TDNA Assessment – Report 2: Vulnerable Active Directory Environment

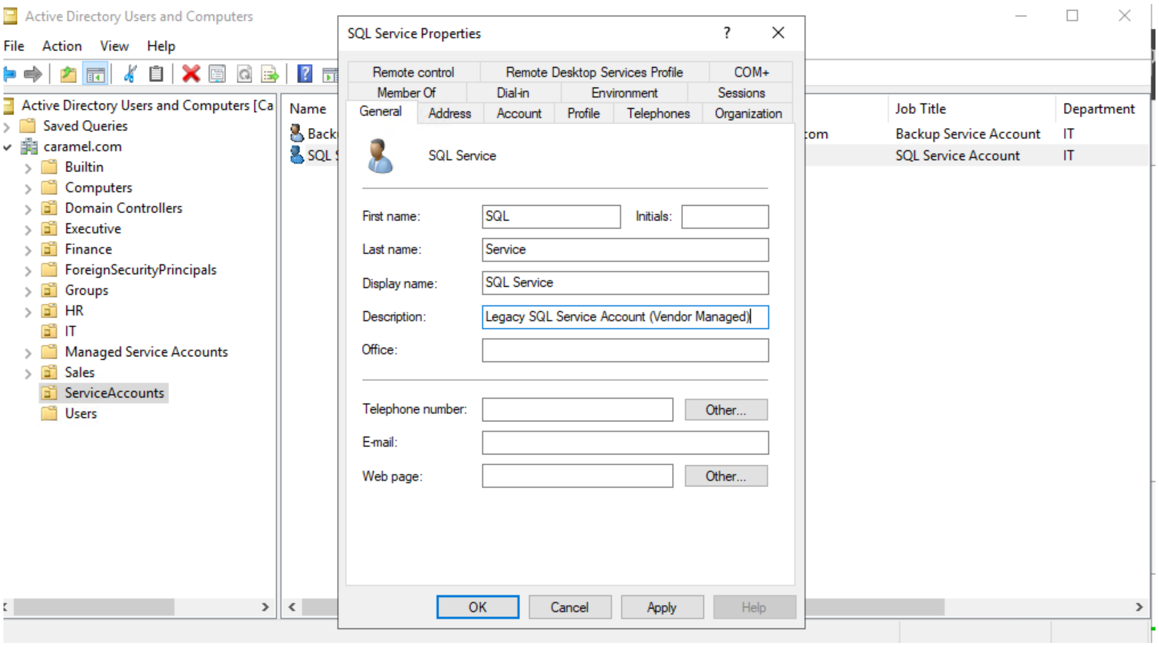
This report documents a purposefully misconfigured Active Directory environment designed to demonstrate Kerberoasting feasibility under insecure service account configurations. This environment contrasts directly with the hardened baseline documented in Report 1.

Executive Summary

A controlled misconfiguration was introduced by creating a user-managed service account with a registered Service Principal Name (SPN) and non-expiring credentials. As a result, Kerberos service tickets encrypted with legacy RC4-HMAC were issued, making the environment vulnerable to Kerberoasting attacks.

