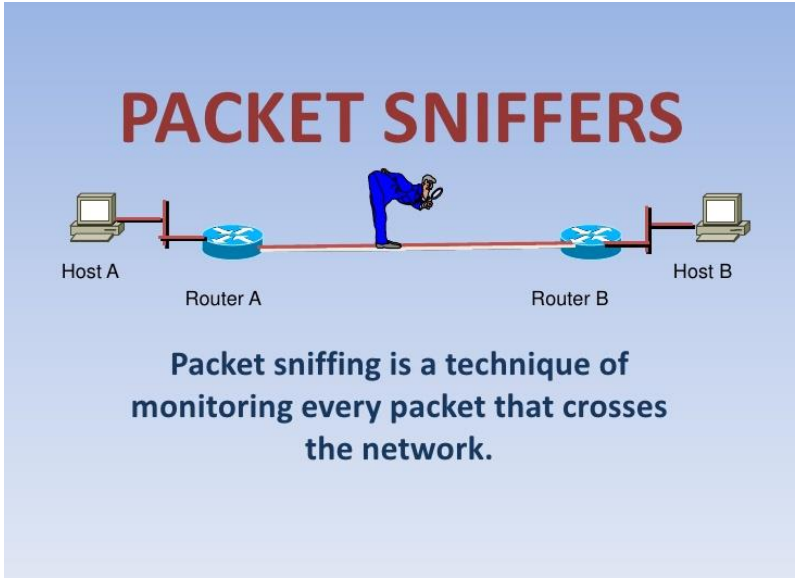
Network Sniffing

Presented by:
Aastha Sahni

What is Sniffing ?



- A *network sniffers* monitors data flowing over computer network links. It can be a self-contained software program or a hardware device with the appropriate software or Firmware programming.

Types Of Sniffing

PASSIVE SNIFFING - It involves listening and capturing traffic, and is useful in a network connected by hubs

ACTIVE SNIFFING - It involves launching an Address Resolution Protocol (ARP) spoofing or traffic-flooding attack against a switch in order to capture traffic.

How Sniffing Works

A hacker discovers a switch to a network in order to access it.

Then after getting access attacker tries to discover network topology using networking tools.

By analyzing the network topology, the attacker identifies victim machine.

The attacker using ARP spoofing techniques send fake messages , in this way attacker transfers message to his computer instead of victim’s computer, this is called Man In Middle type of attack.

Protocols prone to Sniffing

HTTP- While using HTTP data is sent in plaintext format which can easily be sniffed.

FTP- Same goes with FTP, sending files online in clear text format can easily lead to information leakage.

IMAP- Coming to IMAP, again data and password are sent in plaintext format.

POP- Same as IMAP

MAC ATTACKS- MAC FLOODING

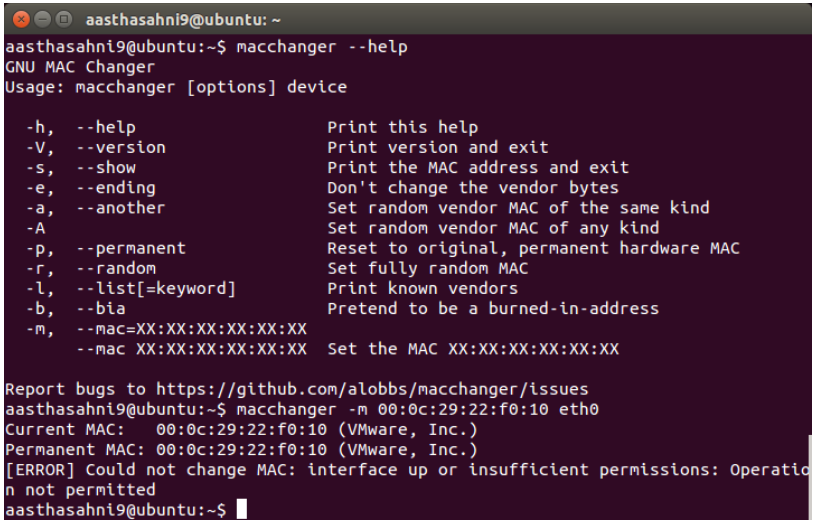
In MAC flooding series of steps takes place by an attacker:

- An attacker sends fake MAC address to switch,Switch updates that.
- In this way the attacker keep sending fake MAC addresses to the switch till its CAM table floods.
- As a result, Switch starts acting like hub and whatever frame it gets , it broadcast it to every port since it cannot find it in its CAM table
- The attacker will essentially now can capture frames.

