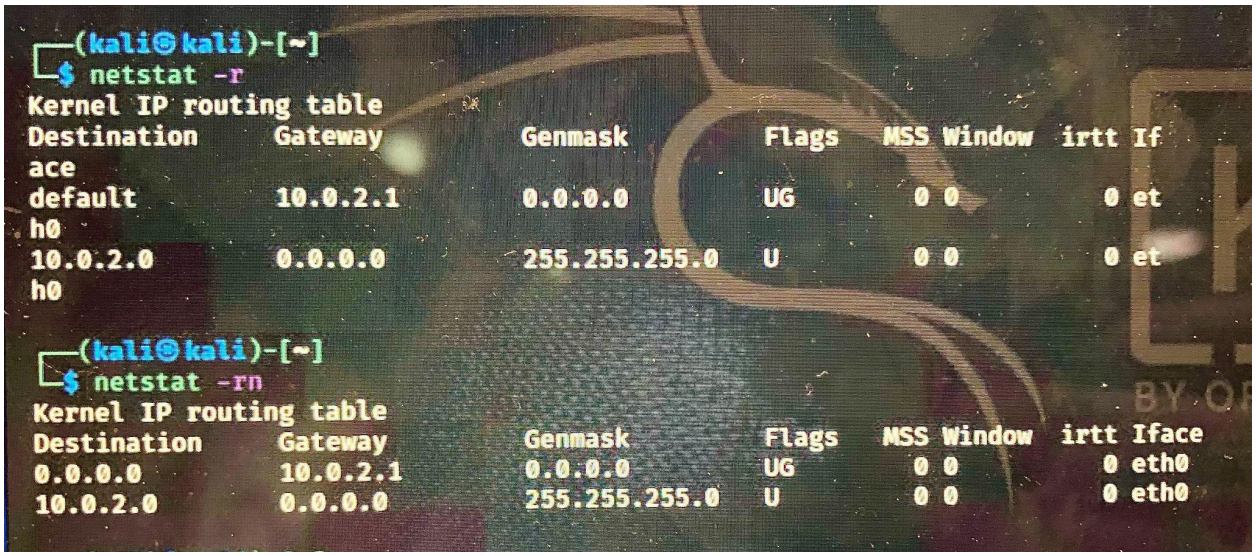
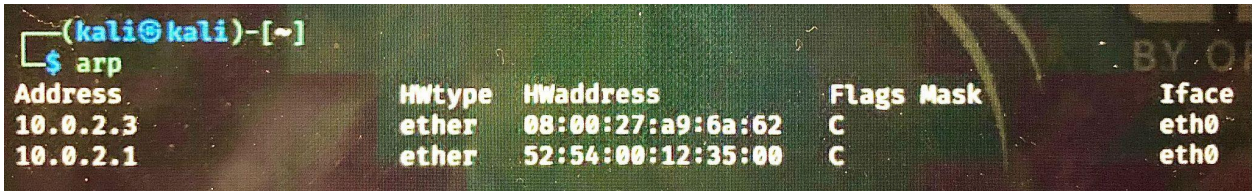
Adela Dujsikova & Ethan Li
Professor Jeff Ondich
CS 231

# ARP Spoofing

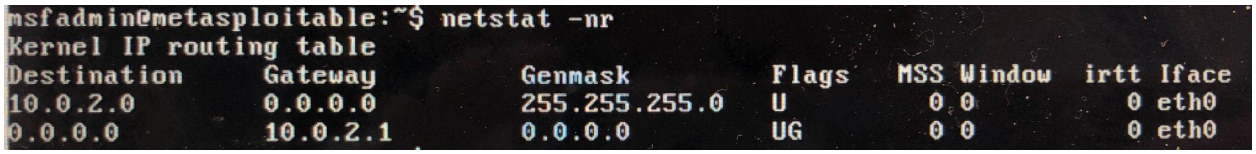
a. 08:00:27:11:cf:53 (ifconfig | grep ether)
b. 10.0.2.15 (used the very first IP address, command: ifconfig eth0 | grep 'inet')
c. 08:00:27:1a:45:12 (ifconfig | grep HWaddr)
d. 10.0.2.4 (ifconfig eth0 | grep 'inet addr:' | cut -d: -f2 | awk '{ print $1}')
e. Kali's routing table:



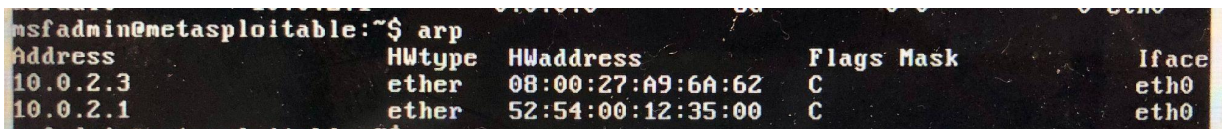

f. Kali's ARP cache:



