ADscan | CLIENT DELIVERABLE KIT

ACTIVE DIRECTORY HARDENING PLAYBOOK

Your *30-day* path from findings to a hardened domain.

Built from the 23 findings ADscan confirmed against north.sevenkingdoms.local, sequenced into shippable work and mapped to the compliance controls each one closes.

FINDINGS	CRITICAL / HIGH	REMEDIATION WINDOW	FRAMEWORKS MAPPED
23	11	30 days	6

PREPARED

Confidential

November 16, 2026
Scope: north.sevenkingdoms.local

prepared for the named engagement

Where your domain is *exposed*, and what to ship first.

100% of standard user accounts (8 of 8) hold a reachable path to full domain compromise. 7 reachable route(s) to full domain compromise.

This engagement against north.sevenkingdoms.local surfaced 23 confirmed findings, 3 of which sit on a validated path to full domain compromise. The remaining findings widen the attack surface without, on their own, completing that path.

The highest-confidence fix, proven in this environment, is Service Account Credential Theft (Kerberoasting) on sql_svc, jon.snow (finding F-005, Kerberoasting, ADscan Priority 8): it breaks the most validated attack paths ADscan walked against your domain. Close it first; the remaining findings follow on the 30-day roadmap below, in this same remediation order.

These findings map to 73 distinct controls across ISO 27001:2022, DORA, ENS, NIS2, PCI DSS 4.0, CIS Windows Server. The compliance-gap summary on this page lists the exact control codes each finding leaves open, so the roadmap doubles as an audit-remediation register.



CRITICAL · 2 (9%) HIGH · 9 (39%) MEDIUM · 11 (48%) LOW · 1 (4%)

CONFIRMED FINDINGS

23

surfaced in this engagement, de-duplicated across scope.

FINDINGS ON A VALIDATED PATH

3

findings whose technique sits on a path to full domain compromise, confirmed by configuration. Routes where only the entry step is proven and the chain is not walked end to end (partially validated) are detailed in the Security Assessment Report.

TOP EXPOSURE

Service Account Credential Theft (Kerberoasting)

F-005 · ADscan Priority 8 · close it first.

Week one. *Remediation order first.* The rest is in the full playbook.

W1 Break the validated attack paths first. These are the fixes ADscan proved reduce exposure most.

DAY 1–7

Path-breaker 1 of 3 HIGH **Kerberoasting**

sql_svc

Where possible, migrate the SPN to a Group Managed Service Account (gMSA), whose machine-managed password rotates automatically and resists offline cracking (see the detailed runbook)

OWNER / DONE

Path-breaker 2 of 3 HIGH **Constrained Kerberos Delegation Misconfiguration**

castelblack.north.sevenkingdoms.local (192.168.180.22)

Audit msDS-AllowedToDelegateTo attributes and remove any delegations to sensitive services such as CIFS, LDAP, or HOST on Domain Controllers

OWNER / DONE

Path-breaker 3 of 3 MEDIUM **AS-REP Roasting**

brandon.stark

Re-enable Kerberos pre-authentication on the affected account: clear the DONT_REQ_PREAUTH flag with Set-ADAccountControl -Identity brandon.stark -DoesNotRequirePreAuth $false (see the detailed runbook)

OWNER / DONE

PREVIEW · THE OPENING OF THE FULL PLAYBOOK

The full 30-day plan continues with *weeks 2–4*.

This preview shows the cover, the executive narrative, and the first week of the 30-day plan. The full **AD Hardening Playbook** continues with a step-by-step remediation runbook for every finding, six tactic chapters (Credential Access, Privilege Escalation, Lateral Movement, Persistence, Defense Evasion, Initial Access), the compliance controls your findings leave open, and the remaining prioritized actions across weeks 2, 3 and 4, each paired with its re-test command.

Request the full PDF at adscanpro.com/samples and we will send it to you.