**Module 31: Wireless and android hacking**

1. Wireless Terminologies

Here are some common wireless terminologies:

Access Point (AP): An access point is a networking device that connects wireless devices to a wired network. It serves as a central hub for wireless communication and provides a bridge between wireless and wired networks.

Wireless Network Interface Controller (WNIC): A WNIC is a hardware component that enables a device to connect to a wireless network. It is also referred to as a wireless network adapter.

SSID: SSID stands for Service Set Identifier, which is the name given to a wireless network. The SSID is used to identify and differentiate one wireless network from another.

WEP: Wired Equivalent Privacy (WEP) is a security protocol used to encrypt wireless network traffic. It is the oldest and least secure encryption method.

WPA: Wi-Fi Protected Access (WPA) is a security protocol that improves upon the security of WEP. It uses stronger encryption and authentication methods to protect wireless network traffic.

WPA2: WPA2 is the most secure wireless security protocol currently available. It uses Advanced Encryption Standard (AES) encryption and offers improved authentication methods over WPA.

MAC address: A Media Access Control (MAC) address is a unique identifier assigned to a network interface controller (NIC). It is used to identify devices on a network.

Beacon frames: Beacon frames are packets sent by an access point to announce its presence and advertise network details such as the SSID and security protocols.

Channel: A channel is a frequency band used for wireless communication. In the 2.4 GHz frequency band, there are 11 channels available, while in the 5 GHz frequency band, there are 23 non-overlapping channels available.

1. Types of Wireless Antenna

Here are some common types of wireless antennas:

Omnidirectional antenna: An omnidirectional antenna radiates its signal in all directions, providing a 360-degree coverage pattern. This type of antenna is commonly used in wireless access points and mobile devices.

Directional antenna: A directional antenna focuses its signal in a specific direction, providing a more focused coverage pattern. This type of antenna is commonly used in point-to-point wireless links, such as wireless backhaul connections between buildings.

Yagi antenna: A Yagi antenna is a directional antenna that consists of multiple elements arranged in a specific pattern. It provides a high gain and a narrow beamwidth, making it ideal for long-distance point-to-point wireless links.

Patch antenna: A patch antenna is a directional antenna that is flat and thin, with a rectangular or circular shape. It is commonly used in wireless access points and mobile devices due to its compact size.

Dipole antenna: A dipole antenna consists of two conductive elements that are aligned in opposite directions. It radiates its signal perpendicular to the axis of the antenna, providing an omnidirectional coverage pattern.

Parabolic dish antenna: A parabolic dish antenna is a directional antenna that uses a curved reflector to focus its signal in a specific direction. It provides a high gain and a narrow beamwidth, making it ideal for long-distance point-to-point wireless links.

Helical antenna: A helical antenna is a directional antenna that consists of a wire wound in a spiral shape around a cylindrical core. It provides a high gain and a narrow beamwidth, making it ideal for satellite communication and mobile radio applications.

The choice of antenna type will depend on the specific requirements of the wireless network, such as coverage area, distance, and interference.

1. How to secure your mobile phone

Here are some steps you can take to secure your mobile phone:

Use a strong password or PIN: Set a strong password or PIN to protect your phone from unauthorized access. Avoid using common or easily guessed passwords, such as "1234" or "password."

Enable two-factor authentication: Enable two-factor authentication for any accounts that you use on your phone. This adds an extra layer of security by requiring a second form of verification, such as a code sent to your phone.

Keep your phone up to date: Keep your phone's operating system and apps up to date with the latest security patches and updates. This helps to protect your phone from known vulnerabilities and exploits.

Use antivirus software: Install antivirus software on your phone to help protect against malware and other security threats.

Avoid public Wi-Fi: Avoid using public Wi-Fi networks, as these are often unsecured and can be used by hackers to intercept your data.

Be cautious of suspicious links and downloads: Be cautious of links and downloads from unknown sources, as these could contain malware or other security threats.

Use encryption: Enable encryption on your phone to protect your data in case your phone is lost or stolen.

Backup your data: Regularly backup your phone's data to a secure location, such as a cloud storage service or an external hard drive. This helps to ensure that you can recover your data in case your phone is lost, stolen, or damaged.

1. List of Android Phones Security Tools

Avast Mobile Security: This app offers antivirus and anti-malware protection, along with features such as a privacy advisor, app lock, and anti-theft tools.

Lookout Mobile Security: This app offers malware and phishing protection, as well as features such as theft protection, backup, and find-my-phone tools.

Norton Mobile Security: This app offers malware protection, anti-theft features, and tools for blocking unwanted calls and text messages.

Malwarebytes Security: This app offers real-time protection against malware, ransomware, and other threats, as well as privacy features such as app lock and call blocking.

Kaspersky Mobile Antivirus: This app offers antivirus and anti-malware protection, as well as anti-theft tools and web filtering to block malicious websites.

McAfee Mobile Security: This app offers antivirus and anti-malware protection, as well as anti-theft tools, app lock, and a VPN for secure browsing.

Sophos Intercept X for Mobile: This app offers malware protection, web filtering, and anti-phishing features, as well as a VPN for secure browsing and remote access control.

These tools can help to protect your Android phone from a range of security threats, including malware, phishing, and theft. However, it's important to note that no security tool can offer complete protection, and it's still important to follow best practices for mobile security, such as keeping your phone up to date and being cautious of suspicious links and downloads.

1. Perform practical Android phone hacking

In addition to manual coding, there are many applications built around hacking Android systems. These range from apps targeted at end users who want to extend their Android device's battery life or customize other parts of its operating system to deep system hacks used by more sophisticated hackers and attackers.

Here are a few of the most popular:

* [Apktool](https://ibotpeaches.github.io/Apktool/) – This tool is used for reverse engineering third party, closed, binary Android applications.
* [Dex2jar](https://github.com/pxb1988/dex2jar) – This widely available tool works with Android .dex and Java .class files, enabling the conversion of one binary format to another.
* [JD-GUI](https://github.com/java-decompiler/jd-gui) – This is a graphic utility tool that stands alone and displays Java sources from .class files.