5.3. Session Hijacking

Session hijacking is when a hacker takes control of a user session after the user has successfully authenticated with a server. Session hijacking involves an attack identifying the current session IDs of a client/server communication and taking over the client's session. Session hijacking is made possible by tools that perform sequence-number prediction.

Spoofing attacks are different from hijacking attacks. In a spoofing attack, the hacker performs sniffing and listens to traffic as it's passed along the network from sender to receiver. The hacker then uses the information gathered to spoof or uses an address of a legitimate system. Hijacking involves actively taking another user offline to perform the attack. The attacker relies on the legitimate user to make a connection and authenticate.

After that, the attacker takes over the session, and the valid user's session is disconnected.

Session hijacking involves the following three steps to perpetuate an attack:

Tracking the Session The hacker identifies an open session and predicts the sequence number of the next packet.

Desynchronizing the Connection The hacker sends the valid user's system a TCP reset (RST) or finish (FIN) packet to cause them to close their session.

Injecting the Attacker's Packet The hacker sends the server a TCP packet with the predicted sequence number, and the server accepts it as the valid user's next packet.

Hackers can use two types of session hijacking: active and passive. The primary difference between active and passive hijacking is the hacker's level of involvement in the session. In an active attack, an attacker finds an active session and takes over the session by using tools that predict the next sequence number used in the TCP session.

In a passive attack, an attacker hijacks a session and then watches and records all the traffic that is being sent by the legitimate user. Passive session hijacking is really no more than sniffing. It gathers information such as passwords and then uses that information to authenticate as a separate session.

Sequence Prediction

TCP is a connection-oriented protocol, responsible for reassembling streams of packets into their original intended order. Every packet has to be assigned a unique session number that enables the receiving machine to reassemble the stream of packets into their original and intended order; this unique number is known as a *sequence number*. If the packets arrive out of order, as happens regularly over the Internet, then the SN is used to stream the packets correctly. As just illustrated, the system initiating a TCP session transmits a packet with the SYN bit set. This is called a *synchronize packet* and includes the client's ISN. The ISN is a pseudo-randomly generated number with over 4 billion possible combinations, yet it is statistically possible for it to repeat.

When the ACK packet is sent, each machine uses the SN from the packet being acknowledged, plus an increment. This not only properly confirms receipt of a specific packet, but also tells the sender the next expected TCP packet SN. Within the three-way handshake, the increment value is 1. In normal data communications, the increment value equals the size of the data in bytes (for example, if you transmit 45 bytes of data, the ACK responds using the incoming packet's SN plus 45).

Fig: Sequence numbers and acknowledgment during the TCP three-way handshake

Hacking tools used to perform session hijacking do sequence number prediction. To successfully perform a TCP sequence prediction attack, the hacker must sniff the traffic between two systems. Next, the hacker or the hacking tool must successfully guess the SN or locate an

ISN to calculate the next sequence number. This process can be more difficult than it sounds, because packets travel very fast.

When the hacker is unable to sniff the connection, it becomes much more difficult to guess the next SN. For this reason, most session-hijacking tools include features to permit sniffing the packets to determine the SNs.

Hackers generate packets using a spoofed IP address of the system that had a session with the target system. The hacking tools issue packets with the SNs that the target system is expecting. But the hacker's packets must arrive before the packets from the trusted system whose connection is being hijacked. This is accomplished by flooding the trusted system with packets or sending an RST packet to the trusted system so that it is unavailable to send packets to the target system.

Dangers Posed by Session Hijacking

TCP session hijacking is a dangerous attack: most systems are vulnerable to it, because they use TCP/IP as their primary communication protocol. Newer operating systems have attempted to secure themselves from session hijacking by using pseudo-random number generators to calculate the ISN, making the sequence number harder to guess. However, this security measure is ineffective if the attacker is able to sniff packets, which gives all the information required to perform this attack.

The following are reasons why it's important for a CEH to be aware of session hijacking:

- Most computers are vulnerable.
- Few countermeasures are available to adequately protect against it.
- Session hijacking attacks are simple to launch.
- Hijacking is dangerous because of the information that can be gathered during the attack.

Preventing Session Hijacking

To defend against session hijack attacks, a network should employ several defenses. The most effective protection is encryption, such as Internet Protocol Security (IPSec). This also defends against any other attack vectors that depend on sniffing. Attackers may be able to passively

monitor your connection, but they won't be able to interpret the encrypted data. Other countermeasures include using encrypted applications such as Secure Shell (SSH, an encrypted telnet) and Secure Sockets Layer (SSL, for HTTPS traffic).

You can help prevent session hijacking by reducing the potential methods of gaining access to your network—for example, by eliminating remote access to internal systems. If the network has remote users who need to connect to carry out their duties, then use virtual private networks (VPNs) that have been secured with tunneling protocols and encryption (Layer 3 Tunneling Protocol [L3TP]/Point-to-Point Tunneling Protocol [PPTP] and IPSec).

The use of multiple safety nets is always the best countermeasure to any potential threat. Employing any one countermeasure may not be enough, but using them together to secure your enterprise will make the attack success rate minimal for anyone but the most professional and dedicated attacker. The following is a checklist of countermeasures that should be employed to prevent session hijacking:

- Use encryption.
- Use a secure protocol.
- Limit incoming connections.
- Minimize remote access.
- Have strong authentication.
- Educate your employees.
- Maintain different username and passwords for different accounts.
- Use Ethernet switches rather than hubs to prevent session hijacking attacks.