

TCP RST

TCP RST

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

A TCP RST flagged spoofed packet is sent either to any one of the active TCP session host machines. The attacker sniffs the network packets with help of network sniffing tools like Wireshark. The attacker targets the high value network connection based on network traffic and number of active connections and sends the TCP RST message resulting in 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.

No.	Time	Source	Destination	Protocol	Length	Info
20	2019-06-30 21:35:40.0663816...	192.168.198.130	192.168.198.129	TCP	66	35694 → 23 [ACK] Seq=4109889096 Ack=149492353 Win=245 Len=0 TSval=49738 TSec...
21	2019-06-30 21:35:40.1339857...	Vmware_65:fe:f5	Broadcast	ARP	60	Who has 192.168.198.130? Tell 192.168.198.128
22	2019-06-30 21:35:40.1341004...	Vmware_b3:84:66	Vmware_65:fe:f5	ARP	60	192.168.198.130 is at 00:0c:29:b3:84:66
23	2019-06-30 21:35:40.2223209...	192.168.198.129	192.168.198.130	TCP	60	23 → 35694 [RST, ACK] Seq=149492330 Ack=4109889095 Win=0 Len=0
24	2019-06-30 21:35:40.2626872...	Vmware_65:fe:f5	Broadcast	ARP	60	Who has 192.168.198.129? Tell 192.168.198.128
25	2019-06-30 21:35:40.2627272...	Vmware_54:d6:4e	Vmware_65:fe:f5	ARP	42	192.168.198.129 is at 00:0c:29:54:d6:4e
26	2019-06-30 21:35:40.3503995...	192.168.198.130	192.168.198.129	TCP	60	35694 → 23 [RST, ACK] Seq=4109889096 Ack=149492331 Win=0 Len=0
27	2019-06-30 21:35:40.3504960...	192.168.198.129	192.168.198.130	TCP	60	[TCP ACKed unseen segment] 23 → 35694 [RST, ACK] Seq=149492332 Ack=410988909...
28	2019-06-30 21:35:40.3505000...	192.168.198.130	192.168.198.129	TCP	60	35694 → 23 [RST, ACK] Seq=4109889096 Ack=149492333 Win=0 Len=0
29	2019-06-30 21:35:40.3507839...	192.168.198.129	192.168.198.130	TCP	60	[TCP ACKed unseen segment] 23 → 35694 [RST, ACK] Seq=149492353 Ack=410988909...
30	2019-06-30 21:35:45.1223833...	Vmware_54:d6:4e	Vmware_b3:84:66	ARP	42	Who has 192.168.198.130? Tell 192.168.198.129
31	2019-06-30 21:35:45.1240236...	Vmware_b3:84:66	Vmware_54:d6:4e	ARP	60	192.168.198.130 is at 00:0c:29:b3:84:66

▶ Frame 23: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▶ Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: Vmware_b3:84:66 (00:0c:29:b3:84:66)
▶ Internet Protocol Version 4, Src: 192.168.198.129, Dst: 192.168.198.130
▶ **Transmission Control Protocol, Src Port: 23, Dst Port: 35694, Seq: 149492330, Ack: 4109889095, Len: 0**
Source Port: 23
Destination Port: 35694
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 149492330
Acknowledgment number: 4109889095
Header Length: 20 bytes
▶ **Flags: 0x014 (RST, ACK)**
Window size value: 0
[Calculated window size: 0]