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	June 22, 2026
REPORT TYPE	Active Directory Security Assessment
PROFILE	Full
DOMAINS	3 scoped

OVERALL POSTURE **CRITICAL**

3	24	12	0
CRITICAL	HIGH	MEDIUM	ATTACK PATHS

DOC · SAMPLE ENGAGEMENT · ADSCAN

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 critical. 27 high-priority findings (3 critical, 24 high) need immediate action.

0% exposed

EXPOSURE TO DOMAIN COMPROMISE

PROVEN 0% · VALIDATED, NOT ESTIMATED

POSTURE SCORE 30/100 · CRITICAL

0% 25% 50% 75% 100%

0

PATHS TO FULL DOMAIN COMPROMISE

Routes proving total control of the domain.

0

TIER-0 HOST FOOTHOLDS

Access to a Tier-0 host. Post-exploitation required.

0

PRIVILEGE-ESCALATION ENABLERS

Reach a privileged asset, not domain takeover.

3

CRITICAL FINDINGS

Issues requiring action within the next 7 days.

SEVERITY DISTRIBUTION

49 findings

Critical 3 · High 24 · Medium 12 · Low 10

BOTTOM LINE

Score: 30/100 (critical). 3 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

DOCUMENT MAP

Contents

Executive findings, technical evidence, compliance mapping, and the prioritised remediation roadmap for this engagement.

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

Critical risk: immediate executive attention required

3	24	12	10	0
CRITICAL	HIGH	MEDIUM	LOW	ATTACK PATHS

SEVERITY DISTRIBUTION

Critical (3) High (24) Medium (12) Low (10)

An automated Active Directory security assessment was conducted across 3 Active Directory domains. A total of 49 security findings were detected. **27 high-priority findings (3 critical, 24 high)** were identified that represent an immediate threat to business operations and regulatory standing.

The highest-priority issues requiring management attention are *DCSync Privilege Abuse*, *DCSync Privilege Abuse*, and *DCSync Privilege Abuse*. 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 DORA (Digital Operational Resilience Act). 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.

Immediate executive escalation is required. The security team should initiate emergency remediation within **30 days**. Board-level oversight of the remediation programme is recommended.

Compliance Snapshot

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

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

DORA

AT RISK

0%

ASSESSED CONTROLS CONFORMANT

8 major non-conformities require action

Critical Findings

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

CRITICAL · 9.8

DCSync Privilege Abuse

The DCSync attack exploits Active Directory's directory replication protocol (MS-DRSR) to simulate the behavior of a Domain Controller requesting credential replication....

Domain: `essos.local` CWE: `CWE-269`

CRITICAL · 9.8

DCSync Privilege Abuse

The DCSync attack exploits Active Directory's directory replication protocol (MS-DRSR) to simulate the behavior of a Domain Controller requesting credential replication....

Domain: `sevenkingdoms.local` CWE: `CWE-269`

CRITICAL · 9.8

DCSync Privilege Abuse

The DCSync attack exploits Active Directory's directory replication protocol (MS-DRSR) to simulate the behavior of a Domain Controller requesting credential replication....

Domain: `north.sevenkingdoms.local` CWE: `CWE-269`

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

DCSync Privilege Abuse

CRITICAL

ADscan Priority **9.8** Critical CVSS Base 9.8 ACTIVE DIRECTORY • VULNERABILITY

CWE-269 essos.local

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

DESCRIPTION

The DCSync attack exploits Active Directory's directory replication protocol (MS-DRSR) to simulate the behavior of a Domain Controller requesting credential replication. Accounts holding the Replicating Directory Changes and Replicating Directory Changes All permissions — typically reserved for Domain Controllers and directory synchronisation services — can invoke the GetNCChanges RPC call to retrieve NTLM password hashes, Kerberos keys (AES-128, AES-256), and historical credentials for any domain account. The attack requires no local access to Domain Controllers and generates no authentication event on the target DC, making it extremely difficult to detect without dedicated tools. The KRBTGT account hash, in particular, enables Golden Ticket forgery that persists independently of all other credential rotations.

IMPACT

An attacker with DCSync capability can silently extract credentials for every privileged account in the domain, including Domain Admins, the KRBTGT account, and all service accounts. Possession of the KRBTGT hash enables Golden Ticket attacks that remain valid even after domain-wide password resets, providing persistent, undetectable access to the entire domain for up to 10 years without further exploitation.

AFFECTED ASSETS

- ESSOS.LOCAL

RECOMMENDED FIX

Remove the unauthorised replication ACEs from the domain head (+1 alternative)

> Full step-by-step runbook, commands and validation: **`AD Hardening Playbook → F-001`**.

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

F-002

DCSync Privilege Abuse

CRITICAL

ADscan Priority **9.8** Critical CVSS Base 9.8 ACTIVE DIRECTORY • VULNERABILITY

CWE-269 sevenkingdoms.local

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

DESCRIPTION

The DCSync attack exploits Active Directory's directory replication protocol (MS-DRSR) to simulate the behavior of a Domain Controller requesting credential replication. Accounts holding the Replicating Directory Changes and Replicating Directory Changes All permissions — typically reserved for Domain Controllers and directory synchronisation services — can invoke the GetNCChanges RPC call to retrieve NTLM password hashes, Kerberos keys (AES-128, AES-256), and historical credentials for any domain account. The attack requires no local access to Domain Controllers and generates no authentication event on the target DC, making it extremely difficult to detect without dedicated tools. The KRBTGT account hash, in particular, enables Golden Ticket forgery that persists independently of all other credential rotations.

IMPACT

An attacker with DCSync capability can silently extract credentials for every privileged account in the domain, including Domain Admins, the KRBTGT account, and all service accounts. Possession of the KRBTGT hash enables Golden Ticket attacks that remain valid even after domain-wide password resets, providing persistent, undetectable access to the entire domain for up to 10 years without further exploitation.

AFFECTED ASSETS

- SEVENKINGDOMS.LOCAL

RECOMMENDED FIX

Remove the unauthorised replication ACEs from the domain head (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-002**.

F-003

DCSync Privilege Abuse

CRITICAL

ADscan Priority **9.8** Critical CVSS Base 9.8 ACTIVE DIRECTORY • VULNERABILITY

CWE-269 north.sevenkingdoms.local

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

DESCRIPTION

The DCSync attack exploits Active Directory's directory replication protocol (MS-DRSR) to simulate the behavior of a Domain Controller requesting credential replication. Accounts holding the Replicating Directory Changes and Replicating Directory Changes All permissions — typically reserved for Domain Controllers and directory synchronisation services — can invoke the GetNCChanges RPC call to retrieve NTLM password hashes, Kerberos keys (AES-128, AES-256), and historical credentials for any domain account. The attack requires no local access to Domain Controllers and generates no authentication event on the target DC, making it extremely difficult to detect without dedicated tools. The KRBTGT account hash, in particular, enables Golden Ticket forgery that persists independently of all other credential rotations.

IMPACT

An attacker with DCSync capability can silently extract credentials for every privileged account in the domain, including Domain Admins, the KRBTGT account, and all service accounts. Possession of the KRBTGT hash enables Golden Ticket attacks that remain valid even after domain-wide password resets, providing persistent, undetectable access to the entire domain for up to 10 years without further exploitation.

AFFECTED ASSETS

- NORTH.SEVENKINGDOMS.LOCAL

RECOMMENDED FIX

Remove the unauthorised replication ACEs from the domain head (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-003**.

F-004

PrintNightmare Vulnerable Hosts Detected

HIGH

ADscan Priority **8.8** High CVSS Base 8.8 CVE • VULNERABILITY

CWE-269 essos.local

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

DESCRIPTION

PrintNightmare (CVE-2021-34527) is a critical vulnerability in the Windows Print Spooler service that allows authenticated users to load arbitrary DLLs through the AddPrinterDriverEx() RPC call by specifying a UNC path to a malicious driver package. The vulnerability exists in both a remote variant (RCE via network RPC) and a local variant (LPE via local named pipe). Remote exploitation is possible when the Print Spooler service accepts remote client connections, which is common on servers that act as print servers. The service runs as SYSTEM, meaning any loaded DLL executes with the highest privilege level on the host.

IMPACT

An authenticated domain user can remotely execute arbitrary code as SYSTEM on any vulnerable host where the Print Spooler accepts remote connections. When the affected host is a Domain Controller, this results in immediate domain-level compromise. The low authentication bar (any valid domain account) makes this vulnerability high-severity in any Active Directory environment where Print Spooler is running on critical systems.

AFFECTED ASSETS

- essos.local

RECOMMENDED FIX

Patch and disable the Print Spooler where unused (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-004**.

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

F-005

ADCS ESC9 - No Security Extension on Certificate Template

HIGH

ADscan Priority **8.5** High CVSS Base 8.5 ADCS • VULNERABILITY

CWE-269 essos.local

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

DESCRIPTION

ADCS ESC9 exploits the CT_FLAG_NO_SECURITY_EXTENSION flag on a certificate template. When this flag is set, the szOID_NTDS_CA_SECURITY_EXT extension — which embeds the requester's SID into the issued certificate — is omitted. Without this SID binding, certificate-to-account mapping relies on UPN matching rather than strong SID-based identity verification. An attacker with GenericWrite access to an account that can enroll in the affected template can modify that account's UPN to match a high-privilege target (e.g., a Domain Admin UPN), obtain a certificate during that window, restore the UPN, and then use the issued certificate to authenticate as the target user. This technique bypasses the KB5014754 strong mapping protections when the security extension is absent.

