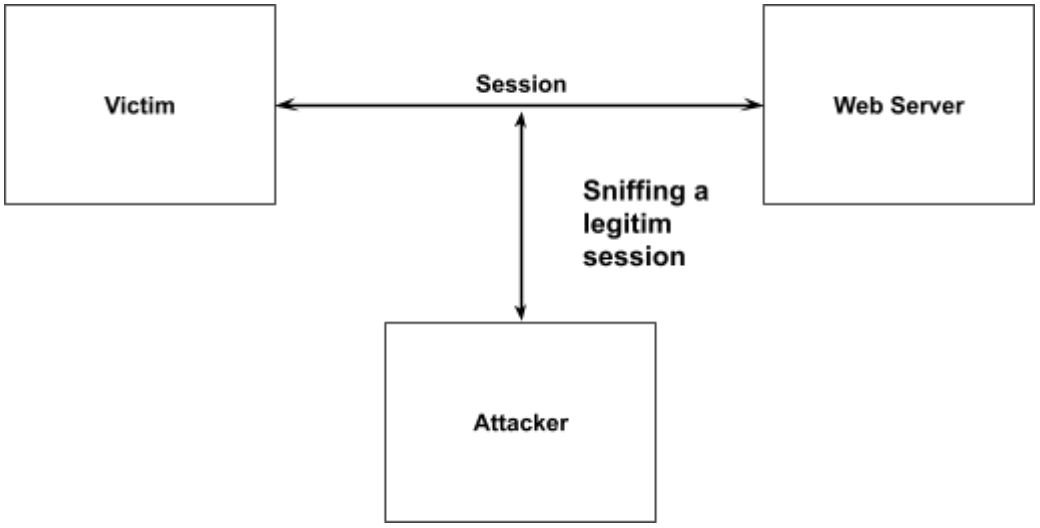
IP Sniffing and Spoofing

What is Sniffing

Sniffing is a process to monitor and capture the packet through a network. Now hackers use sniffing to capture data packets containing sensitive information just like email-id, username, password, aadhar card details, personal information, bank account details, etc information.

Example:



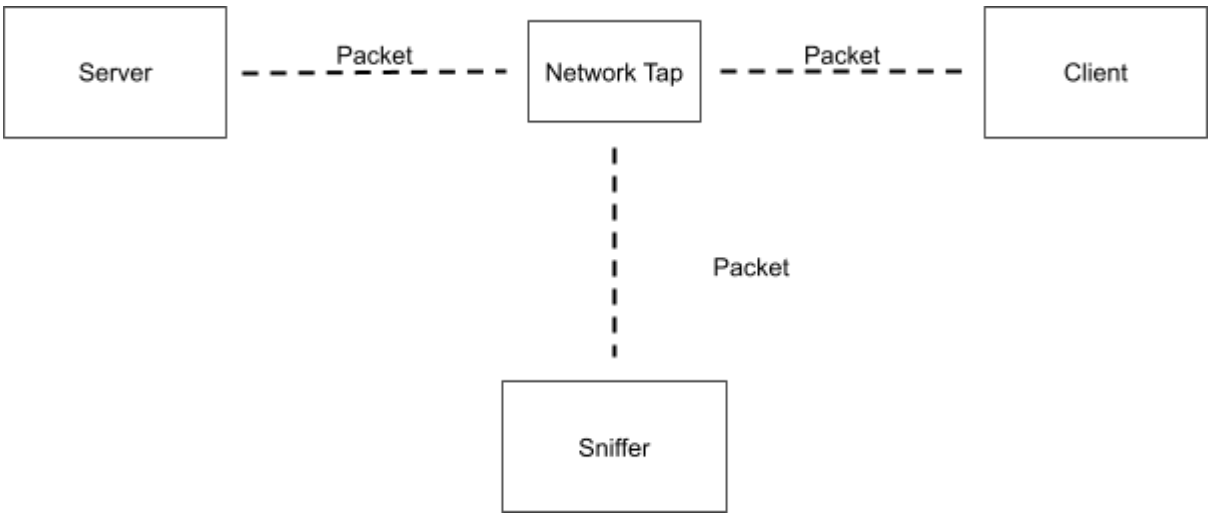
Types of Sniffing

There are two types of sniffing techniques: passive sniffing and active sniffing. The type of sniffing technique used depends on the structure of the network.

