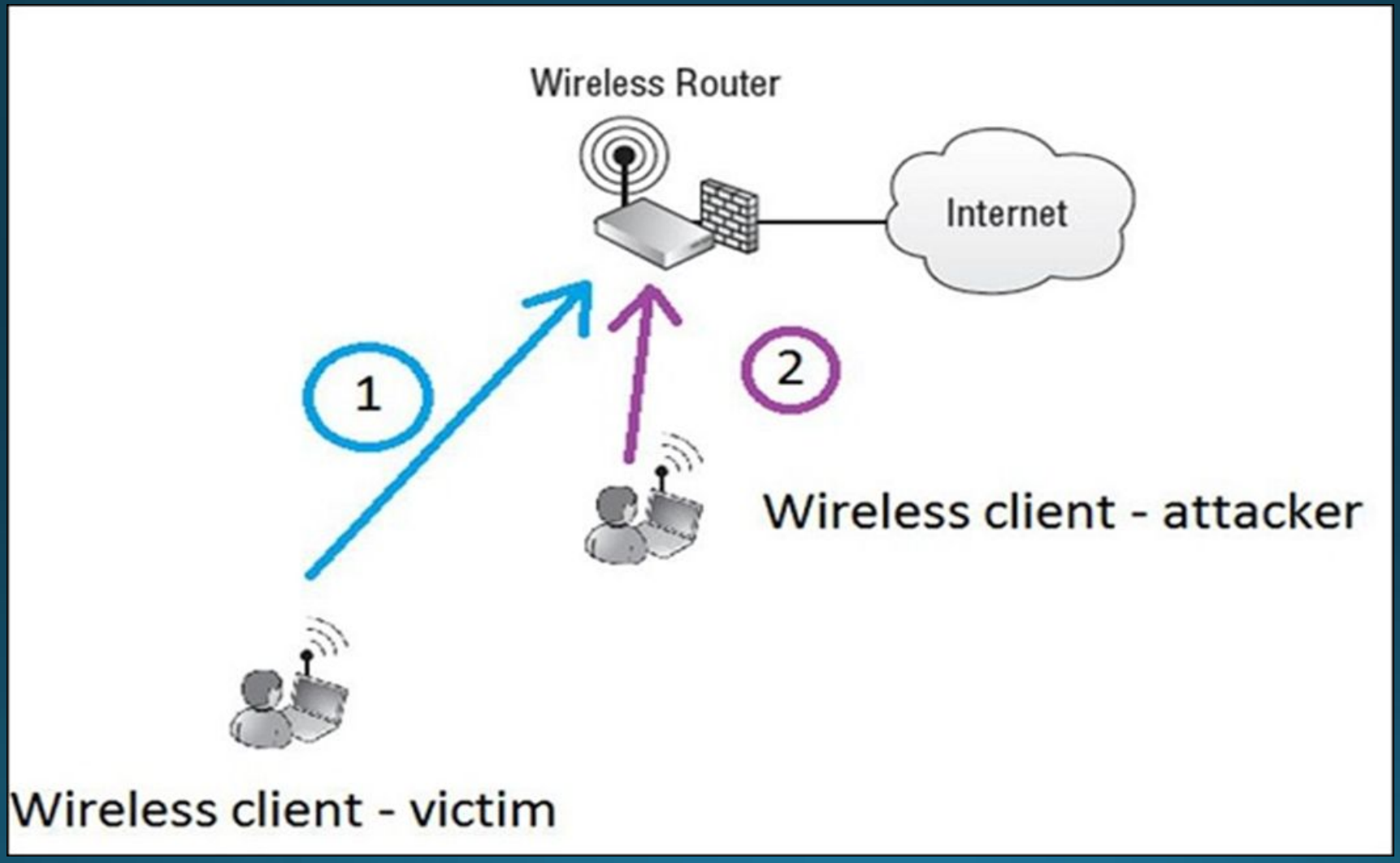
ATTACKS ON WIRELEES NETWORK

What is wireless network attack?

