Users and Authenticate Access to System Components

All access must be uniquely attributable to an individual or service and protected with strong authentication controls.

No gaps identified — control appears effective.

10 MONITORING & TESTING — CONFORMANT

Log and Monitor All Access to System Components and Cardholder Data

Logging and monitoring must provide a complete record of access and security-relevant activity to support detection and investigation.

No gaps identified — control appears effective.

11 MONITORING & TESTING — CONFORMANT

Test Security of Systems and Networks Regularly

Security controls, segmentation, and exposure must be tested regularly so weaknesses are identified before they are exploited.

No gaps identified — control appears effective.

12 MONITORING & TESTING — CONFORMANT

Support Information Security with Organizational Policies and Programs

Security must be governed through documented policies, risk management, service-provider oversight, and formal operational procedures.

No gaps identified — control appears effective.

CERTIFICATION & AUDIT IMPACT

No critical gaps were identified in PCI DSS v4.0.1 controls assessed during this engagement. The organization demonstrates adequate control implementation for the Active Directory attack surface assessed.

SECTION 07

07 Remediation Roadmap

Prioritised action plan to reduce risk across the environment.

IMMEDIATE · 0-30 DAYS

Contain critical exposure

- **noPac/sAMAccountName Spoofing (CVE-2021-42278 + CVE-2021-42287)** · example.local · CVSS 9.8
- **Unsigned SMB Relay Targets Detected** · corp.local · CVSS 9.0
- **Sensitive Data Found in SMB Shares** · example.local · CVSS 7.5
- **Sensitive Data Found in SMB Shares** · puppy.htb · CVSS 7.5

SHORT-TERM · 30-90 DAYS

Reduce attack surface

- **AS-REP Roasting** · example.local · CVSS 6.9
- **Kerberoasting** · example.local · CVSS 5.3

LONG-TERM · 90+ DAYS

Harden baseline

- No long-term items.