IMPACT

Attackers can impersonate arbitrary domain users by temporarily manipulating UPN attributes on controllable accounts. The absence of the security extension means certificates cannot be reliably bound to their true issuance context, enabling persistent authentication bypass for accounts with enrollment access.

AFFECTED ASSETS

- SPYS@ESSOS.LOCAL
- ACCOUNT OPERATORS@ESSOS.LOCAL
- KHAL.DROGO@ESSOS.LOCAL
- MISSANDEI@ESSOS.LOCAL
- VISERYS.TARGARYEN@ESSOS.LOCAL

RECOMMENDED FIX

Remove CT_FLAG_NO_SECURITY_EXTENSION so the SID security extension is embedded (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-005**.

F-006

ADCS ESC14 - Weak Explicit Certificate Mapping Abuse

HIGH

ADscan Priority **8.5** High CVSS Base 8.5 ADCS • VULNERABILITY

CWE-290 essos.local

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

DESCRIPTION

ADCS ESC14 abuses weak explicit certificate mappings configured through the altSecurityIdentities attribute. When administrators or applications rely on explicit mappings that are not strongly bound to the certificate holder's SID, an attacker who can enroll or obtain a suitable certificate can craft a cert that matches the weak mapping format and authenticate as the mapped account. This bypasses the intended identity binding guarantees of certificate-based authentication and can expose privileged accounts if they are explicitly mapped.

IMPACT

A weak explicit mapping can turn certificate enrollment or certificate theft into immediate privileged impersonation. If the mapped account is an admin, the attacker can authenticate directly as that identity and operate with the same rights as the victim without knowing the victim's password.

AFFECTED ASSETS

- `ENTERPRISE READ-ONLY DOMAIN CONTROLLERS@ESSOS.LOCAL`
- `KERBEROS AUTHENTICATION@ESSOS.LOCAL`

RECOMMENDED FIX

Remove weak altSecurityIdentities explicit mappings (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-006**.

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

F-007

ADCS ESC1 - Misconfigured Certificate Template

HIGH

ADscan Priority **8.5** High CVSS Base 8.5 ADCS • VULNERABILITY

CWE-269 essos.local

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

DESCRIPTION

ADCS ESC1 occurs when a certificate template is configured to allow requesters to specify a Subject Alternative Name (SAN) in their certificate request, combined with an authentication-capable Extended Key Usage (EKU) such as Client Authentication, Smart Card Logon, or PKINIT. Any principal with enroll permissions on such a template can request a certificate asserting the identity of any user in the domain, including Domain Administrators, by specifying their UPN in the SAN field. Active Directory validates Kerberos authentication based on the certificate SAN rather than the requesting identity, allowing the attacker to obtain a TGT for the impersonated user without knowledge of their password.

IMPACT

Any domain user with enrollment rights on the template can obtain a certificate impersonating a Domain Administrator and authenticate to any Kerberos-capable service with full DA privileges. The resulting access bypasses password rotation, MFA tied to passwords, and most authentication monitoring, as the action uses a legitimately issued certificate.

AFFECTED ASSETS

- DOMAIN USERS@ESSOS.LOCAL

RECOMMENDED FIX

Stop the template from honouring a requester-supplied SAN (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-007**.

F-008

ADCS ESC13 - Issuance Policy with Group Link Abuse

HIGH

ADscan Priority **8.5** High CVSS Base 8.5 ADCS • VULNERABILITY

CWE-269 essos.local

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

DESCRIPTION

ADCS ESC13 exploits certificate templates that have an Issuance Policy OID linked to an Active Directory group via the msDS-OIDToGroupLink attribute. When a user is issued a certificate based on such a template, the certificate includes the linked OID, and during Kerberos authentication the KDC automatically adds the linked group's SID to the resulting ticket. If the linked group is a privileged group such as Domain Admins or Enterprise Admins, any user who can enroll in the template is effectively granted membership in that privileged group for the duration of their certificate's validity — without being an actual member of the group in Active Directory.

IMPACT

Enrollment in an ESC13-affected template may grant temporary but fully functional membership in privileged groups such as Domain Admins. An attacker can enroll, use the resulting elevated Kerberos ticket to perform administrative actions including DCSync, and the privilege grant is entirely derived from certificate policy rather than group membership, making it difficult to detect through standard group membership auditing.

AFFECTED ASSETS

- DOMAIN USERS@ESSOS.LOCAL
- ESC13@ESSOS.LOCAL

RECOMMENDED FIX

Break the OID-to-group link for privileged groups (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-008**.

F-009

ADCS ESC2 - Any Purpose Certificate Template

HIGH

ADscan Priority **8.5** High CVSS Base 8.5 ADCS • VULNERABILITY

CWE-269 essos.local

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

DESCRIPTION

ADCS ESC2 occurs when a certificate template is configured with the Any Purpose EKU or with no EKU at all. A certificate with Any Purpose EKU is valid for all certificate usages including client authentication, code signing, server authentication, and email encryption. Combined with low-privilege enrollment rights, this allows an attacker to obtain a certificate that can be used to authenticate as the enrolling user against any Kerberos-capable service. Unlike ESC1, the certificate is issued with the requester's own identity, but the Any Purpose EKU makes the resulting certificate a powerful credential for lateral movement and service access that typically bypasses certificate-based access controls.

IMPACT

Attackers can obtain a maximally privileged certificate with their own identity that can be used for authentication, code signing, and other sensitive operations. Combined with ESC3 (enrollment agent), an ESC2 certificate can be leveraged to request certificates on behalf of other users, effectively bridging to ESC1-class exploitation.

AFFECTED ASSETS

- `DOMAIN USERS@ESSOS.LOCAL`

RECOMMENDED FIX

Replace the Any Purpose / no-EKU configuration with scoped EKUs (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-009**.

F-010

ADCS ESC3 - Enrollment Agent Template Abuse

HIGH

ADscan Priority **8.5** High CVSS Base 8.5 ADCS • VULNERABILITY

CWE-269 essos.local

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

DESCRIPTION

ADCS ESC3 exploits the Certificate Request Agent EKU, which enables a principal to request certificates on behalf of other users. When a template with the Certificate Request Agent EKU is accessible to low-privilege users, an attacker can enroll to obtain an enrollment agent certificate. Using this agent certificate, the attacker can then request certificates on behalf of any domain user — including Domain Administrators — against a second template that permits agent enrollment. This two-step abuse chain allows complete identity impersonation without requiring knowledge of the target user's credentials or any direct interaction with them.

IMPACT

An attacker can impersonate any domain user, including Domain Administrators, through a legitimate two-stage certificate issuance chain. The resulting certificate provides full authentication capability as the impersonated user against all Kerberos-enabled services in the domain.

AFFECTED ASSETS

- DOMAIN USERS@ESSOS.LOCAL

RECOMMENDED FIX

Restrict the enrollment-agent template and enforce Enrollment Agent Restrictions on the CA (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-010**.

F-011

ADCS ESC5 - Vulnerable CA Object ACL

HIGH

ADscan Priority **8.5** High CVSS Base 8.5 ADCS • VULNERABILITY

CWE-269 essos.local

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

DESCRIPTION

ADCS ESC5 involves misconfigured access controls on CA-level objects in Active Directory beyond certificate templates — including the CA server computer object, the CA object in the NTAuthCertificates store, the Enrollment Services container, and RPC/DCOM interfaces. When non-privileged principals hold write access to these objects, they can manipulate the CA infrastructure itself. Attacks may include modifying the CA computer object to enable RBCD-based impersonation, altering the NTAuthCertificates store, or exploiting delegated CA management permissions to issue fraudulent certificates directly.

IMPACT

Compromise of CA-level objects can undermine the entire PKI trust infrastructure for the domain. An attacker may be able to issue certificates for arbitrary identities, modify CA policy, or compromise the CA server itself, resulting in complete and persistent domain compromise that survives standard remediation procedures.

AFFECTED ASSETS

- BRAAVOS$@ESSOS.LOCAL

RECOMMENDED FIX

Lock down ACLs on CA infrastructure objects (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-011**.

F-012

ADCS ESC7 - Certificate Authority Privilege Abuse

HIGH

ADscan Priority **8.5** High CVSS Base 8.5 ADCS • VULNERABILITY

CWE-269 essos.local

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

DESCRIPTION

ADCS ESC7 occurs when non-privileged users hold the Manage CA or Manage Certificates permissions on a Certificate Authority. The Manage CA right grants control over CA configuration and security settings, including the ability to enable the EDITF_ATTRIBUTESUBJECTALTNAME2 flag (ESC6), modify CA ACLs, and add certificate officers. The Manage Certificates right allows approval of pending certificate requests, including those that were submitted with a fraudulent SAN. An attacker with Manage Certificates can submit a certificate request for a privileged user's identity, set it to a pending state requiring approval, and then approve it themselves using their own management permission.