- Wireless network attacks aim to capture the information sent across the network.
- Wireless networks are much more vulnerable to attacks and intruders.
- Commonly known as wireless network attacks, penetration and intrusion acts that target wireless networks pose serious threats.


Wireless Router
Internet
1
2
Wireless client - attacker
Wireless client - victim

Types of Wireless Network Attacks

- Rouge Access Point
- Packet Sniffing
- Evil Twinning
- WEP cracking /WPA Cracking
- WPS (Wi-Fi Protected setup) attack

Wireless Reconnaissance

What is wireless reconnaissance?

- The basic goal of wireless reconnaissance is to locate the target network and gather as much information about its configuration and associated clients as possible.
- This information includes what is needed to connect to the target network such as network identifiers, authentication credentials, encryption keys, and addressing information.

SSID Decloaking

- Many network administrators feel it’s enough to not broadcast the existence of their wireless network.
- For most access points, this is referred to as SSID cloaking.

Passive Packet Capture

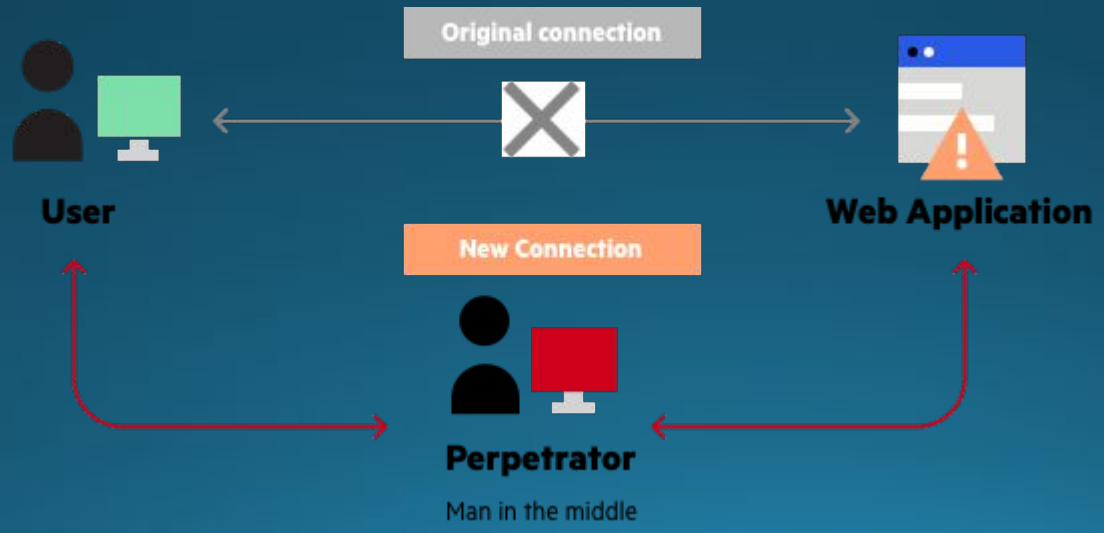
- For you to be able to capture traffic, you need to be within range of the target communicating station.
- At this point, you should understand that with the assistance of antennas, “within range” is a very flexible term.
- This means that as you’re sitting in your favorite coffee shop, the websites you visit could be watched by someone sitting at the next table, a building across the street, or even a few blocks away.
- Keep in mind that tests have been performed that have successfully picked up wireless transmissions over a few miles away with high-gain antennas.

Store and Crack at Your Convenience

- If someone were to capture their network traffic and crack it years later, the data might be worthless as all the passwords have expired and all the communication is old news (hopefully).
- Now consider a highly sensitive government agency. If an attacker were to capture their network traffic and crack it later, the data could contain confidential information that has no expiration date.
- For example: Social Security Numbers, government secrets, names of undercover agents, Nuclear launch codes, etc.