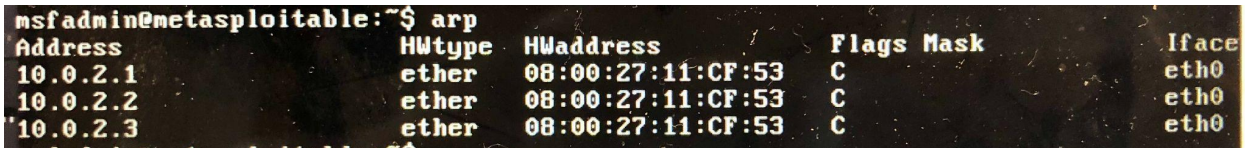

g. Metasploitable's routing table:




h. Metasploitable's ARP cache:

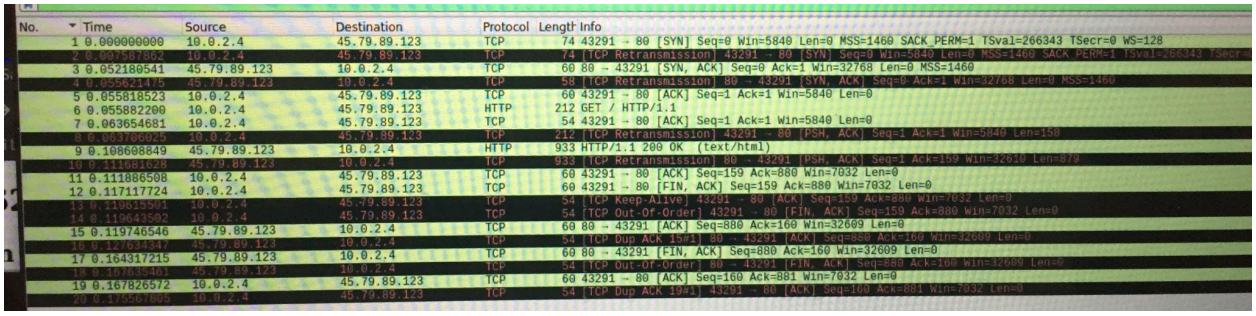


i. The server MAC address, 52:54:00:12:35:00. This is because the gateway of reaching the default address (0.0.0.0) is through 10.0.2.1, as listed on the routing table. And by looking up the ARP cache, the associated MAC address is the one listed above.
j. There is a response from Metasploitable, but no packets are captured from Wireshark on Kali.
k. Did that
l. Metasploitable's ARP cache:




After using Ettercap, all HWaddress values were changed to the one that is actually associated with Kali. This means that whenever Metasploitable tries to send packets to a certain IP address, it will use the Kali's MAC address to do so. Therefore all the outgoing packets will be directed to Kali.

m. To Kali's MAC address, 08:00:27:11:cf:53, because that is the MAC address that Metasploitable associates with the server now. The ARP cache is like a phonebook that stores which IP address corresponds to which MAC address. Ettercap changed the MAC addresses to Kali's address, therefore even though Metasploitable wanted to communicate with the server, it actually communicated with Kali. Kali became the man in the middle!
n. Did that
o. Yes, yes, and yes. We can see the response on Metasploitable and also capture the packets on Wireshark. This means that the packets from Metasploitable are sent to Kali, Kali sends them to the server (intended destination), and then it forwards the packets it receives to Metasploitable. This way Kali observes the whole exchange and Metasploitable receives what it asked for. The picture below shows the whole captured exchange in Wireshark.




p. About every 10 seconds, Kali's MAC address will claim to be the IP address of the target (Metasploitable, at 10.0.2.4), and telling all of its contacts that Metasploitable's IP address is at the MAC address of Kali. At the same time, Kali's MAC address will claim to be the IP address of all of the targets' contacts

(10.0.2.1 to 10.0.2.3), sending messages to Metasploitable and telling it that all of their associated MAC addresses are Kali's MAC address. As a result, the poisoning "floods" the ARP cache so that all of the IP addresses are linked to the MAC address of Kali and Kali becomes the person-in-the-middle.

q. Check ARP cache for multiple IP addresses being associated with one MAC address. False positives would be generated in cases when a legitimate organisation/server has multiple IP addresses connected to the same MAC address.
   Alternatively, check if ARP packages are being "flooded" frequently. As the poisoning seems to occur by repeatedly sending ARP packages. False positives could occur if there were legitimate reasons for a machine that is repeatedly setting up new connections with other machines and sending the ARP packages frequently.