

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

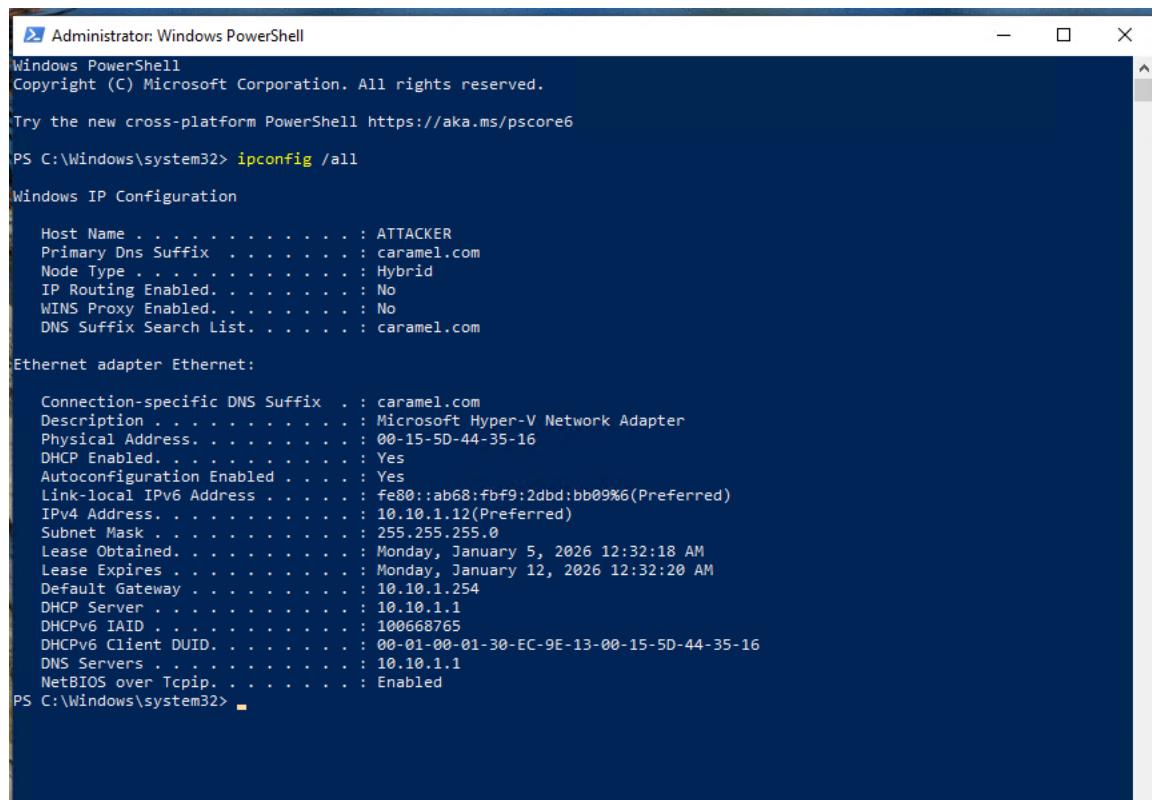
Attacker Context: Domain-joined Windows workstation (ATTACKER)

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.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> ipconfig /all

