-: Wireless Hacking :-

Wireless networks broadcast their packets using radio frequency or optical wavelengths. A modern laptop computer can listen in. Worse, an attacker can manufacture new packets on the fly and persuade wireless stations to accept his packets as legitimate.
The step by step procerdure in wireless hacking can be explained with help of different topics as follows:-

1) Stations and Access Points :- A wireless network interface card (adapter) is a device, called a station, providing the network physical layer over a radio link to another station.
An access point (AP) is a station that provides frame distribution service to stations associated with it.
The AP itself is typically connected by wire to a LAN. Each AP has a 0 to 32 byte long Service Set Identifier (SSID) that is also commonly called a network name. The SSID is used to segment the airwaves for usage.

2) Channels :- The stations communicate with each other using radio frequencies between 2.4 GHz and 2.5 GHz. Neighboring channels are only 5 MHz apart. Two wireless networks using neighboring channels may interfere with each other.

3) Wired Equivalent Privacy (WEP) :- It is a shared-secret key encryption system used to encrypt packets transmitted between a station and an AP. The WEP algorithm is intended to protect wireless communication from eavesdropping. A secondary function of WEP is to prevent unauthorized access to a wireless network. WEP encrypts the payload of data packets. Management and control frames are always transmitted in the clear. WEP uses the RC4 encryption algorithm.

4) Wireless Network Sniffing :- Sniffing is eavesdropping on the network. A (packet) sniffer is a program that intercepts and decodes network traffic broadcast through a medium. It is easier to sniff wireless networks than wired ones. Sniffing can also help find the easy kill as in scanning for open access points that allow anyone to connect, or capturing the passwords used in a connection session that does not even use WEP, or in telnet, rlogin and ftp connections.

5) Passive Scanning :- Scanning is the act of sniffing by tuning to various radio channels of the devices. A passive network scanner instructs the wireless card to listen to each channel for a few messages. This does not reveal the presence of the scanner. An attacker can passively scan without transmitting at all.

6) Detection of SSID :- The attacker can discover the SSID of a network usually by passive scanning because the SSID occurs in the following frame types: Beacon, Probe Requests, Probe Responses, Association Requests, and Reassociation Requests. Recall that management frames are always in the clear, even when WEP is enabled.
When the above methods fail, SSID discovery is done by active scanning

7) Collecting the MAC Addresses :- The attacker gathers legitimate MAC addresses for use later in constructing spoofed frames. The source and destination MAC addresses are always in the clear in all the frames.

8) Collecting the Frames for Cracking WEP :- The goal of an attacker is to discover the WEP shared-secret key. The attacker sniffs a large number of frames An example of a WEP cracking tool is AirSnort (http://airsnort.shmoo.com).

9) Detection of the Sniffers :- Detecting the presence of a wireless sniffer, who remains radio-silent, through network security measures is virtually impossible. Once the attacker begins probing (i.e., by injecting packets), the presence and the coordinates of the wireless device can be detected.

10) Wireless Spoofing :- There are well-known attack techniques known as spoofing in both wired and wireless networks. The attacker constructs frames by filling selected fields that contain addresses or identifiers with legitimate looking but non-existent values, or with values that belong to others. The attacker would have collected these legitimate values through sniffing.

11) MAC Address Spoofing :- The attacker generally desires to be hidden. But the probing activity injects frames that are observable by system administrators. The attacker fills the Sender MAC Address field of the injected frames with a spoofed value so that his equipment is not identified.

12) IP spoofing :- Replacing the true IP address of the sender (or, in rare cases, the destination) with a different address is known as IP spoofing. This is a necessary operation in many attacks.

13) Frame Spoofing :- The attacker will inject frames that are valid but whose content is carefully spoofed.

14) Wireless Network Probing :- The attacker then sends artificially constructed packets to a target that trigger useful responses. This activity is known as probing or active scanning.

15) AP Weaknesses :- APs have weaknesses that are both due to design mistakes and user interfaces

16) Trojan AP :- An attacker sets up an AP so that the targeted station receives a stronger signal from it than what it receives from a legitimate AP.

17) Denial of Service :- A denial of service (DoS) occurs when a system is not providing services to authorized clients because of resource exhaustion by unauthorized clients. In wireless networks, DoS attacks are difficult to prevent, difficult to stop. An on-going attack and the victim and its clients may not even detect the attacks. The duration of such DoS may range from milliseconds to hours. A DoS attack against an individual station enables session hijacking.

18) Jamming the Air Waves :- A number of consumer appliances such as microwave ovens, baby monitors, and cordless phones operate on the unregulated 2.4GHz radio frequency. An attacker can unleash large amounts of noise using these devices and jam the airwaves so that the signal to noise drops so low, that the wireless LAN ceases to function.

19) War Driving :- Equipped with wireless devices and related tools, and driving around in a vehicle or parking at interesting places with a goal of discovering easy-to-get-into wireless networks is known as war driving. War-drivers (http://www.wardrive.net) define war driving as “The benign act of locating and logging wireless access points while in motion.” This benign act is of course useful to the attackers.
Regardless of the protocols, wireless networks will remain potentially insecure because an attacker can listen in without gaining physical access.

Tips for Wireless Home Network Security

1) Change Default Administrator Passwords (and Usernames)
2) Turn on (Compatible) WPA / WEP Encryption
3) Change the Default SSID
4) Disable SSID Broadcast
5) Assign Static IP Addresses to Devices
6) Enable MAC Address Filtering
7) Turn Off the Network During Extended Periods of Non-Use

8) Position the Router or Access Point Safely