Cyber Range - Dunlain

Atharva Velani 20411611 **192.168.10.30**

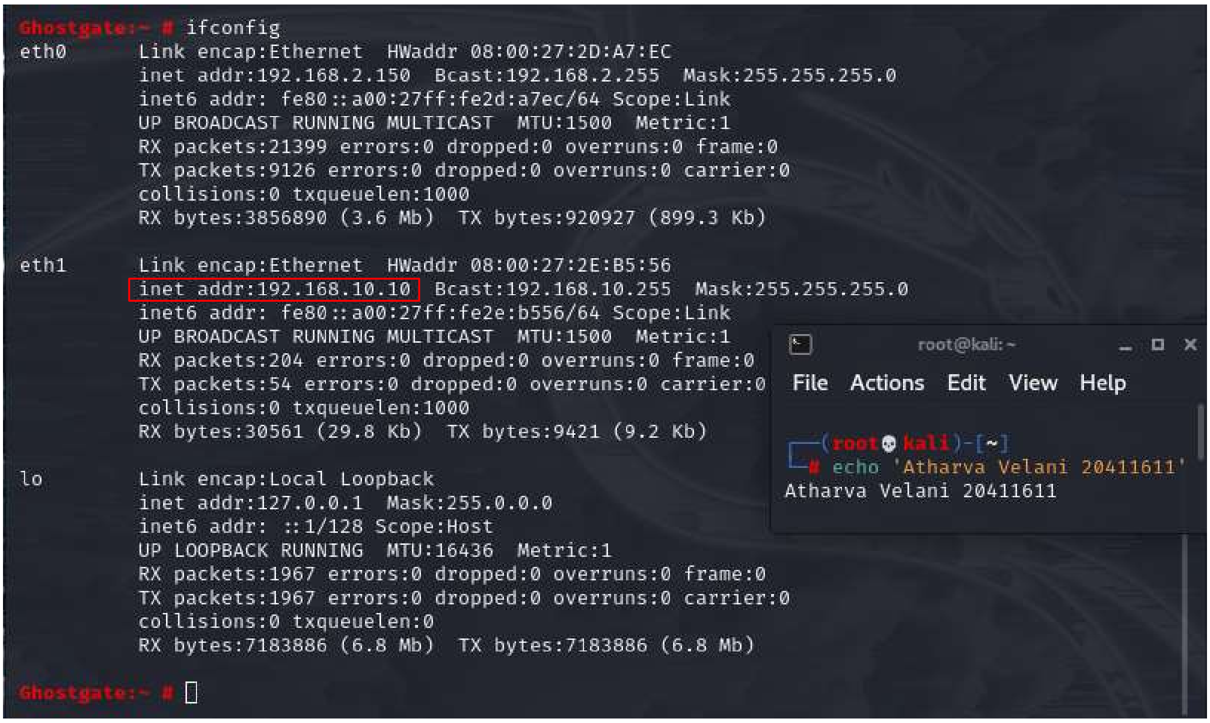
Unable to crack this machine, proxy chains weren't working as intended and the commands just returned errors via kali.

Step 1: Connect to the network via proxychains.

From the previous machine (Ghostgate) we know that we have access to the .2.x subnet but not the .10.x subnet in which Dunlain resides. To get access to this system we muse use proxychains. First lets log into the account with the root access which we had used prior with our dirty cow exploit.

U: firefart
P: password

We have root access as the user and can now check if the Ghostgate is indeed linked to the 192.168.10.x subnet, in which it is.



```
Ghostgate:~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:2D:A7:EC
          inet addr:192.168.2.150  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe2d:a7ec/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:21399 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9126 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3856890 (3.6 Mb)  TX bytes:920927 (899.3 Kb)

eth1      Link encap:Ethernet  HWaddr 08:00:27:2E:B5:56
          inet addr:192.168.10.10  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe2e:b556/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:204 errors:0 dropped:0 overruns:0 frame:0
          TX packets:54 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:30561 (29.8 Kb)  TX bytes:9421 (9.2 Kb)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1967 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1967 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:7183886 (6.8 Mb)  TX bytes:7183886 (6.8 Mb)

Ghostgate:~ # 
```

```
┌──(root💀kali)-[~]
└─# echo 'Atharva Velani 20411611'
Atharva Velani 20411611
```

