**Ethical Hacking Project**

* What is MAC Address
  + **Media Access Control** 
    - Permanent
    - Physical
    - Unique
    - This MAC address is Assigned by Manufacturer
* Why changing the MAC Address?
  + Increase anonymity
  + Impersonate other device such as bypassing filers, connect to network that only specific devices with specific MAC Address can connect. Also, you can able hide your identity
  + How to change MAC address ( **Ether is my mac address on WLan0)**

A close up of a screen

Description automatically generated

* + - Ifconfig wlan0 down
* ifconfig wlan0 HW (hardware) **ether 00:11:22:33:44:55**
* ifconfig wlan0 up

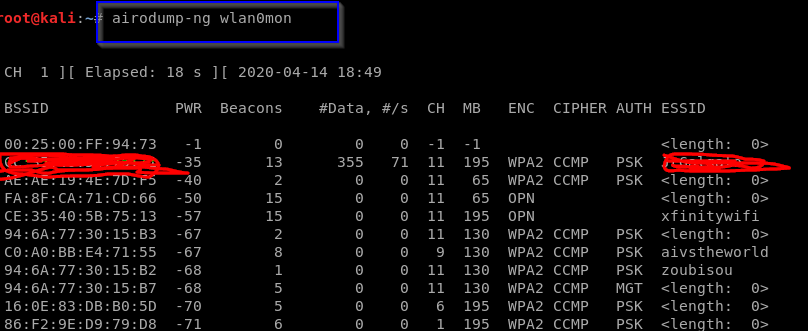
A close up of a sign

Description automatically generated

* PACKET SNIFFING: using Airodump-ng
* Part of aircrack-ng suit
* **Airodump-ng** is packet sniffer
* Used to capture all packet within range
* Display detailed info about network around us
* Connected client …etc. : use **Airodump-ng [ monitormodelterface ]**
* **How to enable your monitor mode: look at this picture**

A screenshot of a cell phone

Description automatically generated

* After you enable your monitor mode: you have to use this command line to discover all the wireless networks around your network and displaying useful information bout them **: Airodump-ng wlan0mon**

**WIFI BANDS**

* **Decides the frequency range that can be used**
* **Determines the channels that can be used**
* **Clients needs to support band used by router to communicate with it**
* **Data can be sniffed from a certain band if the wireless adapter used supports that band**
  + **MOST COMMON WIFI BANDS ARE** 
    - **A use 5 GHZ frequency only**
    - **B , G both use 2.4 GHZ frequency only**
    - **N uses 5 and 2.4 GHZ**
    - **AC uses frequency lower than 6 GHZ**

**Let try this command line : Airodump-ng wlan0**

* Then you can get wireless around you
* Airodum-ng only sniffing on 2.0 GB frequency

**A screenshot of a video game

Description automatically generated**

* How to sniff and discovery 5 GB frequency
* By suing this command line : **Airodum-ng –band a wlan0m**
* You can also add more band to capture more data 2.4 and 5 GB at the same time **( Airodump-ng –band ab wlan0mon)** A screenshot of a cell phone

  Description automatically generated

**TARGETED PACKET SNIFFING**

* How to gather more information about the target network
* **Airodum-ng –bashid F8:23:B2:B9:50:A8 –channel 2 –write test wlan0mon**
* This network I sniff **have 4 devices** connected to network and you can see **the MAC address, and** under station you can see different client or device connect to this network

A black and silver text

Description automatically generated

* So, you have to go back to your Linux command line since you saved our date **( --write test )**
* You will you get 4-5 files that you save to get more information bout the network that you sniffed **( such as test-01csv , test-01.kismet.netxml, text-01.cap etc. )**
* To get more info about the file use test-01.cap because this file contains chat message, username, and password
* To analyze the date, we have to use Wireshark ( you will see what type of device is connect to your network

A screenshot of a cell phone

Description automatically generated

**DE-AUTHENTICATION ATTACK ( WIFI)**

* Disconnect any client from any network
  + Works on encrypted network ( WEP, WPA AND WPA2 )
  + No need to know the network key
  + No need to connect to the network
  + Command line to use to do **DE-AUTHENTICATION** attack : **airplay-ng –death 10** ( how long you need to disconnect this client from the internet **) -a ( the mac address ) – c** ( the client you need to disconnect from the internet ) **wlan0mon**
  + After you run this command you will disconnect all internet from the device ( look at the picture

A screen shot of a computer

Description automatically generated

**GAINING ACCESS : WEP CRACKING**

* Wired E equivalent privacy
* Old encryption
* Uses an algorithm called RC4
* Still used in some networks
* Can be cracked easily

**Section 9: HOW TO CREATE WORLD LIST**

* Creating word list, you will use Crunch
  + Syntax: > crunch [ min] [ max] [ char] -+ [ pattern] -0 [ Filename ]
  + Example > Crunch 6 8 123bc$ -o wordlist -+ a@@@
  + This will be generated passes:
  + To open the file, you create: **cat text.txt**

