TCP RST

TCP RST

TCP RST attack is also known as TCP reset attacks a malicious attacker sends a forge TCP reset packet to interrupt and terminate the TCP session between host machines.

A TCP RST flagged spoofed packet is send either any one of the active TCP session host machines. The attacker sniff the network packets with help of network sniffing tools like Wireshark. The attacker target the high value network connection based on network traffic and number of active connection and send the TCP RST message resulting session termination between the active hosts.

Attacks

- Session hijacking: Session hijacking attacks can use TCP RST spoofing to steal session IDs, granting attackers access to private systems and data.
- Man-in-the-Middle: MITM attacks can also make use of TCP RST attack to intercept and modify traffic between victim machines.

Example

In the following screenshot there is an active TCP session between host 192.168.198.129 and 192.168.198.130. You will notice a TCP RST, ACK flagged message is send from host 192.168.198.130 to 129. But the RST, ACK is marked as unseen segment request from 192.168.198.129. Resulting a suspicious RST request from host 192.168.198.130.