Executive Summary

An internal Active Directory assessment was conducted from a domain-joined Windows workstation to evaluate authentication and Kerberos attack paths using a TDNA-aligned methodology. The environment was found to be hardened against Kerberoasting due to the absence of user-based service accounts with registered Service Principal Names (SPNs). No immediate credential exposure or Kerberos-based privilege escalation paths were identified. This report represents a secure baseline configuration used for comparison against intentionally misconfigured environments.

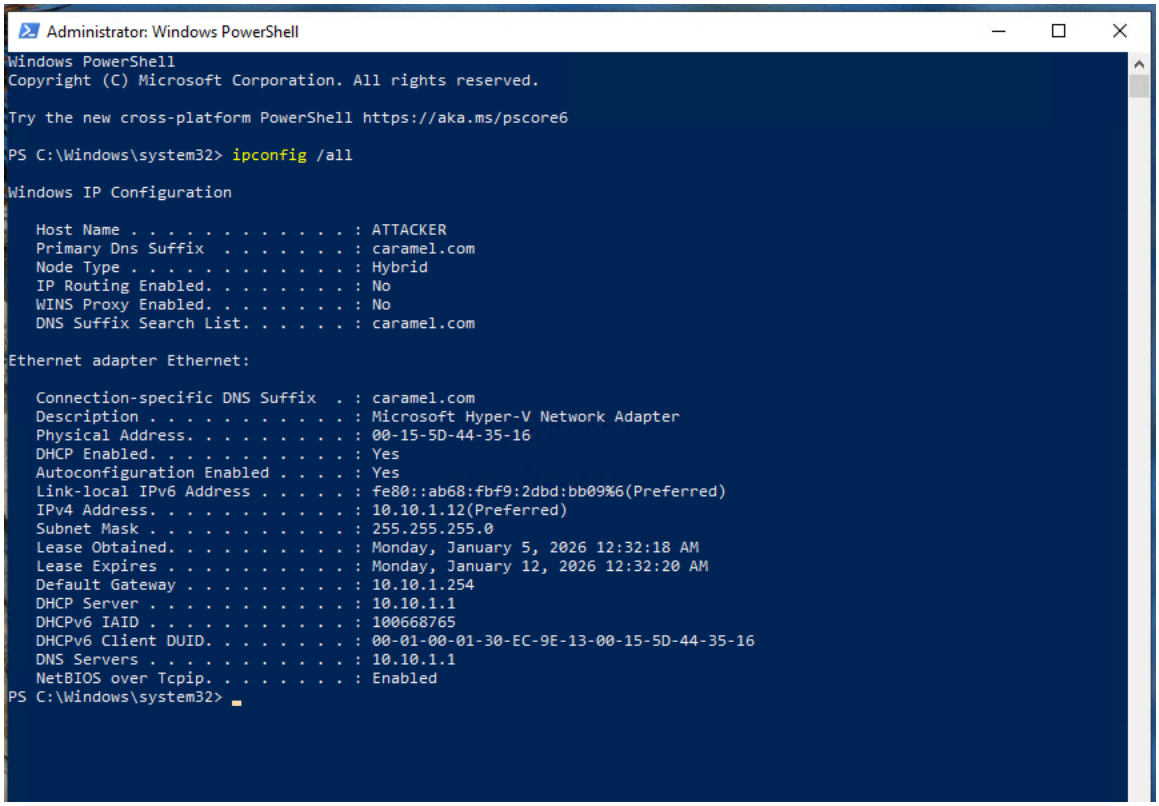
Active Directory Internal Assessment Notes