**A screenshot of a cell phone screen with text

Description automatically generated**

* If you need to use patter option: you can use this command line:
* **Crunch 6 6 abc12 -o test.txt -t a@@@b**
* The generate number goes lower than the previous one because we used -t

A screenshot of a cell phone

Description automatically generated

32. **Discovering Device connected to the same network**

* Discover all device on the network
* Display their :
  + Ip address
  + MAC address
  + Operating system
  + Running service
  + We shall use NMAP and netdiscover

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

* Example is: **netdiscover** -r 10.0.2.1/24
* Connect your wireless adapter to see how many networks is connect to your device in real world
* This are the people / client that are connect to my network device my using **netdiscover**

A close up of a screen

Description automatically generated

* how to check wlan0 to see how many clients is connect to this Wi-Fi by using the same command line
* you see all the info about the client info on the pc

A screen shot of a smart phone

Description automatically generated

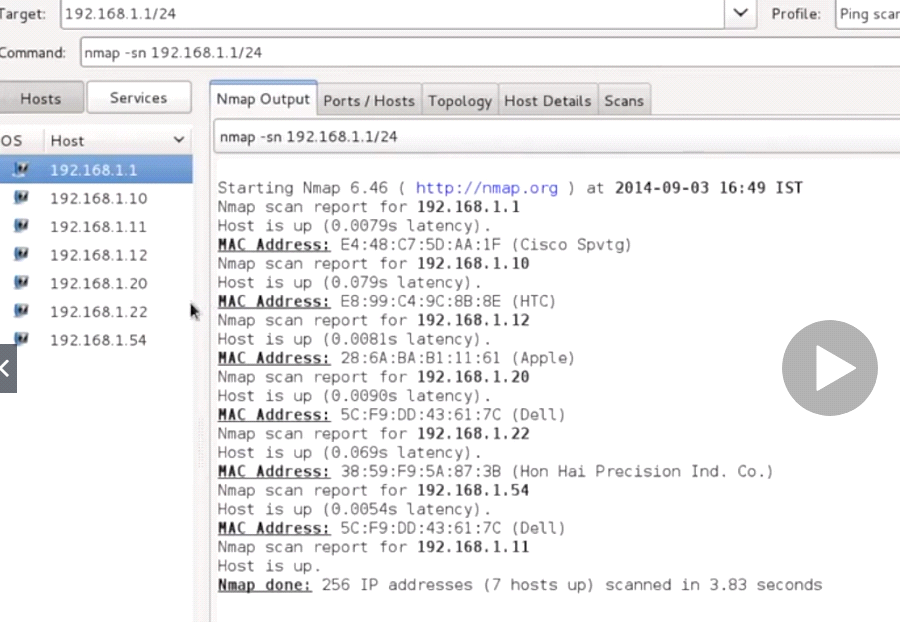
Gathering sensitive information about connected device (Device name, port etc. )

By using **Nmap / ZENMaAP**

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

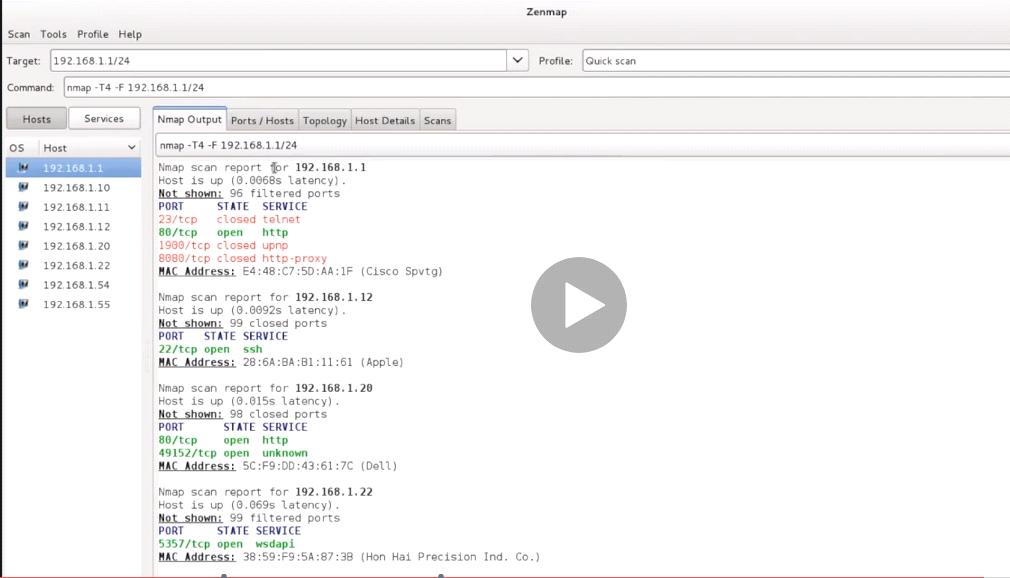
Using zenmap: **scan the Ip address in target space : 10.233.1.1/24**

