Alex Falk

----------EXECUTION----------

a. 00:0c:29:bf:f9:27
b. 192.168.11.128
c. 00:0c:29:e0:57:c5
d. 192:168:11:129
e.

```
┌──(kali㉿kali)-[~]
└─$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Ifac
e
default         192.168.11.2    0.0.0.0         UG        0 0          0 eth0
192.168.11.0    0.0.0.0         255.255.255.0   U         0 0          0 eth0
```

f.

```
┌──(kali㉿kali)-[~]
└─$ arp
Address                  HWtype  HWaddress           Flags Mask            If
ace
192.168.11.2             ether   00:50:56:e5:73:1b   C                     et
h0
192.168.11.254           ether   00:50:56:f1:54:b4   C                     et
h0
```

g.

```
msfadmin@metasploitable:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.11.0    *               255.255.255.0   U         0 0          0 eth0
default         192.168.11.2    0.0.0.0         UG        0 0          0 eth0
```

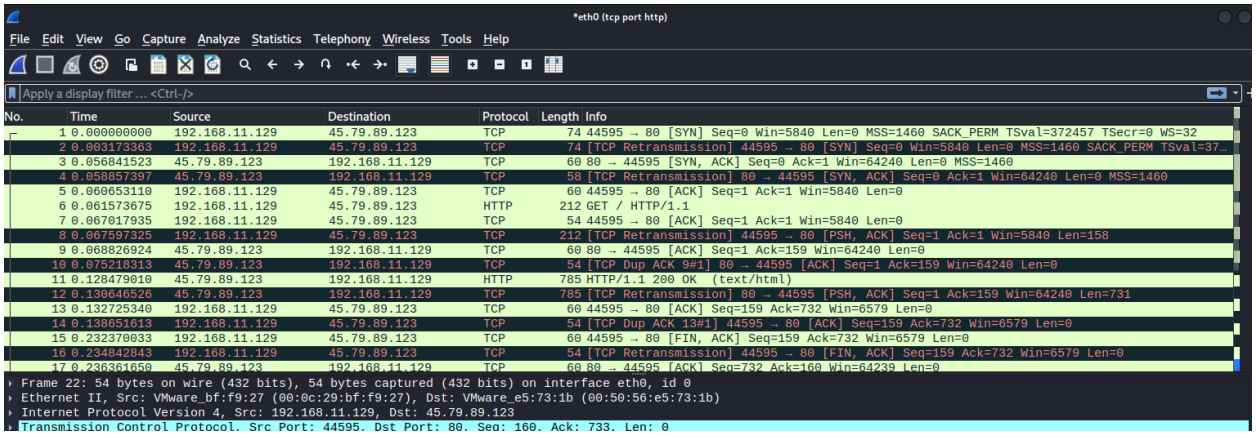
h.

```
msfadmin@metasploitable:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.11.254           ether   00:50:56:F1:54:B4   C                     eth0
192.168.11.2             ether   00:50:56:E5:73:1B   C                     eth0
192.168.11.128           ether   00:0C:29:BF:F9:27   C                     eth0
```

i. 00:50:56:E5:73:1B. This is the MAC address of the default gateway's IP address shown in (g). This IP address connects the machine to the outside world (such as the given url). Therefore, SYN packets must first be sent to its MAC address before being sent further on.

j. Yes, I see an http response on Metasploitable. Yes, I see captured packets on wireshark

k.



l.

```
msfadmin@metasploitable:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.11.254           ether   00:0C:29:BF:F9:27   C                     eth0
192.168.11.1             ether   00:50:56:C0:00:08   C                     eth0
192.168.11.2             ether   00:0C:29:BF:F9:27   C                     eth0
192.168.11.128           ether   00:0C:29:BF:F9:27   C                     eth0
```

2 things changed. First, there's a new IP address (192.168.11.1). Second, the MAC address for the IP address associated with the default gateway changed to the MAC address of the IP address associated with Kali.

m. I predict that Metasploitable will send the TCP SYN packet to the MAC address associated with the IP address of Kali. Because of the poisoning, Metasploitable's ARP table now says that the MAC address of the default gateway is that of Kali's. So when Metasploitable tries to send the SYN packet to the default gateway, it is directed to send it to Kali instead.

n. Ok

o. Yes. Yes. Yes.