Engagement Context

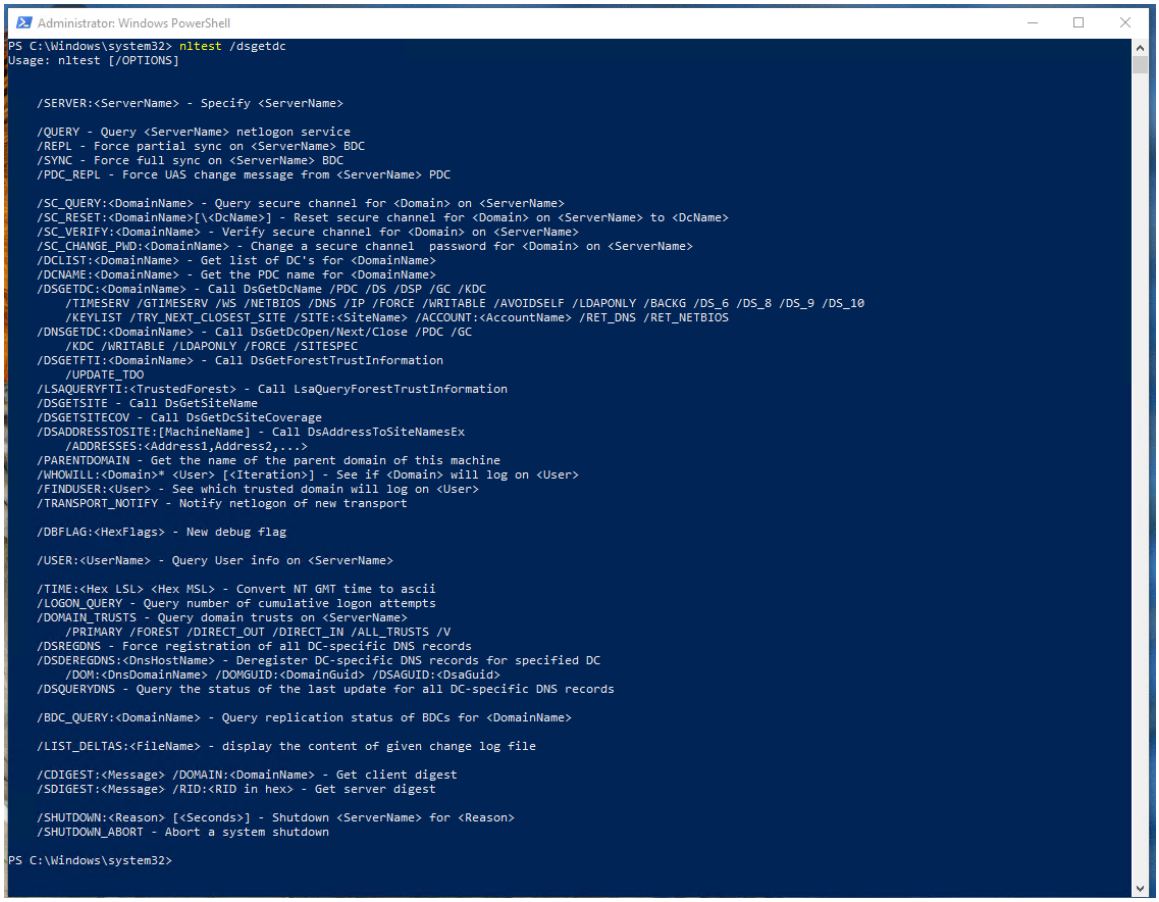
Assessment Type: Internal Active Directory Security Assessment
Attacker Context: Domain-joined Windows workstation (ATTACKER)
Objective: Identify AD misconfigurations enabling credential compromise or privilege escalation
Methodology: TDNA-aligned (Trust → Directory → Network → Authentication)

Phase 1 – Environment & Trust Validation

Network positioning validated using ipconfig /all.



Domain discovery performed with nltest /dsgetdc.

