2.5 Session Hijacking

Another form of attack is session hacking or hijacking. TCP session hijacking is the process where a hacker takes over a TCP session between two machines. Because authentication is frequently done only at the start of a TCP session, this allows the hacker to break into the communication stream and take control of the session. For example, a person might log on to a machine remotely. After establishing a connection with the host, the hacker might use session hacking to take over that session, thereby gaining access to the target machine.

One popular method for session hacking is using source-routed IP packets. This allows a hacker at point A on the network to participate in a conversation between B and C by encouraging the IP packets to pass through the hacker’s machine.

The most common type of session hacking is the “man-in-the-middle attack.” In this scenario, a hacker uses some sort of packet-sniffing program to simply listen the transmissions between two computers, taking whatever information he or she wants, but not actually disrupting the conversation. A common component of such an attack is to execute a DoS attack against one end point to stop it from responding. Because that end point is no longer responding, the hacker can now interject his own machine to stand in for that end point.

The point of hijacking a connection is to exploit trust and gain access into a system to which one would not otherwise have access.