10.2.2 Session Hijacking Facts

Unlike spoofing, where you pretend to be someone else, session hijacking involves taking over a session that has already been authenticated.

Topic	Description
Passive hijacking	With passive hijacking, an attacker uses a sniffer to monitor traffic between a victim and a host.
Active hijacking	With active hijacking, the attacker manipulates the client's connection to boot the real client and allow the server to think that the attacker is the authenticated user.
Session IDs	The key to session hijacking lies in session IDs. Once a client is authenticated, the server provides a period of time that the client can maintain an open connection. The server assumes that information sent and received during this session is being done by the appropriate user. Each reservation, or session, is assigned an alphanumeric session ID, also known as a session token. This token serves as the key--and this is where the opportunity lies for an attacker. If an attacker can capture or even calculate the ID, they can hijack a session. Once a hacker is able to take over a session, they can gather data, enter commands, and complete transactions that they wouldn't have been able to do without the level of authorization gained from the hijacked session. This could result in corrupted data, leakage of sensitive information, or identity theft. It probably goes without saying that the less secure an environment is, the more successful an attacker will be. The ideal scenario for a hacker would be simple, easy-to-guess session ID algorithms, short session IDs, unlimited session times, clear text transmissions, and a lack of account lockouts for invalid session IDs.
Session hijacking methods	Session hijacking is usually done in one of three ways. Brute force hijacking is done by guessing an ID. This method is usually used if the hacker has some knowledge about the IDs being used by the server. An attacker could steal an ID using sniffing, or they could calculate an ID by looking at current session IDs and determining the sequencing algorithm being used.
Session hijacking process	The session hijacking process has five steps. The first step is sniffing the traffic between the target computer and the server. The second step is to monitor traffic with the goal of predicting the packet sequence numbers. The third step involves desynchronizing the current session so you can move onto the fourth step of predicting the session ID and take over the session. The final step is where you start injecting commands targeted at the server.