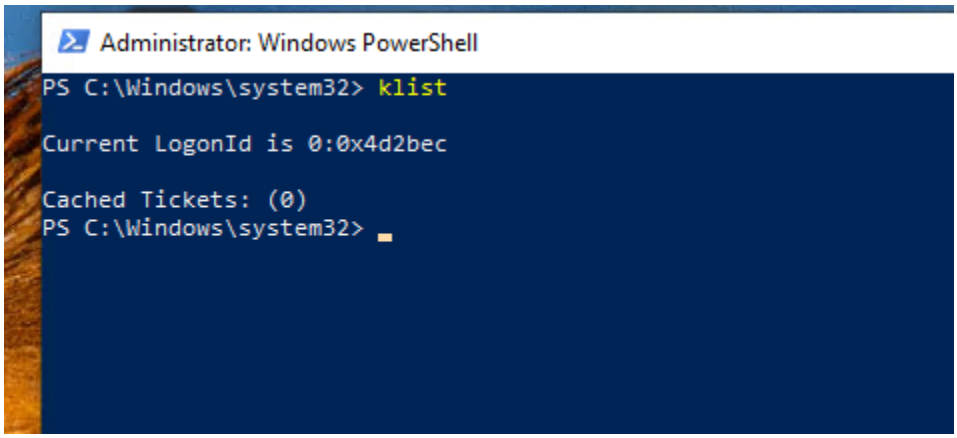


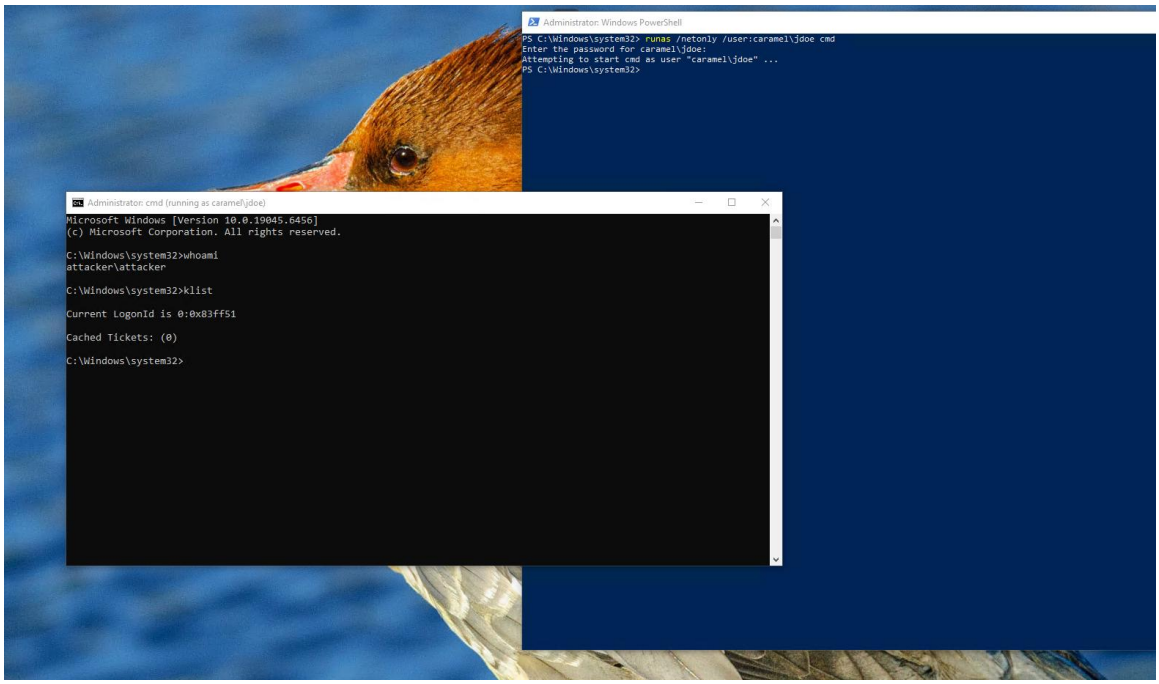
Trust enumeration confirmed single forest with no external trusts.