Passive Sniffing

Passive Sniffing refer to HUB based-network device
It involves reading and capturing traffic but does not change/interact with packets.

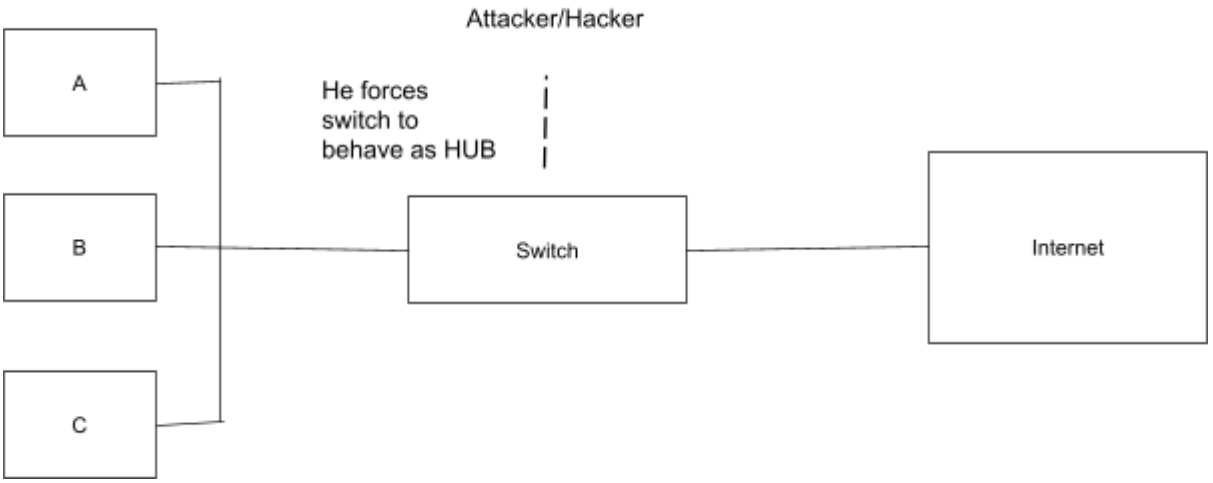
Example:



Active Sniffing
Active Sniffing refer to Switch based-network device
Active Sniffing technique known as MAC Flooding.
It involves injecting ARP (address resolution packet) into a network to flood on the switch CAM table (content addressable memory).

ARP: Is a protocol used mapping an ip address to a computer connected to LAN
CAM: Is a chip in store MAC address, IP address, Physical Port.

Example:



Types of Active Sniffing techniques :

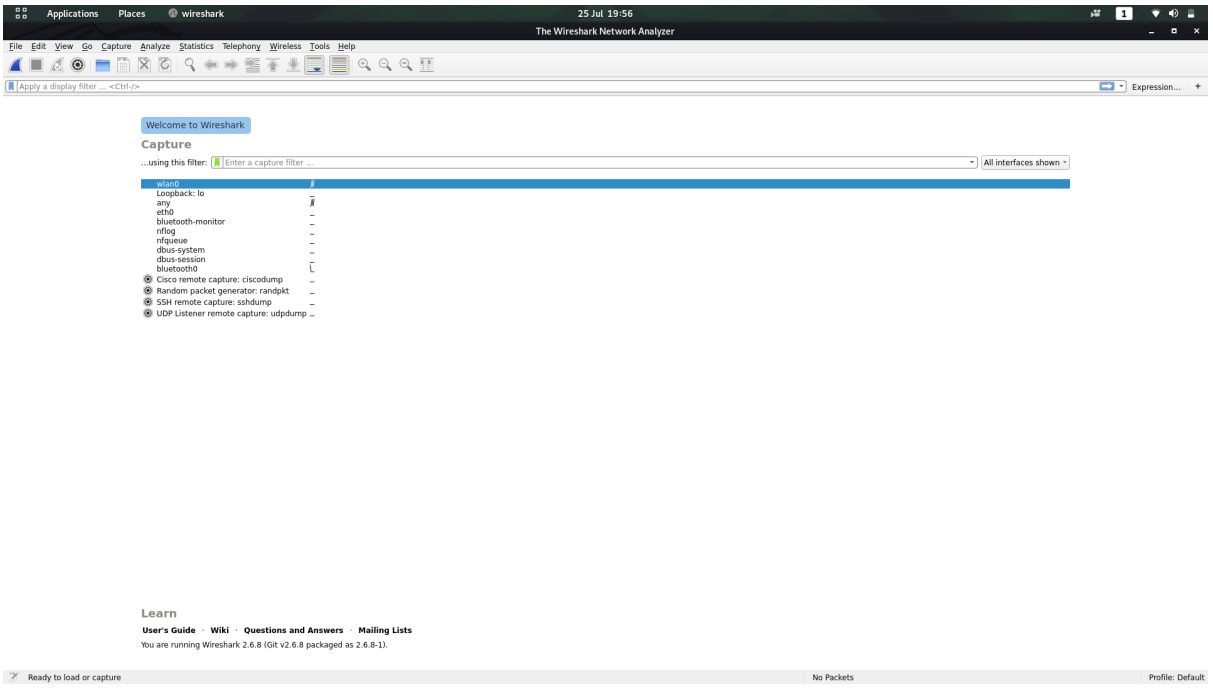
1. MAC Flooding
2. DHCP Attack
3. ARP Poisoning
4. DNS Poisoning