Intentional Misconfiguration

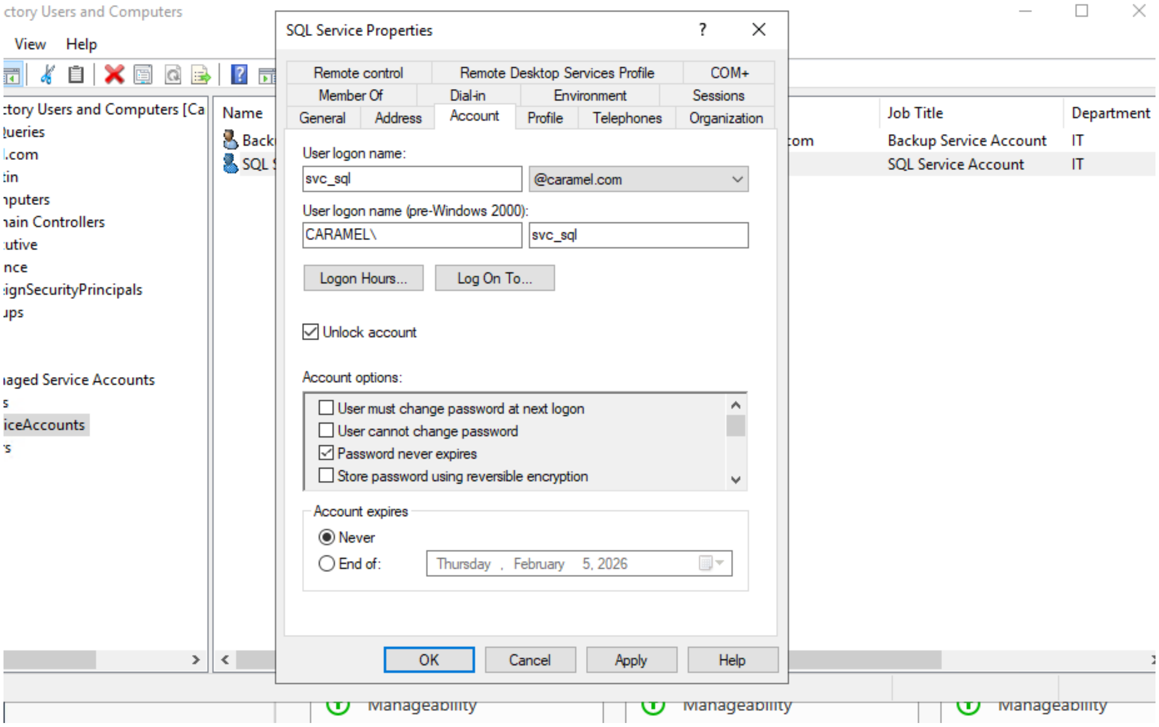
A legacy SQL service account (svc_sql) was created to simulate common enterprise misconfigurations. The account was configured with a non-expiring password and assigned an MSSQL Service Principal Name.



First name: SQL
Initials:
Last name: Service
Display name: SQL Service
Description: Legacy SQL Service Account (Vendor Managed)

Job Title	Department
Backup Service Account	IT
SQL Service Account	IT

Figure 1: Legacy SQL service account created as a standard domain user.



Name		Job Title	Department
Back	om	Backup Service Account	IT
SQL S		SQL Service Account	IT

SQL Service Properties

User logon name:
svc_sql @caramel.com

User logon name (pre-Windows 2000):
CARAMEL\ svc_sql

☑ Unlock account

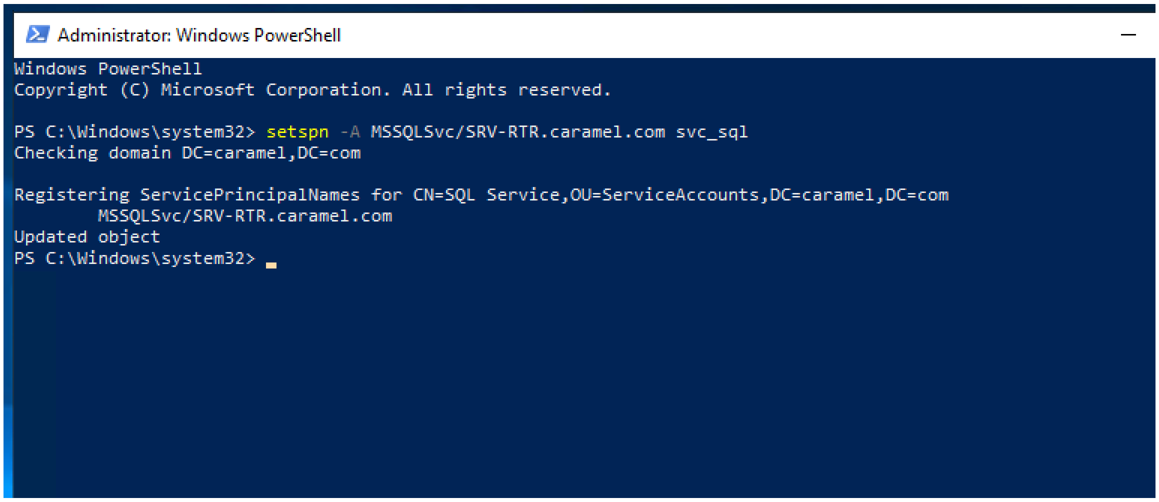
Account options:
☐ User must change password at next logon
☐ User cannot change password
☑ Password never expires
☐ Store password using reversible encryption

Account expires
● Never
○ End of: Thursday , February 5, 2026

Figure 2: Service account configured with non-expiring password.

Kerberoastable Service Discovery

Attacker-side enumeration was performed using native Windows tooling to identify Kerberoastable Service Principal Names.