IMPACT

CA management rights provide near-complete control over the PKI trust infrastructure. An attacker can issue certificates for Domain Admins, modify CA policy to introduce persistent vulnerabilities, or manipulate certificate lifecycle in ways that enable persistent authentication bypass across the domain.

AFFECTED ASSETS

- BRAAVOS$@ESSOS.LOCAL

RECOMMENDED FIX

Remove Manage CA / Manage Certificates from non-PKI principals and enforce separation of duties (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-012**.

F-013

ADCS ESC4 - Vulnerable Certificate Template ACL

HIGH

ADscan Priority **8.5** High CVSS Base 8.5 ADCS • VULNERABILITY

CWE-269 essos.local

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

DESCRIPTION

ADCS ESC4 occurs when non-privileged principals hold write permissions (WriteProperty, WriteDACL, WriteOwner, or GenericWrite) on a certificate template object in Active Directory. Certificate template objects are stored in the Configuration naming context and are subject to standard AD ACL controls. With template modification rights, an attacker can alter the template configuration to introduce ESC1-class vulnerabilities — enabling SAN specification, removing EKU restrictions, or disabling manager approval — obtain a fraudulent certificate, and then optionally revert the changes to avoid detection. This technique escalates an otherwise safe template into an exploitable one without leaving persistent misconfiguration evidence.

IMPACT

An attacker with write access to any template can temporarily transform it into an ESC1-exploitable template, obtain a certificate impersonating a Domain Administrator, then revert the change. The window of exploitation is brief and may not trigger template misconfiguration monitoring, making this a stealthy path to domain compromise.

AFFECTED ASSETS

- KHAL.DROGO@ESSOS.LOCAL

RECOMMENDED FIX

Remove dangerous write ACEs from the template object (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-013**.

F-014

ADCS ESC14 - Weak Explicit Certificate Mapping Abuse

HIGH

ADscan Priority **8.5** High CVSS Base 8.5 ADCS • VULNERABILITY

CWE-290 sevenkingdoms.local

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

DESCRIPTION

ADCS ESC14 abuses weak explicit certificate mappings configured through the altSecurityIdentities attribute. When administrators or applications rely on explicit mappings that are not strongly bound to the certificate holder's SID, an attacker who can enroll or obtain a suitable certificate can craft a cert that matches the weak mapping format and authenticate as the mapped account. This bypasses the intended identity binding guarantees of certificate-based authentication and can expose privileged accounts if they are explicitly mapped.

IMPACT

A weak explicit mapping can turn certificate enrollment or certificate theft into immediate privileged impersonation. If the mapped account is an admin, the attacker can authenticate directly as that identity and operate with the same rights as the victim without knowing the victim's password.

AFFECTED ASSETS

- ENTERPRISE READ-ONLY DOMAIN CONTROLLERS@SEVENKINGDOMS.LOCAL
- KERBEROS AUTHENTICATION@SEVENKINGDOMS.LOCAL
- LORD.VARYS@SEVENKINGDOMS.LOCAL

RECOMMENDED FIX

Remove weak altSecurityIdentities explicit mappings (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-014**.

F-015

ADCS ESC5 - Vulnerable CA Object ACL

HIGH

ADscan Priority **8.5** High CVSS Base 8.5 ADCS • VULNERABILITY

CWE-269 sevenkingdoms.local

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

DESCRIPTION

ADCS ESC5 involves misconfigured access controls on CA-level objects in Active Directory beyond certificate templates — including the CA server computer object, the CA object in the NTAuthCertificates store, the Enrollment Services container, and RPC/DCOM interfaces. When non-privileged principals hold write access to these objects, they can manipulate the CA infrastructure itself. Attacks may include modifying the CA computer object to enable RBCD-based impersonation, altering the NTAuthCertificates store, or exploiting delegated CA management permissions to issue fraudulent certificates directly.

IMPACT

Compromise of CA-level objects can undermine the entire PKI trust infrastructure for the domain. An attacker may be able to issue certificates for arbitrary identities, modify CA policy, or compromise the CA server itself, resulting in complete and persistent domain compromise that survives standard remediation procedures.

AFFECTED ASSETS

- KINGSLANDING$@SEVENKINGDOMS.LOCAL

RECOMMENDED FIX

Lock down ACLs on CA infrastructure objects (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-015**.

F-016

ADCS ESC7 - Certificate Authority Privilege Abuse

HIGH

ADscan Priority **8.5** High CVSS Base 8.5 ADCS • VULNERABILITY

CWE-269 sevenkingdoms.local

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

DESCRIPTION

ADCS ESC7 occurs when non-privileged users hold the Manage CA or Manage Certificates permissions on a Certificate Authority. The Manage CA right grants control over CA configuration and security settings, including the ability to enable the EDITF_ATTRIBUTESUBJECTALTNAME2 flag (ESC6), modify CA ACLs, and add certificate officers. The Manage Certificates right allows approval of pending certificate requests, including those that were submitted with a fraudulent SAN. An attacker with Manage Certificates can submit a certificate request for a privileged user's identity, set it to a pending state requiring approval, and then approve it themselves using their own management permission.

IMPACT

CA management rights provide near-complete control over the PKI trust infrastructure. An attacker can issue certificates for Domain Admins, modify CA policy to introduce persistent vulnerabilities, or manipulate certificate lifecycle in ways that enable persistent authentication bypass across the domain.

AFFECTED ASSETS

- `KINGSLANDING$@SEVENKINGDOMS.LOCAL`

RECOMMENDED FIX

Remove Manage CA / Manage Certificates from non-PKI principals and enforce separation of duties (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-016**.

F-017

ADCS ESC8 - NTLM Relay to Web Enrollment

HIGH

ADscan Priority **8.2** High CVSS Base 8.2 ADCS • VULNERABILITY

CWE-306 essos.local

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

DESCRIPTION

ADCS ESC8 exploits the HTTP-based Certificate Enrollment web interface (certsrv) when NTLM authentication is permitted on the endpoint. An attacker who can coerce outbound NTLM authentication from a privileged host — such as a Domain Controller — using techniques including PetitPotam, PrinterBug, or DFSCoerce can relay that authentication to the CA web enrollment interface. The relayed NTLM session authenticates as the coerced host's machine account and requests a Domain Controller certificate. This DC certificate can then be used in a Pass-the-Certificate attack to request a Kerberos TGT as the DC machine account, enabling DCSync and full domain credential extraction.

IMPACT

Successful ESC8 exploitation against a Domain Controller certificate template enables full domain compromise through a DCSync attack, without requiring any initial privileged access. The attack chain — coerce DC authentication, relay to web enrollment, obtain DC certificate, DCSync — can be executed in minutes from a standard domain user account.

AFFECTED ASSETS

- DOMAIN USERS@ESSOS.LOCAL

RECOMMENDED FIX

Enable Extended Protection for Authentication (EPA) and require HTTPS on the enrollment endpoints (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-017**.

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

F-018

ADCS ESC8 - NTLM Relay to Web Enrollment

HIGH

ADscan Priority **8.2** High CVSS Base 8.2 ADCS • VULNERABILITY

CWE-306 sevenkingdoms.local

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

DESCRIPTION

ADCS ESC8 exploits the HTTP-based Certificate Enrollment web interface (certsrv) when NTLM authentication is permitted on the endpoint. An attacker who can coerce outbound NTLM authentication from a privileged host — such as a Domain Controller — using techniques including PetitPotam, PrinterBug, or DFSCoerce can relay that authentication to the CA web enrollment interface. The relayed NTLM session authenticates as the coerced host's machine account and requests a Domain Controller certificate. This DC certificate can then be used in a Pass-the-Certificate attack to request a Kerberos TGT as the DC machine account, enabling DCSync and full domain credential extraction.

IMPACT

Successful ESC8 exploitation against a Domain Controller certificate template enables full domain compromise through a DCSync attack, without requiring any initial privileged access. The attack chain — coerce DC authentication, relay to web enrollment, obtain DC certificate, DCSync — can be executed in minutes from a standard domain user account.

AFFECTED ASSETS

- DOMAIN USERS@SEVENKINGDOMS.LOCAL

RECOMMENDED FIX

Enable Extended Protection for Authentication (EPA) and require HTTPS on the enrollment endpoints (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-018**.

F-019

LDAP Signing / Channel Binding Not Hardened

HIGH

ADscan Priority **8.1** High CVSS Base 8.1 LDAP • CHAIN PREREQUISITE

CWE-319 essos.local

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

DESCRIPTION

When Domain Controllers do not require LDAP signing or do not enforce channel binding, attackers can relay coerced or captured NTLM authentication to LDAP and perform directory operations in the victim context. This weakness is frequently chained with coercion, name resolution poisoning, or ADCS abuse to reach privilege escalation or domain compromise.

IMPACT

Unsigned or weakly protected LDAP on Domain Controllers materially lowers the cost of relay-based privilege escalation. In hardened Active Directory environments, LDAP signing and channel binding are foundational protections that reduce the blast radius of NTLM relay and related coercion paths.

