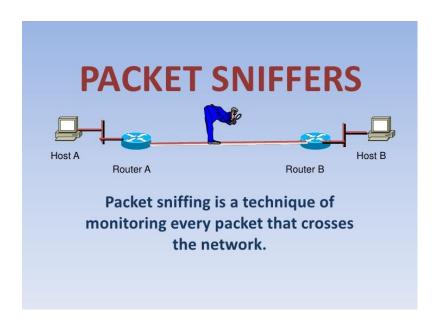
## Network Sniffing

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

```
🛑 🗊 aasthasahni9@ubuntu: ~
aasthasahni9@ubuntu:~$ macchanger --help
GNU MAC Changer
Usage: macchanger [options] device
      --help
                               Print this help
       --version
                               Print version and exit
       --show
                               Print the MAC address and exit
       --ending
                               Don't change the vendor bytes
      --another
                               Set random vendor MAC of the same kind
                               Set random vendor MAC of any kind
                               Reset to original, permanent hardware MAC
      --permanent
       --random
                               Set fully random MAC
      --list[=keyword]
                               Print known vendors
       --bia
                               Pretend to be a burned-in-address
      --mac=XX:XX:XX:XX:XX
       --mac XX:XX:XX:XX:XX:XX Set the MAC XX:XX:XX:XX:XX
Report bugs to https://github.com/alobbs/macchanger/issues
aasthasahni9@ubuntu:~$ macchanger -m 00:0c:29:22:f0:10 eth0
Current MAC: 00:0c:29:22:f0:10 (VMware, Inc.)
Permanent MAC: 00:0c:29:22:f0:10 (VMware, Inc.)
[ERROR] Could not change MAC: interface up or insufficient permissions: Operation
n not permitted
aasthasahni9@ubuntu:~$
```



**What is ARP ??????** 

## ARP POISONING



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-

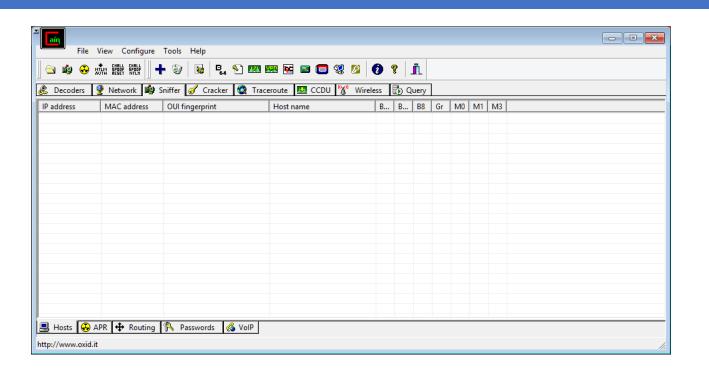
- 1) Now click on the sniffer tab. Now notice the two symbols the one that looks the same as the one on the sniffer tab and the one that looks like a nuclear sign.
- **2)** Mouse over them and they will tell you that one starts the sniffer and the other starts ARP poisoning.
- **3)** Now click on **configure -> click** on the ARP tab and make sure that you are using your real IP and mac address

#### Continued....

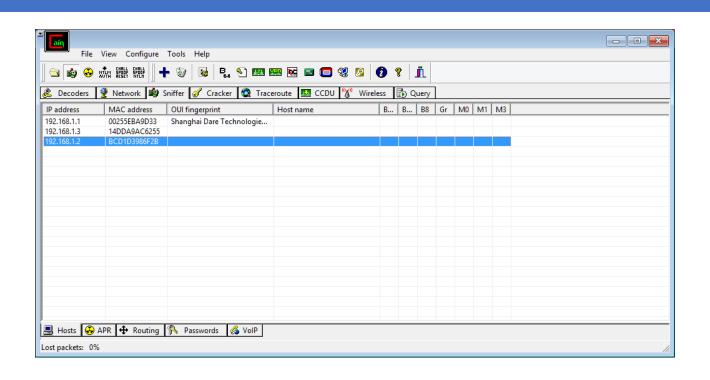
**4)** Now start the sniffer and press the blue plus sign. This will let you scan for hosts in your subnet. Now go back to configure and select use a spoofed IP and mac address.

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

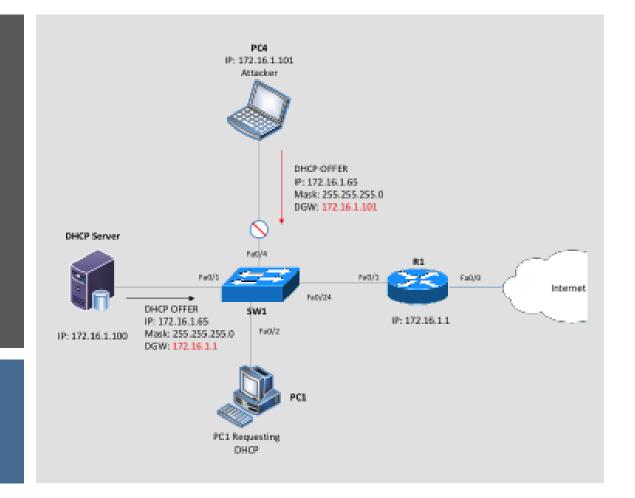
- What is DHCP?
- What's the role of DHCP?

#### Let's Define it :DHCP

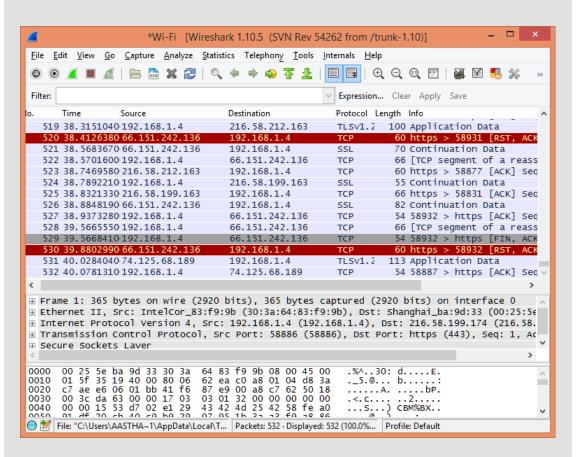
Dynamic Host Configuration
Protocol (**DHCP**) is a client/server
protocol that automatically provides
an Internet Protocol (IP) host with
its IP address and other related
configuration information such as
the subnet mask and default
gateway.

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

```
🛑 🗊 aasthasahni9@ubuntu: ~
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:4247 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2336 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6072481 (6.0 MB) TX bytes:159254 (159.2 KB)
          Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:65536 Metric:1
          RX packets:163 errors:0 dropped:0 overruns:0 frame:0
          TX packets:163 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:13616 (13.6 KB) TX bytes:13616 (13.6 KB)
aasthasahni9@ubuntu:~$ nmap -F 192.168.66.133
Starting Nmap 6.40 ( http://nmap.org ) at 2016-06-11 22:43 IST
Nmap scan report for 192.168.66.133
Host is up (0.00084s latency).
All 100 scanned ports on 192.168.66.133 are closed
Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds
aasthasahni9@ubuntu:~$ nmap -F 192.168.66.133
```

## 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!