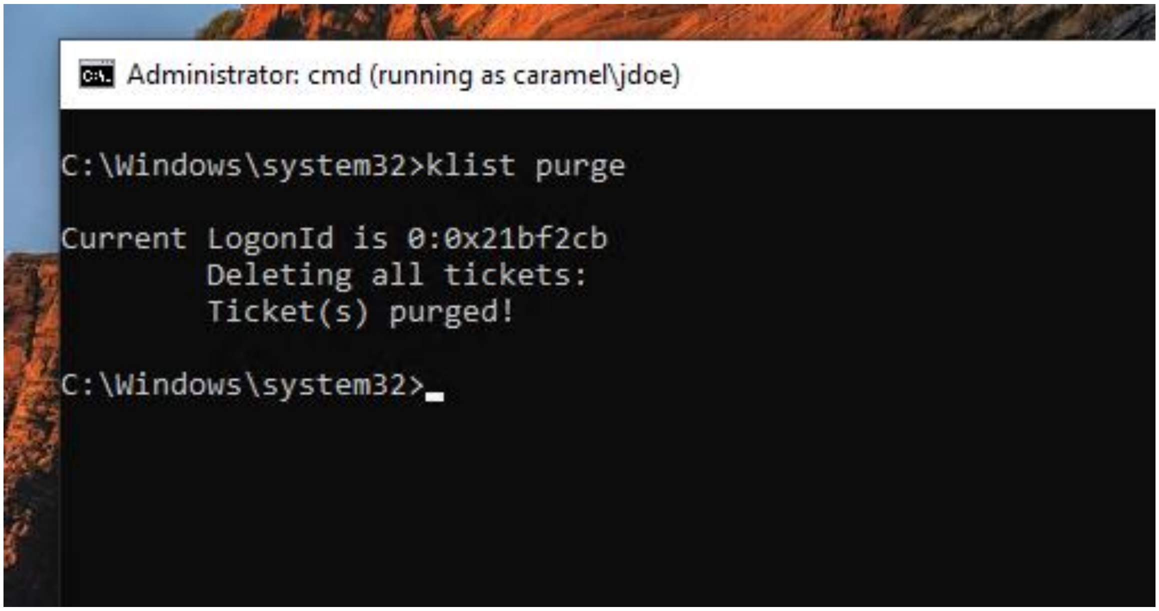
Administrator: Windows PowerShell

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

PS C:\Windows\system32> setspn -A MSSQLSvc/SRV-RTR.caramel.com svc_sql
Checking domain DC=caramel,DC=com

