Owen Barnett and Nick Pandelakis
CS: 231
23 April 2021

Arp Spoofing

A. Kali mac address: 08:00:27:69:24:65
B. Kali Ip address: 10.0.2.15
C. Metasploitable Mac address: 08:00:27:86:68:1f
D. Metasploitable Ip address: 10.0.2.4
E. Kernel IP routing table

Destination	Gateway	Genmask	Flags	MSS	Window	irtt	Iface
default	10.0.2.2	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

F.

Address	HWtype	HWaddress	Flags Mask	Iface
10.0.2.1	ether	52:54:00:12:35:00	C	eth0

G.

Destination	Gateway	Genmask	Flags	MSS	Window	irtt	Iface
10.0.2.0	*	255.255.255.0	U	0	0	0	eth0
default	10.0.2.2	0.0.0.0	UG	0	0	0	eth0

H.

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:E8:B1:CA	C	eth0

I. Metasploitable should send the first SYN packet to the mac address 52:54:00:12:35:00. As near as we can tell, this must be the MAC address of a router or other Carleton network device, since after curl-ing a page on metasploitable, this MAC address showed up in the arp cache. It also matches the MAC address of both of our Kali arp caches.
J. There is an HTTP response on Metasploitable, but we did not see any packets captured by wireshark on Kali.
K.
L.

Address	HWtype	HWaddress	Flags Mask	Iface
10.0.2.1	ether	08:00:27:69:24:65	C	eth0
10.0.2.3	ether	08:00:27:69:24:65	C	eth0
10.0.2.2	ether	08:00:27:69:24:65	C	eth0
10.0.2.15	ether	08:00:27:69:24:65	C	eth0

Metasploitable added Kali's ip address to its arp cache. Additionally another ip address was added. For all of the ip addresses above, however, the MAC address was changed to Kali's MAC address.

M. Metasploitable will send those packets to the MAC address 08:00:27:69:24:65, since every network device it knows of now has this MAC address. When it wants to send the

packets it will first look in the arp cache and since the IP address is in there, it will use the stored MAC address, which happens to be corrupted.

N.

O. We are able to see all of what went back and forth between Metasploitable and cs231.jeffondich.com. We can see the TCP handshake, the get request from Metasploitable, the website's response, and the FIN, ACK sequence after everything is done.

P. Ettercap broadcasts to Metasploitable that the MAC addresses for all of the network devices (as well as Kali's ip address) are Kali's MAC address. Metasploitable then stores these ip and mac addresses in its arp cache.

Q. We could detect this attack if we checked if any pair of ip addresses shared a MAC address. The MAC addresses should be unique, so any 2 or more devices sharing such an address would be extremely fishy.