AFFECTED ASSETS

- meereen

RECOMMENDED FIX

Require LDAP signing and enable channel binding on all DCs (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-019**.

F-020

ADCS ESC11 - NTLM Relay to RPC Certificate Enrollment

HIGH

ADscan Priority **8.0** High CVSS Base 8.0 ADCS • VULNERABILITY

CWE-269 essos.local

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

DESCRIPTION

ADCS ESC11 targets Certificate Authorities where the IF_ENFORCEENCRYPTICERTREQUEST flag is not set, meaning the RPC-based certificate enrollment interface accepts connections without requiring encrypted or mutually authenticated transport. This creates an NTLM relay attack vector analogous to ESC8, but targeting the RPC/DCOM enrollment interface (ICertPassage) instead of the HTTP web enrollment endpoint. An attacker who coerces outbound NTLM from a privileged host can relay the authentication directly to the CA's RPC interface and request certificates in the context of the coerced machine account, bypassing the HTTPS/EPA protections that mitigate ESC8.

IMPACT

Provides an alternative NTLM relay path to ADCS certificate enrollment when the HTTP web enrollment interface has been secured. When combined with authentication coercion against Domain Controllers, enables the same full domain compromise chain as ESC8 via the RPC protocol path.

AFFECTED ASSETS

- DOMAIN USERS@ESSOS.LOCAL

RECOMMENDED FIX

Require encrypted RPC enrollment (IF_ENFORCEENCRYPTICERTREQUEST) (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-020**.

F-021

Domain Admin Sessions on Non-Privileged Hosts

HIGH

ADscan Priority **8.0** High CVSS Base 8.0 PRIVILEGE • VULNERABILITY

CWE-269 essos.local

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

DESCRIPTION

Domain Administrator sessions were discovered on workstations, member servers, or other non-Tier 0 hosts. When a Domain Admin authenticates to a non-privileged system, their credentials — in the form of NTLM hashes, Kerberos TGTs, and potentially cleartext credentials — are loaded into the LSASS process memory of that host and may also be cached in the Windows Credential Manager. An attacker who compromises any such endpoint through phishing, vulnerability exploitation, or lateral movement can harvest these credentials using tools such as Mimikatz or ProcDump without triggering any domain-level security events. The exposure window lasts for the duration of the session and, in the case of cached credentials, potentially indefinitely.

IMPACT

Compromise of any host where a Domain Admin has an active or cached session provides full domain administrative credentials without requiring any additional exploitation. This collapses the security boundary between workstations and the domain tier, meaning a single phishing email or workstation-level vulnerability is sufficient for full domain takeover.

AFFECTED ASSETS

- ADSCAN@ESSOS.LOCAL

RECOMMENDED FIX

Enforce a tiered admin model and Protected Users (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-021**.

F-022

ADCS ESC11 - NTLM Relay to RPC Certificate Enrollment

HIGH

ADscan Priority **8.0** High CVSS Base 8.0 ADCS • VULNERABILITY

CWE-269 sevenkingdoms.local

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

DESCRIPTION

ADCS ESC11 targets Certificate Authorities where the IF_ENFORCEENCRYPTICERTREQUEST flag is not set, meaning the RPC-based certificate enrollment interface accepts connections without requiring encrypted or mutually authenticated transport. This creates an NTLM relay attack vector analogous to ESC8, but targeting the RPC/DCOM enrollment interface (ICertPassage) instead of the HTTP web enrollment endpoint. An attacker who coerces outbound NTLM from a privileged host can relay the authentication directly to the CA's RPC interface and request certificates in the context of the coerced machine account, bypassing the HTTPS/EPA protections that mitigate ESC8.

IMPACT

Provides an alternative NTLM relay path to ADCS certificate enrollment when the HTTP web enrollment interface has been secured. When combined with authentication coercion against Domain Controllers, enables the same full domain compromise chain as ESC8 via the RPC protocol path.

AFFECTED ASSETS

- DOMAIN USERS@SEVENKINGDOMS.LOCAL

RECOMMENDED FIX

Require encrypted RPC enrollment (IF_ENFORCEENCRYPTICERTREQUEST) (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-022**.

F-023

gMSA Password Readable by Non-Admins

HIGH

ADscan Priority **7.5** High CVSS Base 7.5 GMSA • VULNERABILITY

CWE-522 essos.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

Group Managed Service Accounts (gMSA) are a special account type in Active Directory that provides automatic password management for service accounts. The password is stored in the msDS-ManagedPassword attribute of the gMSA object and is only readable by principals listed in the msDS-GroupMSAMembership attribute. When this access control list is misconfigured to include non-privileged groups or overly broad membership, any member can retrieve the gMSA password blob using the DSGetPassword API. The password is returned as an MSDS-MANAGEDPASSWORD_BLOB structure that can be parsed to extract the current NT hash, enabling Pass-the-Hash attacks or Kerberos ticket requests using the gMSA's identity.

IMPACT

Compromise of a gMSA password provides full impersonation of the service account, including all associated service permissions, SPN-based access, and any delegated rights. Service accounts typically have privileged access to databases, web services, backup systems, and other critical infrastructure, making this a high-impact finding depending on the gMSA's configured permissions.

AFFECTED ASSETS

- GMSADRAGON$@ESSOS.LOCAL

RECOMMENDED FIX

Restrict msDS-GroupMSAMembership to the hosts that run the service (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-023**.

F-024

LAPS Password Readable by Non-Admins

HIGH

ADscan Priority **7.5** High CVSS Base 7.5 LAPS • VULNERABILITY

CWE-522 essos.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

The Local Administrator Password Solution (LAPS) stores per-machine local administrator credentials in the ms-Mcs-AdmPwd attribute of computer objects in Active Directory. By design, only designated administrative groups should have read access to this attribute. When the ACL on computer objects grants read access to non-privileged accounts — such as broad user groups, domain users, or helpdesk tiers — any member of those groups can query the attribute and retrieve the current plaintext local administrator password for any LAPS-managed machine. This misconfiguration is commonly introduced during LAPS deployment when access delegation is overly permissive.

IMPACT

Non-privileged users can retrieve local administrator passwords for any LAPS-managed machine in the affected OUs. This enables lateral movement to those machines with full local administrative rights, bypassing the security benefit that LAPS was deployed to provide. In environments where local administrator accounts have network access, this can escalate rapidly.

AFFECTED ASSETS

- BRAAVOS$@ESSOS.LOCAL

RECOMMENDED FIX

Remove non-admin read access to the LAPS password attribute and rotate (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-024**.

F-025

SMBv1 Protocol Enabled

HIGH

ADscan Priority **7.5** High CVSS Base 7.5 NETWORK SECURITY • VULNERABILITY

CWE-1104 essos.local

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

DESCRIPTION

One or more hosts respond to SMBv1 (NT LM 0.12) negotiate requests. SMBv1 is a legacy protocol deprecated by Microsoft since 2014. It lacks modern security features (encryption, secure negotiate, pre-auth integrity) and is directly exploited by EternalBlue (MS17-010), EternalRomance, and related NSA-derived tools that enabled WannaCry and NotPetya ransomware. Microsoft has disabled SMBv1 by default since Windows 10 1709.

IMPACT

Hosts with SMBv1 enabled are vulnerable to EternalBlue (MS17-010) and related exploits if unpatched, and remain exposed to SMBv1-specific attack primitives (NTLM downgrade, signing bypass) regardless of patch status. Domain Controllers with SMBv1 represent a critical exposure.

AFFECTED ASSETS

- `essos.local`

RECOMMENDED FIX

Disable SMBv1 server and client across the estate (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-025**.

F-026

Obsolete Operating Systems

HIGH

ADscan Priority **7.5** High CVSS Base 7.5 ASSET HYGIENE • VULNERABILITY

CWE-1104 essos.local

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

DESCRIPTION

One or more domain-joined systems appear to be running obsolete Windows versions identified through LDAP inventory. Unsupported operating systems no longer receive security updates, often lack modern hardening controls, and materially increase the attack surface of the Active Directory estate.

IMPACT

Obsolete hosts are at elevated risk of compromise through unpatched vulnerabilities and weak legacy configurations. In AD environments this can enable credential theft, lateral movement, relay scenarios, and persistence from a single outdated workstation or server.

AFFECTED ASSETS

- `essos.local`

RECOMMENDED FIX

Upgrade or decommission unsupported operating systems (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-026**.

F-027

LAPS Not Deployed on Domain Hosts (Posture)

HIGH

ADscan Priority **7.0** High CVSS Base 5.5 POSTURE/HYGIENE • POSTURE

CWE-1392 essos.local

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

ADSCAN ANALYSIS

LAPS not deployed on Domain Controllers — static local admin credentials on DCs widen blast radius of any credential leak; no exposure confirmed yet

DESCRIPTION

One or more domain-joined hosts do not have a managed local administrator password solution deployed. Without LAPS (or Windows LAPS), local administrator passwords are typically static, set at image-build time, and frequently shared across many machines. This is a posture/hygiene finding describing the absence of a control — not a confirmed credential exposure. The credential-readability case (a non-admin principal can read the LAPS attribute on a host where LAPS is deployed) is reported separately as 'LAPS Password Readable by Non-Admins'.

