• Wireless Terminologies

Wireless terminology encompasses a wide range of concepts and technologies used to describe communication without physical cables or wires. Key terms include access points, antennas, bandwidth, channels, and various wireless network types like WLAN, WMAN, WPAN, and WWAN. Understanding these terms is crucial for grasping how wireless devices connect and interact within networks.

• Types of Wireless Antenna.

The different types of antennas vary based on the diameter of the region through which the reception of the signal strength is best, called the beam width. Since the beam width of these different types of antennas is different therefore the design, orientation, and radio frequency also vary for all of them.

1. **Omni Directional Antenna**
2. **Semi Directional Antenna**
3. **Highly Directional Antenna.**

• How to secure your mobile phone.

Your cell phone holds some of your most sensitive personal information. Things like your passwords and account numbers, emails, text messages, photos, and videos. If your phone ends up in the wrong hands, someone could steal your identity, buy stuff with your money, or hack into your email or social media accounts. Here’s how to protect your phone.

1. Lock Your Phone
2. Update Your Software
3. Back Up Your Data
4. Get Help Finding a Lost Phone

• List of Android Phones Security Tools

Android security tools include antivirus apps like Bitdefender, Norton, and Avast, which offer features like real-time scanning, web protection, and anti-theft measures. Additionally, tools like Malwarebytes, Sophos Intercept X, and ESET Mobile Security provide comprehensive protection against malware and other threats. For more in-depth security assessment, tools like MobSF, Drozer, and Qark are used for static and dynamic analysis of applications.

• Perform practical Android phone hacking.

1. (1) Sploit: Android implementation of the Metasploit framework. Useful for mapping the local network and detecting open ports.
2. DroidSheep: Web session hijacker that intercepts all Wi-Fi data transmitted between Android devices on a network.
3. FaceNiff: WiFi web traffic sniffer allows you to monitor sessions on Android web browsers.
4. Hackode: Multi-function Android hacker toolbox. Includes port scanning, traceroute, and other common network tools.
5. Kali NetHunter: Penetration testing software for Android. It can simulate several forms of attack.
6. Network Mapper: Android implementation of the Nmap scanner.
7. SSHDroid: Android implementation of the standard SSH server for secure remote access to other devices.
8. Pro: Tool to knock devices off a WiFi network. Can be used to create a  malicious WiFi hotspot
9. zANTI: Pen testing app used for simulating network attacks.
10. AndroRAT: This RAT (“Remote Access Tool”) allows for remote login to Android devices, with more capabilities than standard SSH logins that include capturing pictures using Android device cameras, dumping SMS messages, and more.