Session Hijacking – What is Session Hijacking

Session Hijacking: If you are trying to know all about Session Hijacking, then you are at the exact place.

First of all, read this article till the end. So that you can understand what is Session Hijacking. How it to process & how to implement.

Image Showing: Session Hijacking

now let me introduce with Session Hijacking. First of all, it is a process of taking control of a user session. After an authentication session ID obtains or generates.

The attacker uses it to capture a current session. After the user set up an authenticated session. Basically,
authentication mostly is done at the beginning of a TCP session.

Therefore, hijacking a user session helps an attacker to control the computer of the user. Finally, this control happens successfully.

This is just the overview of Session Hijacking. Now let’s go to know, how it happens. You need to know a few things, while you perform this method.

Now let me introduce all the types of attack in this method. Therefore go through the following aspects of Hijacking attacks.

- How to perform Session Hijacking.
- All the types.
- How to avoid.

So, scroll down to read all about each of these topics, one by one.

How to perform Session Hijacking

Now you have got all the overview of it. So, if you want to perform it, you must follow the following steps.

An attacker usually undertakes all the following steps to
perform this attacking process.

1. First of all monitor all the flow of packets in a network.
2. Identify an open session and predict the sequence number of the next packet to be sent.
3. Send a TCP reset or finish (FIN) packet to the computer of the legitimate user to instruct to close the session.
4. Similarly, send a TCP packet with the predicted sequence number to the server. The server accepts the packet assuming it as the next packet of the legitimate user.

Above mentioned process is the way to implement Hijacking process. You can use different tools, to perform it.

Here I am providing a few important tools for you. So, that you can perform Session Hijacking. Following is a list of tools. You can use these methods to perform. Let’s have a look.

**Hunt**

Hunt is a super tool for Hijacking method. It refers to a program that watches, listens, intercepts, & hijacks sessions.

Hunt hijacks session almost that are active on a network. Therefore you can use Hunt to watch, manage, & reset a connection.
**Juggernaut**

Similarly, the juggernaut is a powerful tool for Session Hijacking. This tool is basically Linux – based. Consequently, you can use it to hijack TCP user sessions.

Certainly, it is used to monitor all the network connections and hijack an ongoing network connection.

**IP Watcher**

IP Watcher tool basically used to monitor and take over user sessions. So, you can use this tool to monitor all the user sessions on a network. This tool is very important for the attacker to perform Hijacking method.

**TTY Watcher**

Also it a useful tool for this method. As a result, it refers to a Sun Solaris system tool, that is used to monitor and control user sessions on a system.

**T- Sight**

It is a very useful tool. Similarly works for hijack sessions. This tool designed for windows platform.
T-Sight tool monitor all connections (traffic) on a network. Also, this tool observes any kind of suspicious activity on the network. So, you can use this tool to hijack any TCP sessions on the network.

**Paros HTTP Hijacker**

Refers to an application vulnerability scanner and acts as a proxy in a man-in-the-middle attack.

You can use this tool to modify and debug HTTP & HTTPS-based data. That is exchanged between a web server and the client.

Related topic: [Social engineering](#)

**Remote TCP Session Reset Utility**

Similarly, this is another powerful tool to hijack session certainly. Therefore this tool used to monitor TCP connections & reset a TCP connection.

I want to bring your kind attention towards little bit notification for using Remote TCP Session Reset tool.

You must start the SNMP Service and SNMP trap service to enable the working of the Remote TCP Session Reset tool.

Also, specify a community string in the SNMP services. This string refers to a password that controls the user’s access to the SNMP Service.

**All the Types of Session Hijacking**

First of all, depending on the attacker’s involvement within the session, Session Hijacking can be classified into two types. Therefore followings are the types.

**Active Session Hijacking**

Active Session Hijacking represents a session hijacking attack in which the attacker finds an active user session first.

As a result, the attacker takes over the session by using tools. That predicts the next sequences number of the session.

**Passive Session Hijacking**
This type of attack represents a session hijacking in which the attacker hijacks a user session. Therefore watches and records all the traffic that the legitimate user sends to the server.

Consequently, it is used to gather information. Such as passwords, IP, even more. The attacker uses all these credentials later to open a separate authenticated session.

how to avoid session hijacking

Session Hijacking poses a great danger. It can be used for crimes. Such as identity theft, fraud even more. But it is quite easy to execute hijacking attacks. Computers that use the TCP / IP protocol are more vulnerable to hijacking attacks.

There is also a way to protect your computer from hijacking. The best way to protect your computer from hijacking is to switch to secure protocols. Such as Secure Socket Layer.

It is called SSL also. Also, you can use Secure Shell. Followings are the list of countermeasure to avoid hijacking attacks.

1. Use a secure protocol.
2. use encryption.
3. put a limit on incoming connections.
4. use strong authentication.
5. use different user names & password for different accounts.
6. minimize remote access.
7. make educate the employees.

Most countermeasures do not work if encryption is not used.

**Conclusion**

I hope you have gone through the whole article & understood all about Session Hijacking.

If you have any doubt about, then don’t hesitate to drop your question in the comment box below.

I will be there for your further assistance.