Registering ServicePrincipalNames for CN=SQL Service,OU=ServiceAccounts,DC=caramel,DC=com
        MSSQLSvc/SRV-RTR.caramel.com
Updated object
PS C:\Windows\system32> _
```

Figure 3: SPN enumeration confirms MSSQLSvc SPN bound to user account.

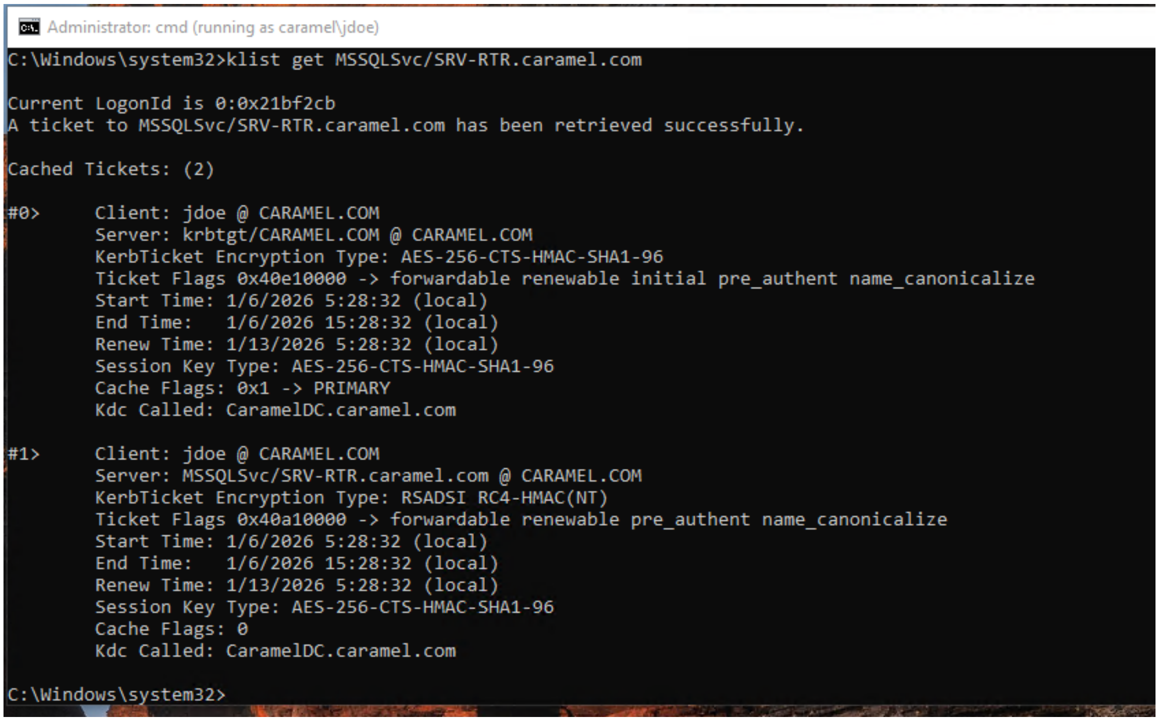
Kerberos Ticket Validation

The Kerberos ticket cache was purged and a service ticket was explicitly requested. The resulting ticket was cached locally and confirmed to use RC4-HMAC encryption.



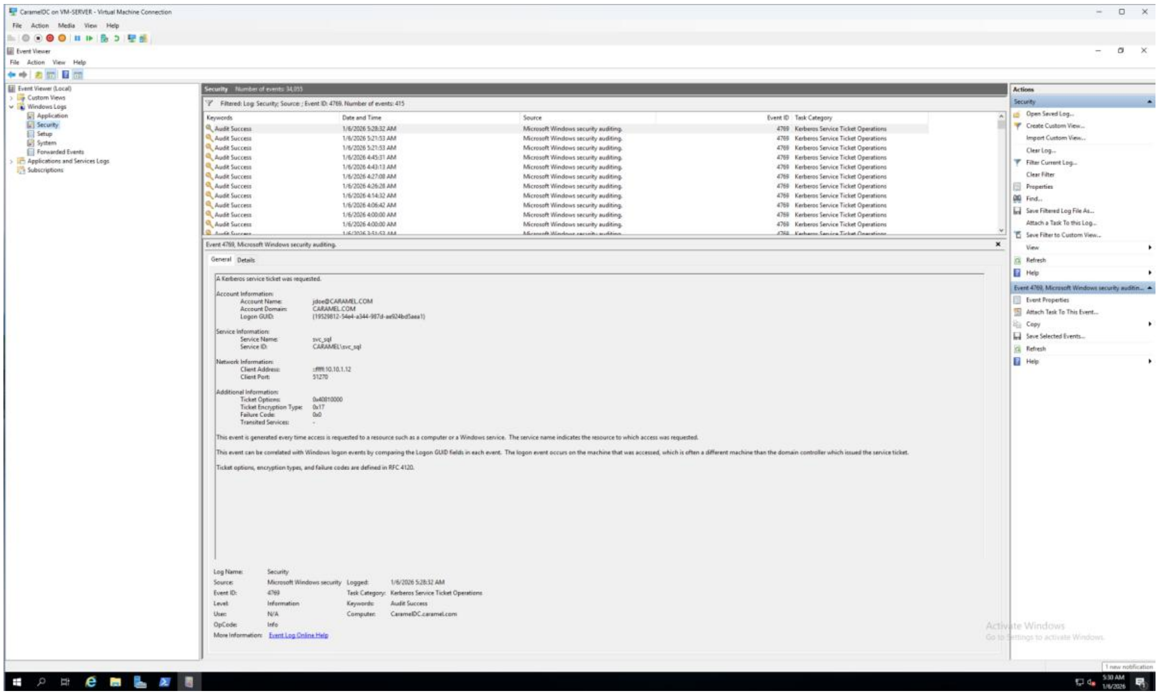
```
C:\Windows\system32>klist purge

Current LogonId is 0:0x21bf2cb
        Deleting all tickets:
        Ticket(s) purged!

C:\Windows\system32>_
```

Figure 4: Kerberos ticket cache purged prior to ticket request.



