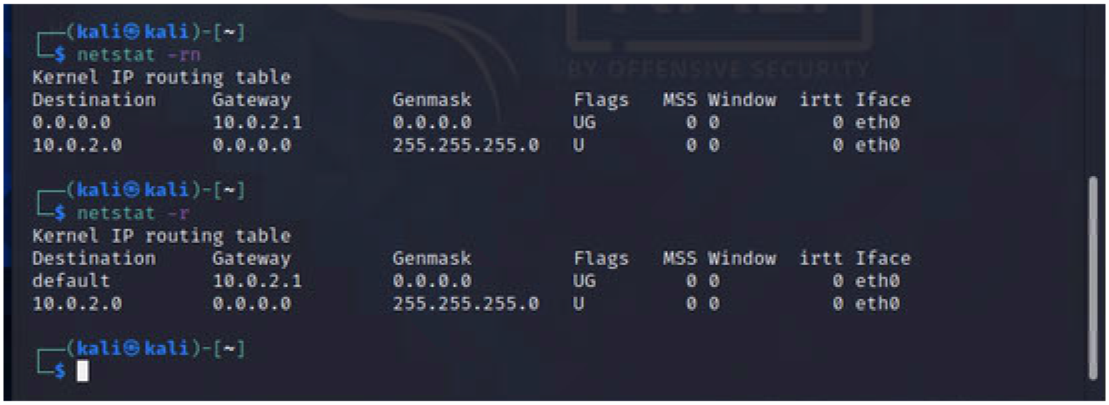
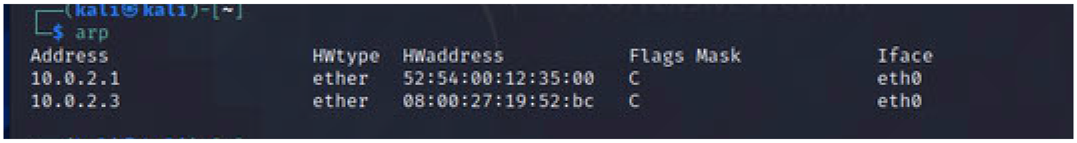
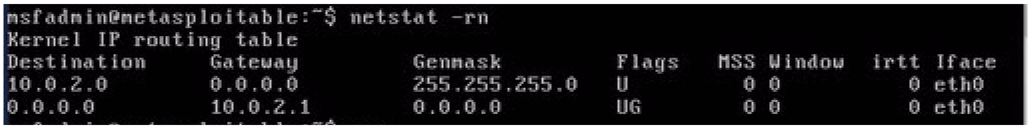
Yasmeen Awad
ARP Spoofing

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. 

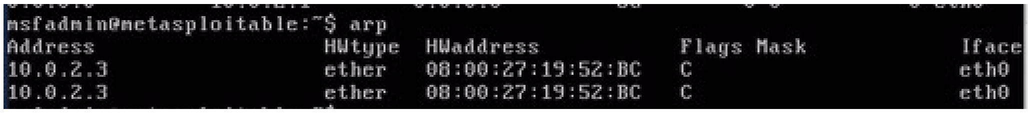
```
┌──(kali㉿kali)-[~]
└─$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         10.0.2.1        0.0.0.0         UG        0 0          0 eth0
10.0.2.0        0.0.0.0         255.255.255.0   U         0 0          0 eth0

┌──(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
```

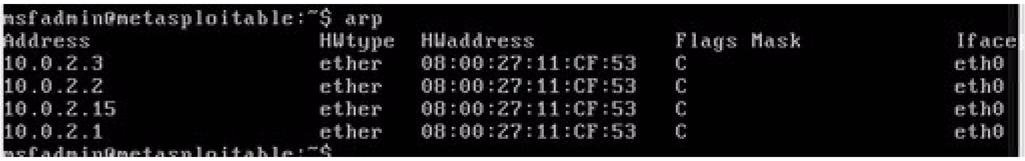
g. 

```
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.
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:~$
```

New IP addresses were added to the ARP cache

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.