ADscan

$197 value · included

Fifteen commands. One domain. Ninety seconds.

Print this sheet, fold it once, keep it next to the keyboard. Every command is real. Every command works on the day you install ADscan.

01 RECON

`adscan check`

Verify host prerequisites — Docker, disk, RAM, network resolvers.

`adscan demo`

60-second deterministic scan against a baked-in fake AD; produces a real PDF.

`adscan welcome`

Editorial dashboard — last scan posture, latest workspace, next moves.

`adscan version`

Print the runtime tag — match it against the launcher before reporting bugs.

`adscan check --fix`

Auto-remediate the launcher prerequisites the preflight just flagged.

02 AUTH & ENUM

`adscan start`

Interactive workbench — guided credentials, target picker, live enumeration.

`adscan tui`

Textual TUI — split-pane attack-graph, finding inspector, command relay.

`adscan tui --demo`

Boot the TUI on top of the deterministic demo workspace, no scan needed.

`adscan ci`

One-shot non-interactive scan — perfect for nightly cron and re-baselines.

`adscan ci --verbose`

Same flow with full per-tool stdout — for triage and bug reports.

03 EXPLOIT & REPORT

`adscan report`

Re-render the PDF from an existing workspace — premium template by default.

`adscan playbook`

Generate the AD Hardening Playbook bonus — 12-page 30-day plan.

`adscan checklist`

Generate the MITRE Remediation Checklist bonus — auditor-grade sign-off PDF.

`adscan cheatsheet`

Re-print this sheet — keep one at every operator desk.

`adscan update`

Pull the latest container image and refresh the host launcher in one shot.

Two hands on the keyboard. Zero clicks.

The ADscan TUI was built so a pentester never has to leave the keyboard during an engagement. Memorize ten bindings; the rest auto-discover.

GLOBAL · NAVIGATION

F1	Help overlay — context-aware bindings for the focused pane.
F2	Switch workspace — fuzzy picker over every recent scan.
F3	Findings table — sort, filter, and pivot to attack-path graph.
F4	Attack-path graph — Cytoscape view of every confirmed kill chain.
F5	Re-render report — produces a fresh PDF without re-scanning.
Ctrl-K	Command palette — every TUI action by name, like VS Code.
Ctrl-L	Toggle log pane — tail the runtime log as the scan runs.

INSPECTOR · ACTION

Enter	Open the focused finding or attack-path step in the inspector.
/	Inline filter — type to narrow the table, Esc to clear.
y	Yank the selected technique ID, command, or principal to the clipboard.
r	Replay the underlying tool with verbose output for triage.
m	Mitigate — mark a finding as mitigated and re-score posture.
Ctrl-G	Jump to the BloodHound graph node corresponding to the focused row.
Ctrl-Q	Quit safely — flushes telemetry and the workspace state file.

WHEN THINGS BREAK · FIVE FAST FIXES

SYMPTOM	LIKELY CAUSE	FAST FIX
KRB_AP_ERR_SKEW	Host clock is >5 min off the DC.	sudo ntpdate <dc-ip> · ADscan auto-syncs and retries.
STATUS_NOT_SUPPORTED	NTLM disabled on the target.	Pass --kerberos / -k everywhere; resolve the FQDN, not the IP.
strongerAuthRequired	LDAP signing or channel binding is enforced.	Use LDAPS (636) — ADscan auto-falls back when 636 is reachable.
Connection refused :636	LDAPS is not exposed on the DC.	Set use_ldaps=True; ADscan downgrades to LDAP transparently.
SERVER_DOWN / DNS	Container cannot resolve the AD domain.	Pass --dns-server <dc-ip> or add a host entry to ~/.adscan/hosts.