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



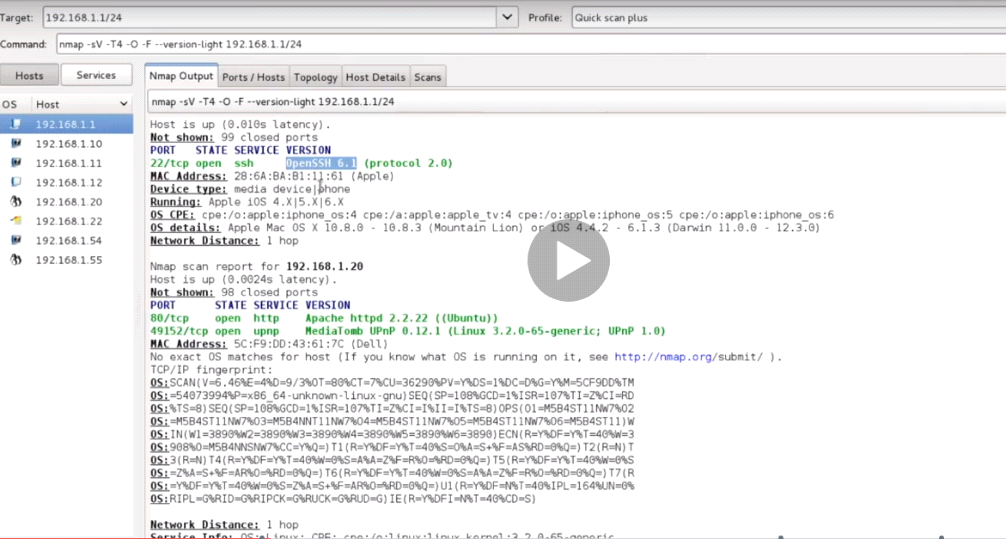
**Getting more details about information from client ( use Quick scan )**

* Showing open ports , close port

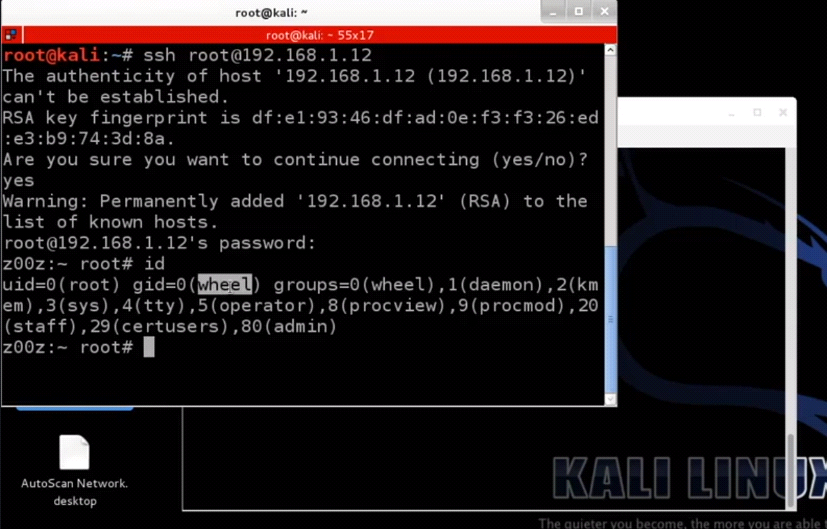


**If you need to get even more information for client (use quick scan plus ) this will give you better info**

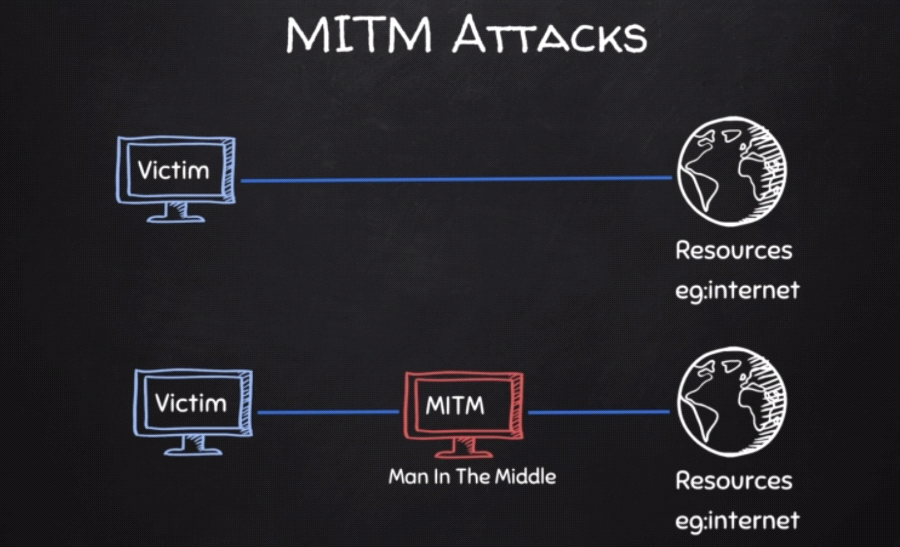
* **Such as OPENSSH 6.1 (protocol 2.0)**



