Arthur Viegas Eguia

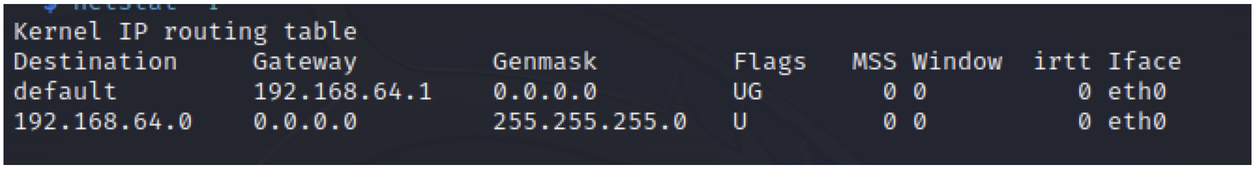
Execution:

a) 12:f4:5c:7b:80:5a

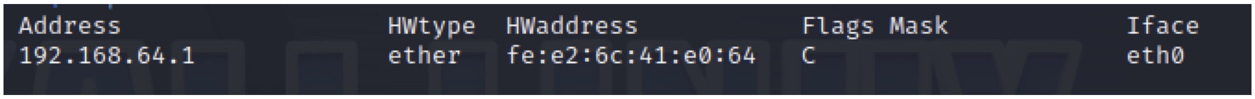
b) 192.168.64.4

c) 32:2e:91:a5:c6:c2

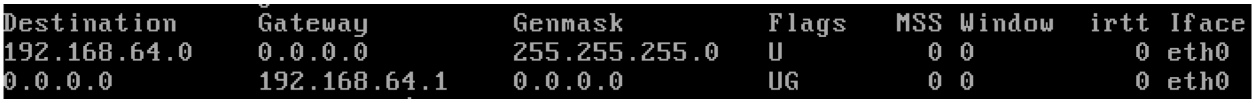
d) 192.168.64.5

e) 

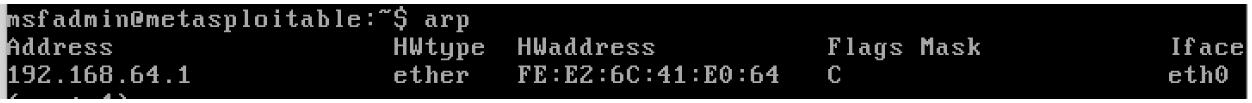
```
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         192.168.64.1    0.0.0.0         UG        0 0          0 eth0
192.168.64.0    0.0.0.0         255.255.255.0   U         0 0          0 eth0
```

f) 

```
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.64.1             ether   fe:e2:6c:41:e0:64   C                     eth0
```

g) 

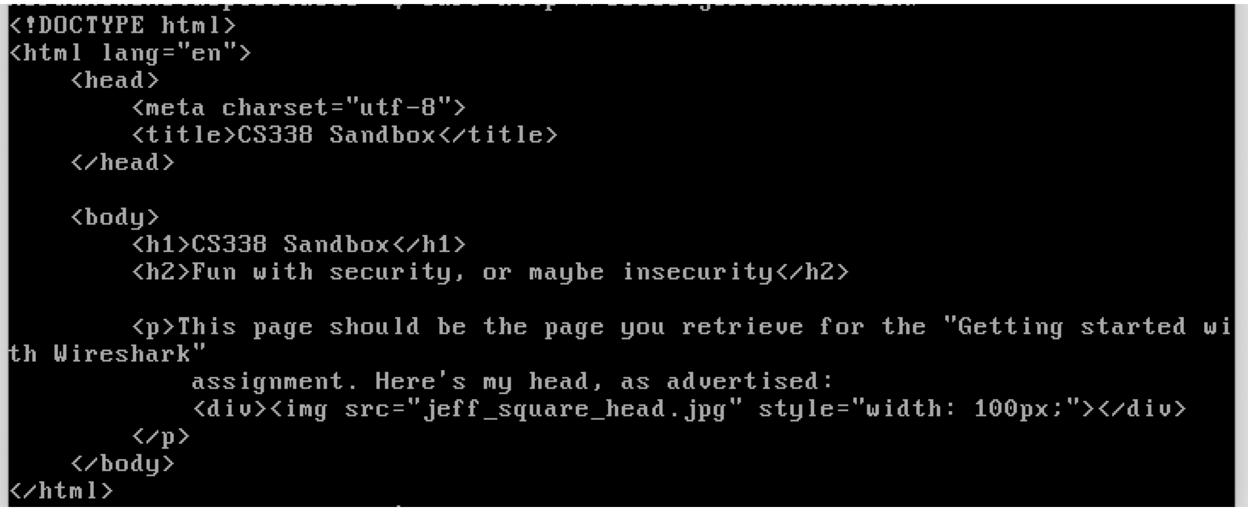
```
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.64.0    0.0.0.0         255.255.255.0   U         0 0          0 eth0
0.0.0.0         192.168.64.1    0.0.0.0         UG        0 0          0 eth0
```

