ANNOTATED TARGET LIST

Internal Network & Active Directory Penetration Test

Client	Navigating Security Corp.
Provider	TadiSec
Associated SOW	TDSC-SOW-2026-001
Associated ROE	TDSC-ROE-2026-001
Version	1.0
Date Issued	March 12, 2026
Prepared By	Rumbidzai Moyo, Principal Consultant
Classification	Confidential

How to Use This Document

This annotated target list identifies the single in-scope system for the NavSec Corp engagement. Annotations highlight testing priorities, caution areas, and ROE constraints. Cross-reference against SOW Section 5 and ROE Section 3.

⚠ = Extra caution or specific testing constraint.

▸ = Standard tester guidance and enumeration priorities.

1. Scope Summary

This engagement is scoped to a single Active Directory domain controller. TadiSec may perform host discovery scanning across the 10.1.1.0/24 subnet for network mapping purposes, but only DC01 is authorized for enumeration, exploitation, and interaction. All other discovered hosts are out of scope.

Parameter	Value
Domain	navigatingsecurity.corp
Network Range (mapping only)	10.1.1.0/24
In-Scope Target	DC01
Domain Controller(s)	1 (DC01)
Forest / Domain Functional Level	Windows Server 2016
Testing Perspective	Assumed Breach - t.chigubhu (Domain Users)
Testing Window	March 24 – April 3, 2026

Blackout Period	March 30–31, 2026 (month-end)
EDR	Windows Defender (passive scanning)

2. In-Scope Target: DC01

IP Address	Hostname	Role	Annotations
10.1.1.10	DC01	Domain Controller	▸ *Windows Server 2019. Hosts AD DS, DNS, DHCP, and ADCS (single-tier enterprise CA). All domain authentication flows through this host.* ▸ *Enumerate: Users, groups, OUs, GPOs, ACLs, SPNs, ADCS certificate templates (ESC1–ESC8), LAPS configuration, DNS zones, delegation settings, SYSVOL contents.* ▸ *Kerberoast all SPNs. Check for AS-REP roastable accounts. Enumerate ADCS for certificate abuse vectors.* ▸ *DCSync and NTLM relay are authorized but require real-time notification to Aarav Patel per ROE Section 6.3.* ▸ *Test Windows Defender detection against: BloodHound/SharpHound, Rubeus, Mimikatz, Impacket tools. Document what gets caught vs. what evades.* ⚠ *SINGLE DC ENVIRONMENT. If DC01 goes down, ALL domain authentication, DNS, and DHCP stops across the entire subnet. Exercise extreme caution with exploit payloads. Avoid memory-heavy operations that could destabilize LSASS. Do not restart any services without explicit approval from Aarav Patel.* ⚠ *ADCS may be installed directly on DC01. Certificate abuse carries elevated risk on the sole domain controller. Notify before any certificate request exploitation.* ⚠ *Do not modify AD schema, domain functional level, replication topology, or GPOs without written pre-approval.*

3. Out-of-Scope Systems

EVERYTHING EXCEPT DC01 IS OUT OF SCOPE

TadiSec may perform host discovery scanning across 10.1.1.0/24 for network mapping, but all hosts other than DC01 are prohibited targets. Do not scan ports, enumerate services, exploit, or interact

with any host other than DC01. If host discovery reveals other live systems, document them in the report as informational context but do not engage.

System / Range	Reason	Action if Encountered
All hosts on 10.1.1.0/24 except DC01	Not authorized - DC01-only engagement	Document in report as informational. Do not interact.
10.1.1.1 (Network Gateway)	Network infrastructure - disruption risk	Do not scan or interact.
Any IP outside 10.1.1.0/24	Not authorized	Do not scan. Report unexpected routing.
Azure AD / Microsoft 365 / Cloud	Not in scope	Do not attempt cloud authentication.

Boundary Rule

If an attack path leads to or through a non-DC01 host, stop exploitation at the boundary. Document the path as a finding. Notify Aarav Patel (Technical POC). Written authorization from Oliver Whitaker required to extend scope.

4. Assumed Breach Starting Position

Parameter	Value
User Account	t.chigubhu (Tonderai Chigubhu)
Role / Title	TadiSec Lead Tester (using provisioned domain account)
Domain Group Membership	Domain Users only - no elevated privileges
Tester Workstation	Hostname & IP TBD
Objective	Escalate from Domain Users to Domain Admin or equivalent via DC01

All privilege escalation must be achieved through discovered vulnerabilities and misconfigurations on DC01 and within the navigatingsecurity.corp AD domain. No interaction with other hosts is permitted.

5. Pre-Engagement Clarification Points

Resolve during kickoff on March 23, 2026. Answers recorded by Rumbidzai Moyo.

#	Question	Answer

1	Confirm ADCS is installed on DC01. Standalone or enterprise CA?	TBD
2	Is LAPS deployed and enforced across the domain?	Deployed domain-wide - verify during testing
3	Windows Defender: Active blocking on DC01? Any reduced policies?	Active blocking; server policy TBC at kickoff
4	Current account lockout policy settings?	5 attempts / 30-min window / auto-unlock
5	Does the environment have a SIEM? Which product?	Splunk Cloud - SOC monitors via Splunk
6	Any service accounts we should be cautious with?	TBC at kickoff
7	Scheduled jobs or maintenance during testing hours?	Nightly backups at 2:00 AM; month-end batch March 30–31
8	Domain functional level confirmed at 2016? Any planned changes?	2016 confirmed; no changes planned

6. Annotation Legend

Symbol	Meaning
▸	Standard annotation - testing guidance, enumeration priorities, or areas of interest
⚠	Caution - elevated risk of disruption, data sensitivity, or specific ROE constraint

- End of Annotated Target List -