Ariana Borlak

===== EXECUTION =====
a. 00:0c:29:cb:83:65

b. 172.16.27.129

c. 00:0c:29:c8:47:c4

d. 172.16.27.128

e.

```
┌──(kali㉿kali)-[~]
└─$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         172.16.27.2     0.0.0.0         UG        0 0          0 eth0
172.16.27.0     0.0.0.0         255.255.255.0   U         0 0          0 eth0
```

f.

```
┌──(kali㉿kali)-[~]
└─$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
172.16.27.254            ether   00:50:56:f1:f7:2f   C                     eth0
```

g.

```
msfadmin@metasploitable:~$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
172.16.27.0     0.0.0.0         255.255.255.0   U         0 0          0 eth0
0.0.0.0         172.16.27.2     0.0.0.0         UG        0 0          0 eth0
```

h.

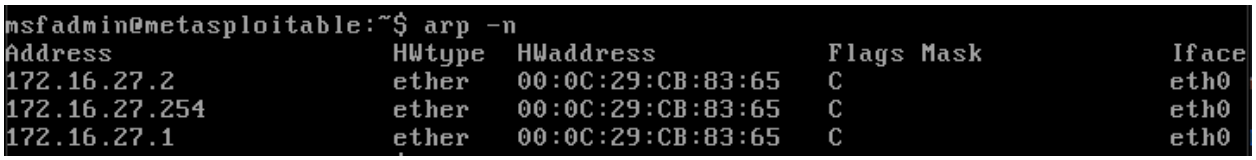
```
msfadmin@metasploitable:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
172.16.27.254            ether   00:50:56:F1:F7:2F   C                     eth0
msfadmin@metasploitable:~$
```

i. The website has an ip address of 172.233.221.124, and if you bitwise and the first genmask with the ip address, the result is 172.233.221.0, which does not match the destination address so the website is not on the local server. The only destination left is the default, 0.0.0.0, and using the mask on the ip address gets the destination, so Metasploitable should first send the SYN

packet to the gateway 172.16.27.2. Looking in the arp cache, this ip address has a MAC address of 00:50:56:f1:f7:2f.

j. Metasploitable receives an HTML document as a response. There are no captured packets on Wireshark.

l.



It has two more entries, and all the entries point to the MAC address of Kali.

m. I predict Metasploitable will send the packet to the Kali MAC address, 00:0c:29:cb:83:65 because that is the address in the arp cache for all the stored ip addresses.

o. There is the same HTTP response on Metasploitable of an HTML document. There are also captured packets on Wireshark. Yes, you can see that Metasploitable and cs338.jeffondich.com did the TCP handshake, Metasploitable sent an HTTP request, and cs338.jeffondich.com sent the HTML document, among numerous TCP retransmissions.

p. Kali sends multiple broadcasts announcing that the ip address of Metasploitable is at Kali's MAC address. Every time an ARP request for the Metasploitable ip address goes out, Kali also responds with its MAC address.

q. The detector would have to keep a log of past broadcasts and compare them to broadcasts going out. Detecting the frequency of arp broadcasts would also be useful, since an attack sends out many more broadcasts than regular arp broadcasts. There could be false positives if the MAC address of a device actually changes.

===== SYNTHESIS =====

a. Mal sends arp broadcasts that change the routers' arp caches to route packets meant for Alice to instead go to Mal. This means that when Bob sends Alice a message, the message will get routed to Mal instead of Alice. Mal can then choose to forward packets to Alice to keep her from noticing the attack.

b. No the attack is not detectable because Alice still receives the HTTP response from Bob. Alice would need to know the path of the packets and which MAC addresses move the packets to her.

c. No the attack is not detectable, unless Bob detects the retransmission of almost all the packets and finds it suspicious.

d. Using HTTPS would not prevent Mal from poisoning arp caches and routing packets to herself instead of Alice, but it would prevent Mal from being able to decipher or change any of the packets without Alice or Bob detecting the changes, since HTTPS encrypts any communication with a key, and validates the key with Bob's certificate.