10.2.13 Session Hijacking Countermeasure Facts

Session hijacking can be difficult to detect. As a result, prevention is a group effort. The penetration tester, the network administrators, the web developers, and even the users have a part in this defense plan.

This lesson covers the following topics:

- Penetration tester's role
- Administrator's role
- Developer's role
- User's role

Penetration Tester's Role

As a penetration tester, the first step to securing your network is to understand potential threats. The more you understand what could happen, the better prepared you are to prevent bad things from happening. Frequent penetration testing will go a long way toward discovering the weaknesses in your network. (That is, after all, the primary idea behind ethical hacking.) In most situations, you begin session hijacking penetration testing by sniffing packets for an active session. You then sniff the session traffic as it’s sent from one machine to the other. If there is no encryption, you can retrieve the session ID. If there is encryption, you should still be able to retrieve the session ID; you just need to crack the encryption. Once you have the session ID, you can use the session fixation method to connect to the victim machine and take action as an authorized network user. At this point, you are able to gather additional session IDs, making it easier to guess additional IDs as needed.

Administrator's Role

A network administrator can configure gateways and other appliances to look for spoofed IP addresses. They can also implement intrusion detection systems and intrusion prevention systems to aid in the detection and prevention of suspicious network activity. Encrypting network traffic can help to prevent attacks from both inside and outside your network. The down side, of course, is that it also limits your ability to monitor your own network. There are several methods to encrypt and authenticate packets, but Internet Protocol Security, IPsec, is one of the most common methods used to protect packet information and to defend against network attacks. IPsec is a set of protocols that provides encrypted communication between computers over an unsecured network. The data sent from one computer is encrypted before it is sent across an unsecured network to the receiving computer. IPsec negotiates an access key with the receiving computer so that only that computer can access and decrypt the data being sent.

There are several protocols within the IPsec architecture, including:

- The Internet Key Exchange (IKE), which creates the encryption keys.
- The Authentication Header (AH), which authenticates the sender of the packets.
- The Encapsulating Security Payload (ESP), which provides sender authentication and encryption.

In tunnel mode, the security is provided from one gateway to another. In this mode, the entire packet is protected. Tunnel mode, or Virtual Private Networks, are the most commonly used IPsec method.

Developer's Role

Most forms of session hijacking rely heavily on the ability to read packets and predict session IDs. Web developers can create session keys that incorporate long strings or random numbers, making it more difficult to guess or predict a session key. Additionally, they could regenerate the session ID after a user logs in, encrypt the key being transferred between the web server and the user, and stop the session after a period of time or as soon as the user logs off.

User's Role

User education is an important part of security. Because attacks like session fixation rely on a user clicking on a link in an email or instant message, users should be trained not to click on these links. Additionally, session hijacking can be prevented at the browser level by restricting cookies, clearing the history of temporary cookies, using log files, using session IDs, and restricting offline content.