Sean Lee and Eli Arbogast

Tasks

A. Kali's main interface's MAC address is 08:00:27:8e:dc:b3
B. Kali's main interface's IP address is 10.0.2.15
C. Metasploitable's main interface's MAC address is 08:00:27:62:2b:b1
D. Metasploitable's main interface's IP address is 10.0.2.4
E. Kernel IP routing table

| Destination | Gateway | Genmask | Flags | MSS | Window | irtt | Iface |
|---|---|---|---|---|---|---|---|
| default | 10.0.2.1 | 0.0.0.0 | UG | 0 | 0 | 0 | eth0 |
| 10.0.2.0 | 0.0.0.0 | 255.255.255.0 | U | 0 | 0 | 0 | eth0 |

F.

| Address | HWtype | HWaddress | Flags | Mask | Iface |
|---|---|---|---|---|---|
| 10.0.2.1 | ether | 52:54:00:12:35:00 | C | | eth0 |
| 10.0.2.3 | ether | 08:00:27:4a:ba:9a | C | | eth0 |

G.

```
msfadmin@metasploitable:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
10.0.2.0        *               255.255.255.0   U         0 0          0 eth0
default         10.0.2.1        0.0.0.0         UG        0 0          0 eth0
msfadmin@metasploitable:~$
```

H.

```
msfadmin@metasploitable:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.3                 ether   08:00:27:4A:BA:9A   C                     eth0
10.0.2.1                 ether   52:54:00:12:35:00   C                     eth0
msfadmin@metasploitable:~$
```

I. 52:54:00:12:35:00, as it corresponds to the gateway IP through which packets get sent to jeffondich.com
J. No
K.

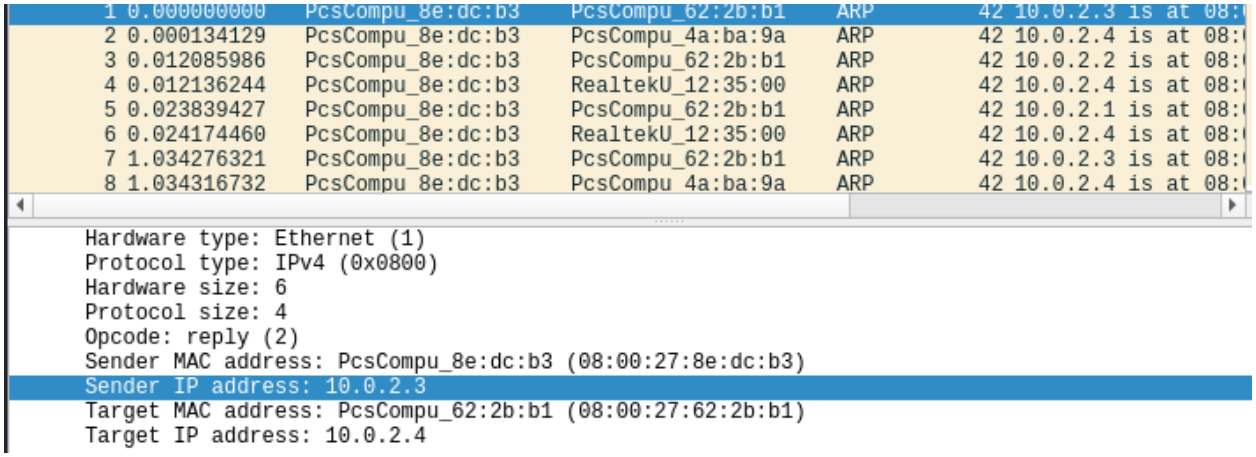
L.

```
msfadmin@metasploitable:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.2                 ether   08:00:27:8E:DC:B3   C                     eth0
10.0.2.1                 ether   08:00:27:8E:DC:B3   C                     eth0
10.0.2.15                ether   08:00:27:8E:DC:B3   C                     eth0
10.0.2.3                 ether   08:00:27:8E:DC:B3   C                     eth0
msfadmin@metasploitable:~$ _
```

There are two new IP address

M. Now, Metasploitable will send the TCP SYN pack to 08:00:27:8E:DC:B3 because that is the MAC address now corresponding to the gateway IP.
N.
O. Yes to all three
P. What's happening is that by running the ARP poisoning, the attacker, which is Kali in this case, is able to associate the attacker's host MAC address with the IP address of the host, which is Metasploitable in this case. Kali was able to use Ettercap to scan for the IP and MAC addresses of the host, Metasploitable. The attacker can then choose its target, Metasploitable, and begins sending ARP packets that contain the attacker's MAC address and the target's IP address. The data that the hosts send to the victim will now be going to the attacker instead. As seen in the image below of one of the packets, you can observe that the sender MAC address which is Kali's main interface's MAC address

is associated with Metasploitable's IP address.




Q. We would want our detector to filter packets, and detect whether the packets being sent across the network are coming from inside the network when they actually originate from outside the network. To prevent false positives, we would also want our detector to keep track of pairings between IP addresses and MAC addresses, so that any legitimate changes to these pairings wouldn't be flagged as malicious packet changes. Changes to the pairings would need to be recorded and verified to be legitimate.