Let See Some of the commands for MAC Flooding

Let’s try using MACCHANGER :

- First you need to install MACCHANGER using command
- Sudo apt-get install MACCHANGER
- Then type ifconfig, see your mac address, copy it
- Type MACCHANGER -m yourmacaddress eth0



ARP POISONING

What is ARP ??????

What does it do???

What can you infer from ARP poisoning?

DEFINING ARP POISONING

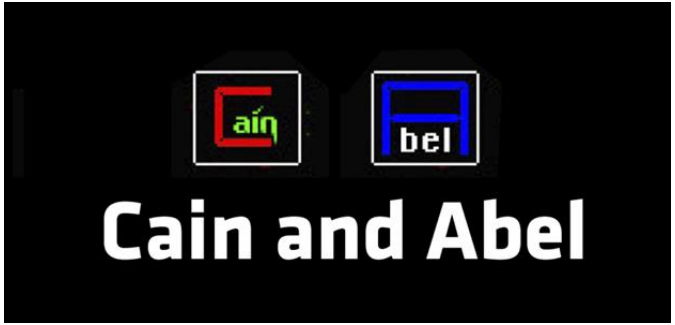
- ARP spoofing or poisoning is a type of attack in which a malicious actor sends falsified ARP messages over a local area network.
- Once the attacker’s MAC address is connected to an authentic IP address, the attacker will begin receiving any data that is intended for that IP address.

How Does ARP Poisoning Works?

How to implement an ARP poisoning attack?

What you will need:

- A laptop.
- Cain and abel. Download it from, www.oxid.it/index.html
- A network to sniff.



Continued

.....

Start Cain and Abel-

1) Now click on the sniffer tab. Now notice the two symbols – the one that looks the same as the one on the sniffer tab and the one that looks like a nuclear sign.

2) Mouse over them and they will tell you that one starts the sniffer and the other starts ARP poisoning.

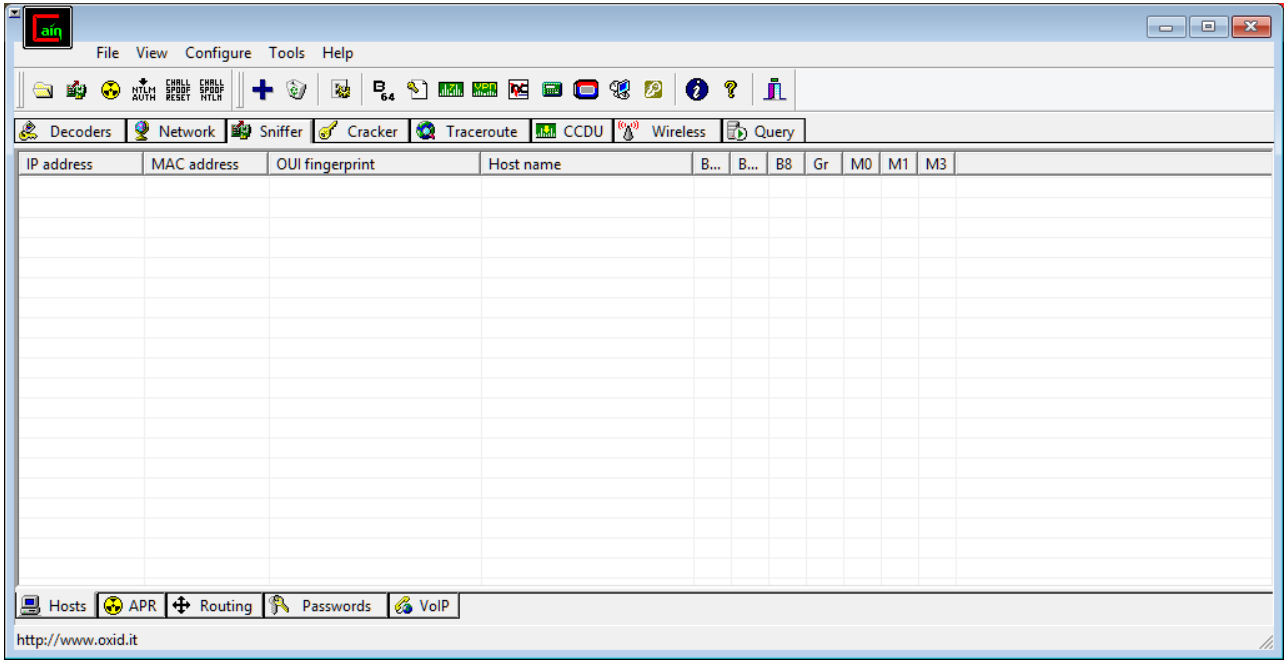
3) Now click on **configure -> click** on the ARP tab and make sure that you are using your real IP and mac address

Continued….

