CS338 Assignment ARP Spoofing

Kuo Wang

April 2022

1 Tasks

a. 00:0c:29:dc:1d:df

b. 192.168.88.128

c. 00:0c:29:8c:02:4b

d. 192.168.88.129

e. it is as below:

Destination	Gateway	Genmask	Flags	MSS Window	irtt	Iface
default	192.168.88.2	0.0.0.0	UG	0 0	0	eth0
192.168.88.0	0.0.0.0	255.255.255.0	U	0 0	0	eth0

f. it is as below:

Address	HWtype	HWaddress	Flags Mask	Iface	irtt	Iface
192.168.88.254	ether	00:50:56:fd:27:c4	C	eth0	0	eth0
192.168.88.2	ether	00:50:56:e2:9f:ea	C	eth0	0	eth0

g. it is as below:

Destination	Gateway	Genmask	Flags	MSS Window	irtt	Iface
default	192.168.88.2	0.0.0.0	UG	0 0	0	eth0
192.168.88.0	*	255.255.255.0	U	0 0	0	eth0

h. I ping'd google.com and this is the resulting cache:

address	HWtype	HWaddress	Flags	Flags	Iface
192.168.88.2	ether	00:50:56:E2:9F:EA	C	0 0	eth0

i. The user needs to send it to 00:50:56:E2:9F:EA to get it started, since it is the foremost interface out of which all requests are sent.

j. I see an HTTP response on MS, and I see some captured packets following DHCP, ICMPv6, and ARP protocol. They do not contain interesting information.

k. I followed the guide. This answer holds place for "k".

l. It changed quite considerably. All the IP addresses point to the MAC address of the Kali machine.

address	HWtype	HWaddress	Flags	Mask	Iface
192.168.88.2	ether	00:0C:29:DC:1D:DF	C		eth0
kuo-homePC	ether	00:0C:29:DC:1D:DF	C		eth0
192.168.88.254	ether	00:0C:29:DC:1D:DF	C		eth0
192.168.88.254	ether	00:0C:29:DC:1D:DF	C		eth0

m. It will go to 00:0C:29:DC:1D:DF, since ettercap spoofed the ARP so the sheep connects to 00:0C:29:DC:1D:DF (mal) instead of the correct MAC address.

n. Wireshark started. This answer holds the place for "n".

o. I see an HTTP response on MS. I also see the captured packets in Wireshark including HTTP GET requests and reponses. From Kali, I can also see the sequence of TCP handshake and the back-and-forth of HTTP communications between MS and the web server.

p. Here is what happens:

- After the attack begins, Kali sends to the router the rule that ALL IP's direct to Kali's MAC address. This changes the contents of the ARP cache of MS.
- When MS executes curl, it sends the data packets to Kali via the spoofed MAC address.
- In Kali, Ettercap receives data from MS and relays it to the actual destination. When Ettercap receives the destination's response, it relays the data to MS.
- Meanwhile, all those activities are logged by Wireshark and visible to Mal.

q. One scheme I can think of is an alarm that's triggered whenever a certain numbers of IP addresses direct to the same MAC address in the ARP cache, which is scanned periodically. A false positive alarm is possible when many IP addresses legitimately point to the same MAC address without spoofing.