IMPACT

Without LAPS, a single local administrator credential compromise (via a memory dump, an old image, or a poorly-rotated build) often grants lateral movement across many hosts that share the same static password. Severity escalates when the affected hosts include Domain Controllers or Tier-0 assets, where the absence of a rotation control directly increases the blast radius of a credential leak. Treat as a Medium-grade hygiene gap unless paired with a confirmed reuse or readability finding.

AFFECTED ASSETS

- `braavos.essos.local`
- `COMPU240.essos.local`
- `meereen.essos.local`

RECOMMENDED FIX

Deploy Windows LAPS across all domain-joined hosts (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-027**.

F-028

AS-REP Roasting

MEDIUM

ADscan Priority **6.9** Medium CVSS Base 6.9 KERBEROS • VULNERABILITY

CWE-522 essos.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.

AFFECTED ASSETS

- MISSANDEI@ESSOS.LOCAL

RECOMMENDED FIX

Re-enable Kerberos pre-authentication on affected accounts (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-028**.

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

F-029

AS-REP Roasting

MEDIUM

ADscan Priority **6.9** Medium CVSS Base 6.9 KERBEROS • VULNERABILITY

CWE-522 north.sevenkingdoms.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.

AFFECTED ASSETS

- BRANDON.STARK@NORTH.SEVENKINGDOMS.LOCAL

RECOMMENDED FIX

Re-enable Kerberos pre-authentication on affected accounts (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-029**.

F-030

Unsigned SMB Relay Targets Detected

MEDIUM

ADscan Priority **6.8** Medium CVSS Base 6.8 SMB • CHAIN PREREQUISITE

CWE-287 essos.local

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

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.

AFFECTED ASSETS

- 192.168.180.23

RECOMMENDED FIX

Require SMB signing on every host via GPO (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-030**.

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

F-031

All Extended Rights Assigned

MEDIUM

ADscan Priority **6.5** Medium CVSS Base 6.5 PERMISSIONS • VULNERABILITY

CWE-284 essos.local

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

DESCRIPTION

The AllExtendedRights ACE grants a principal the ability to perform all extended operations on an Active Directory object in a single permission grant. For user objects, AllExtendedRights encompasses the User-Force-Change-Password right, the ability to read confidential attributes such as LAPS passwords and BitLocker recovery keys, and all other extended operations defined on the object class. This broad permission frequently results from overly permissive ACL delegation during AD administrative setup, Help Desk delegation, or legacy configuration that was never scoped down. The actual exploitability depends on the target object type, but the combination of rights included under AllExtendedRights generally exceeds any legitimate delegation requirement.

IMPACT

Depending on the target object, AllExtendedRights may allow password resets, access to confidential attributes, modification of security-sensitive properties, or other privileged operations. When present on high-value targets such as Domain Admin accounts or service accounts with elevated permissions, this represents a direct privilege escalation path.

AFFECTED ASSETS

- COMPU240$@ESSOS.LOCAL

RECOMMENDED FIX

Replace AllExtendedRights with specific scoped rights (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-031**.

F-032

SMBv1 Protocol Enabled (Legacy Posture)

MEDIUM

ADscan Priority **6.5** Medium CVSS Base 5.5 SMB • CHAIN PREREQUISITE

CWE-1104 essos.local

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

ADSCAN ANALYSIS

SMBv1 enabled on DCs — legacy protocol surface; not equivalent to a confirmed CVE such as EternalBlue (MS17-010)

DESCRIPTION

SMBv1 is a deprecated and insecure file-sharing protocol with a long history of serious implementation and downgrade weaknesses. Hosts that still accept SMBv1 broaden the legacy attack surface and may serve as preconditions for relay or downgrade chains. Note: this finding reports protocol exposure, not confirmation of a specific CVE such as MS17-010 (EternalBlue) — concrete RCE requires a separately validated vulnerable build.

IMPACT

Hosts with SMBv1 enabled retain compatibility with a protocol that Microsoft has deprecated for years due to systemic security weaknesses. In Active Directory environments, SMBv1 exposure raises the likelihood of legacy exploit chains, relay preconditions, and lateral movement through outdated file-sharing paths. Impact escalates to High/Critical only when paired with a confirmed exploitable CVE on the same host.

AFFECTED ASSETS

- MEEREEN
- BRAAVOS

RECOMMENDED FIX

Remove the SMBv1 feature domain-wide (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-032**.

F-033

Force Change Password Rights Assigned

MEDIUM

ADscan Priority **6.5** Medium CVSS Base 6.5 PERMISSIONS • VULNERABILITY

CWE-284 sevenkingdoms.local

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

DESCRIPTION

The User-Force-Change-Password extended right in Active Directory allows a principal to reset another user's password without knowing the current password. This permission is often legitimately delegated to Help Desk or tier-1 support groups, but may be over-scoped to include sensitive or privileged accounts. In an attack chain, an adversary who compromises an account holding this right can reset the target account's password and immediately authenticate with the new credentials. This bypasses any existing authentication factors tied to the original password and can provide access to high-value accounts without triggering credential-based detection rules.

IMPACT

An attacker can silently take over any account for which they hold ForceChangePassword rights, gaining that account's access context, group memberships, and delegated permissions. If the targeted account is privileged or leads to a privilege escalation path, the impact extends to full domain compromise.

AFFECTED ASSETS

- JAIME.LANNISTER@SEVENKINGDOMS.LOCAL

RECOMMENDED FIX

Remove over-scoped User-Force-Change-Password ACEs (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-033**.

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

F-034

Constrained Kerberos Delegation Misconfiguration

MEDIUM

ADscan Priority **6.5** Medium CVSS Base 6.5 DELEGATION • VULNERABILITY

CWE-269 north.sevenkingdoms.local

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

DESCRIPTION

Constrained delegation restricts a service account's impersonation capability to specific target services, configured via the msDS-AllowedToDelegateTo attribute. The Kerberos S4U2Self and S4U2Proxy extensions enable the service to request service tickets on behalf of other users to the allowed targets. When the TrustedToAuthForDelegation (Protocol Transition) flag is also set, the service can obtain impersonation tickets for users who did not originally authenticate via Kerberos, bypassing the normal user interaction requirement. Misconfiguration risks include overly broad target service scope, delegation to high-value services (e.g., CIFS on Domain Controllers, LDAP), and unreviewed protocol transition permissions that expand the attack surface significantly.

IMPACT

Exploitation of misconfigured constrained delegation enables an attacker who compromises the delegating account to impersonate arbitrary domain users to the allowed target services. If the allowed services include administrative interfaces on Domain Controllers, this can lead to full domain compromise.

AFFECTED ASSETS

- `WINTERFELL$@NORTH.SEVENKINGDOMS.LOCAL`

RECOMMENDED FIX

Tighten msDS-AllowedToDelegateTo and drop unneeded protocol transition (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-034**.

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

F-035

Kerberoasting

MEDIUM

ADscan Priority **5.3** Medium CVSS Base 5.3 KERBEROS • VULNERABILITY

CWE-522 essos.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.

AFFECTED ASSETS

- GMSADRAGON$@ESSOS.LOCAL
- SQL_SVC@ESSOS.LOCAL

RECOMMENDED FIX

Migrate the SPN to a Group Managed Service Account (gMSA) (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-035**.

F-036

Kerberoasting

MEDIUM

ADscan Priority **5.3** Medium CVSS Base 5.3 KERBEROS • VULNERABILITY

CWE-522 north.sevenkingdoms.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.

AFFECTED ASSETS

- JON.SNOW@NORTH.SEVENKINGDOMS.LOCAL
- SANSA.STARK@NORTH.SEVENKINGDOMS.LOCAL
- SQL_SVC@NORTH.SEVENKINGDOMS.LOCAL

RECOMMENDED FIX

Migrate the SPN to a Group Managed Service Account (gMSA) (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-036**.

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

F-037

SMB Signing Not Required

MEDIUM

ADscan Priority **5.0** Medium CVSS Base 5.0 NETWORK SECURITY • POSTURE

CWE-300 essos.local

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

DESCRIPTION

One or more domain-joined computers do not require SMB packet signing. When SMB signing is not enforced, an attacker in a man-in-the-middle position can relay NTLM authentication from these hosts to other services (NTLMrelayx, Responder), authenticate as the relayed identity, and potentially execute code or access resources without knowing the credential.

IMPACT

Hosts with SMB signing disabled are viable relay targets. If the relayed credential belongs to a Domain Admin or computer account with unconstrained delegation, a single intercepted authentication can lead to full domain compromise. Domain Controllers with signing disabled are particularly severe as they represent the highest-value relay target in the environment.

AFFECTED ASSETS

- `essos.local`

RECOMMENDED FIX

Require SMB signing on both server and client via GPO (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-037**.

