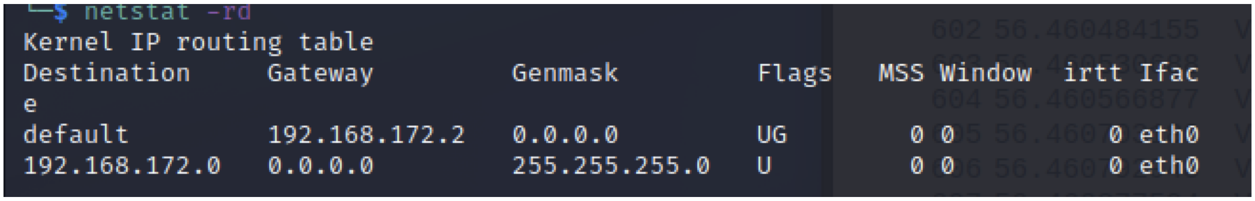
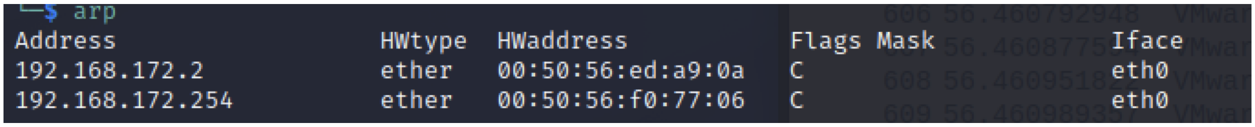
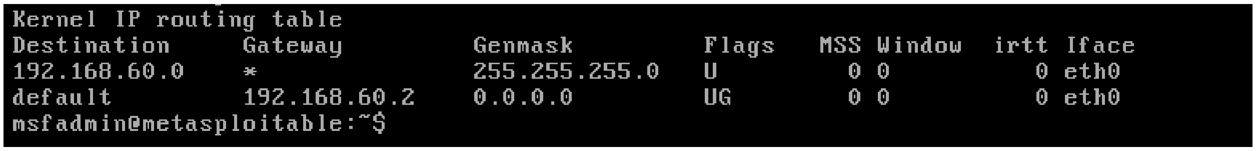
Charlie Roslansky and Silas Rhyneer

a. 00:0c:29:59:88:5c
b. 192.168.172.130
c. 00:0c:29:08:07:fe
d. 192.168.172.131
e. 

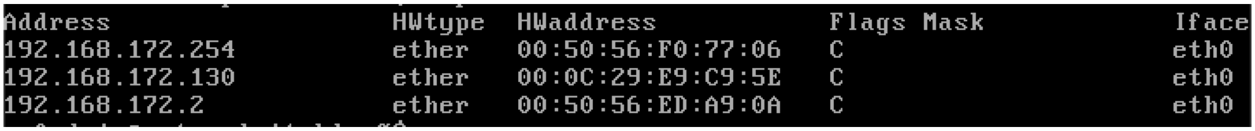
```
└─$ netstat -rd
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Ifac
e
default         192.168.172.2   0.0.0.0         UG        0 0          0 eth0
192.168.172.0   0.0.0.0         255.255.255.0   U         0 0          0 eth0
```

f. 

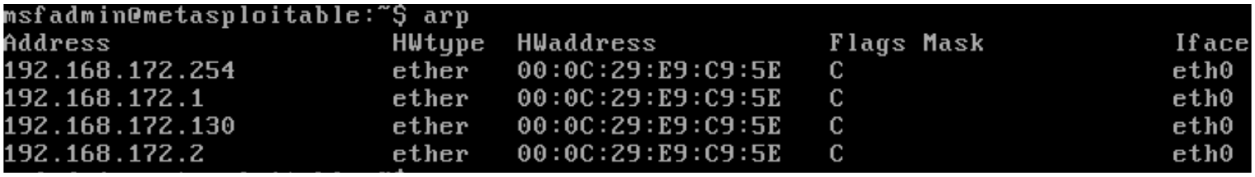
```
└─$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.172.2            ether   00:50:56:ed:a9:0a   C                     eth0
192.168.172.254          ether   00:50:56:f0:77:06   C                     eth0
```

g. 

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.60.0    *               255.255.255.0   U         0 0          0 eth0
default         192.168.60.2    0.0.0.0         UG        0 0          0 eth0
msfadmin@metasploitable:~$
```

h. 

```
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.172.254          ether   00:50:56:F0:77:06   C                     eth0
192.168.172.130          ether   00:0C:29:E9:C9:5E   C                     eth0
192.168.172.2            ether   00:50:56:ED:A9:0A   C                     eth0
```

i. 00:50:56:ED:A9:0A - it is the MAC address associated with the IP 192.168.60.2, which is listed as the default gateway in Metaspoitable's routing table. All connections outside of Carleton's local network get sent through the gateway.
j. We do see a response on metasploitable consisting of the html for the requested page. We also see the TCP handshake, GET request, and ACK and FIN messages between jeffondich.com and metasploitable.
k. Stuff
l. 

```
msfadmin@metasploitable:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.172.254          ether   00:0C:29:E9:C9:5E   C                     eth0
192.168.172.1            ether   00:0C:29:E9:C9:5E   C                     eth0
192.168.172.130          ether   00:0C:29:E9:C9:5E   C                     eth0
192.168.172.2            ether   00:0C:29:E9:C9:5E   C                     eth0
```

They are all now the same MAC address, specifically Kali's. Bwahahaha…
m. We predict it will send its GET request to the kali machine first, which will forward it on to the gateway. The MAC address points to the Kali machine, so we will be able to evesdrop on their outgoing packets.
n. More stuff
o. On metasploitable, we still still see the same http response and html for the sandbox page. On Wireshark, we are seeing all the the packets involved in this exchange.
p. Kali sends a bunch of ARP messages to Metasploitable, telling it that each IP address corresponds to Kali's MAC address (a "gratuitous ARP message", according to the wikipedia page on ARP). In this way, all of metasploitable's ARP cache was "poisoned"

with our MAC address, so whenever it sends a message to any IP address in its cache, it will route it through Kali first.

q. There are quite a few steps we could take

    i. Whenever the cached MAC address changes, it’s a red flag that something’s up. We’ll get false positives when a MAC address changes for normal reasons, but this doesn’t happen super frequently.

    ii. If we have a lot of IP addresses all pointing to the same MAC address, it’s also suspicious. If they ALL point to the same MAC address, it’s even more suspicious. This would be more difficult to implement on super small networks, where there might only be one of two machines.