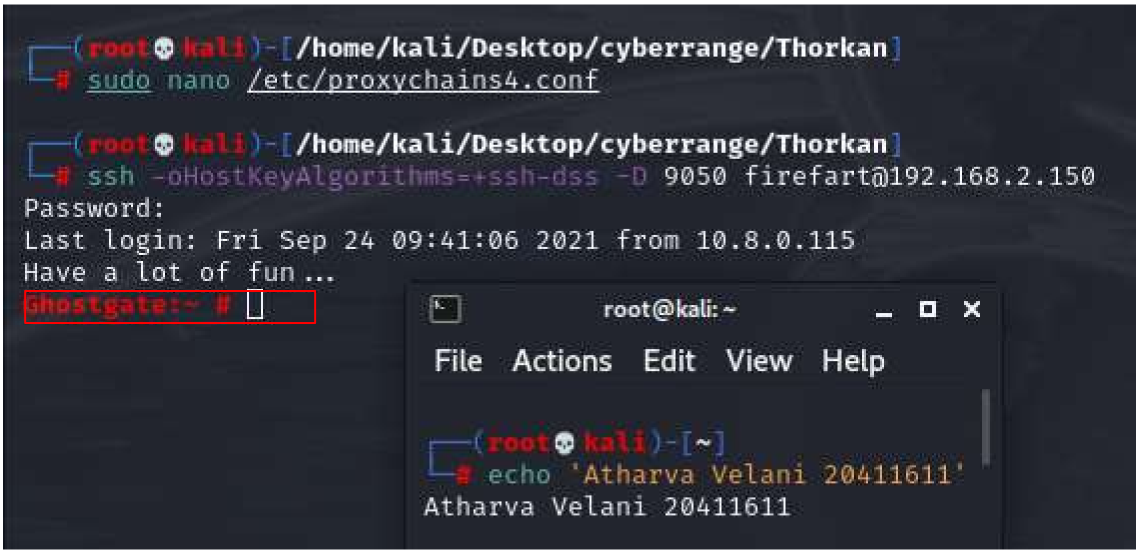
Lets configure our proxy chains to get access to the 192.168.10.xx subnet.

Firstly you need to modify the proxychains4 config file.
sudo nano /etc/proxychains4.conf

Uncomment dynamic_chain
comment strict_chain
append at the end: socks5 127.0.0.1 9050

Run ssh through the proxychains4 port.
ssh -oHostKeyAlgorithms=+ssh-dss -D 9050 firefart@192.168.2.150
password

Now have root access through proxychains.



