ARP Poisoning

Time required: 30 minutes

How to Create Screenshots: Please use the Windows Snip and Sketch Tool or the Snipping Tool. Paste a screenshot of just the program you are working on. If you are snipping a virtual machine, make sure your focus is outside the virtual machine before you snip.

1. Press and hold down the **Windows key** & **Shift**, then type **S.** This brings up the on-screen snipping tool.
2. Click and Drag your mouse around whatever you want to snip.
3. Release the mouse button. This places the snip into the Windows Clipboard.
4. Go into Word or wherever you want to paste the snip. Hold down **CTRL**, then type **V** to paste the snip.

Lab Description

Attackers frequently modify the Address Resolution Protocol (ARP) table to redirect communications away from a valid device to an attacker's computer. In this project, you will view the ARP table on your computer and make modifications to it.

NOTE: This will disrupt internet access. You can do this in bridged or NAT. If you do this in bridged, it will stop your internet.

1. Start **Kali**, start a **Terminal** prompt.
2. To view your current ARP table, type **sudo arp** press Enter. The Address is the IP address of another device on the network while the HWaddress is the MAC address of that device.
   NOTE: Help for the arp command: **sudo arp -?**
3. To determine your local network address, type **ip a** and then press Enter.
4. **Insert a screenshot:**

Click or tap here to enter text.

5. To determine your DNS servers, type **sudo cat /etc/resolv.conf**
6. **Insert a screenshot:**

Click or tap here to enter text.

7. To determine your gateway IP address, type **sudo route -n**
8. Record the IP address of the default gateway.
9. **Insert a screenshot:**

Click or tap here to enter text.

10. Change the ARP table entry of the default gateway by typing
    sudo arp -s gatewayaddress madeupmacaddress
    Example in D1: sudo arp -s 10.0.1.1 14:10:12:10:00:00
11. Verify that you can no longer ping the gateway or access the internet.
12. **Insert a screenshot:**

Click or tap here to enter text.

13. Delete the spoofed entry by typing: **sudo arp -d 10.0.1.1** (Substitute your gateway address)
14. Ping your gateway address to re populate your arp table. Use CTRL C to break the ping command after a few successful replies.
15. Type **sudo arp** to see that the gateway no longer has the fake mac address.
16. **Insert a screenshot:**

Click or tap here to enter text.

17. Ping the gateway. Verify internet access.
18. Verify that the correct entry is in your arp table: type **sudo arp**
19. **Insert a screenshot:**

Click or tap here to enter text.

20. **Reflect on what you learned in this assignment.**

Click or tap here to enter text.

Assignment Submission

Attach this completed document to the assignment in Blackboard.