Windows IP Configuration

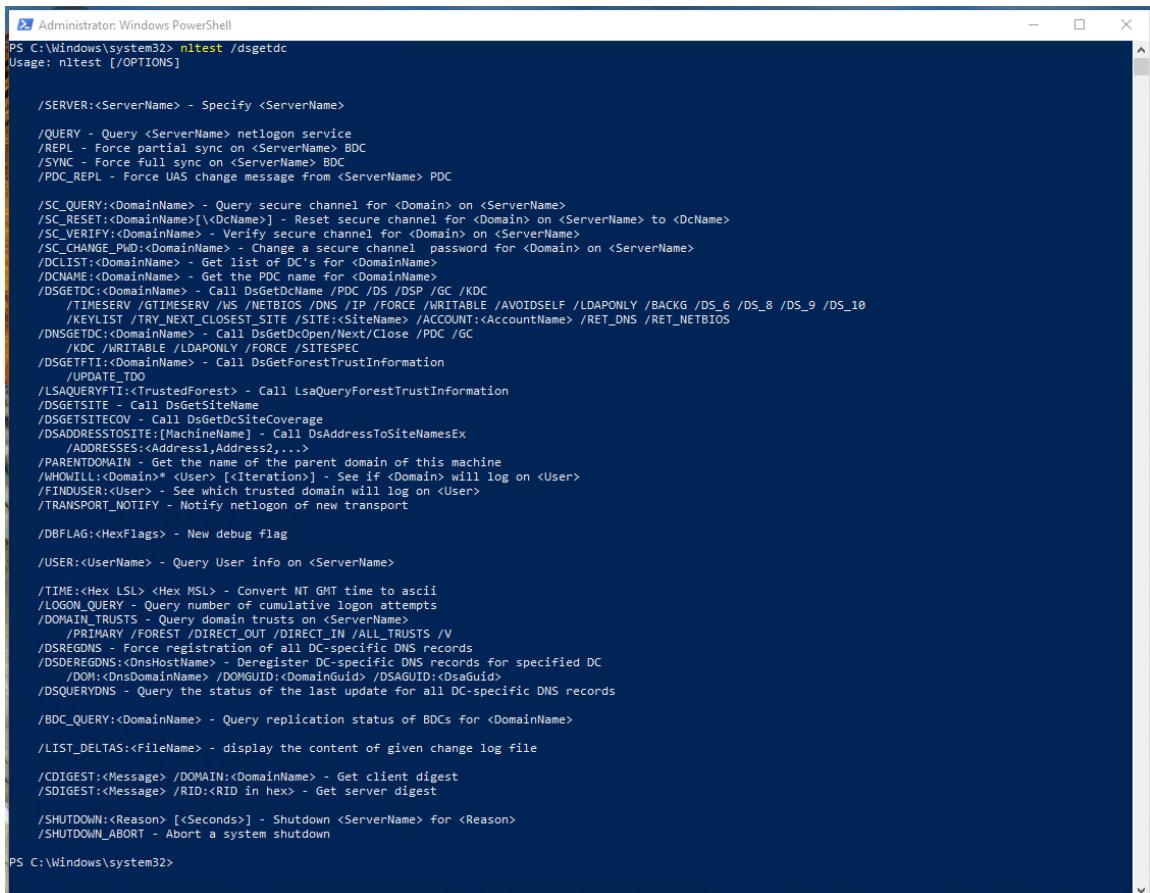
Host Name . . . . . : ATTACKER
Primary Dns Suffix . . . . . : caramel.com
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : caramel.com

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : caramel.com
Description . . . . . : Microsoft Hyper-V Network Adapter
Physical Address. . . . . : 00-15-5D-44-35-16
DHCP Enabled . . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::ab68:fbf9:2dbd:bb09%6(PREFERRED)
IPv4 Address . . . . . : 10.10.1.12(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, January 5, 2026 12:32:18 AM
Lease Expires . . . . . : Monday, January 12, 2026 12:32:20 AM
Default Gateway . . . . . : 10.10.1.254
DHCP Server . . . . . : 10.10.1.1
DHCPv6 IAID . . . . . : 100668765
DHCPv6 Client DUID. . . . . : 00-01-00-01-30-EC-9E-13-00-15-5D-44-35-16
DNS Servers . . . . . : 10.10.1.1
NetBIOS over Tcpip. . . . . : Enabled

PS C:\Windows\system32>
```

Domain discovery performed with nlttest /dsgetdc.



```
Administrator: Windows PowerShell
PS C:\Windows\system32> nlttest /dsgetdc
Usage: nlttest [/OPTIONS]

/SERVER:<ServerName> - Specify <ServerName>
/QUERY - Query <ServerName> netlogon service
/REPL - Force partial sync on <ServerName> BDC
/SYNC - Force full sync on <ServerName> BDC
/PDC_REPL - Force PDC UAS change message from <ServerName> PDC

