23/11/22

Experiment:- 9

Objective:- Perform an experiment to Snift traffic using ARP poisoning.

Procedure:-

Step1- Install the VMware workstation and install the kali Linux operating system.

Step2:- Login into the kali Linux using username pass "root, toor".

Step3:- Make sure you are connected to local LAN and check IP address by typing the command ifconfig ~~step4:~~ in the terminal.

Step4:- Open up the terminal and type "Ettercap -G" to start the graphical version of Ettercap.

Step5:- Now click the tab "sniff" in the menu bar and select "unified sniffing" and click ok to select the interface. We are going to use "eth0" which means Ethernet connection.

Step6:- Now click the "hosts" tab in the menu bar and click "scan for hosts". It will start scanning the whole network for the alive hosts.

Step7:- Next, click the "hosts" tab and select "hosts list" to see the number of hosts available in the network. This list also includes the default gateway address. We have to be careful when we select the targets.

Step8:- Now, we have to choose the targets. In MITM, our target is the host machine, and the route will be the router address to forward the traffic. In an MITM attack, the attacker intercepts the network and sniffs the packets. So, we will add the victim as "target 1" and router address as "target 2."

In VMware environment, the default gateway will always end with "2" because "1" is assigned to the physical machine.

Step9: In this scenario, our targets is "192.168.121.129" and the route is "192.168.121.2". So we will add target 1 as victim IP and target 2 as route IP.

Step10: Now click on "MITM" and click "ARP Poisoning". Thereafter, check the option "Sniff remote connection" and click OK.

Step 11:- Click "Start" and select "Start sniffing". This will start ARP Poisoning in the network which means we have enabled our network card in "Promiscuous mode" and now the local traffic can be sniffed.

Step 12: Now it's time to see the results; if our victims logged into some websites. You can see the result in the toolbar of Ettercap.

Note: We have allowed only HTTP Sniffing with Ettercap, so don't expect HTTPS packets to be sniffed with this process.