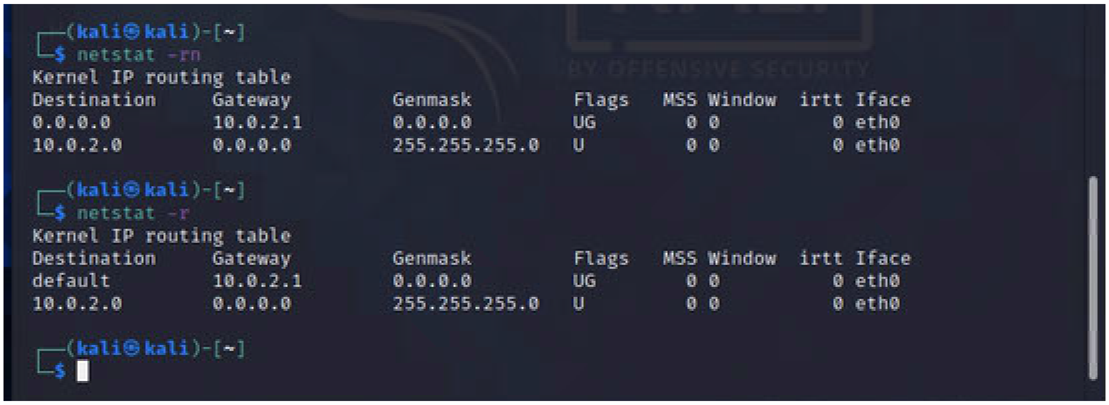
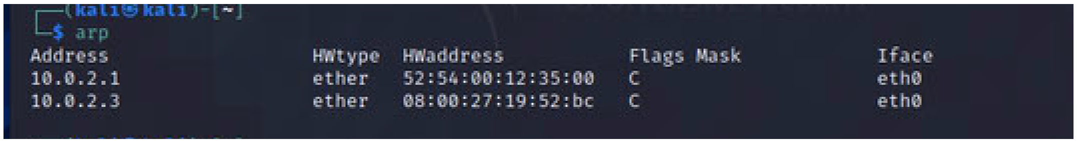
Yasmeen Awad
ARP Spoofing

a. 08:00:27:11:cf:53
b. 10.0.2.15
c. 08:00:27:1a:45:12
d. 10.0.4.2
e.



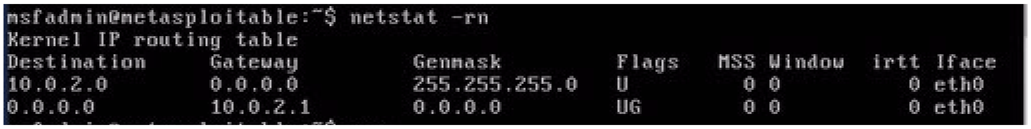
```
┌──(kali㉿kali)-[~]
└─$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         10.0.2.1        0.0.0.0         UG        0 0          0 eth0
10.0.2.0        0.0.0.0         255.255.255.0   U         0 0          0 eth0

┌──(kali㉿kali)-[~]
└─$ netstat -r
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

┌──(kali㉿kali)-[~]
└─$ █
```

f.



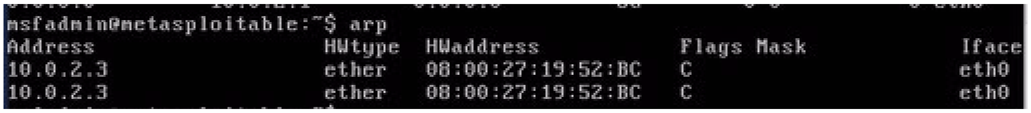
```
┌──(kali㉿kali)-[~]
└─$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.1                 ether   52:54:00:12:35:00   C                     eth0
10.0.2.3                 ether   08:00:27:19:52:bc   C                     eth0
```

g.



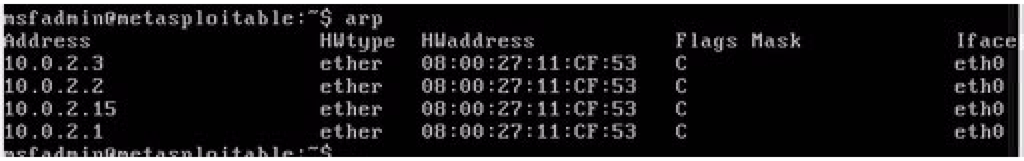
```
msfadmin@metasploitable:~$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
10.0.2.0        0.0.0.0         255.255.255.0   U         0 0          0 eth0
0.0.0.0         10.0.2.1        0.0.0.0         UG        0 0          0 eth0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

h.



```
msfadmin@metasploitable:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.3                 ether   08:00:27:19:52:BC   C                     eth0
10.0.2.3                 ether   08:00:27:19:52:BC   C                     eth0
```

i. 52:54:00:12:35:00
j. There is a response on Metasploitable with the webpage HTML, but no packets are captured on wireshark because it is running on a separate virtual machine. It cannot capture packets sent from Metasploitable to jeffondich.com because we have not started the MITM attack yet.
k. Done.
l. New ARP cache:



```
msfadmin@metasploitable:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.3                 ether   08:00:27:11:CF:53   C                     eth0
10.0.2.2                 ether   08:00:27:11:CF:53   C                     eth0
10.0.2.15                ether   08:00:27:11:CF:53   C                     eth0
10.0.2.1                 ether   08:00:27:11:CF:53   C                     eth0
msfadmin@metasploitable:~$
```

Kali has convinced the Metasploitable machine to send transmissions to its MAC (08:00:27:11:cf:53) address, and has drawn a “link” between Kali’s MAC address and the IPs 10.0.2.3, 10.0.2.2, 10.0.2.15, and 10.0.2.1.

m. It will send to the Kali MAC address 08:00:27:11:cf:53 because we are doing a MITM attack and have convinced Metasploitable that the Kali MAC address is the destination address, when in reality Metasploitable is talking to Kali which is talking to cs231.jeffondich.com.
n. Done.
o. Yes, we still get a response on Metasploitable of the HTML webpage we requested. Yes, we see captured packets in wireshark, including the "messages" to and from Metasploitable and cs231.jeffondich.com
p. We have convinced Metasploitable to link the Kali MAC address with cs231.jeffondich.com's IP address, meaning it will send all of its transmissions to cs231.jeffondich.com through Kali, which will pass on the information (both ways), acting as cs231.jeffondich.com. We did this convincing by having Kali respond when Metasploitable asked "who has 10.0.2.3?" on the local network (which Kali and Metasploitable are both connected to). Metasploitable then uses its modified ARP cache (which links all IP addresses to Kali's MAC address) to lookup the IP it wants to send a packet to, and the corresponding MAC address. It then initiates contact with that MAC address (in this case, Kali's) and starts the HTTP query.
q. To detect ARP spoofing: keep an eye out for servers requesting to change the ARP cache who claim that their own MAC address is tied to multiple IP addresses. Use some cutoff to restrict MAC addresses from being linked to too many different IP addresses (no more than 2 or 3?). This leaves some room for false positives, as MAC addresses can be linked to multiple IPs, so it would be good to have another layer of checking which allows computers to petition to bind multiple IPs to one MAC address, with some verification that the MAC address listed actually corresponds to the IP addresses.