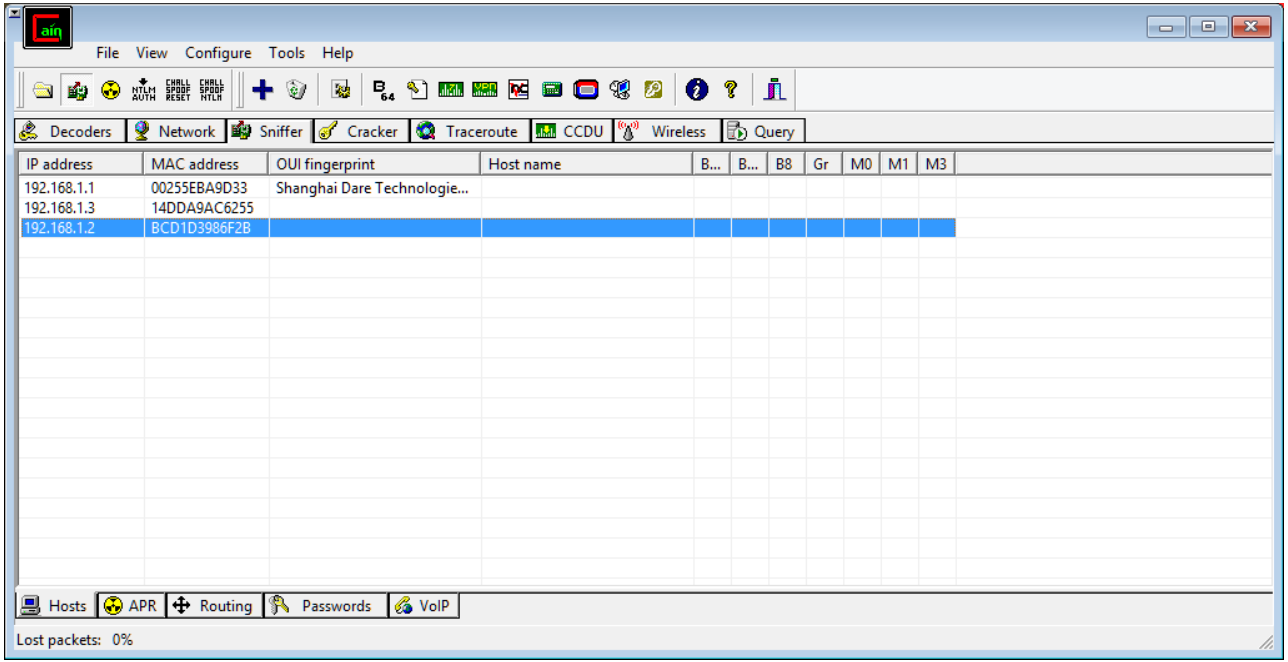
4) Now start the sniffer and press the blue plus sign. This will let you scan for hosts in your subnet. Now go back to configure and select use a spoofed IP and mac address.

5) Select all the hosts you find and right click and go resolve host name. Now try to find the router, it will usually stand out easily.

