# 5.2.2 Session-Based Attack Facts

In a *session-based attack*, the attacker takes over the TCP/IP session or captures information that can be used at a later date. Common session-based attacks include the following methods:

| Attack | Description |
|---|---|
| Man-in-the-Middle | A *man-in-the-middle* attack is used to intercept information passing between two communication partners. During a man-in-the-middle attack:<br>▪ An attacker inserts himself in the communication flow between the client and server. The client is fooled into authenticating to the attacker.<br>▪ Both parties at the endpoints believe they are communicating directly with the other, while the attacker intercepts and/or modifies the data in transit. The attacker can then authenticate to the server using the intercepted credentials.<br>Man-in-the-middle attacks are commonly used to steal credit cards, online bank credentials, and confidential personal and business information. |
| TCP/IP (Session) Hijacking | TCP/IP hijacking is an extension of a man-in-the-middle attack where the attacker steals an open and active communication session from a legitimate user.<br>▪ The attacker takes over the session and cuts off the original source device.<br>▪ The TCP/IP session state is manipulated so that the attacker is able to insert alternate packets into the communication stream.<br>Countermeasures for hijacking include using:<br>▪ IPSec or other encryption protocols<br>▪ Certificate authentication<br>▪ Mutual authentication<br>▪ Randomizing sequencing mechanisms<br>▪ Packet time stamps<br>▪ Packet sequencing |
| HTTP (Session) Hijacking | HTTP (session) hijacking is a real-time attack in which the attacker hijacks a legitimate user's cookies and uses them to take over the HTTP session. |
| Replay Attack | In a *replay attack*, the attacker uses a protocol analyzer or sniffer to capture authentication information going from the client to the server. The attacker then uses this information to connect at a later time and pretend to be the client. To carry out a replay attack, intruders do not need to decrypt the intercepted packet. They can simply forward the packet to an application or service and gain access to the victim's resources or data. To prevent a replay attack, use a secure authentication method, such as Kerberos. The Kerberos protocol embeds additional data, such as the client's timestamp, into network packets. |
| Null Session | A *null session* is a connection that is made using a blank user name and password.<br>▪ Older Microsoft systems used null sessions between computers. Attackers can use this vulnerability to log on and discover information about the system, such as a list of user names or shared folders.<br>▪ Null sessions are allowed through the SMB and NetBIOS protocols used on Microsoft systems.<br>▪ To prevent null session attacks, block ports 139 and 445 on network firewalls. Windows NT uses TCP port 139 to establish NetBIOS sessions, and Windows 2000 uses TCP port 445 for SMB sessions. |

TestOut Corporation All rights reserved.