Phase 2 – Authentication & Kerberos Reconnaissance

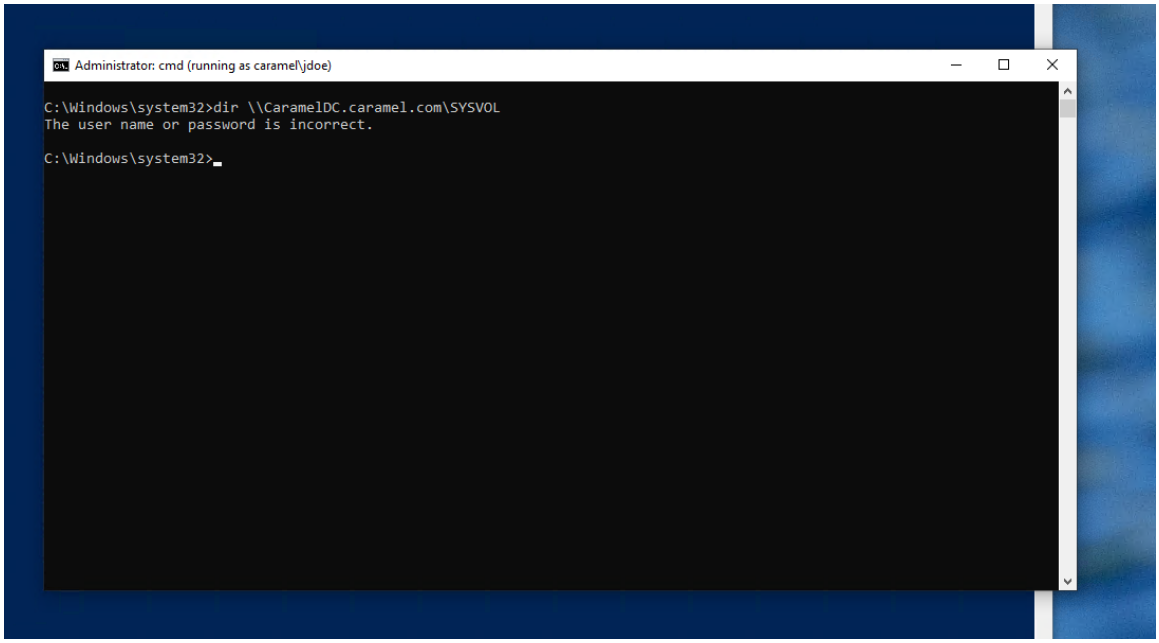
Identity context validated using whoami and klist.

Kerberos tickets observed via runas /netonly.