Some Screenshot of Cain and Abel



Sniffing Using Cain & Abel



DHCP Attacks

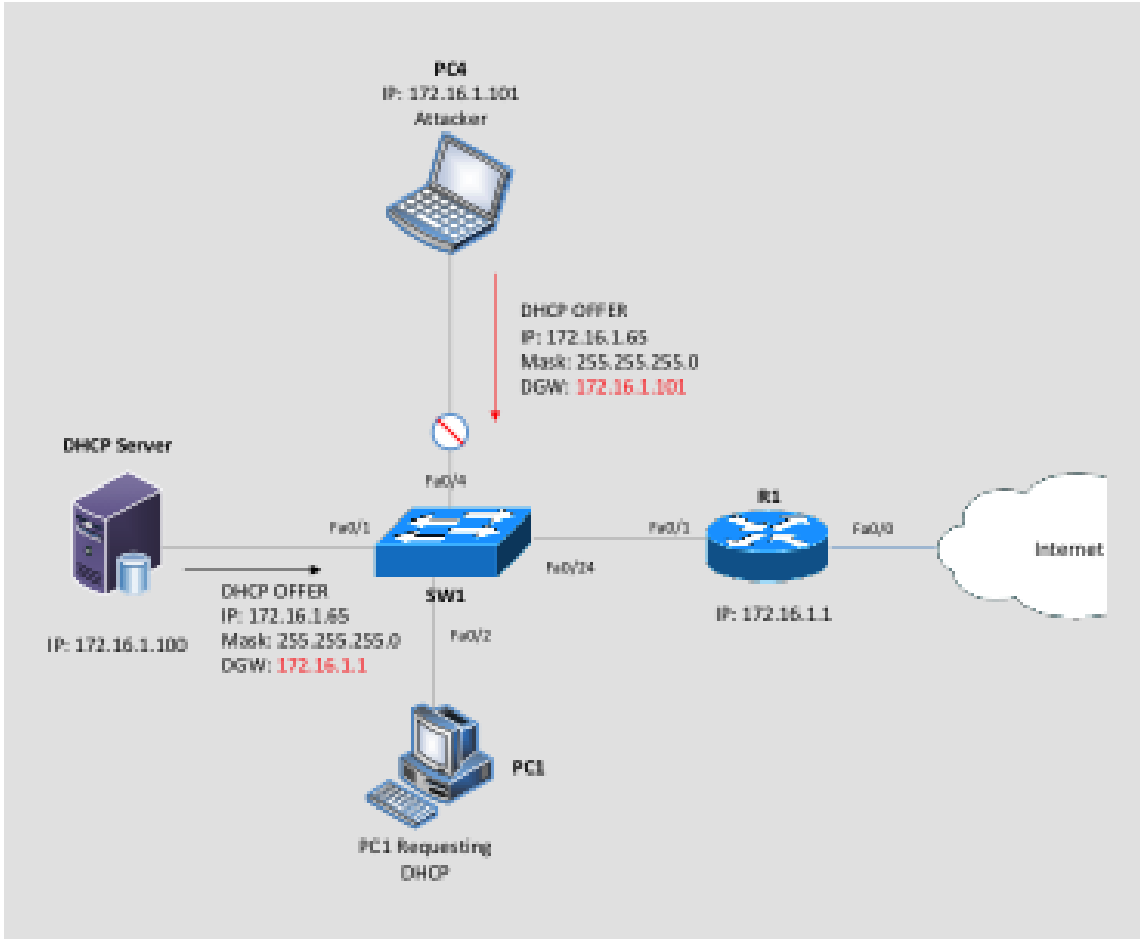
- **What is DHCP?**
- **What's the role of DHCP?**

