<https://chatgpt.com/c/c076abde-4d29-4d24-b544-7908d61cc03d>

1. What is session hijacking?

Sidejacking, also known as session hijacking, is a technique where an attacker intercepts and takes control of a user's session. This is typically done by stealing the session cookie—a small piece of data stored on the user's device that identifies their session with a web service. Once the attacker obtains the session cookie, they can impersonate the user and gain access to their account without needing to know the user's login credentials.

**How Sidejacking Works**

1. **Capturing Traffic**: The attacker uses tools to capture network traffic between the user and the web service. This is often done on unsecured Wi-Fi networks or through other means of intercepting communication.
2. **Extracting Session Cookies**: From the captured traffic, the attacker extracts the session cookie.
3. **Using the Session Cookie**: The attacker then uses the stolen cookie to impersonate the user. Since the session cookie is what authenticates the user's session with the web service, the attacker can gain access to the user's account.

**Prevention Measures**

* **Use HTTPS**: Ensuring that all communication between the user's device and the web server is encrypted using HTTPS makes it difficult for attackers to intercept traffic and steal session cookies.
* **Secure Cookies**: Setting cookies with the **Secure** and **HttpOnly** flags helps prevent cookies from being accessed through client-side scripts or transmitted over non-secure connections.
* **Session Expiration**: Implementing short session expiration times and automatic session termination after inactivity can limit the window of opportunity for an attacker.
* **Two-Factor Authentication (2FA)**: Using 2FA adds an extra layer of security, making it harder for attackers to gain access even if they have stolen a session cookie.
* **Regular Monitoring**: Regularly monitoring for unusual activity can help detect and respond to potential sidejacking attempts quickly.

Sidejacking is a significant threat, especially on unsecured networks, but with proper security measures, its risks can be mitigated.

1. What is Evil twin attack.

It is a wifi based attack.

An **evil twin attack** is a type of Wi-Fi attack where an attacker sets up a rogue access point (AP) that mimics a legitimate Wi-Fi network. The goal is to trick users into connecting to this malicious AP, allowing the attacker to intercept the victim's network traffic. Here’s a breakdown:

* **Objective**: Deceive users into connecting to a malicious Wi-Fi access point.
* **Method**: Create a rogue AP with the same SSID as a legitimate network.
* **Outcome**: Capture sensitive information, perform man-in-the-middle (MitM) attacks, inject malicious content, etc.

**How an Evil Twin Attack Works**

1. **Setup**: The attacker sets up a rogue Wi-Fi access point with the same SSID (network name) as a legitimate Wi-Fi network. The rogue access point might have a stronger signal to lure users into connecting to it instead of the legitimate one.
2. **Deception**: Users in the vicinity see the rogue access point and assume it is the legitimate one. They connect to it, thinking they are connecting to the trusted network.
3. **Data Interception**: Once users connect to the rogue access point, the attacker can intercept and monitor all network traffic. This can include capturing login credentials, credit card numbers, and other sensitive information.

### **Man-in-the-Middle (MitM) Attacks**: The attacker can perform additional attacks such as injecting malicious content into web pages, redirecting users to phishing websites, or manipulating data in transit. **Example Scenario**

1. **Legitimate Network**: A coffee shop offers free Wi-Fi with the SSID "CoffeeShopWiFi".
2. **Evil Twin**: An attacker sets up a rogue access point with the SSID "CoffeeShopWiFi", possibly with a stronger signal.
3. **User Connection**: A user sees two networks with the same name and unknowingly connects to the attacker's network.
4. **Data Capture**: The attacker captures the user's login credentials and other sensitive information as they browse the internet.

### Prevention and Protection

To protect against evil twin attacks, consider the following measures:

* **Use HTTPS**: Ensure that websites you visit use HTTPS, which encrypts data between your browser and the server, making it harder for attackers to intercept sensitive information.
* **VPN (Virtual Private Network)**: Use a VPN to encrypt all your internet traffic, providing an additional layer of security.
* **Disable Auto-Connect**: Disable the auto-connect feature on your devices to prevent them from automatically connecting to available Wi-Fi networks without your knowledge.
* **Verify Network Details**: Double-check the network name and, if possible, the MAC address of the access point before connecting, especially in public places.
* **Network Scanners**: Use network scanning tools to identify rogue access points. Some tools can detect discrepancies between legitimate and rogue access points.
* **Wireless Intrusion Detection Systems (WIDS)**: Organizations can deploy WIDS to monitor wireless networks and detect rogue access points.