h) 

```
msfadmin@metasploitable:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.64.1             ether   FE:E2:6C:41:E0:64   C                     eth0
```

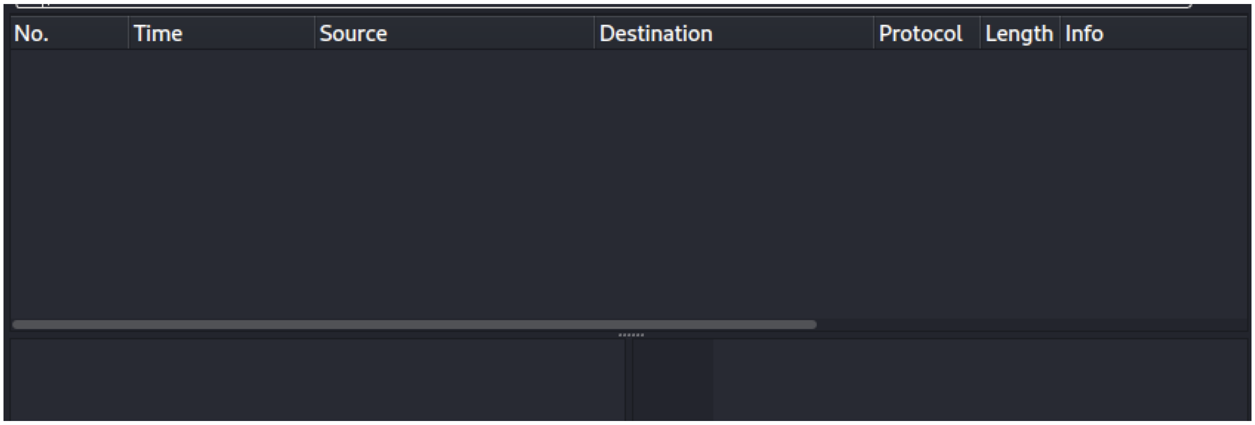
i) Metasploitable will first get the IP address of cs338.jeffondich.com using DNS. When it has finally found the correct IP address it will check the routing table to see if the IP address of cs338.jeffondich.com is an internal one by using the genmask. It will and the IP address of the website to the genmask of the IP addresses, and compare it to the address column. However, it will not find a local address. As it is not a local IP address it will go to default, or 192.168.64.1, in this case (it is on the gateway column). Then metasploitable will check on the ARP table to see what the MAC address of 192.168.61.1 is. The arp table will say it is FE:E2:6C:41:E0:64. So it will forward the packet to that address.

j) I do see an HTTP response on metasploitable, it is an html file like the following:



