BONUS · ACTIVE DIRECTORY HARDENING PLAYBOOK

From assessment to hardening in 30 days.

> A founder-led, opinionated playbook for the six tactics that account for 80% of confirmed Active Directory breaches — paired with a 30-day calendar your team can ship.

$497 value

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

included free with ADscan

The work most teams skip is the work that breaks the domain.

Most Active Directory environments do not fail audits for lack of tooling. They fail because hygiene work is everyone's job, and therefore nobody's job. The findings repeat across every engagement: an SPN account with a 2014 password, a stale Kerberos pre-auth flag, an ACL nobody can explain. Each is trivial. Combined, they break the domain by Tuesday.

Of every hundred reported breaches against AD, eighty follow one of five attack paths: kerberoast a service account, AS-REP roast a forgotten user, relay coerced authentication, abuse an ACL nobody audited, or chain a delegation to DCSync. This playbook treats those five paths as the work — the rest is decoration.

Read the six chapters back-to-back, then run the 30-day calendar in order. Pair every action with a re-scan in ADscan to prove the path closed. If a chapter feels too obvious, you are exactly the team that has the unpatched version of it in production today.

> Tight, opinionated, and built to ship in 30 days. Not 30 weeks.

30-DAY ACTION CALENDAR · SHIP IN ORDER

Week 1 preview. Six actions. Then it gets serious.

1 WEEK 1 · DAY 1–7

☐	Reset every SPN account password to 30+ char random.	`adscan ci --kerberoast`	CREDENTIAL ACCESS
☐	Enable Kerberos pre-auth on every human account.	`adscan ci --asreproast`	CREDENTIAL ACCESS
☐	Audit Domain Admins / Enterprise Admins / krbtgt membership.	`adscan start`	PRIVILEGE ESCALATION
☐	Empty Backup / Server / Account Operators groups.		PRIVILEGE ESCALATION
☐	Rotate krbtgt twice with a 24h gap.		PERSISTENCE
☐	Set ms-DS-MachineAccountQuota to 0 domain-wide.		LATERAL MOVEMENT
☐	Re-scan with ADscan and confirm no kerberoast / AS-REP findings.	`adscan ci`	VALIDATION

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

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 calendar. The full **AD Hardening Playbook** continues with six tactic chapters (Credential Access, Privilege Escalation, Lateral Movement, Persistence, Defense Evasion, Initial Access) and the remaining 22 prioritized actions across weeks 2, 3 and 4 — paired with re-test commands.

> Get the complete 30-day plan with control checklists and post-engagement re-test guidance.

Drop your email at `adscanpro.com/samples/ad-hardening-playbook` and we will send you the full PDF.

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