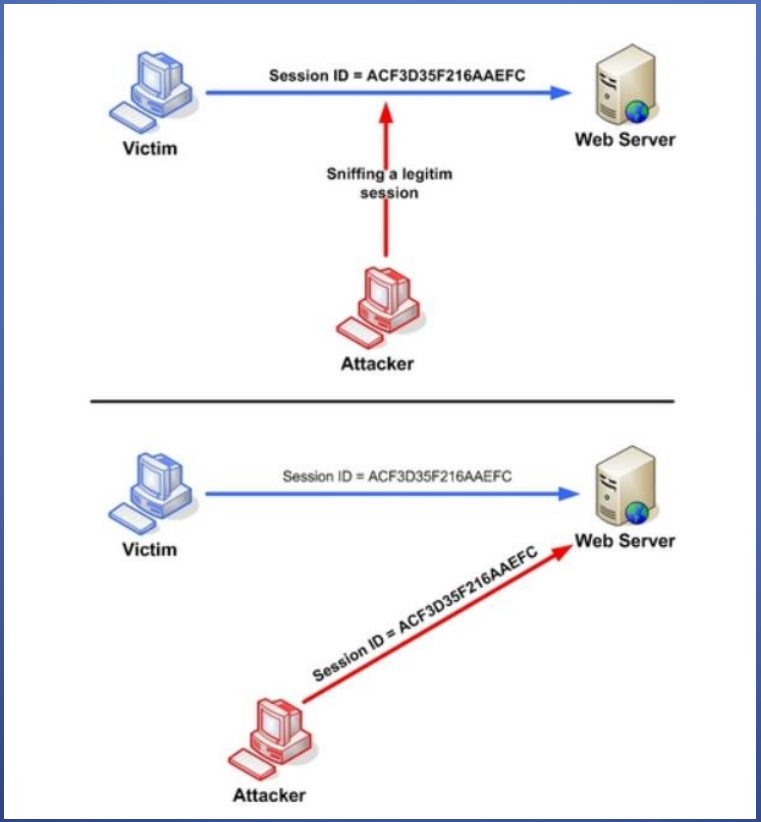
TCP Session Hijacking

Introduction

- TCP hijacks are meant to intercept the already established TCP sessions between any two communicating parties and then pretending to be one of them, finally redirecting the TCP traffic to it by injecting spoofed IP packets so that your commands are processed on behalf of the authenticated host of the session.
- It desynchronizes the session between the actual communicating parties and by intruding itself in between.
- The goal of the TCP session hijacker is to create a state where the client and server are unable to exchange data; enabling him/her to forge acceptable packets for both ends, which mimic the real packets. Thus, the attacker is able to gain control of the session.
- TCP session hijacks can be implemented in two different ways: Middle Man Attack and the Blind attack.

Session Hijacking Implementation

IP Spoofing: IP spoofing is a technique which is used to gain unauthorized access to computers where the intruder sends a message to a computer with an IP address indicating that the message is coming from a trusted host.



Session Hijacking Implementation

Man in the middle Attack: Attacker tries to get the session Id by doing ARP spoofing and man in the middle attack.

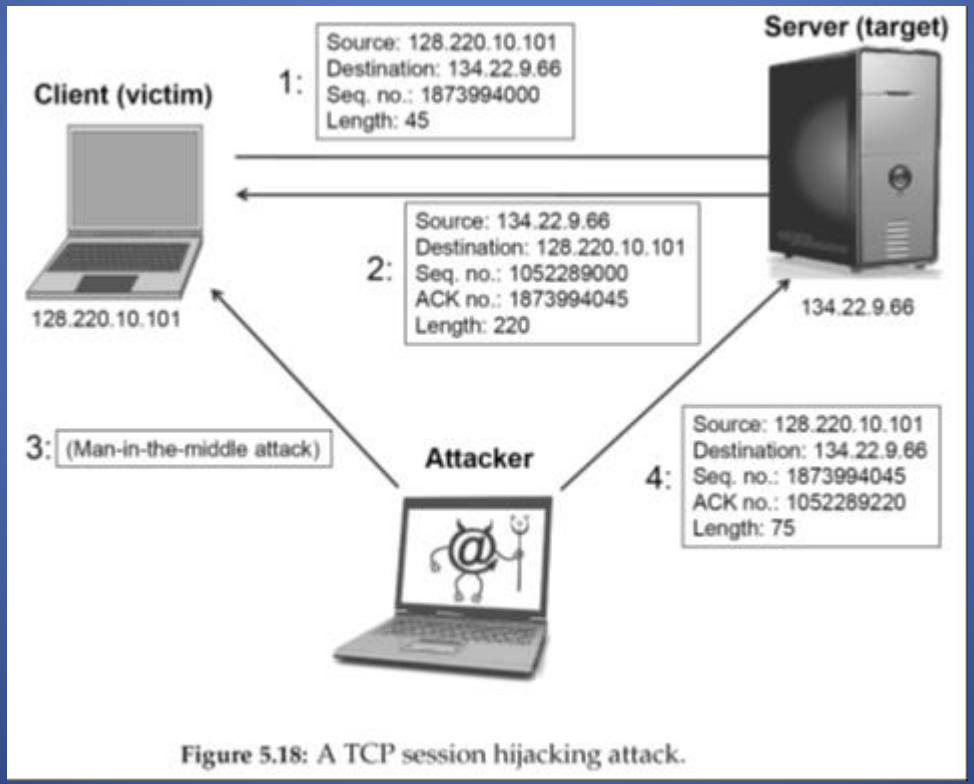


Figure 5.18: A TCP session hijacking attack.