Let’s Define it :DHCP

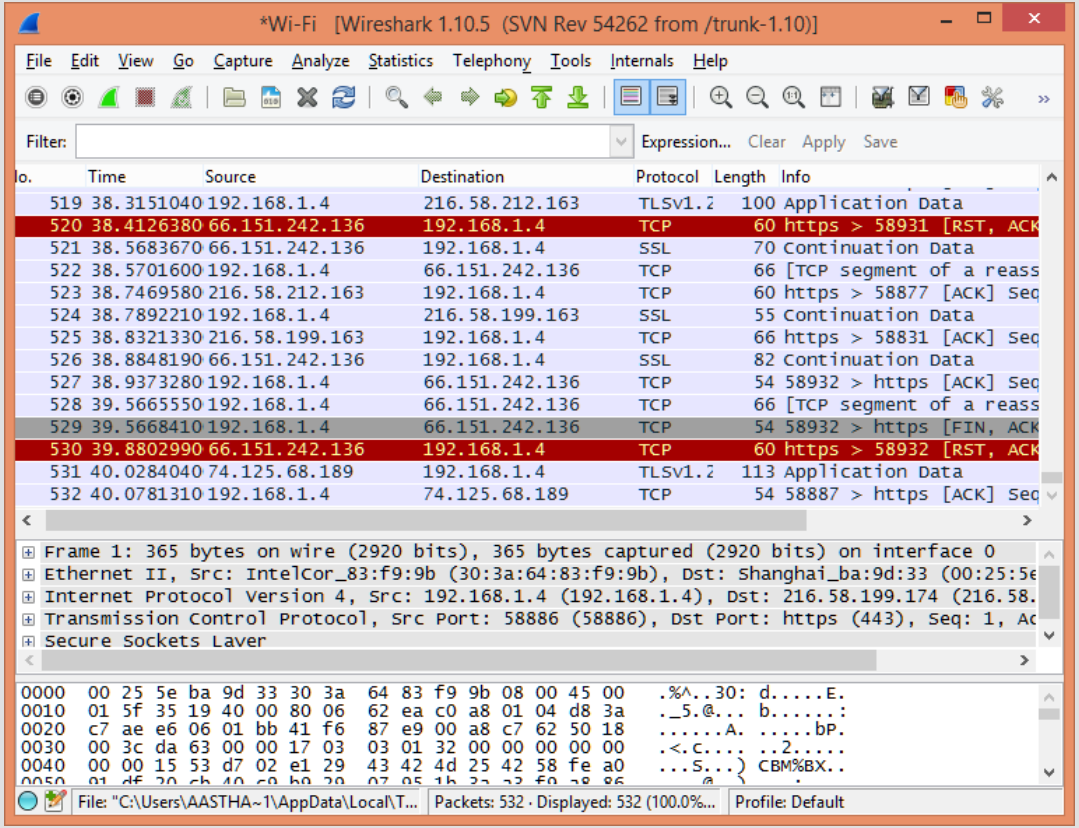
Dynamic Host Configuration Protocol (**DHCP**) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.

There are two things one is configuring DHCP client to obtain IP address dynamically , other is statically configuring the DHCP to obtain IP address.

Attacking DHCP server



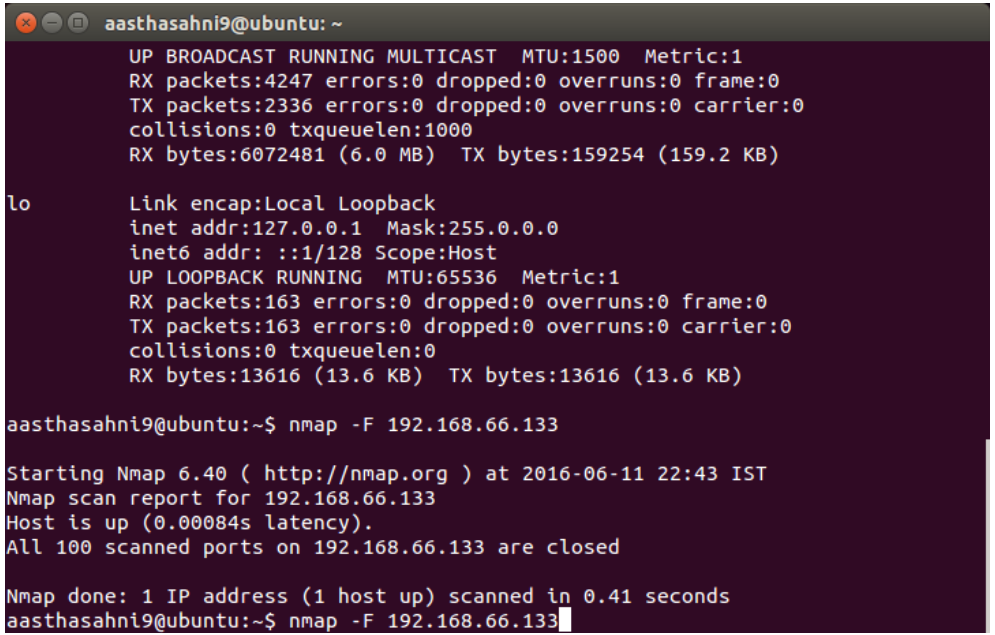
Sniffing Tools : Wireshark



Sniffing Tools : NMAP- Network Mapper

- Nmap ("Network Mapper") is a free and open-source utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

NMAP- Example



NMAP Continued…

- Identifying the OS of a host-**nmap -O target ip(root access).**
- Identifying host name on network- **nmap -sL target ip.**
- Tcp connect scan- **nmap -sT target ip.**
- Fast scan - **nmap -F target ip**

You can try these commands and see how wonderfully it works!

THANK YOU!