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



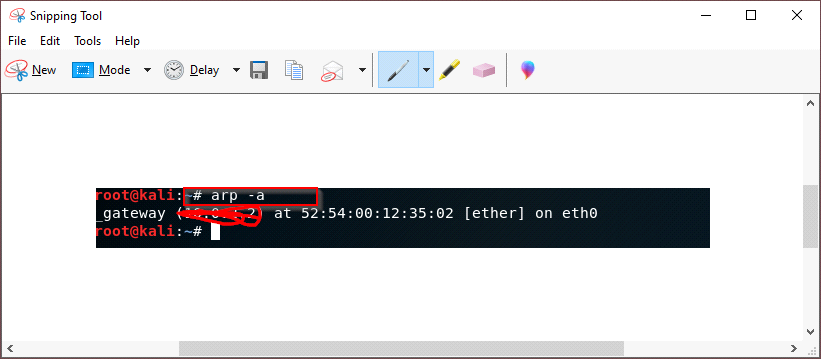
**Man-In the middle attacks**



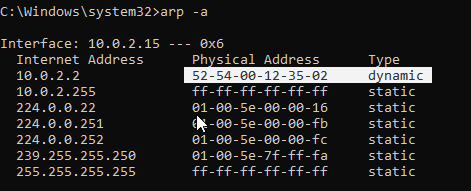
**What is ARP : Address Resolution Protocol**

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

Examples of ARP on kali Linux and Windows



**Windows ARP**



Using ARP Spoofing

**: using ARPSPOOF**

* Arpspoof tool to run arp spoofing attacks
* Simple and reliable
* Ported to most operating systems including Android and iOS
* Usage is always the same

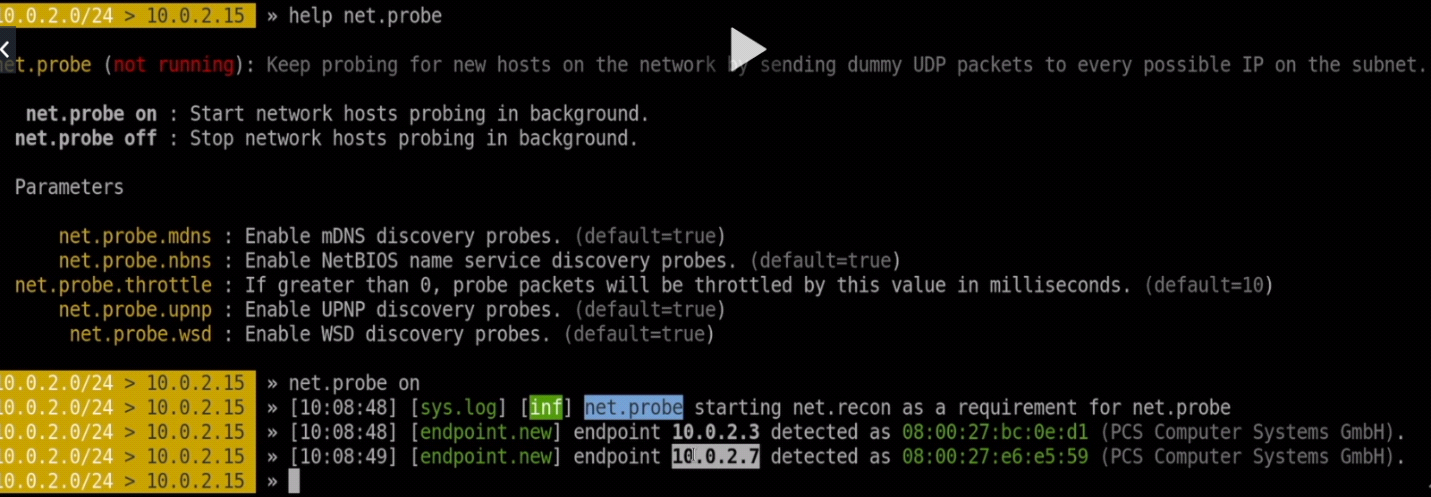
Use:

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

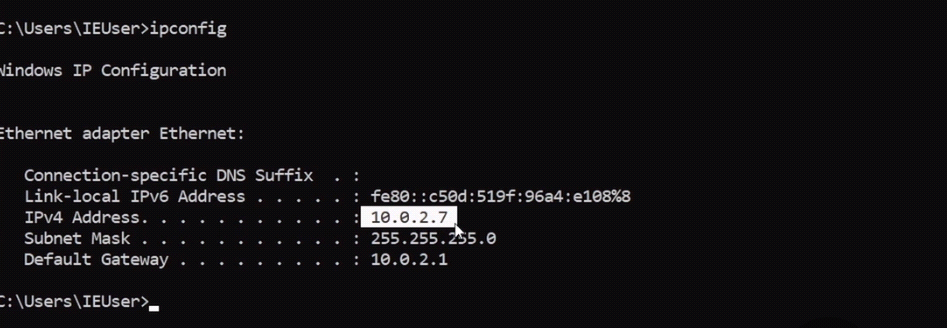
. arpspoof -I [ interface ] -t [ gateway IP ] [ client IP ]

**Using Better Cap:**

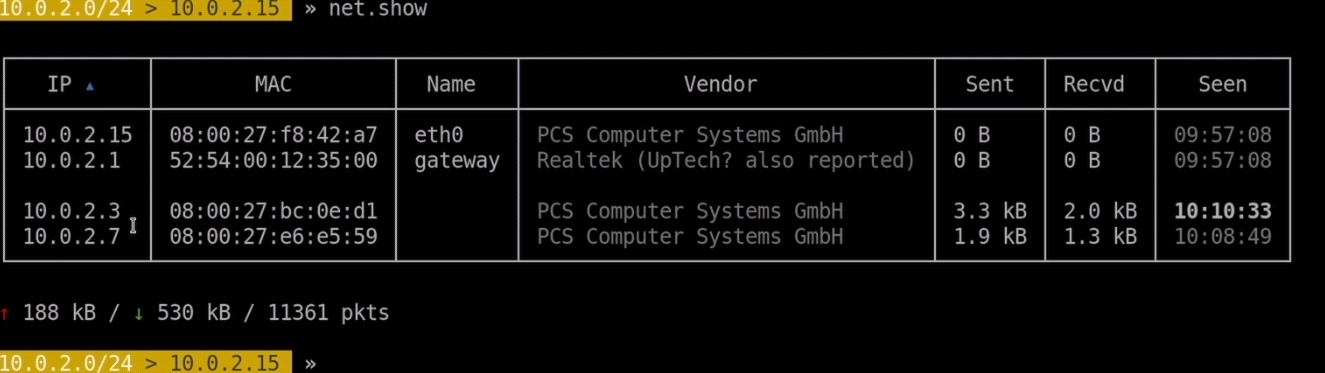
* **Framework to run network attack**
* **Can be used to :**
* ARP Spoof target ( redirect the flow of packets )
* Sniff data ( URLs , username passwords)
* Bypass HTTPs
* Redirect domain request ( DNS spoofing )
* Inject code in loaded pages and more
* Use : battercap -iface ( interface ) > install 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**



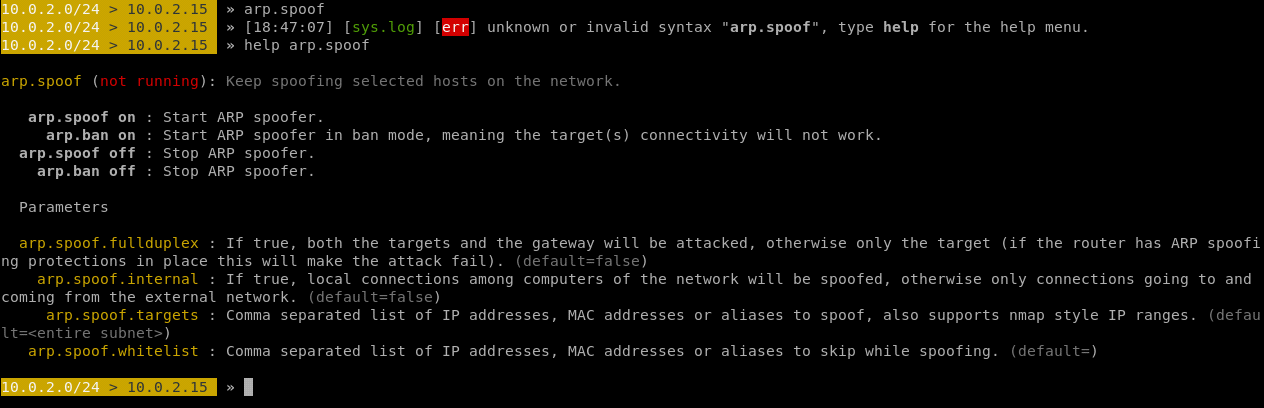
Using Arpspoof using bettercap to access more information **such as password, login**