```
C:\Windows\system32>klist get MSSQLSvc/SRV-RTR.caramel.com

Current LogonId is 0:0x21bf2cb
A ticket to MSSQLSvc/SRV-RTR.caramel.com has been retrieved successfully.

Cached Tickets: (2)

#0>     Client: jdoe @ CARAMEL.COM
        Server: krbtgt/CARAMEL.COM @ CARAMEL.COM
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
        Start Time: 1/6/2026 5:28:32 (local)
        End Time:   1/6/2026 15:28:32 (local)
        Renew Time: 1/13/2026 5:28:32 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called: CaramelDC.caramel.com

#1>     Client: jdoe @ CARAMEL.COM
        Server: MSSQLSvc/SRV-RTR.caramel.com @ CARAMEL.COM
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
        Start Time: 1/6/2026 5:28:32 (local)
        End Time:   1/6/2026 15:28:32 (local)
        Renew Time: 1/13/2026 5:28:32 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0
        Kdc Called: CaramelDC.caramel.com

C:\Windows\system32>
```

Figure 5: Kerberos service ticket successfully requested for MSSQLSvc service.



```
Security   Number of events: 34,055
Filtered: Log: Security; Source: ; Event ID: 4769. Number of events: 415

Keywords        Date and Time          Source                               Event ID  Task Category
Audit Success   1/6/2026 5:28:32 AM    Microsoft Windows security auditing.  4769     Kerberos Service Ticket Operations
Audit Success   1/6/2026 5:21:53 AM    Microsoft Windows security auditing.  4769     Kerberos Service Ticket Operations
Audit Success   1/6/2026 5:21:53 AM    Microsoft Windows security auditing.  4769     Kerberos Service Ticket Operations
Audit Success   1/6/2026 4:45:31 AM    Microsoft Windows security auditing.  4769     Kerberos Service Ticket Operations
Audit Success   1/6/2026 4:43:13 AM    Microsoft Windows security auditing.  4769     Kerberos Service Ticket Operations
Audit Success   1/6/2026 4:27:08 AM    Microsoft Windows security auditing.  4769     Kerberos Service Ticket Operations
Audit Success   1/6/2026 4:26:28 AM    Microsoft Windows security auditing.  4769     Kerberos Service Ticket Operations
Audit Success   1/6/2026 4:14:32 AM    Microsoft Windows security auditing.  4769     Kerberos Service Ticket Operations
Audit Success   1/6/2026 4:06:42 AM    Microsoft Windows security auditing.  4769     Kerberos Service Ticket Operations
Audit Success   1/6/2026 4:00:00 AM    Microsoft Windows security auditing.  4769     Kerberos Service Ticket Operations
Audit Success   1/6/2026 4:00:00 AM    Microsoft Windows security auditing.  4769     Kerberos Service Ticket Operations
```

```
Event 4769, Microsoft Windows security auditing.

General  Details

A Kerberos service ticket was requested.

Account Information:
        Account Name:           jdoe@CARAMEL.COM
        Account Domain:         CARAMEL.COM
        Logon GUID:             {19529812-54e4-a344-987d-ae924bd5aea1}

Service Information:
        Service Name:           svc_sql
        Service ID:             CARAMEL\svc_sql

Network Information:
        Client Address:         ::ffff:10.10.1.12
        Client Port:            51270

Additional Information:
        Ticket Options:         0x40810000
        Ticket Encryption Type: 0x17
        Failure Code:           0x0
        Transited Services:     -

This event is generated every time access is requested to a resource such as a computer or a Windows service.  The service name indicates the resource to which access was requested.

This event can be correlated with Windows logon events by comparing the Logon GUID fields in each event.  The logon event occurs on the machine that was accessed, which is often a different machine than the domain controller which issued the service ticket.

Ticket options, encryption types, and failure codes are defined in RFC 4120.

Log Name:         Security
Source:           Microsoft Windows security  Logged:         1/6/2026 5:28:32 AM
Event ID:         4769                        Task Category:  Kerberos Service Ticket Operations
Level:            Information                 Keywords:       Audit Success
User:             N/A                         Computer:       CaramelDC.caramel.com
OpCode:           Info
More Information: Event Log Online Help
```

Figure 6: Cached RC4-HMAC Kerberos service ticket present in ticket cache.

Conclusion

Kerberoasting was enabled in this environment as a direct result of service account misconfiguration. This demonstrates how user-managed service accounts with SPNs and long-lived credentials introduce significant credential exposure risk.