/SC_QUERY:<DomainName> - Query secure channel for <Domain> on <ServerName>
/SC_RESET:<DomainName>\<DcName> - Reset secure channel for <Domain> on <ServerName> to <DcName>
/SC_VERIFY:<DomainName> - Verify secure channel for <Domain> on <ServerName>
/SC_CHANGE_PWD:<DomainName> - Change a secure channel password for <Domain> on <ServerName>
/DCLIST:<DomainName> - Get list of DC's for <DomainName>
/DCNAME:<DomainName> - Get the PDC name for <DomainName>
/DSGETDC:<DomainName> - Call DsGetDcName /PDC /DS /DSP /GC /KDC
    /TIMESERV /GTIMESERV /WS /NETBIOS /DNS /IP /FORCE /WRITABLE /AVOIDSELF /LDAPONLY /BACKG /DS_6 /DS_8 /DS_9 /DS_10
    /KEYLIST /TRY_NEXT_CLOSEST_SITE /SITE:<SiteName> /ACCOUNT:<AccountName> /RET_DNS /RET_NETBIOS
/DSGETDC:<DomainName> - Call DsGetDcOpen/Next/Close /PDC /GC
    /KDC /WRITABLE /LDAPONLY /FORCE /SITESPEC
/DSGETFTI:<DomainName> - Call DsGetForestTrustInformation
    /UPDATE_TDO
/LSAQUERYFTI:<TrustedForest> - Call LsaQueryForestTrustInformation
/DSGETSITE - Call DsGetSiteName
/DSGETSITECOV - Call DsGetCsSiteCoverage
/DSADDRESSTOSITE:[<MachineName>] - Call DsAddressToSiteNamesEx
    /ADDRESSES:<Address1,Address2,...>
/PARENTDOMAIN - Get the name of the parent domain of this machine
/WHO WILL:<Domain>*<User> [<Iteration>] - See if <Domain> will log on <User>
/FINDUSER:<User> - See which trusted domain will log on <User>
/TRANSPORT_NOTIFY - Notify netlogon of new transport

/DBFLAG:<HexFlags> - New debug flag

/USER:<UserName> - Query User info on <ServerName>

/TIME:<Hex LSL> <Hex MLS> - Convert NT GMT time to ascii
/LOGON_QUERY - Query number of cumulative logon attempts
/DOMAIN_TRUSTS - Query domain trusts on <ServerName>
    /PRIMARY /FOREST /DIRECT_OUT /DIRECT_IN /ALL_TRUSTS /V
/DSREGDNS - Force registration of all DC-specific DNS records
/DSDEREGDNS:<OnHostName> - Deregister DC-specific DNS records for specified DC
    /DOM:<DsDomainName> /DOMGUID:<DomainGuid> /DSAGUID:<DsGuid>
/DSQUERYDNS - Query the status of the last update for all DC-specific DNS records

/BDC_QUERY:<DomainName> - Query replication status of BDCs for <DomainName>

/LIST_DELTAS:<FileName> - display the content of given change log file

/CDIGEST:<Message> /DOMAIN:<DomainName> - Get client digest
/SDIGEST:<Message> /RID:<RID in hex> - Get server digest

/SHUTDOWN:<Reason> [<Seconds>] - Shutdown <ServerName> for <Reason>
/SHUTDOWN_ABORT - Abort a system shutdown