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



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

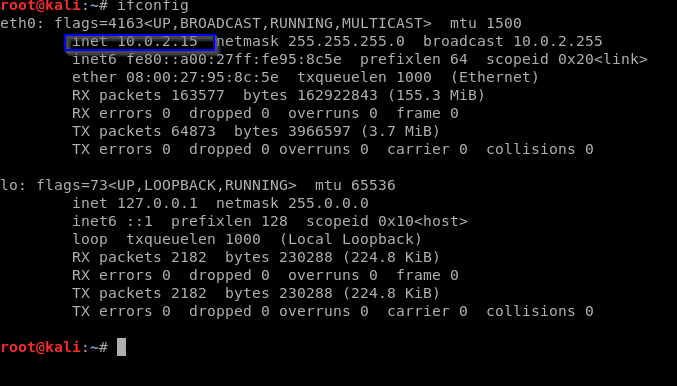
* We have to modify the option they give as with yellow colors



* 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 target : which are windows **( 10.0.2.15)**
* **So, we have to** turn on the **arp.spoof ( look at the picture )**
* All the information on windows such as password login will go thru kali Linux since we did man in the middle

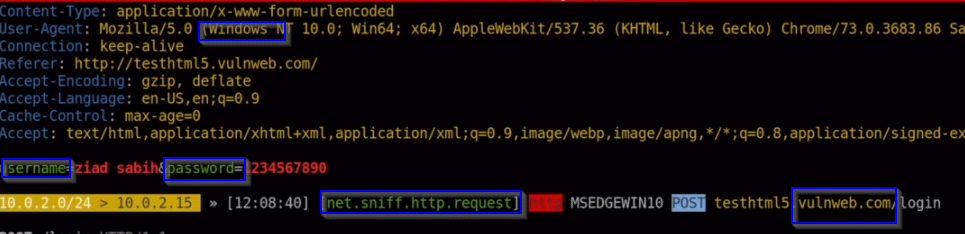


* As you can see both IP address of windows and kali are the same
* Anything you are doing at windows such visiting website or login, kail will capture it



**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
* After we turn on the sniff : we capture the login and the password on the website we visited

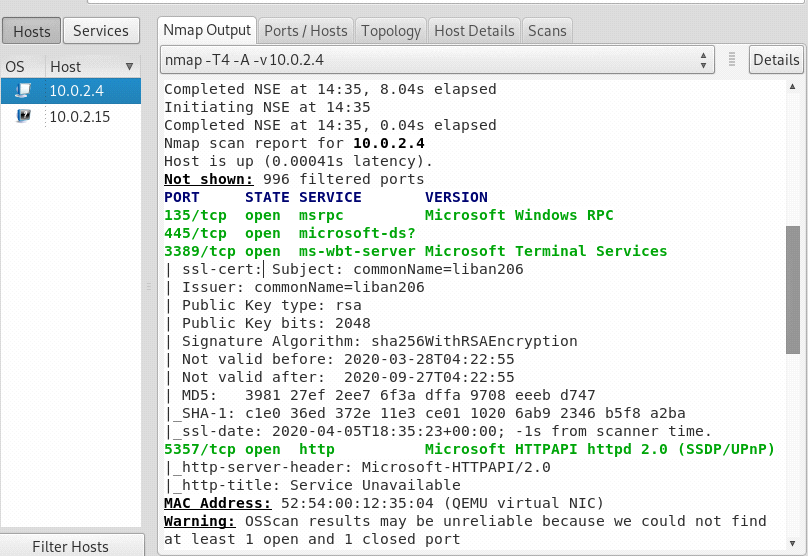


**Client -side Attacks**

* Need an IP address
* Very simple if target is on the same network ( net discover or Zen map )
* If target has a domain , then a simple ping will return IP > example : ping [www.facebook.com](http://www.facebook.com/)
* Getting the IP is trickier if the target is a personal computer, might be useless if the target is accessing the internet through a network as the IP will be the router IP and not the target, client-side attacks and more effective in the

**Information Gathering**

* Try default password ( ssh ipad case )
* Service might be mis-configured such as the “r” service . Ports 541.513,514
* Some might even contain backdoors
* Code execution vulnerabilities
* We will use Zenmap to get more Info such as which ports is open
* <https://machn1k.wordpress.com/2012/10/29/smb-exploitation-port-445/>