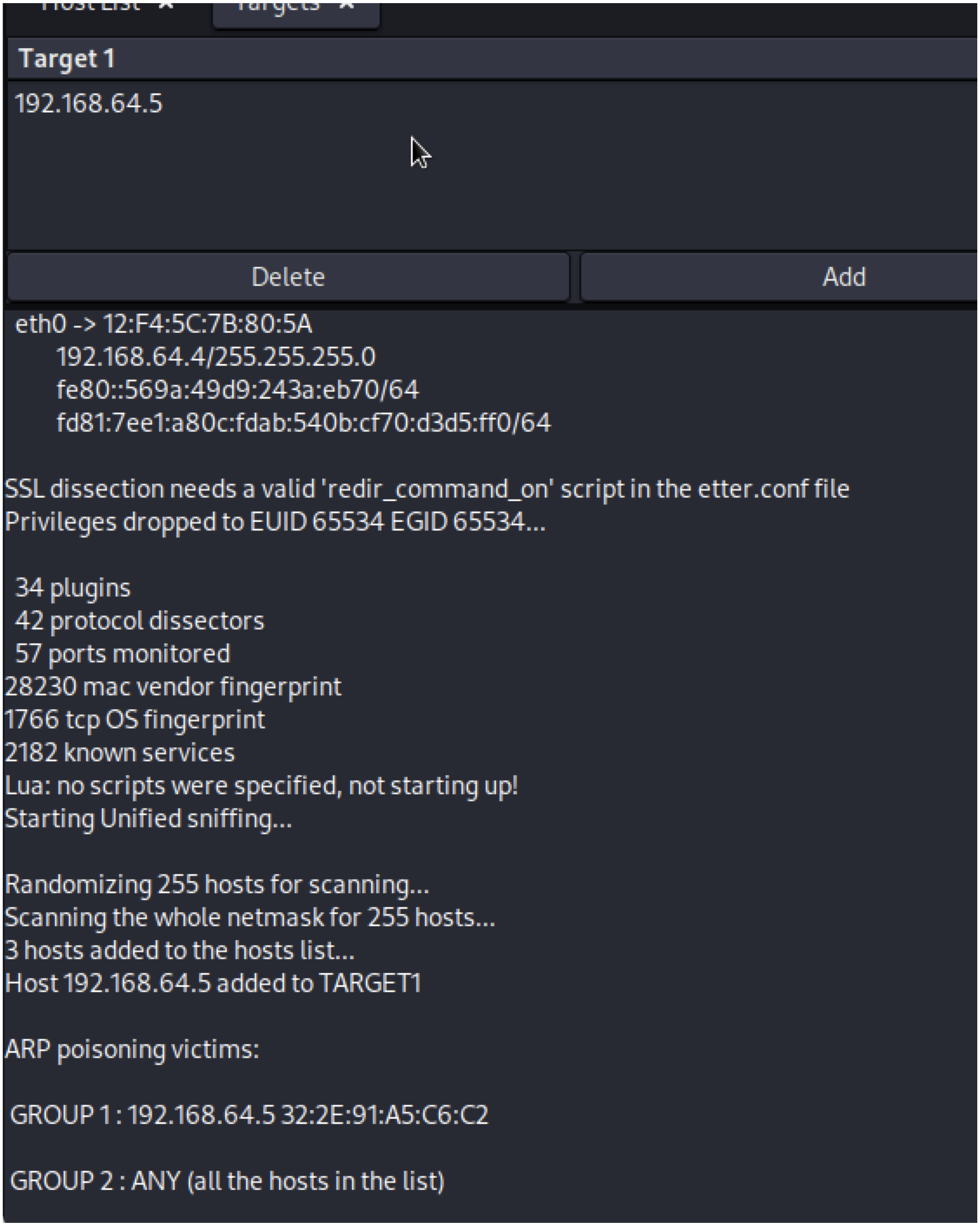
```
<!DOCTYPE html>
<html lang="en">
    <head>
        <meta charset="utf-8">
        <title>CS338 Sandbox</title>
    </head>

    <body>
        <h1>CS338 Sandbox</h1>
        <h2>Fun with security, or maybe insecurity</h2>

        <p>This page should be the page you retrieve for the "Getting started wi
th Wireshark"
            assignment. Here's my head, as advertised:
            <div><img src="jeff_square_head.jpg" style="width: 100px;"></div>
        </p>
    </body>
</html>
```

So yeah, I do have a response on metasploitable. However, I do not have a response on Wireshark. I assume that my laptop routed the response directly to metasploitable and Kali did not receive it at all.
Here is a screenshot of Wireshark:



No.	Time	Source	Destination	Protocol	Length	Info

k)



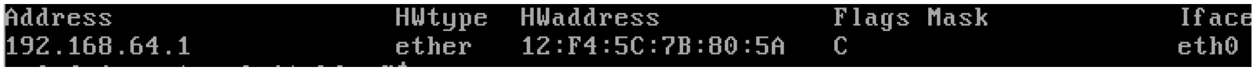
Target 1

```
192.168.64.5
```

```
eth0 -> 12:F4:5C:7B:80:5A
    192.168.64.4/255.255.255.0
    fe80::569a:49d9:243a:eb70/64
    fd81:7ee1:a80c:fdab:540b:cf70:d3d5:ff0/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to EUID 65534 EGID 65534...

 34 plugins
 42 protocol dissectors
 57 ports monitored
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
3 hosts added to the hosts list...
Host 192.168.64.5 added to TARGET1

ARP poisoning victims:

 GROUP 1 : 192.168.64.5 32:2E:91:A5:C6:C2

 GROUP 2 : ANY (all the hosts in the list)
```

Done!

l)



```
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.64.1             ether   12:F4:5C:7B:80:5A   C                     eth0
```

Now the MAC address on it is Kali’s MAC address.

