METHODOLOGY CHEAT SHEET

PTES — Adapted for Internal AD Assessment

Engagement: **Q2 2026 NavSec Corp Internal Pentest** | Domain: **navigatingsecurity.corp** | Target: **DC01 (10.1.1.10)** | Starting User: **t.chigubhu (Domain Users)**

PHASE 01
IntelligenceGathering

Key Questions

- What OS is DC01 running?
- Who are the Domain Admins?
- Any SPNs? Delegations?
- ADCS templates present?
- What's in SYSVOL?

Tools

Nmap, BloodHound, ADRecon, PowerView, ldapsearch

Output

- Host/port inventory
- AD user/group map
- SPN list
- Trust map (none expected)

PHASE 02
VulnerabilityAnalysis

Key Questions

- Kerberoastable accounts?
- AS-REP roastable users?
- Weak password policy?
- ADCS ESC1–ESC8 present?
- GPP passwords in SYSVOL?

Tools

Rubeus, Certify, CrackMapExec, GPP-decrypt, BloodHound queries

Output

- Vulnerability list (pre-exploit)
- Attack path map
- Risk prioritization

PHASE 03
Exploitation

Key Questions

- Can I crack these hashes?
- Does relay work against DC01?
- Can I abuse DACL perms?
- Does CrowdStrike catch this?

Tools

Hashcat, Responder, ntlmrelayx, Impacket, Rubeus

Output

- Confirmed vulnerabilities
- Captured credentials
- Initial foothold evidence
- EDR detection results

PHASE 04
Post-Exploitation

Key Questions

- Can I reach Domain Admin?
- DCSync possible?
- ADCS cert abuse viable?
- What sensitive data exposed?
- Persistence mechanisms?

Tools

Mimikatz, Impacket secretsdump, Certify, SharpHound

Output

- Privilege escalation chain
- Domain compromise evidence
- Sensitive data access proof
- Full attack narrative

PHASE 05
Cleanup

Key Questions

- All tools removed from DC01?
- C2 sessions terminated?
- DACL changes reverted?
- Kerberos tickets expired?
- Any un-removable artifacts?

Tools

Manual verification, artifact checklist

Output

- Cleanup confirmation log
- Un-removable artifact list
- Handoff to Client IT

PHASE 06
Reporting

Key Questions

- Is every finding evidenced?
- CVSS scores assigned?
- Attack narrative clear?
- Remediation actionable?
- Exec summary non-technical?

Tools

SysReptor, Flameshot, CVSS Calculator

Output

- Draft report (PDF)
- Final report (PDF)
- Executive summary
- Evidence package (ZIP)
- Readout slide deck

Remember: Enumerate the right things first, not everything. Follow paths to business-critical access. Document as you go; timestamps, commands, output, screenshots, context notes.