Hacking Wireless Networks :

1. **GSM** : A Universal system used for mobile transportation for wireless networks worldwide
2. **ISM band** : A set of frequencies for the international industrial, scientific, and medical communities
3. **Association** : the process of connecting a wireless device to an AP
4. **MIMO-OFDM** : An Air interface for 4g and 5g broadband wireless communication
5. **Direct Sequence spread spectrum** : An Original data signal multiplied with a pseudo-random noise spreading the code
6. **Frequency Hopping spread spectrum** : a method of transmitting radio signals by rapidly switching a carrier among many frequency channels.

Wifi Authentication Process Using a centralized authentication server :

In this wifi authentication process, a centralized authentication server known as the Remote Authentication Dial in user service (RADIUS) send authentication keys to both the AP and client that require authentication with the AP.
This key enables the AP to identify a particular wireless clients.

Types of Antenna :

1. **Directional Antenna** : Used to broadcast and obtain radio waves from a single direction
2. **OminDirectional Antenna** : Provides 360 horizontal radiation pattern
3. **Parabolic Grid Antenna** : Based on the principle of a satellite dish but lacks a solid backing, can pick up wifi signals from 10 miles or more.
4. **Yagi Antenna** : A unidirectional Antenna commonly used in communication for a freq. band of 10MHz to VHF and UHF
5. **Dipole Antenna** : A Bidirectional Antenna used to support client connection rather than site-to-site application
6. **Reflector Antenna** : used to concentrate EM Energy which is radiated or received at a focal point.

Types of Wireless Encryption :

EAP : supports multiple authentication methods, such as token cards, kerberos, and certificates
TKIP : Temporal key integrity protocol : A Security Protocol used in a WPA as a replacement for WEP
CCMP : **(Counter Cipher Mode and BlockChain Message Authentication Code Protocol)** An Encryption protocol used in a WPA2 for stronger encrption and authentication.
PEAP : A Protocol that encapsulate the EAP with an ecrypted and authenticated transport layer security (TLS) Tunnel (EAP + TLS)
WPA3 ; A Third Generation wifi security protocol that uses GCMP-256 for encryption and HMAC-SHA-384 for authentication

WPA-2 Encryption :

It include mandatory support of CCMP, an AES-based encryption mode with strong security.

Modes of Operation :

1. WPA-2 personal :
    It uses a set-up password PSK to protect from unauthorized access
    In PSK Mode, each wireless network device encrypts the network traffic using a 128 bits key which is derived from a passphrase of 8 to 63 ASCII characters.

2. WPA-2 Enterprise :
    It includes EAP or RADIUS for centralized client authentication using multiple authentication methods such as token cards, and kerberos.

users are assigned login credentials by the centralized server which they must present

WPA-3 Encryption :

WPA3 is an advanced implementation of WPA2 providing tailblazing protocol and uses the AES-GCMP-256 encryption algorithm

Modes of operation :

1. WPA-3 Personal :
   It is mainly used to deliver password based authentication using the SAE Protocol, also known as Dragonfly Key Exchange
   It is resistance to offline dictonary attacks and key recovery attacks

2. WPA3 Enterprise :
   It protects sensitive data using many cryptographic algorithm
   It provide authenticated encryption using GCMP-256
   It uses HMAC-SHA-384 to generate cyptographic keys
   it uses ECDSA-384 for exchanging keys

ISSUES IN WEP, WAP, WAP2

Issues in WEP :

1. CRC-32 does not ensure cryptographic integrity
2. IVs are 24 bits and sent in clear text
3. vulnerable to known plaintext attack
4. prone to password cracking attack
5. Associate/disassociate messages are not authenticated
6. lack of centralized key management
7. IV is a part of the RC4 encryption key, which lead to an analytical attack

Issues in WAP :

1. Pre-Shared key is vulnerable to eavesdropping and dictonary attack
2. Lack of Forward Secreacy
3. WPA-TKIP is vulnerable to packet spoofing and decryption attacks
4. Insecure Random number generator (RNG) in WPA allows the discover of GTK generated by AP

Issues in WPA2 :

1. Pre-Shared key is vulnerable to eavesdropping and dictonary attack
2. Lack of Forward Secreacy
3. Hole96 vulnerability makes WPA2 Vulnerable to MiTM and DoS Attacks
4. Insecure Random number generator (RNG) in WPA allows the discover of GTK generated by AP
5. KRACK vulnerability makes WPA2 vulnerable to Packet Sniffing, Connection Hijacking, Malware Injection, and decryption attack.