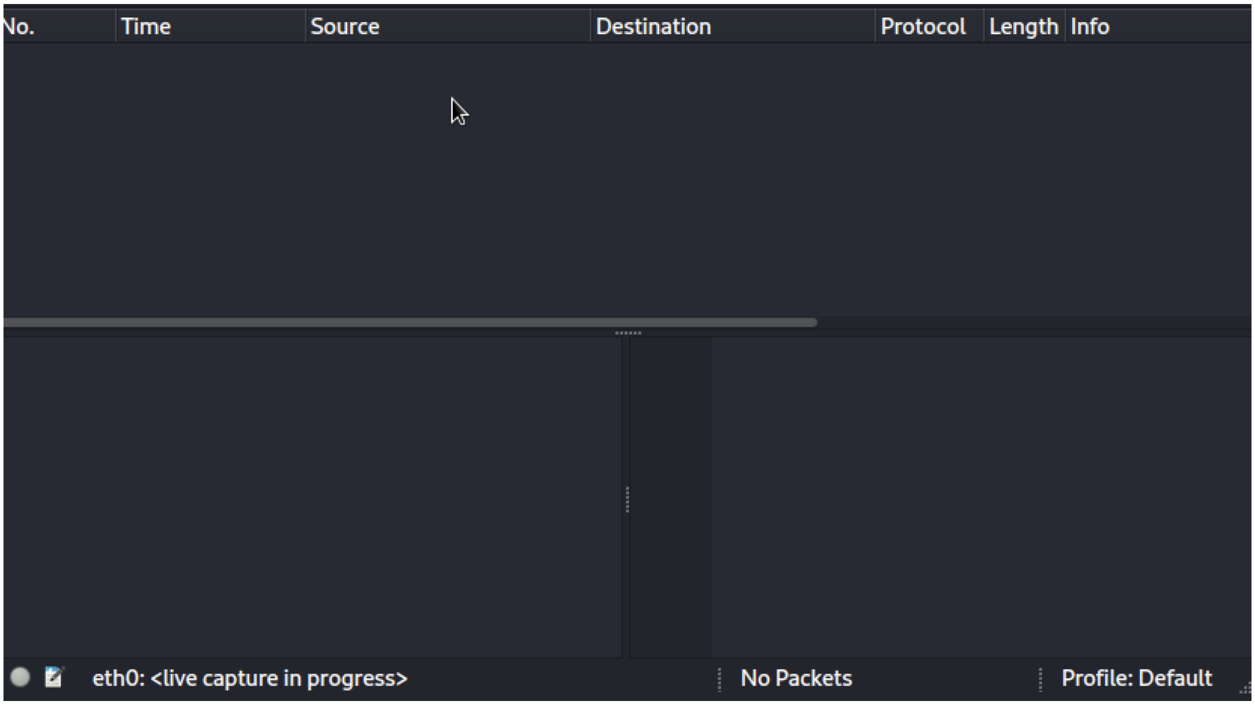
Originally it was the MAC address of the device Metasploitable had to send packages to when it wanted to communicate with external machines (or external IP addresses). However, Kali changed it. Now it is Kali’s MAC address.

m) Wireshark will be able to capture and read the packets. Now Kali is in the middle of Metasploitable and the router, so it will receive the packets that metasploitable sends. Kali will read them before sending them along.

The Metasploitable cache originally had the correct MAC address Metasploitable had to forward packets to when it wanted to communicate with external IP addresses. This was the correct MAC address and it would just help send the packets to the target IP address. However, Metasploitable’s ARP cache has been poisoned. This means that Kali managed to convince Metasploitable that Kali’s MAC address is the one that should receive packets when Metasploitable wants to communicate with an external IP. However, Mal operates Kali and will be able to read the packets. In other words, it is an MAC address in the middle of Alice and the router. Kali will read the packets before forwarding them to the correct MAC address that (that will help deliver the packets to cs338.jeffondich.com).