F-038

Accounts with Password Not Required Flag

MEDIUM

ADscan Priority **5.0** Medium CVSS Base 5.0 POLICY • VULNERABILITY

CWE-521 essos.local

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

DESCRIPTION

The PASSWD_NOTREQD flag in the userAccountControl attribute of an Active Directory user account allows that account to authenticate without a password, bypassing the domain password policy minimum length and complexity requirements. This flag can be set intentionally for legacy systems that do not support passwords, or it may persist unnoticed through account migrations, provisioning scripts, or administrative errors. An account with this flag may have an empty password, which can be trivially tested using standard authentication tools against SMB, LDAP, Kerberos, or other domain-joined services.

IMPACT

Accounts with PASSWD_NOTREQD and an empty password provide immediate unauthenticated access to any service that the account has permissions on. Even if the password is not empty, the flag disables policy enforcement permanently, meaning weak or empty passwords can be set at any time without policy rejection.

AFFECTED ASSETS

- `DefaultAccount`
- `Guest`

RECOMMENDED FIX

Clear PASSWD_NOTREQD on all affected accounts and set a compliant password (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-038**.

F-039

SMB Signing Not Required

MEDIUM

ADscan Priority **5.0** Medium CVSS Base 5.0 NETWORK SECURITY • POSTURE

CWE-300 north.sevenkingdoms.local

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

DESCRIPTION

One or more domain-joined computers do not require SMB packet signing. When SMB signing is not enforced, an attacker in a man-in-the-middle position can relay NTLM authentication from these hosts to other services (NTLMrelayx, Responder), authenticate as the relayed identity, and potentially execute code or access resources without knowing the credential.

IMPACT

Hosts with SMB signing disabled are viable relay targets. If the relayed credential belongs to a Domain Admin or computer account with unconstrained delegation, a single intercepted authentication can lead to full domain compromise. Domain Controllers with signing disabled are particularly severe as they represent the highest-value relay target in the environment.

AFFECTED ASSETS

- `north.sevenkingdoms.local`

RECOMMENDED FIX

Require SMB signing on both server and client via GPO (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-039**.

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

F-040

Accounts with Non-Expiring Passwords

LOW

ADscan Priority **3.7** Low CVSS Base 3.7 POLICY • POSTURE

CWE-521 essos.local

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

DESCRIPTION

Accounts configured with the DONT_EXPIRE_PASSWORD flag are exempt from the domain's password expiration policy, meaning their credentials remain valid indefinitely unless manually changed. While this configuration is sometimes necessary for service accounts running as specific identities, it is frequently applied broadly to user accounts for convenience, or inherited from legacy configurations. Long-lived credentials are statistically more likely to have been exposed through phishing, credential dumping incidents, data breaches, or pass-the-hash attacks that were not detected at the time. An attacker in possession of a non-expiring credential retains access indefinitely unless the compromise is specifically identified and the password is manually rotated.

IMPACT

Compromised non-expiring credentials provide persistent access with no natural remediation deadline. In environments where password rotation is the primary credential invalidation mechanism, these accounts create permanent persistence opportunities for attackers who have obtained the credentials through any means.

AFFECTED ASSETS

- `Administrator`
- `adscan`
- `daenerys.targaryen`
- `DefaultAccount`
- `drogon`
- `Guest`
- `jorah.mormont`
- `khal.drogo`
- `missandei`
- `sql_svc`

... and 2 more

RECOMMENDED FIX

Remove DONT_EXPIRE_PASSWORD from standard accounts (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-040**.

F-041

Accounts with Non-Expiring Passwords

LOW

ADscan Priority **3.7** Low CVSS Base 3.7 POLICY • POSTURE

CWE-521 sevenkingdoms.local

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

DESCRIPTION

Accounts configured with the DONT_EXPIRE_PASSWORD flag are exempt from the domain's password expiration policy, meaning their credentials remain valid indefinitely unless manually changed. While this configuration is sometimes necessary for service accounts running as specific identities, it is frequently applied broadly to user accounts for convenience, or inherited from legacy configurations. Long-lived credentials are statistically more likely to have been exposed through phishing, credential dumping incidents, data breaches, or pass-the-hash attacks that were not detected at the time. An attacker in possession of a non-expiring credential retains access indefinitely unless the compromise is specifically identified and the password is manually rotated.

IMPACT

Compromised non-expiring credentials provide persistent access with no natural remediation deadline. In environments where password rotation is the primary credential invalidation mechanism, these accounts create permanent persistence opportunities for attackers who have obtained the credentials through any means.

AFFECTED ASSETS

- `sevenkingdoms.local`

RECOMMENDED FIX

Remove DONT_EXPIRE_PASSWORD from standard accounts (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-041**.

F-042

Accounts with Non-Expiring Passwords

LOW

ADscan Priority **3.7** Low CVSS Base 3.7 POLICY • POSTURE

CWE-521 north.sevenkingdoms.local

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

DESCRIPTION

Accounts configured with the DONT_EXPIRE_PASSWORD flag are exempt from the domain's password expiration policy, meaning their credentials remain valid indefinitely unless manually changed. While this configuration is sometimes necessary for service accounts running as specific identities, it is frequently applied broadly to user accounts for convenience, or inherited from legacy configurations. Long-lived credentials are statistically more likely to have been exposed through phishing, credential dumping incidents, data breaches, or pass-the-hash attacks that were not detected at the time. An attacker in possession of a non-expiring credential retains access indefinitely unless the compromise is specifically identified and the password is manually rotated.

IMPACT

Compromised non-expiring credentials provide persistent access with no natural remediation deadline. In environments where password rotation is the primary credential invalidation mechanism, these accounts create permanent persistence opportunities for attackers who have obtained the credentials through any means.

AFFECTED ASSETS

- `north.sevenkingdoms.local`

RECOMMENDED FIX

Remove DONT_EXPIRE_PASSWORD from standard accounts (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-042**.

F-043

Machine Account Quota Allows Domain Join

LOW

ADscan Priority **3.5** Low CVSS Base 3.5 DOMAIN CONFIGURATION • POSTURE

CWE-284 essos.local

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

DESCRIPTION

The ms-DS-MachineAccountQuota attribute is set to a value greater than 0. This allows any authenticated domain user to join computers to the domain up to the configured limit, which can be abused for RBCD attacks, DNS poisoning via fake computer objects, or Kerberos relay attack preparation.

IMPACT

An attacker with any valid domain credential can create computer objects under their control, enabling Resource-Based Constrained Delegation (RBCD) attacks, Kerberos relay setups (e.g. noPac), and persistence via machine accounts.

AFFECTED ASSETS

- essos.local

RECOMMENDED FIX

Set ms-DS-MachineAccountQuota to 0 (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-043**.

F-044

Passwords Predating Current Policy

LOW

ADscan Priority **3.5** Low CVSS Base 3.5 IDENTITY HYGIENE • POSTURE

CWE-521 essos.local

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

DESCRIPTION

One or more enabled user accounts have a password that was last set before the most recent modification to the applicable password policy (Default Domain Policy or a Fine-Grained PSO). The current policy requirements — minimum length, complexity, or maximum age — were not in effect when the credential was created. Active Directory does not retroactively force a reset on policy changes, so these accounts may carry credentials that do not comply with the organisation's current security baseline.

IMPACT

Credentials established under a weaker policy may be shorter, simpler, or older than the current standard allows. Attackers obtaining these hashes through LDAP, Kerberoasting, or credential dumping face a reduced cracking workload. When affected accounts are Tier-0 or high-value identities, the impact escalates to potential domain compromise.

AFFECTED ASSETS

- `essos.local`

RECOMMENDED FIX

Force a reset on accounts whose pwdLastSet predates the policy change (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-044**.

F-045

Enabled Stale User Accounts Detected

LOW

ADscan Priority **3.5** Low CVSS Base 3.5 IDENTITY HYGIENE • POSTURE

CWE-16 essos.local

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

DESCRIPTION

Enabled user accounts with prolonged inactivity represent stale identity surface. These accounts are frequently overlooked during joiner-mover-leaver processes, may retain standing access, and often remain exempt from scrutiny until they are abused during password spraying, credential stuffing, or post-compromise privilege escalation.

IMPACT

Inactive but enabled accounts increase the attack surface and complicate identity governance. When stale accounts belong to Tier-0 or high-value users, the resulting exposure is materially more severe because these identities can preserve privileged access long after operational need has disappeared.

AFFECTED ASSETS

- `essos.local`

RECOMMENDED FIX

Disable then prune accounts inactive beyond the threshold (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-045**.

F-046

Machine Account Quota Allows Domain Join

LOW

ADscan Priority **3.5** Low CVSS Base 3.5 DOMAIN CONFIGURATION • POSTURE

CWE-284 sevenkingdoms.local

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

DESCRIPTION

The ms-DS-MachineAccountQuota attribute is set to a value greater than 0. This allows any authenticated domain user to join computers to the domain up to the configured limit, which can be abused for RBCD attacks, DNS poisoning via fake computer objects, or Kerberos relay attack preparation.

IMPACT

An attacker with any valid domain credential can create computer objects under their control, enabling Resource-Based Constrained Delegation (RBCD) attacks, Kerberos relay setups (e.g. noPac), and persistence via machine accounts.

AFFECTED ASSETS

- `sevenkingdoms.local`

RECOMMENDED FIX

Set ms-DS-MachineAccountQuota to 0 (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-046**.