5. Switch Port Stealing

Packet sniffing practical

We used a wireshark tool for packet sniffing. It is one of the most widely known and used packet sniffers. It has a Graphical user interface (gui) .

$ Open wireshark



$ Choose interface (eth0, wlan0)

$ Start capturing packets

Select target ip and check packet
And all packet present in layers

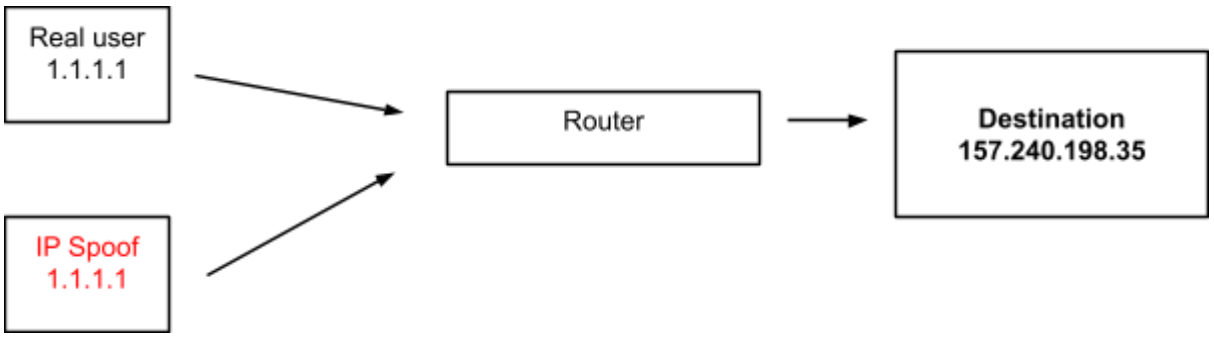
What is IP Spoofing

Is a technique used to gain unauthorized access to a computer, whereby the attacker sends a message to a computer with a fake ip address indicating that the message is coming from a trusted host.

Uses:

IP Spoofing is usually to injection of malicious data on command into an existing streams of data

Example :



Two techniques

1. An attacker uses an authorized external IP address that is trusted.
2. An attacker uses an IP address that is within the range of trusted IP addresses.

IP Spoofing practical

We used windows operating system for IP spoofing

First check your IP address
How to check
Open command prompt
Type
    # ipconfig
Check IP address

Now How to spoof
Open Control panel
Select Network and Sharing center
Click adapter setting
Choose network interface
Right click and go to properties
Choose Internet protocol version 4 then click properties
Fill this details then save

- Choose use the following IP address

IP address : _____

Subnet mask : _____

Default gateway : _____

- Use the following DNS server address

Preferred DNS server : _____

Alternate DNS server : _____

Check again IP address now change your IP address

Created by CBKALI
Follow in Instagram: https://www.instagram.com/i.m.cbkali/