In summary, instead of forwarding the packets to FE:E2:6C:41:E0:64, Alice will forward packets to 12:f4:5c:7b:80:5a that is Kali’s MAC address.

n)



No. Time Source Destination Protocol Length Info

eth0: <live capture in progress> No Packets Profile: Default

Done

o) Yes, I see a response on Metasploitable. Yes, I captured packets on Wireshard. I can tell which messages whent back and forth.

The connection started when Alice sent a SYN packet to connect to Bob. Kali captured that and retransmitted it to Bob (it is the adversary in the Middle). As Alice had not received an ACK packet before the timer expired, Alice assumed the packet had been lost, so she retransmitted the SYN packet.

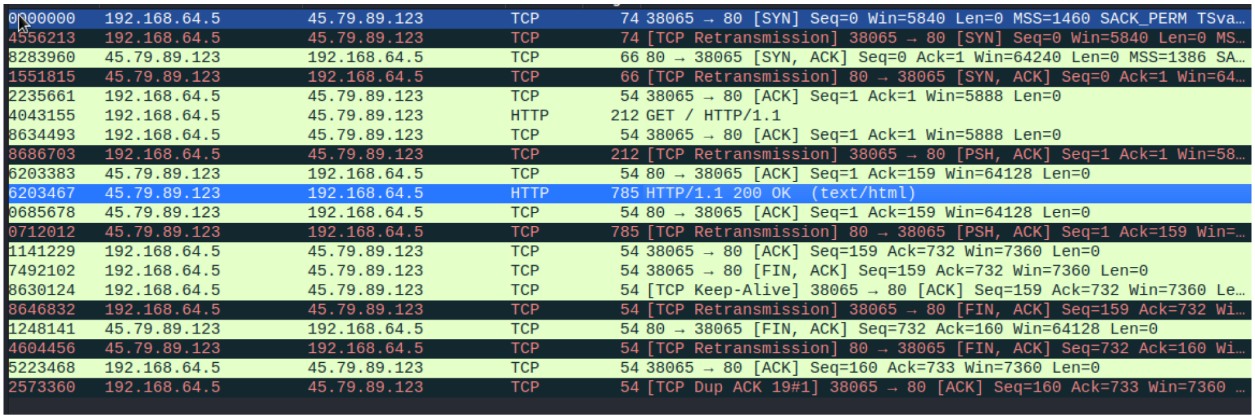
The server replies to this with a [SYN, ACK] packet, meaning that bob received the SYN packet forwarded by Mal (who is in the middle of Alice and Bob), and that it also wants to be able to send messages (the communication will happen both ways). Similarly, this packet also had to be retransmitted.

Mal forwarded this packet to Alice, who replied with an ACK packet, confirming that she received the packet and concluding the three way handshake. Alice then sends to Mal (who will forward to Bob) the HTTP request in the GET / HTTP/1.1 packet. Bob replies with an ACK packet confirming the reception of the packet.

Alice then sends a [PSH, ACK] packet. PSH is sent by Alice. It means that if the receiving machine's TCP implementation has not yet provided the data it received a request for, it should do so at that point. In other words, this means that Bob should not wait for more data to start sending Alice the packets. There is also a package acknowledgement there.

Bob responds with an ACK and the very next packet he sends has code 200 OK and is the desired HTML file.