PS C:\Windows\system32>
```

Trust enumeration confirmed single forest with no external trusts.

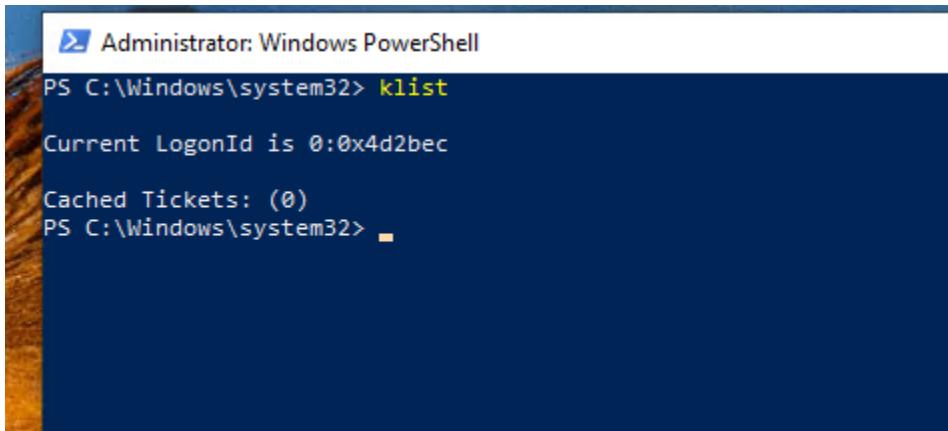
Phase 2 – Authentication & Kerberos Reconnaissance

Identity context validated using whoami and klist.

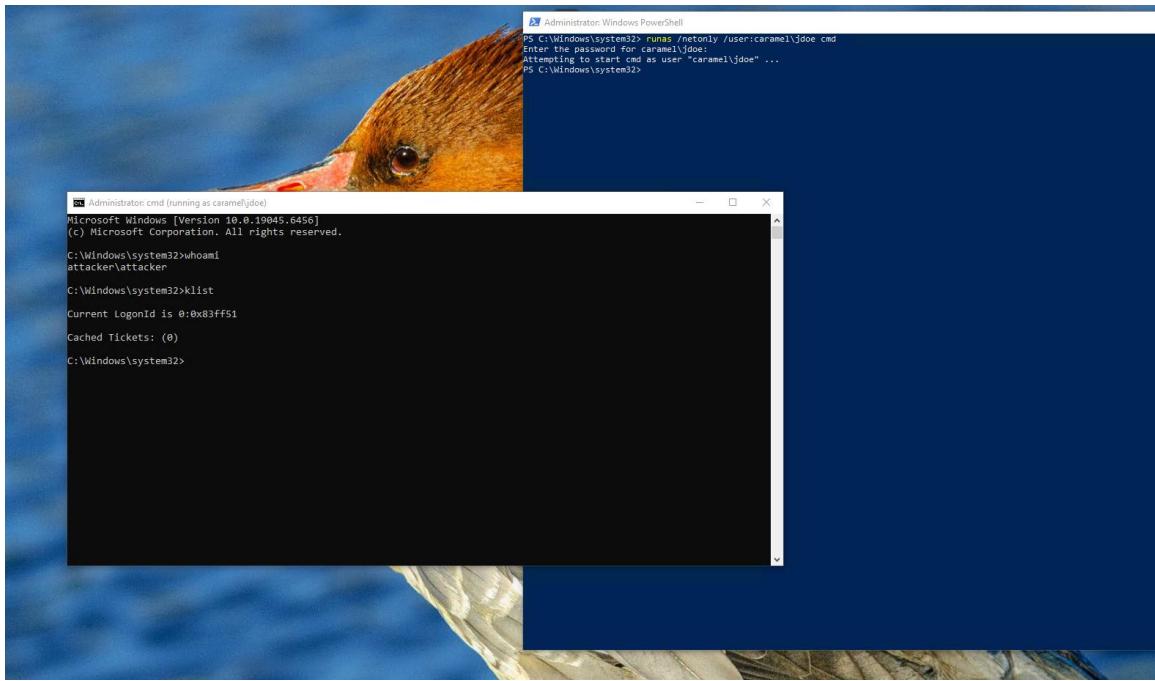