Man-in-the-Middle Attacks

- A man-in-the-middle (MITM) attack is a cyber attack in which a threat actor puts themselves in the middle of two parties, typically a user and an application, to intercept their communications and data exchanges and use them for malicious purposes like making unauthorized purchases or hacking.



The following are some of the more common techniques for establishing a man-in-the-middle attack:-

- ARP spoofing or ARP poisoning (Address Resolution Protocol)
- Rogue DHCP server (Dynamic Host Control Protocol)
- ICMP redirects (Internet Control Message Protocol)

WEP Authentication

WEP natively supports two very basic authentication mechanisms:-

1. Shared-key authentication.
2. Open authentication.

Shared-Key Authentication

- In shared-key authentication:-
- The WEP key is used to verify whether the user should have access to the wireless network.
- The access point and client go through what is called a four-way handshake.

- The process for the four-way handshake is as follows:-

1. The client sends an authentication request to the access point.
2. The access point sends the client a pseudo-random number (typically referred to as a nonce value).
3. The client encrypts the nonce value using the WEP key and sends it back to the access point.
4. The access point encrypts the same nonce value with the WEP key and compares it to what the client sent. If the values match, the client has the correct WEP key and the access point acknowledges the authentication attempt.

Open Authentication

- In open authentication:-
- There are essentially two messages:-

1. The client sends an authentication request to the access point.
2. The access point sends back a message that the station is authenticated.

Encryption

- Encryption is the process of obscuring data so that any unauthorized person who intercepts the data won't be able to understand it.
- Encryption would be relatively meaningless without being able to return the "jumbled" data to its original form.
- Thus, encryption is a two-way process. Taking encrypted data and returning it to readable data is called decryption.
- There are two main systems for encrypting data:-

1. Shared-key encryption
2. Public Key encryption

S.NO	Block Cipher	Stream Cipher
1	Block Cipher Converts the plain text into cipher text by taking plain text's block at a time	Stream Cipher Converts the plain text into cipher text by taking 1 byte of plain text at a time.
2	Block cipher uses either 64 bits or more than 64 bits.	While stream cipher uses 8 bits.
3	The complexity of block cipher is simple.	While stream cipher is more complex.
4	In block cipher, reverse encrypted text is hard.	While in-stream cipher, reverse encrypted text is easy.
5	Block cipher is slow as compared to a stream cipher.	While stream cipher is fast in comparison to block cipher.

How WEP Works

- Wired Equivalent Privacy (WEP) was part of the original 802.11 wireless standard introduced in 1997.
- WEP provides encryption at Layer 2 of the OSI model, the MAC or Link layer.
- Uses RC4 (Rivest cipher) stream cipher and 64-bit or 128-bit key .
- It encrypts messages one byte at a time via an algorithm.
- Static master key must be manually entered in each devices .

History of Breaking WEP

- In 2001, WEP was cryptographically broken by three security researchers: **Scott Fluhrer, Itsik Mantin, and Adi Shamir.**
- The attack is commonly known as the FMS attack, referring to the last names of the researchers who discovered the vulnerability.
- At its core, the vulnerability in WEP is due to its use of the 24-bit Initialization Vector.
- The FMS attack allows an attacker to discover the WEP key after passively capturing encrypted packets. For the attack to have a 50-percent success rate.
- Because WEP's IV is 24 bits in length, there are 16,777,216 unique Initialization Vector values. Yes, that sounds like a lot, but on a busy network you can easily send 16 million packets in a very short period of time.

Attacking WEP Encrypted Networks

The basic attack flow would look like this:

- Identify target wireless network.
- Passively monitor encrypted packets sent between the client and the access point using a sniffer.
- Save around 50,000 encrypted packets to a file on the attacking laptop.
- Run the aircrack-ng program against the saved encrypted packets to determine WEP key.

- Once you have successfully obtained the WEP key, either you can associate to the access point or you can continue to passively monitor network traffic.
- Remember that because WEP uses the same shared key among all hosts on the network, any host can decrypt communications between any client.
- After associating to the access point, an attacker could try to infiltrate deeper into the network