Client Mis-association :

Attacker sets up a rogue AP outside the corporate perimeter and lures the employee of the oprganization to connect with it
Once Associated, attacker may bypass the enterprise security policies. ALso Known as EVIL TWIN ATTACK.

Key Re-Installation Attacks (KRACK) :

All Secure Wi-Fi Network use the 4-way Handshake process to join the network and generate the fresh encryption key that will be used to encrypt the network traffic
The KRACK Attack works by exploiting the 4-way handshake of the WPA2 protocol by forcing Nonce reuse.
KRACK Work against all modern protected Wi-Fi networks and allows attacker to steals sensitive information, such as credit card numbers, password, emails

aLTEr Attacks :

aLTEr attacks are usually performed on LTE Devices
Attacker installs a virtual(FAke) Communication tower between two authentic end points intending to mislead the victim
the virtual tower is used to interrupt the data transmission between the user and real tower attempting to hijack the active session.

Finding WPS-Enabled APs

Attackers use wash utility to identify the WPS-enabled APs and detect if the AP is in locked or unlocked state
the wash commands can supports the 5Ghz Channel
The attacker discovers the AP, ESSID, and BSSID of device or router using the wash command :

```
sudo wash -i wlan0
```

Fragmentation Attack :

- A Fragmentation attack, when successful, can obtain 1500 bytes of pseudo random generation algorithm (PRGA)
- This attack does not recover the WEP key itself, but merely obtains the PRGA
- The PRGA cabn be used to generate packets with packetforge-ng which are in turns used for various injection attacks
- it requires at least one data packets to be received for the ap to initiate the attack.

Evil Twin Attacks :

Evil Twin is a wireless AP that pretend to be a legitimate AP by replicating another network name
Attacker sets up a rogue AP outside the corporate perimeter and lures user to sign into the wronge ap
Evil Twin can be configured with a common residential SSID hotspot SSID or a company's WLAN SSID

WPA3 Encryption Cracking :

Dragonblood is a set of vulnerabilities in the WPA3 security standard that allow attacker to recover keys, downgrade, security mechanism, and launch various information-theft attacks

Attackers can use various tools such as Dragonslayer, Dragonforce, Dragondrain and Dragontime to exploit these vulnerabilites and launch attack on WPA3-enabled netwotk.

Downgrade Security Attacks :

1. **Exploiting Backward Compaitibility** :
   An Attacker installs a rogue AP and forces the user to involve in WPA2 encryption
   Then the attacker performs all the attacking techniques available to exploit WPA2

2. **Exploiting the Dragonfly handshake** :

an Attacker with the rogue AP discard the user's WPA3 Dragonfly Mechanism
The attacker forces the user to use a weaker encryption algorithm, such as WPA2

Side Channel attacks :

1. Timing Based :
An Attacker analyzes the amount of time dragonfly handshake takes for certain password authentication
the attacker notice the number of iteration the encoding process takes and short list the passwords to launch further attacks

2. Cache-Based :
An Attacker install malicious javascript code on the client's Browser and observe memory access. pattern
the attacker retrieves the password to perform malicious actions with the user's credentials

Bluetooth Attacks :

1. **Bluesmacking** : DoS Attack
2. **Bluejacking** : Sending unsolicited message
3. **Bluesnarfing** : theft of information
4. **Bluesniff** : Proof of concept code for a bluetooth wardriving utility
5. **Bluebugging** : Remotely accessing a Bluetooth-enabled device and using its feature
6. **BluePrinting** : The art of collecting information about bluetooth enabled device such as manuf. model, firmware version
7. **Btlejacking** : It is used to bypass security mechanism and listen to information being shared
8. **KNOB Attack** : Exploiting a vulnerability in bluetooth to eavesdrop all the data being shared such as keystrokes, chats, documents