p.

```
394 173.392859975 VMware_bf:f9:27 VMware_bf:f9:27 ARP 42 192.168.11.254 is at 00:0c:29:bf:f9:27 (duplicate use of 192.168.11.129 detected!)
395 173.393272559 VMware_bf:f9:27 VMware_bf:f9:27 ARP 42 192.168.11.129 is at 00:0c:29:bf:f9:27 (duplicate use of 192.168.11.254 detected!)
396 173.403896810 VMware_bf:f9:27 VMware_bf:f9:27 ARP 42 192.168.11.2 is at 00:0c:29:bf:f9:27 (duplicate use of 192.168.11.129 detected!)
397 173.404335561 VMware_bf:f9:27 VMware_bf:f9:27 ARP 42 192.168.11.129 is at 00:0c:29:bf:f9:27 (duplicate use of 192.168.11.2 detected!)
398 173.414891923 VMware_bf:f9:27 VMware_bf:f9:27 ARP 42 192.168.11.1 is at 00:0c:29:bf:f9:27 (duplicate use of 192.168.11.129 detected!)
399 173.415243932 VMware_bf:f9:27 VMware_c0:00:08 ARP 42 192.168.11.129 is at 00:0c:29:bf:f9:27
400 183.426633345 VMware_bf:f9:27 VMware_bf:f9:27 ARP 42 192.168.11.254 is at 00:0c:29:bf:f9:27 (duplicate use of 192.168.11.129 detected!)
401 183.427054575 VMware_bf:f9:27 VMware_bf:f9:27 ARP 42 192.168.11.129 is at 00:0c:29:bf:f9:27 (duplicate use of 192.168.11.254 detected!)
402 183.437594483 VMware_bf:f9:27 VMware_bf:f9:27 ARP 42 192.168.11.2 is at 00:0c:29:bf:f9:27 (duplicate use of 192.168.11.129 detected!)
403 183.437981525 VMware_bf:f9:27 VMware_bf:f9:27 ARP 42 192.168.11.129 is at 00:0c:29:bf:f9:27 (duplicate use of 192.168.11.2 detected!)
404 183.448675044 VMware_bf:f9:27 VMware_bf:f9:27 ARP 42 192.168.11.1 is at 00:0c:29:bf:f9:27 (duplicate use of 192.168.11.129 detected!)
405 183.449038382 VMware_bf:f9:27 VMware_c0:00:08 ARP 42 192.168.11.129 is at 00:0c:29:bf:f9:27
```

Kali changed Metaspolitabale's ARP cache by sending out a bunch of messages on the network saying that such and such's MAC address is Kali's MAC address. Metasploitable picked up these messages, looked at their own ARP cache, and cached the new MAC address that Kali told Metasploitable was associated with the IP.

q. It could look at the information going over the network and look for suspicious activity. This could include looking out for a machine that keeps saying that different IPs should be associated with the same MAC address as this is a sign of poisoning. The detector could also check whether a lot of traffic suddenly starts heading to a new machine on the network instead of the gateway. This could result in a false positive, however, if the new machine is simply trying to talk to other machines on the network.

----------SYNTHESIS----------

a. First I'll make clear what an ARP cache is and why it is important. In order to send a packet from one machine to another, it's essential to know the destination machine's IP address. When a packet is sent off, it is addressed with this IP address. However, the packet often cannot directly go to that IP. This is because most machines are outside of the network of most other machines. That means that the packet must first get sent to an intermediary machine or machines before it reaches its destination. Each machine has a routing table that indicates the IP of the next machine in this chain of machines. In order to send a packet to these machines, you must know not only its IP address but also its MAC address. The IP address and the corresponding MAC address for each machine on a network are stored by each machine on the network. In order to establish the MAC address for an IP address, a machine sends out a broadcast to the network seeking a reply. If all actors on the network are playing nicely, then the machine with the called-out IP will respond with its MAC address. This IP address/MAC address pairing is stored by each machine in what is called an ARP cache. When a machine wants to send a packet to a specific IP, it looks up the IP's corresponding MAC address and sends the packet to that address. Let's say Alice wants to send a packet to Bob. Alice looks up Bob's IP, finds his MAC address, and sends the packet along to that address. Now, let's say Mal wants to intercept that packet and then forward it on to Bob. Here is how she would do this. Mal first listens and generates an ARP cache of her own. Importantly, she stores Bob's IP/MAC addresses. When Alice sends out a call for the MAC address associated with Bob's IP, Mal sends Alice Mal's MAC address. Accordingly, Alice stores Mal's MAC address with Bob's IP. By doing this, Mal has poisoned Alice's ARP cache with false information. Now, when Alice wants to send a packet to Bob, she looks Bob's IP in the ARP cache and sends the packet to the associated MAC address. However, this MAC address is actually Mal's MAC address. As a result, Mal receives the packet intended for Bob. Mal can then send this packet along to Bob so that suspicion does not arise. Mal can then do the same thing to Bob (poison his cache, forward the packets on, etc.)
b. I don't think that Alice would be able to detect the attack (maybe if she checked her ARP cache and saw that multiple IPs were using the same MAC address she would become suspicious). Her ARP cache tells her to send the packet to Mal (which she does) and when she receives a packet she can't confirm whether it's from Bob. To detect it, Alice and Bob could perform DH and then send each other challenges. When these challenges inevitably fail, they'll know that their connection is not secure.
c. No. Bob is just receiving packets. They could be from anyone on the network.
d. Yes. As mentioned above, if the communication between Alice and Bob was encrypted, they would figure out that their connection was not secure after issuing challenges.