**Information Gathering:**

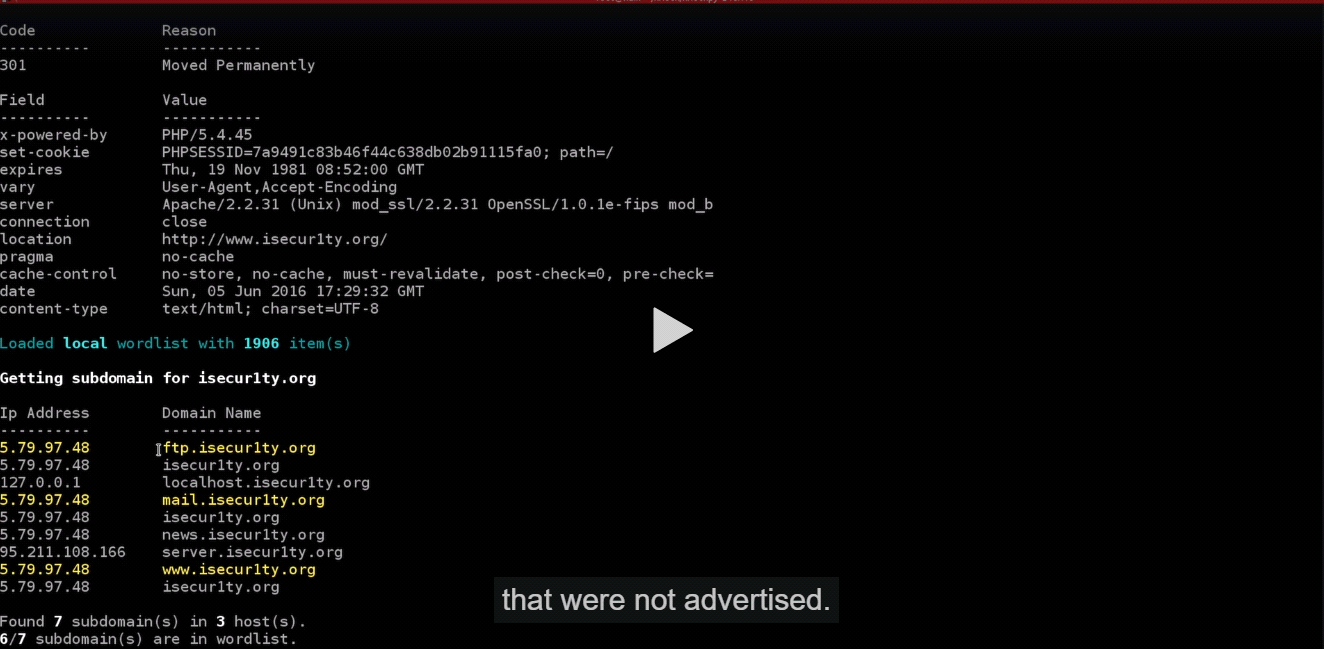
* Ip address
* Domain name info
* Technology used ( what type of programming did they used on website )
* Another website on the same server
* DNS record
* Unlisted files sub-domains, directories ( files that are not visible to other people )
* Whois lookup : Finding info about the owner of the target
* 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 HYPERLINK "https://www.bing.com/?toWww=1&redig=CA1A174E28964BC1BB7A257436666E64"& HYPERLINK "https://www.bing.com/?toWww=1&redig=CA1A174E28964BC1BB7A257436666E64"redig=CA1A174E28964BC1BB7A257436666E64](https://www.bing.com/?toWww=1&redig=CA1A174E28964BC1BB7A257436666E64)

**Subdomains :**

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

Knock can be used to find subdomains of target

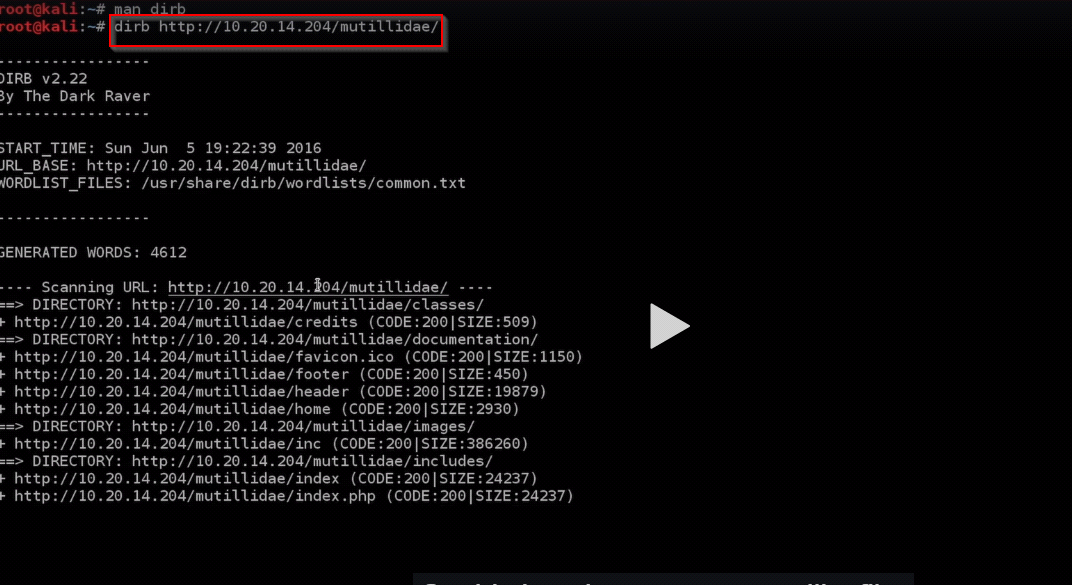
* Download it > gitclonehttps://github.com/guelfoweb/knock.git
* Navigate to knock > cd knock/kock.py
* Run it > python knock.py [ target]