F-047

Passwords Predating Current Policy

LOW

ADscan Priority **3.5** Low CVSS Base 3.5 IDENTITY HYGIENE • POSTURE

CWE-521 sevenkingdoms.local

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

DESCRIPTION

One or more enabled user accounts have a password that was last set before the most recent modification to the applicable password policy (Default Domain Policy or a Fine-Grained PSO). The current policy requirements — minimum length, complexity, or maximum age — were not in effect when the credential was created. Active Directory does not retroactively force a reset on policy changes, so these accounts may carry credentials that do not comply with the organisation's current security baseline.

IMPACT

Credentials established under a weaker policy may be shorter, simpler, or older than the current standard allows. Attackers obtaining these hashes through LDAP, Kerberoasting, or credential dumping face a reduced cracking workload. When affected accounts are Tier-0 or high-value identities, the impact escalates to potential domain compromise.

AFFECTED ASSETS

- `sevenkingdoms.local`

RECOMMENDED FIX

Force a reset on accounts whose pwdLastSet predates the policy change (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-047**.

F-048

Machine Account Quota Allows Domain Join

LOW

ADscan Priority **3.5** Low CVSS Base 3.5 DOMAIN CONFIGURATION • POSTURE

CWE-284 north.sevenkingdoms.local

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

DESCRIPTION

The ms-DS-MachineAccountQuota attribute is set to a value greater than 0. This allows any authenticated domain user to join computers to the domain up to the configured limit, which can be abused for RBCD attacks, DNS poisoning via fake computer objects, or Kerberos relay attack preparation.

IMPACT

An attacker with any valid domain credential can create computer objects under their control, enabling Resource-Based Constrained Delegation (RBCD) attacks, Kerberos relay setups (e.g. noPac), and persistence via machine accounts.

AFFECTED ASSETS

- `north.sevenkingdoms.local`

RECOMMENDED FIX

Set ms-DS-MachineAccountQuota to 0 (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-048**.

F-049

Passwords Predating Current Policy

LOW

ADscan Priority **3.5** Low CVSS Base 3.5 IDENTITY HYGIENE • POSTURE

CWE-521 north.sevenkingdoms.local

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

DESCRIPTION

One or more enabled user accounts have a password that was last set before the most recent modification to the applicable password policy (Default Domain Policy or a Fine-Grained PSO). The current policy requirements — minimum length, complexity, or maximum age — were not in effect when the credential was created. Active Directory does not retroactively force a reset on policy changes, so these accounts may carry credentials that do not comply with the organisation's current security baseline.

IMPACT

Credentials established under a weaker policy may be shorter, simpler, or older than the current standard allows. Attackers obtaining these hashes through LDAP, Kerberoasting, or credential dumping face a reduced cracking workload. When affected accounts are Tier-0 or high-value identities, the impact escalates to potential domain compromise.

AFFECTED ASSETS

- `north.sevenkingdoms.local`

RECOMMENDED FIX

Force a reset on accounts whose pwdLastSet predates the policy change (+1 alternative)

> Full step-by-step runbook, commands and validation: **AD Hardening Playbook → F-049**.

SECTION 04

04 MITRE ATT&CK Coverage

Techniques exercised across the identified attack surface.

TECHNIQUE	NAME	LINKED FINDINGS
T1003.006	**OS Credential Dumping: DCSync**	DCSync Privilege Abuse
T1021.002	**Remote Services: SMB/Windows Admin Shares**	SMBv1 Protocol Enabled (Legacy Posture)
T1068	**Exploitation for Privilege Escalation**	PrintNightmare Vulnerable Hosts Detected
T1078	**Valid Accounts**	Accounts with Non-Expiring Passwords, Passwords Predating Current Policy, Accounts with Password Not Required Flag, Enabled Stale User Accounts Detected
T1078.002	**Valid Accounts: Domain Accounts**	Domain Admin Sessions on Non-Privileged Hosts
T1078.003	**Valid Accounts: Local Accounts**	LAPS Not Deployed on Domain Hosts (Posture)
T1098	**Account Manipulation**	All Extended Rights Assigned, Force Change Password Rights Assigned
T1210	**Exploitation of Remote Services**	SMBv1 Protocol Enabled
T1555	**Credentials from Password Stores**	gMSA Password Readable by Non-Admins, LAPS Password Readable by Non-Admins
T1557	**Adversary-in-the-Middle**	LDAP Signing / Channel Binding Not Hardened
T1557.001	**LLMNR/NBT-NS Poisoning and SMB Relay**	SMB Signing Not Required, Unsigned SMB Relay Targets Detected, LDAP Signing / Channel Binding Not Hardened
T1558	**Steal or Forge Kerberos Tickets**	Constrained Kerberos Delegation Misconfiguration
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.

TECHNIQUE	NAME	LINKED FINDINGS
T1649	**Steal or Forge Authentication Certificates**	ADCS ESC9 - No Security Extension on Certificate Template, ADCS ESC14 - Weak Explicit Certificate Mapping Abuse, ADCS ESC1 - Misconfigured Certificate Template, ADCS ESC11 - NTLM Relay to RPC Certificate Enrollment, ADCS ESC13 - Issuance Policy with Group Link Abuse, ADCS ESC2 - Any Purpose Certificate Template, ADCS ESC3 - Enrollment Agent Template Abuse, ADCS ESC8 - NTLM Relay to Web Enrollment, ADCS ESC5 - Vulnerable CA Object ACL, ADCS ESC7 - Certificate Authority Privilege Abuse, ADCS ESC4 - Vulnerable Certificate Template ACL

15 techniques observed across 4 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 (2) **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 (8) **Valid Accounts**	T1070 Indicator Removal	T1003.001 LSASS Memory	T1069 Permission Groups Discovery	T1021.002 (1) **Remote Services: SMB/Windows Admin Shares**				
					T1078.002 (1) **Domain Accounts**	T1556.007 Hybrid Identity	T1003.006 (3) **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 Credentials in Files						
							T1552.006 Group Policy Preferences						
							T1555 (2) **Credentials from Password Stores**						
							T1557.001 (4) **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

15 techniques · 4 tactics · 49 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.

PERSISTENCE

T1098	Account Manipulation	2 findings	MEDIUM

PRIVILEGE ESCALATION

T1068	Exploitation for Privilege Escalation	1 finding	HIGH
T1078.002	Domain Accounts	1 finding	HIGH
T1078	Valid Accounts	8 findings	MEDIUM

CREDENTIAL ACCESS

T1003.006	DCSync	3 findings	CRITICAL
T1078.003	T1078.003	1 finding	HIGH
T1210	T1210	1 finding	HIGH
T1555	Credentials from Password Stores	2 findings	HIGH
T1557	T1557	1 finding	HIGH
T1557.001	LLMNR/NBT-NS Poisoning + SMB Relay	4 findings	HIGH
T1649	Steal or Forge Authentication Certificates	16 findings	HIGH
T1558	Steal or Forge Kerberos Tickets	1 finding	MEDIUM
T1558.003	Kerberoasting	2 findings	MEDIUM
T1558.004	AS-REP Roasting	2 findings	MEDIUM

LATERAL MOVEMENT

T1021.002	Remote Services: SMB/Windows Admin Shares	1 finding	MEDIUM

The assessment surfaced 3 critical findings mapped to 15 ATT&CK techniques across 4 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.

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

SECTION 05

05 DORA Compliance

DORA ICT risk management obligations affected by AD security findings.

DORA: Digital Operational Resilience Act

DORA focuses on ICT risk management and operational resilience for financial entities. Active Directory attack paths and identity control gaps indicate where compromise could disrupt critical ICT services and trigger reporting obligations.

8	1	0	9	1
NON-CONFORMANT	PARTIAL	CONFORMANT	CONTROLS ASSESSED	NOT ASSESSED

CERTIFICATION RISK · HIGH

8 major non-conformities identified. Address before the next certification or surveillance audit.

*Conformance of assessed AD-relevant controls only. ADscan evaluates the Active Directory attack surface in scope for this engagement; controls outside that scope are marked **Not assessed** and are excluded from this percentage. This figure is therefore the conformance of what was tested, not an overall framework certification posture.*

ICT RISK MANAGEMENT

6 controls · **5** non-conformant · **0** conformant · **1** not assessed

RESILIENCE & RECOVERY

1 controls · **1** non-conformant · **0** conformant

INCIDENT MANAGEMENT

2 controls · **2** non-conformant · **0** conformant

GOVERNANCE

1 controls · **1** partial · **0** conformant

Non-conformity Summary

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

MAJOR NON-CONFORMITIES

art_9_2	Protection: access control	9.8
art_9_4	Protection: identity & MFA	9.8
art_11	Response and recovery	9.8

MINOR NON-CONFORMITIES / OBSERVATIONS

art_5	Governance and organisation	5.0

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

art_17	ICT-related incident management process	9.8
art_19	Reporting of major ICT-related incidents	9.8
art_9_3	Protection: network security	8.2
art_6	ICT risk management framework	8.1
art_8	Identification	7.5

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.

art_9_2 ICT RISK MANAGEMENT NON-CONFORMANT · MAJOR

Protection: access control

Financial entities must implement access control policies based on least-privilege principles, ensuring that access to systems is granted only as necessary for ...

