**DAY 17**

**ARP Spoofing:**

ARP: Address resolution protocol

ARP is used to map MAC address to their respective IP address and vice versa

1. PCI (Peripheral component interconnect) sends ARP request to the network requesting the destination device’s MAC address in order to transmit the data later.

ARP request:

WHO HAS 192.168.0.1 | REPLY TO 00-5B-57-23-78-90

2. Router will give ARP reply to PCI confirming that router is at its MAC address

ARP reply:

192.168.0.1 IS AT 00-5F-34-13-37-00 | REPLY TO

CAM (Content Addressable Memory) is maintained by router and switch to identify which MAC address is on which port

**ARP spoofing attack:**

**Victim:** 192.168.0.10 00-50-56-C0-00-58

**Hacker:** 192.168.0.20 22-3C-5D-7B-8A-4F

**Router:** 192.168.0.1 00-50-56-C0-00-58

1. The hacker will send a forged ARP reply to the router saying that his device is victim device.

A) Spoofed ARP reply to the router

192.168.0.10 IS AT 22-3C-5D-7B-8A-4F | REPLY TO ROUTER

B) Spoofed ARP reply to victim

192.168.0.10 IS AT 22-3C-5D-7B-8A-4F | REPLY TO VICTIM

* Ettercap in kali is used to perform ARP spoofing attack

Use VPN to protect from ARP spoofing