```
Administrator: Windows PowerShell
PS C:\Windows\system32> whoami
attacker\attacker
PS C:\Windows\system32> klist
Current LogonId is 0:0x4d2bec
Cached Tickets: (0)
PS C:\Windows\system32>
```

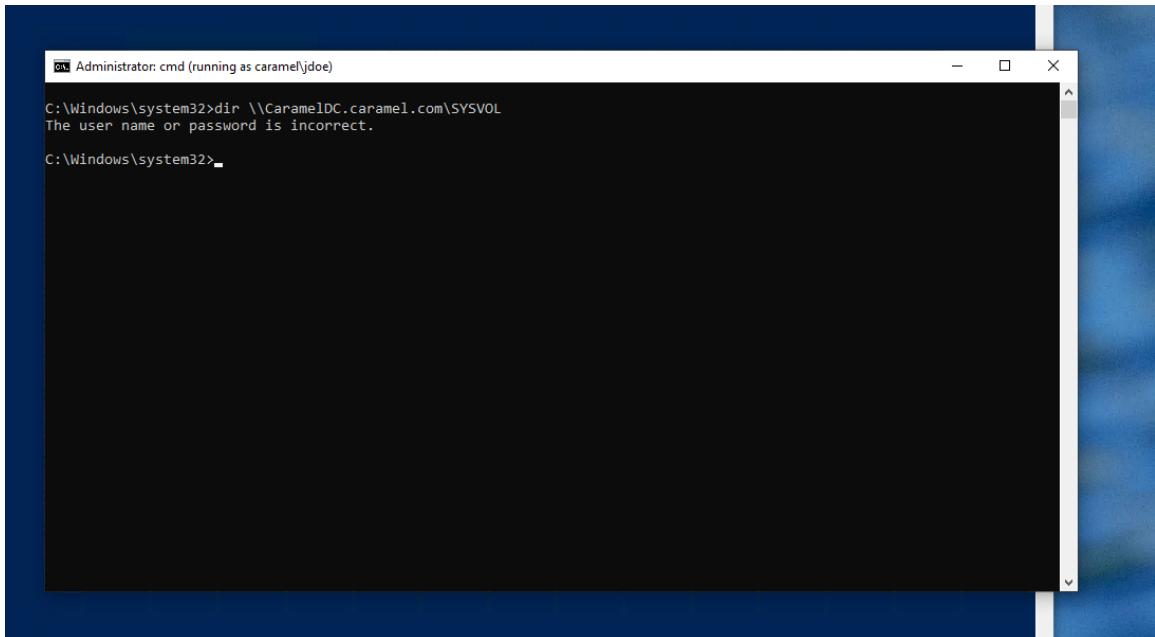
Kerberos tickets observed via runas /netonly.



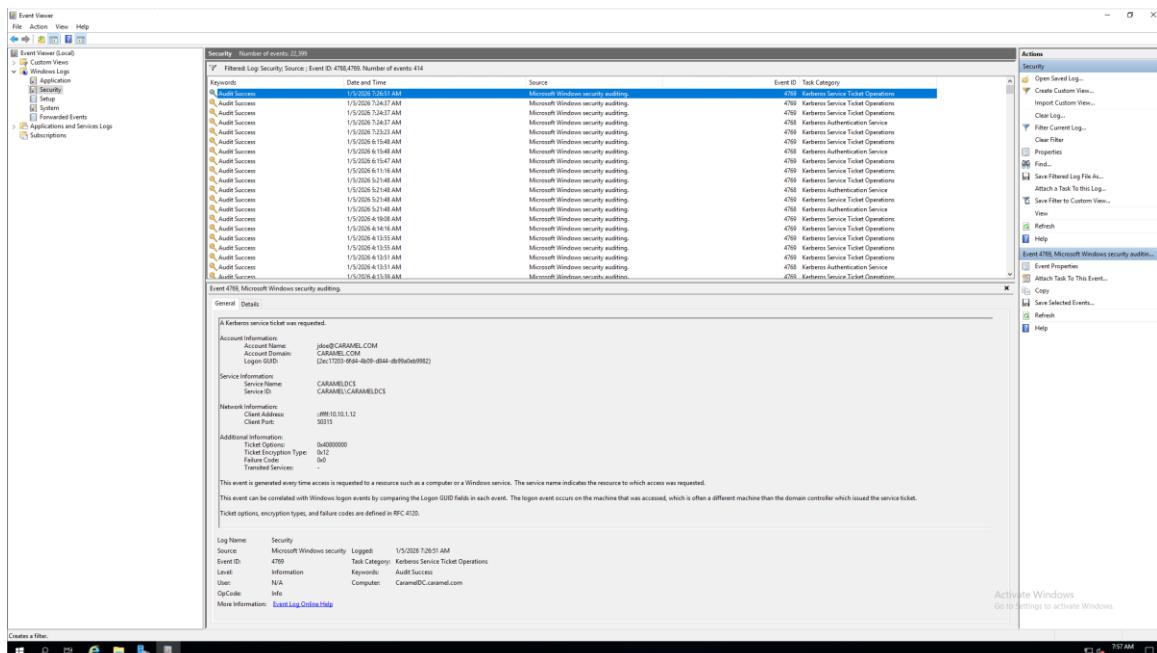
```
Administrator: Windows PowerShell
PS C:\Windows\system32> klist
Current LogonId is 0:0x4d2bec
Cached Tickets: (0)
PS C:\Windows\system32>
```



SYSVOL access tested and confirmed.



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



SPN enumeration conducted using setspn -Q /*.