AFFECTED FINDINGS

- DCSync Privilege Abuse 9.8
- LDAP Signing / Channel Binding Not Hardened 8.1
- LAPS Password Readable by Non-Admins 7.5
- gMSA Password Readable by Non-Admins 7.5
- All Extended Rights Assigned 6.5
- +3 more

art_9_4 ICT RISK MANAGEMENT NON-CONFORMANT · MAJOR

Protection: identity & MFA

Financial entities must implement strong authentication mechanisms. Per Art. 9(4) and Commission Delegated Regulation (EU) 2024/1774, this explicitly requires: ...

AFFECTED FINDINGS

- DCSync Privilege Abuse 9.8
- PrintNightmare Vulnerable Hosts Detected 8.8
- ADCS ESC1 - Misconfigured Certificate Template 8.5
- ADCS ESC13 - Issuance Policy with Group Link Abuse 8.5
- ADCS ESC14 - Weak Explicit Certificate Mapping Abuse 8.5
- +16 more

art_11 RESILIENCE & RECOVERY NON-CONFORMANT · MAJOR

Response and recovery

Financial entities must implement a dedicated ICT business continuity policy that enables rapid response to, and recovery from, major ICT-related incidents. Thi...

AFFECTED FINDINGS

- DCSync Privilege Abuse 9.8
- PrintNightmare Vulnerable Hosts Detected 8.8
- Obsolete Operating Systems 7.5

art_17 INCIDENT MANAGEMENT NON-CONFORMANT · MAJOR

ICT-related incident management process

Financial entities must define, establish and implement an ICT-related incident management process to detect, manage and notify ICT-related incidents. This is t...

AFFECTED FINDINGS

- DCSync Privilege Abuse 9.8
- PrintNightmare Vulnerable Hosts Detected 8.8
- ADCS ESC1 - Misconfigured Certificate Template 8.5

art_19 INCIDENT MANAGEMENT NON-CONFORMANT · MAJOR

Reporting of major ICT-related incidents

Financial entities must report major ICT-related incidents to the relevant competent authority. Per Art. 19 and Commission Delegated Regulation (EU) 2025/301, t...

AFFECTED FINDINGS

- DCSync Privilege Abuse 9.8
- PrintNightmare Vulnerable Hosts Detected 8.8
- ADCS ESC1 - Misconfigured Certificate Template 8.5

art_9_3 ICT RISK MANAGEMENT NON-CONFORMANT · MAJOR

Protection: network security

Financial entities must have in place security measures against network intrusions and data misuse. This includes network segmentation, perimeter protections, a...

AFFECTED FINDINGS

- ADCS ESC8 - NTLM Relay to Web Enrollment 8.2
- LDAP Signing / Channel Binding Not Hardened 8.1
- Unsigned SMB Relay Targets Detected 6.8
- SMBv1 Protocol Enabled (Legacy Posture) 5.5
- SMB Signing Not Required 5.0

art_6 ICT RISK MANAGEMENT NON-CONFORMANT · MAJOR

ICT risk management framework

Financial entities must have a sound, comprehensive and well-documented ICT risk management framework as part of their overall risk management system. The frame...

AFFECTED FINDINGS

- LDAP Signing / Channel Binding Not Hardened 8.1
- Obsolete Operating Systems 7.5
- AS-REP Roasting 6.9
- SMBv1 Protocol Enabled (Legacy Posture) 5.5
- Kerberoasting 5.3
- +4 more

art_8 ICT RISK MANAGEMENT NON-CONFORMANT · MAJOR

Identification

Financial entities must identify, classify and adequately document all ICT supported business functions, roles and responsibilities, information assets and ICT ...

AFFECTED FINDINGS

- Obsolete Operating Systems 7.5

art_5 GOVERNANCE PARTIALLY CONFORMANT · MINOR

Governance and organisation

The management body of the financial entity must define, approve, oversee and be accountable for the implementation of all arrangements related to the ICT risk ...

AFFECTED FINDINGS

- Accounts with Password Not Required Flag 5.0
- Accounts with Non-Expiring Passwords 3.7
- Enabled Stale User Accounts Detected 3.5

art_10 ICT RISK MANAGEMENT NOT ASSESSED

Detection

Financial entities must have mechanisms to promptly detect anomalous activities, including ICT network performance and ICT-related incidents. Detection mechanis...

Outside the scope of this AD assessment. Not assessed.

SECTION 06

06 Remediation Roadmap

Prioritised action plan to reduce risk across the environment.

IMMEDIATE · 0-30 DAYS

Contain critical exposure

- **DCSync Privilege Abuse** · essos.local · CVSS 9.8
- **DCSync Privilege Abuse** · sevenkingdoms.local · CVSS 9.8
- **DCSync Privilege Abuse** · north.sevenkingdoms.local · CVSS 9.8
- **PrintNightmare Vulnerable Hosts Detected** · essos.local · CVSS 8.8
- **ADCS ESC9 - No Security Extension on Certificate Template** · essos.local · CVSS 8.5
- **ADCS ESC14 - Weak Explicit Certificate Mapping Abuse** · essos.local · CVSS 8.5
- **ADCS ESC1 - Misconfigured Certificate Template** · essos.local · CVSS 8.5
- **ADCS ESC13 - Issuance Policy with Group Link Abuse** · essos.local · CVSS 8.5
- **ADCS ESC2 - Any Purpose Certificate Template** · essos.local · CVSS 8.5
- **ADCS ESC3 - Enrollment Agent Template Abuse** · essos.local · CVSS 8.5
- **ADCS ESC5 - Vulnerable CA Object ACL** · essos.local · CVSS 8.5
- **ADCS ESC7 - Certificate Authority Privilege Abuse** · essos.local · CVSS 8.5
- **ADCS ESC4 - Vulnerable Certificate Template ACL** · essos.local · CVSS 8.5
- **ADCS ESC14 - Weak Explicit Certificate Mapping Abuse** · sevenkingdoms.local · CVSS 8.5
- **ADCS ESC5 - Vulnerable CA Object ACL** · sevenkingdoms.local · CVSS 8.5
- **ADCS ESC7 - Certificate Authority Privilege Abuse** · sevenkingdoms.local · CVSS 8.5
- **ADCS ESC8 - NTLM Relay to Web Enrollment** · essos.local · CVSS 8.2
- **ADCS ESC8 - NTLM Relay to Web Enrollment** · sevenkingdoms.local · CVSS 8.2
- **LDAP Signing / Channel Binding Not Hardened** · essos.local · CVSS 8.1
- **ADCS ESC11 - NTLM Relay to RPC Certificate Enrollment** · essos.local · CVSS 8.0
- **Domain Admin Sessions on Non-Privileged Hosts** · essos.local · CVSS 8.0
- **ADCS ESC11 - NTLM Relay to RPC Certificate Enrollment** · sevenkingdoms.local · CVSS 8.0
- **gMSA Password Readable by Non-Admins** · essos.local · CVSS 7.5
- **LAPS Password Readable by Non-Admins** · essos.local · CVSS 7.5
- **SMBv1 Protocol Enabled** · essos.local · CVSS 7.5
- **Obsolete Operating Systems** · essos.local · CVSS 7.5
- **LAPS Not Deployed on Domain Hosts (Posture)** · essos.local · CVSS 7.0

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

SHORT-TERM · 30-90 DAYS

Reduce attack surface

- **AS-REP Roasting** · essos.local · CVSS 6.9
- **AS-REP Roasting** · north.sevenkingdoms.local · CVSS 6.9
- **Unsigned SMB Relay Targets Detected** · essos.local · CVSS 6.8
- **All Extended Rights Assigned** · essos.local · CVSS 6.5
- **SMBv1 Protocol Enabled (Legacy Posture)** · essos.local · CVSS 6.5
- **Force Change Password Rights Assigned** · sevenkingdoms.local · CVSS 6.5
- **Constrained Kerberos Delegation Misconfiguration** · north.sevenkingdoms.local · CVSS 6.5
- **Kerberoasting** · essos.local · CVSS 5.3
- **Kerberoasting** · north.sevenkingdoms.local · CVSS 5.3
- **SMB Signing Not Required** · essos.local · CVSS 5.0
- **Accounts with Password Not Required Flag** · essos.local · CVSS 5.0
- **SMB Signing Not Required** · north.sevenkingdoms.local · CVSS 5.0

LONG-TERM · 90+ DAYS

Harden baseline

- **Accounts with Non-Expiring Passwords** · essos.local
- **Accounts with Non-Expiring Passwords** · sevenkingdoms.local
- **Accounts with Non-Expiring Passwords** · north.sevenkingdoms.local
- **Machine Account Quota Allows Domain Join** · essos.local
- **Passwords Predating Current Policy** · essos.local
- **Enabled Stale User Accounts Detected** · essos.local
- **Machine Account Quota Allows Domain Join** · sevenkingdoms.local
- **Passwords Predating Current Policy** · sevenkingdoms.local
- **Machine Account Quota Allows Domain Join** · north.sevenkingdoms.local
- **Passwords Predating Current Policy** · north.sevenkingdoms.local

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