Bob then sends an ACK, and proceeds to send a [PSH, ACK] packet. Alice replies with an ACK and later sends the [FIN, ACK] packet, aiming to finish the communication. There are a few retransmissions and Keep alives in this part. But the communication is concluded.



```
0000000  192.168.64.5   45.79.89.123   TCP    74 38065 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSva…
4556213  192.168.64.5   45.79.89.123   TCP    74 [TCP Retransmission] 38065 → 80 [SYN] Seq=0 Win=5840 Len=0 MS…
8283960  45.79.89.123   192.168.64.5   TCP    66 80 → 38065 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1386 SA…
1551815  45.79.89.123   192.168.64.5   TCP    66 [TCP Retransmission] 80 → 38065 [SYN, ACK] Seq=0 Ack=1 Win=64…
2235661  192.168.64.5   45.79.89.123   TCP    54 38065 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0
4043155  192.168.64.5   45.79.89.123   HTTP  212 GET / HTTP/1.1
8634493  192.168.64.5   45.79.89.123   TCP    54 38065 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0
8686703  192.168.64.5   45.79.89.123   TCP   212 [TCP Retransmission] 38065 → 80 [PSH, ACK] Seq=1 Ack=1 Win=58…
6203383  45.79.89.123   192.168.64.5   TCP    54 80 → 38065 [ACK] Seq=1 Ack=159 Win=64128 Len=0
6203467  45.79.89.123   192.168.64.5   HTTP  785 HTTP/1.1 200 OK  (text/html)
0685678  45.79.89.123   192.168.64.5   TCP    54 80 → 38065 [ACK] Seq=1 Ack=159 Win=64128 Len=0
0712012  45.79.89.123   192.168.64.5   TCP   785 [TCP Retransmission] 80 → 38065 [PSH, ACK] Seq=1 Ack=159 Win=…
1141229  192.168.64.5   45.79.89.123   TCP    54 38065 → 80 [ACK] Seq=159 Ack=732 Win=7360 Len=0
7492102  192.168.64.5   45.79.89.123   TCP    54 38065 → 80 [FIN, ACK] Seq=159 Ack=732 Win=7360 Len=0
8630124  192.168.64.5   45.79.89.123   TCP    54 [TCP Keep-Alive] 38065 → 80 [ACK] Seq=159 Ack=732 Win=7360 Le…
8646832  192.168.64.5   45.79.89.123   TCP    54 [TCP Retransmission] 38065 → 80 [FIN, ACK] Seq=159 Ack=732 Wi…
1248141  45.79.89.123   192.168.64.5   TCP    54 80 → 38065 [FIN, ACK] Seq=732 Ack=160 Win=64128 Len=0
4604456  45.79.89.123   192.168.64.5   TCP    54 [TCP Retransmission] 80 → 38065 [FIN, ACK] Seq=732 Ack=160 Wi…
5223468  192.168.64.5   45.79.89.123   TCP    54 38065 → 80 [ACK] Seq=160 Ack=733 Win=7360 Len=0
2573360  192.168.64.5   45.79.89.123   TCP    54 [TCP Dup ACK 19#1] 38065 → 80 [ACK] Seq=160 Ack=733 Win=7360 …
```

p) The first ARP packet is sent by Kali. I know that as the sender's MAC address is 12:f4:5c:7b:80:5a. The target MAC address is 32:2e:91:a5:c6:c2 that is metasploitable. The packet also contains both the IP address Kali is trying to impersonate (Sender IP address: 192.168.64.1) and Metasploitable's real IP address (Target IP address: 192.168.64.5). The Opcode of this packet is reply (2), and the protocol type is IPv4. It is important to outline that 192.168.64.1 is NOT Kali's IP address, it is the address of the router (that Kali is trying to impersonate). So, Kali is introducing itself to Metsploitable saying it has the IP address Metasploitable forwards its packets to (when metasploitable wants to communicate with external machines). In other words, Mal introduces himself to Alice as the router she should forward packets to.

The second ARP packet is also sent from Kali (MAC address 12:f4:5c:7b:80:5a), but this time it is sent to fe:e2:6c:41:e0:64, that is the address Metasploitable was supposed to send external packets to in the first place (the router). However, Kali lies that its IP is 192.168.64.5 (which is Metasploitable's IP address). The target IP address is

192.168.64.1, that is the target's real IP address. The Opcode of this packet is reply (2), and the protocol type is IPv4. So Kali is telling that IP address (which is responsible for forwarding packets that metasploitable sends) that it is Metasploitable.
So it impersonates the machine that forwards external packets to Metasploitable and impersonates Metasploitable to the machine it has to send packets to.
It is introducing itself to both machines, pretending to be a machine it is not.
In a communication, the router thinks it is talking to Alice, while it is talking to Mal, and Alice thinks she is forwarding packets to the router, when it is forwarding packets to Mal.
Observe that there is a target machine and a destination machine. So I assume the packet is only sent to that MAC address, or if it is sent to another MAC address the packet is discarded.
For some reason it does this operation 5 times, maybe it may be rejected once, so the packets are sent a bunch of times to make sure they will be eventually accepted. Or maybe it might take a while for ARP addresses to be updates.

q) First of all, it would not allow ARP packets to have a target and destination machine. They would be visible to everyone on the shared medium. So, if Alice receives an ARP packet from Mal with the claiming he has the router's IP address, the router would be able to send an ARP packet claiming that the packet sent by Mal is false, and that the IP address sent by Mal does not belong to him.
Mal could do this a couple of times, and be rejected every single time.
The only way for Alice to update the IP address she is forwarding packets to is if a new device is introduced (a new router for example), the old device is no longer in the network. In this case, the new device would send the instruction for Alice to update the MAC address related to that IP address, and the old device would not contest it, as it would no longer be in the network.