```
Administrator: cmd (running as caramel\jdoe)
C:\Windows\system32>setspn -Q */
Checking domain DC=caramel,DC=com
CN=CARAMELDC,OU=Domain Controllers,DC=caramel,DC=com
Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/CaramelDC.caramel.com
TERMSRV/CARAMELDC
TERMSRV/CaramelDC.caramel.com
ldap/CaramelDC.caramel.com/ForestDnsZones.caramel.com
ldap/CaramelDC.caramel.com/DomainDnsZones.caramel.com
DNS/CaramelDC.caramel.com
GC/CaramelDC.caramel.com/caramel.com
RestrictedKrbHost/CaramelDC.caramel.com
RestrictedKrbHost/CARAMELDC
RPC/025e35d2-f647-4e0e-b200-79ffe11ace8a._msdcs.caramel.com
HOST/CARAMELDC/CARAMEL
HOST/CaramelDC.caramel.com/CARAMEL
HOST/CARAMELDC
HOST/CaramelDC.caramel.com
HOST/CaramelDC.caramel.com/caramel.com
E3514235-4B06-11D1-AB04-00C04FC2DCD2/025e35d2-f647-4e0e-b200-79ffe11ace8a/caramel.com
ldap/CARAMELDC/CARAMEL
ldap/025e35d2-f647-4e0e-b200-79ffe11ace8a._msdcs.caramel.com
ldap/CaramelDC.caramel.com/CARAMEL
ldap/CARAMELDC
ldap/CaramelDC.caramel.com
ldap/CaramelDC.caramel.com/caramel.com
CN=krbtgt,CN=Users,DC=caramel,DC=com
kadmin/changepw
CN=SRV-RTR,CN=Computers,DC=caramel,DC=com
WSMAN/SRV-RTR
WSMAN/SRV-RTR.caramel.com
TERMSRV/SRV-RTR
TERMSRV/SRV-RTR.caramel.com
RestrictedKrbHost/SRV-RTR
HOST/SRV-RTR
RestrictedKrbHost/SRV-RTR.caramel.com
HOST/SRV-RTR.caramel.com
CN=ONLYFANDC,OU=Domain Controllers,DC=caramel,DC=com
DNS/OnlyFanDC.caramel.com
HOST/OnlyFanDC.caramel.com/CARAMEL
RPC/8c8c0668-1fa1-4415-a788-a6faf93e12da._msdcs.caramel.com
GC/OnlyFanDC.caramel.com/caramel.com
HOST/OnlyFanDC.caramel.com/caramel.com
HOST/ONLYFANDC/CARAMEL
ldap/ONLYFANDC/CARAMEL
ldap/8c8c0668-1fa1-4415-a788-a6faf93e12da._msdcs.caramel.com
ldap/OnlyFanDC.caramel.com/CARAMEL
ldap/ONLYFANDC
ldap/OnlyFanDC.caramel.com
ldap/OnlyFanDC.caramel.com/ForestDnsZones.caramel.com
ldap/OnlyFanDC.caramel.com/DomainDnsZones.caramel.com
ldap/OnlyFanDC.caramel.com/caramel.com
E3514235-4B06-11D1-AB04-00C04FC2DCD2/8c8c0668-1fa1-4415-a788-a6faf93e12da/caramel.com
Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/OnlyFanDC.caramel.com
TERMSRV/ONLYFANDC
TERMSRV/OnlyFanDC.caramel.com
RestrictedKrbHost/ONLYFANDC
HOST/ONLYFANDC
RestrictedKrbHost/OnlyFanDC.caramel.com
HOST/OnlyFanDC.caramel.com
CN=CARAMEL-CLT-1,CN=Computers,DC=caramel,DC=com
TERMSRV/CARAMEL-CLT-1
TERMSRV/Caramel-CLT-1.caramel.com
RestrictedKrbHost/CARAMEL-CLT-1
HOST/CARAMEL-CLT-1
RestrictedKrbHost/Caramel-CLT-1.caramel.com
HOST/Caramel-CLT-1.caramel.com
CN=ATTACKER,CN=Computers,DC=caramel,DC=com
TERMSRV/ATTACKER
TERMSRV/ATTACKER.caramel.com
RestrictedKrbHost/ATTACKER
HOST/ATTACKER
RestrictedKrbHost/ATTACKER.caramel.com
HOST/ATTACKER.caramel.com

Existing SPN found!
```

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.