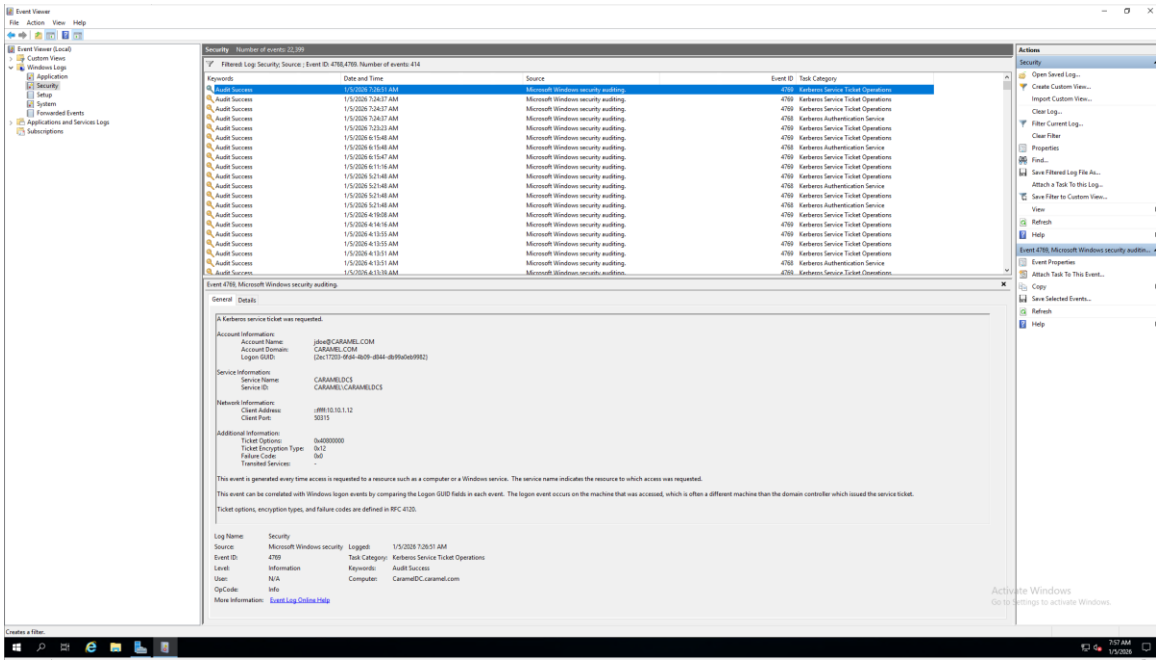




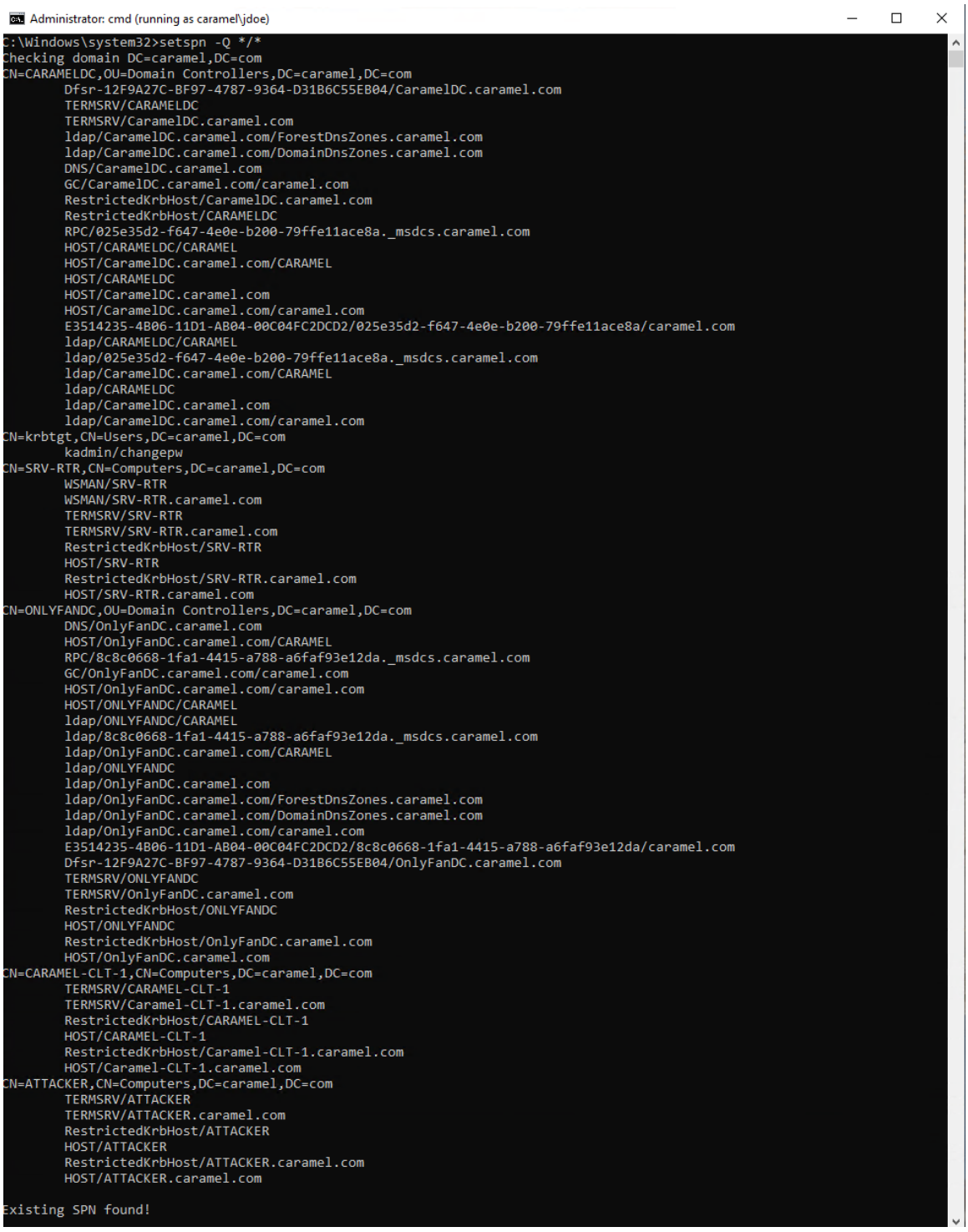
SYSVOL access tested and confirmed.



Kerberos-related Security Event IDs (4768, 4769) reviewed.



SPN enumeration conducted using setspn -Q */*.



Key Findings

No user-based service accounts with SPNs were identified.

Domain appears secure by default against Kerberoasting.

No immediate privilege escalation paths identified.

Kerberoasting Feasibility Assessment

During testing, Service Principal Name (SPN) enumeration was performed across the domain. All identified SPNs were bound to computer accounts (domain controllers, member servers, and workstations). No user-based service accounts with associated SPNs were identified.

As a result, Kerberoasting attacks are not applicable in the current Active Directory configuration. The environment is considered hardened against Kerberoasting due to the absence of long-lived, user-managed service accounts with Kerberos service tickets that could be requested and cracked offline.