Synthesis

a) Alice is connected to a network and she is potentially sharing packets over the internet. The IP addresses she wants to talk to might not be on the same shared medium (let alone her computer). So, in order to communicate with them, she must forward those packets to the router, which will help the packets reach whoever Alice wants to talk to. Mal wants to intercept the packets sent by Alice to Bob, and he has a plan. Instead of Alice sending her IP packets to the router, Mal wants Alice to send him the packets first, so he can read (and potentially modify them), before he forwards the packets to the router. To do so, Mal's computer sends an ARP packet to Alice's computer saying that his MAC address (which is exclusive to Mal's device) has the IP address that is responsible to forward Alice's packets to Bob. In other words, he is impersonating the router to Alice. He is introducing himself to Alice saying "hey, I have this IP address, and this MAC address can you update your ARP cache?" Alice will update her cache, and whenever she wants to communicate with an external IP address, she will forward her packets to Mal.

Mal also wants the router to think he is Alice. So he sends it an ARP packet with his MAC address and Alice's IP address. In other words, Mal is introducing himself to the router saying "Hey, I am Alice, this is my IP address and this is my MAC address, can you update your ARP cache?" The router will do that.

This way Alice will forward her packets to Mal (who then forwards them to the router), and the router will forward packets to Mal (instead of Alice).

b) No. Alice does not know she is sending packets to Mal. She thinks she is sending packets to the router who will forward them to Bob. She knows that she updated the ARP cache, but she does not know that the updated entry on her ARP cache is Mal and not the router. She does not make any checks when she receives an ARP request telling her to update a MAC address. She just believes it and updates the router's MAC address (or better the MAC address associated with that IP address). At no point she tried to reach the router's previous MAC address to see if it still exists. And she does not ask the original MAC address whether it still has the same IP address.

   Whenever Alice receives an ARP packet that tells her to update a MAC address on her ARP cache, she should make some checks. She can reach out to the previous MAC address on her ARP cache to see if it is still associated with that IP address. If it is, she should not update it. If she gets no response she should update the MAC address (this might mean that the router has been replaced), and if the router responds that it changed its IP address she can update her ARP cache.

c) Bob also does not know. This happens because Mal is impersonating Alice to Bob as well. So, Bob thinks that the packages are coming from Alice, when they are in fact coming from Mal. Whenever Bob's packets reach the router, the router sends them directly to Mal (the router believes Mal is Alice). So the server does not detect this. Bob really believes that he is talking to Alice.

   Realistically, Bob is a web server, and web servers usually talk to everybody, and not to just some specific IP addresses. So he does not care whether he is talking to Mal or to Alice, Bob will just respond. The most he will do is demand some sort of authentication to access some pages, but he will send the pages to whoever is authorized.

d) Yes, this attack could be detected. In an HTTPS connection Alice will start by doing the Diffie-Helmann key exchange and will then check Bob's certificate. She will get the data on the certificate (which says Bob.com, his private key, hash, and a lot of other information), and hash it. She will then decrypt the signature on the certificate with the public key of the certificate authority that is hardcoded in her laptop. She will see that the digest that she produced matches the signature, and so the certificate is valid. She will then send Bob a challenge. She will send a number for him to encrypt with his private key. She will receive the number encrypted with his private key and will be able to decrypt it. So it was encrypted with Bob's private key. However, Bob will concatenate his Diffie-Hellman numbers to the key. If they match with what Alice is expecting she is indeed talking to Bob. Otherwise, she is talking to Mal and can end the communication (as the Diffie-Hellman numbers are likely very different).

https://osqa-ask.wireshark.org/questions/20423/pshack-wireshark-capture/

https://wiki.wireshark.org/TCP_Analyze_Sequence_Numbers#:~:text=TCP%20Retransmission%20%2D%20Occurs%20when%20the,expiration%20of%20the%20acknowledgement%20timer.