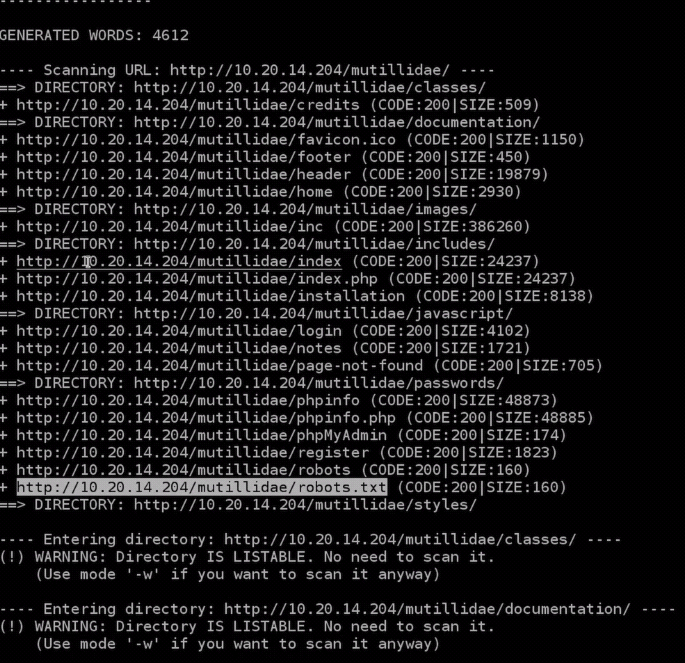
**Files + Directories**

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

For more info > main dirb



**Analyzing Discovering files**



**Exploitation : File upload values**

[**http://www.dvwa.co.uk/**](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**
* **Generate backdoor > weevly generate [ password ] [ file name]**
* **Upload generate file**
* **Connect to it > weevly [ URL to file] [ password ]**
* **Find out how to use weevly > help**

**Code Execution Vulns**

* **Allows an att**

**Exploitation – Xss Vluns**

**XSS – Cross-site scripting Vulus**

* Allow an attack to inject JavaScript code into the page
* Code is executed when the page is load
* Code is executed on the client **machine, not the server**

**Three main types of XSS scripts**

* **Persistent/Stored XSS**
* Reflected XSS
* DOM ( **Documents object model-based** ) based XSS

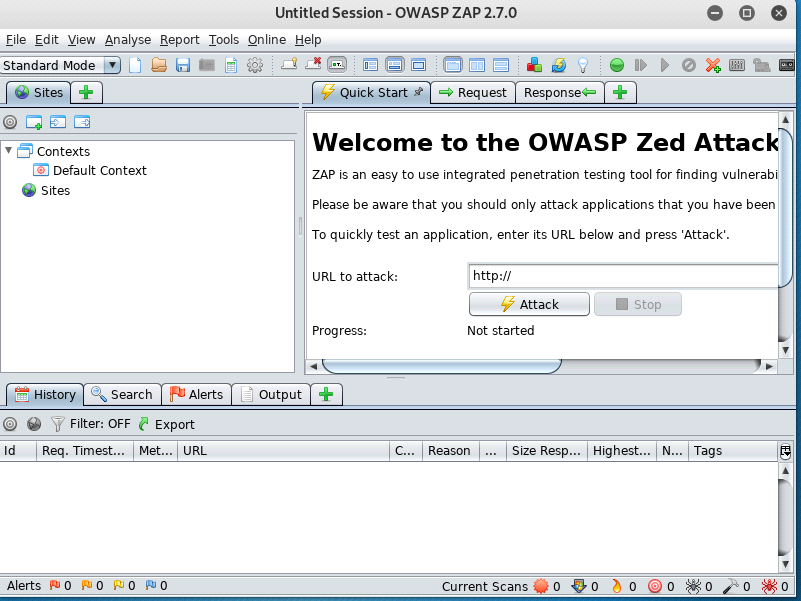
**client-Side Attacks** Social Engineering

* Gather info about the user
* Build a strategy based on the info
* Build a backdoor based on the info

**We will use maltego: this is information-gathering tools that can be used to collect information about anything**

* The target can be a website, company, person ...etc.
* Discover entities associated with the target
* Display info on a graph
* Come up with an attack strategy

rooZED Attack proxy ZAP

* Automatically find vulnerabilities in web application
* Free and easy to use
* Can also be sued for manual testing
* Something ZAP can give you a false alarm
* 
* After we open OWASP Zap, we know target a website
* Practices website : go to google dork its open source for everyone
* Look at the results on the picture after we did the target ( **look at the alert and the context )**
* You can get more information by click alert and contexts



* By attack this website we found 6 which are **red is high alert , orange medium alert and yellow low alert**
* You can see the red is 0 thread and the rest have number of threads