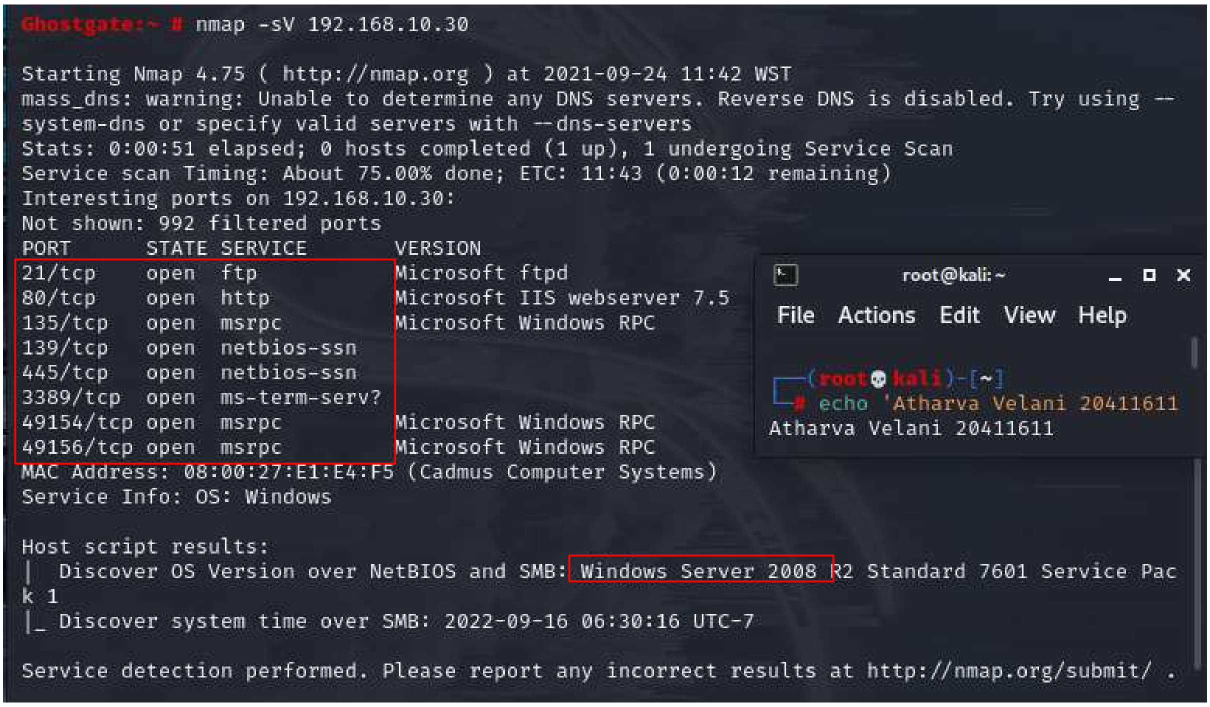
```
┌──(root💀kali)-[/home/kali/Desktop/cyberrange/Thorkan]
└─# sudo nano /etc/proxychains4.conf

┌──(root💀kali)-[/home/kali/Desktop/cyberrange/Thorkan]
└─# ssh -oHostKeyAlgorithms=+ssh-dss -D 9050 firefart@192.168.2.150
Password:
Last login: Fri Sep 24 09:41:06 2021 from 10.8.0.115
Have a lot of fun...
Ghostgate:~ #
```

```
┌──(root💀kali)-[~]
└─# echo 'Atharva Velani 20411611'
Atharva Velani 20411611
```

Step 2: Scanning the network.

Lets perform a simple scan to see which services are open and the service version to determine if we can exploit any available open ports.



```
Ghostgate:~ # nmap -sV 192.168.10.30

Starting Nmap 4.75 ( http://nmap.org ) at 2021-09-24 11:42 WST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --
system-dns or specify valid servers with --dns-servers
Stats: 0:00:51 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 75.00% done; ETC: 11:43 (0:00:12 remaining)
Interesting ports on 192.168.10.30:
Not shown: 992 filtered ports
PORT      STATE SERVICE       VERSION
21/tcp    open  ftp           Microsoft ftpd
80/tcp    open  http          Microsoft IIS webserver 7.5
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn
3389/tcp  open  ms-term-serv?
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)
Service Info: OS: Windows

Host script results:
|  Discover OS Version over NetBIOS and SMB: Windows Server 2008 R2 Standard 7601 Service Pac
k 1
|_ Discover system time over SMB: 2022-09-16 06:30:16 UTC-7

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
```

```
┌──(root💀kali)-[~]
└─# echo 'Atharva Velani 20411611
Atharva Velani 20411611
```

Not enough information on these ports, lets perform a more detailed scan to get an idea of what we can exploit. We do now know that the server is running on windows and port 445 is open which always opens up the possibility of Eternal Blue vulnerability. Lets perform a more detailed scan with the ***'-A'***.

nmap -sV -A 192.168.10.30

Couldn't execute any commands through proxychains with this machine, no clue why Microsoft wasn't working but thorkan was working as expected (almost).