What is a Session Hijacking?

TCP hijacking is another term for Session Hijacking. It is a way of hijacking a web user's active session ID when two users or devices interact, such as when a user checks or logs into their account or other online services; at that point, an attacker can take the user's session ID.

Once a hijacker knows a user's session ID, they can act as that user on the network and perform everything the user is allowed to do. The browser and online app sessions are the most common targets of session hijackers.
You can refer to:

Session Hijacking Attacks

There are several forms of session hijacking attacks; let's look at a few of the most common ones and how they work.

1. **Cross-site scripting:** Cross-site scripting (XSS) is a type of client-side code injection attack in which an attacker injects malicious scripts into the source code of a trusted website. Hijackers can impersonate users, control access, and steal the user's active session cookie when the scripts are executed on the web.

1. **Session side jacking:** Session side jacking is a security threat in which cybercriminals employ packet sniffing to hijack a session and intercept network communications between two parties to acquire the session ID.

1. **Session fixation:** In a session fixation attack, an attacker creates a session id, delivers it to the victim via email as a malicious link, and tricks the user into initiating a session with it to discover the victim's cookie.

1. **Man-in-the-browser:** A man-in-the-browser attack is similar to a man-in-the-middle or malware attack in which the attacker infects the victim's computer with malware first. When malware is installed on a victim's computer and the user visits a website, the hijacker functions as a man-in-the-middle attack, intercepting data and changing the user's activities.

How to prevent Session Hijacking?

There are various ways to safeguard your company and its users from a Session Hijacking attack.

1. Enable HTTPS on your website to encrypt all session traffic with SSL/TLS.
2. You should only share session IDs with the people you trust.
3. Avoid using public Wi-Fi and use a Virtual Private Network (VPN) to prevent hackers from intercepting your data.
4. Use strong passwords and multi-factor authentication on your website.
5. Install trusted security software on your devices used for online activity, and keep it up to date.
6. Update the session key right after authentication to avoid session fixation attacks.
7. Avoid phishing emails from unknown senders that contain malware.
8. Security threats continuously increase, so staying up to date on the latest attack strategies.

How can InfosecTrain help you?

With the rise in cyberattacks, you need to be more prepared than ever to safeguard yourself and your enterprises from these cyber threats and cybercriminals. Enroll InfosecTrain's Certified Ethical Hacker (CEH v12) certification training to understand the various session hijacking techniques and tools in-depth.