CSE 406

TCP Reset Attack On Video Streaming Application

Submitted by-
1605078
Md.Mohib Hossain

1. TCP Reset Attack

TCP reset attack also known as “forged TCP resets” or “spoofed TCP reset packets” is a way to tamper and terminate an established internet connection between a server and a client by sending a forged TCP reset packet.

A TCP connection can be terminated in two ways

i. A **FIN** Packet
ii. A **RST** Packet

A **FIN** Packet contains a packet with the **FIN** bit set in TCP header and used in normal condition for terminating the connection.

A **RST** packet contains a packet with the **RST** bit set in TCP header and used to terminate the connection immediately.

RST packets are necessary for a firewall to use in goodwill, but they can also be abused by attackers to interrupt internet connections.

2. RST Timing Diagram

A RST packet is sent to terminate the established connection immediately.

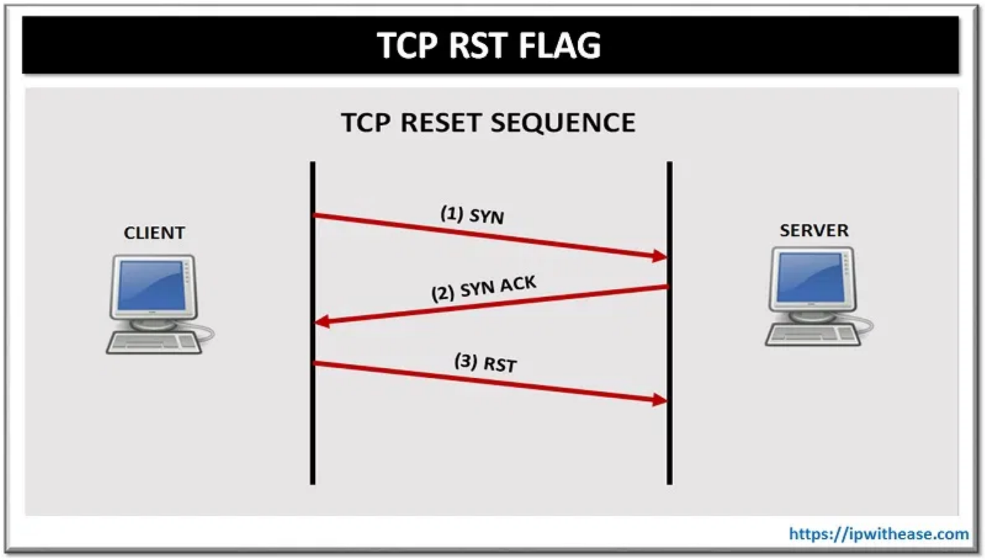

Fig: RST Timing diagram

3. Network Topology

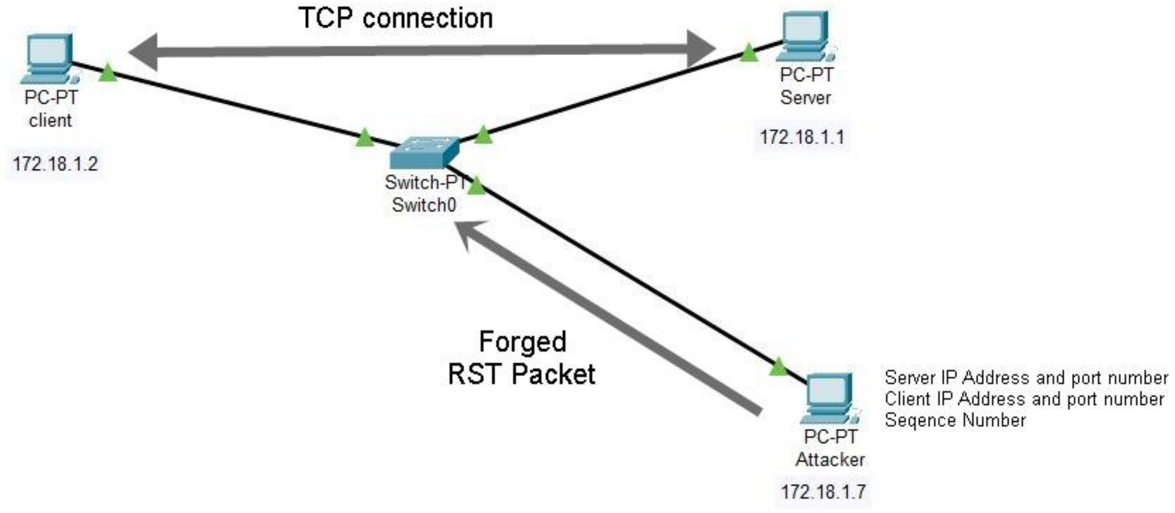

Fig: TCP reset attack

Here the server, client(victim) and the attacker are in the same LAN. Server will stream the video and the client will view the video using a video streaming application. The attacker will forge a **RST** packet and send it to the client, upon receiving the **RST** packet, the client will terminate the connection.

4. Attack Strategy

For a TCP reset attack, an attacker would need to know few information

i. Source (Victim) IP Address
ii. Destination (Server) IP Address
iii. Source Port Number
iv. Destination Port Number
v. Sequence Number in TCP header

The Attack Procedure is given bellow:

i. **ARP Spoofing:** ARP Spoofing to update ARP tables of both the server and client so that all traffic between the server and the client (victim) are passed through the attacker.

ii. **Packet Sniffing:** After ARP Spoofing, the attacker would be able to intercept the packets between the server and the client (victim). Sniffing the packets, the attacker would be able collect the above required information.

iii. **Packet Spoofing:** After collecting the required information, the attacker would be able to forge a **RST** TCP packet with the server's IP as the source IP Address and the victim's IP as the destination IP Address and setting the **RST** bit in TCP header. Then the attacker would spoof these forged TCP packets to the client. Upon receiving the **RST** packet, the client will terminate the TCP connection

5. Packet details

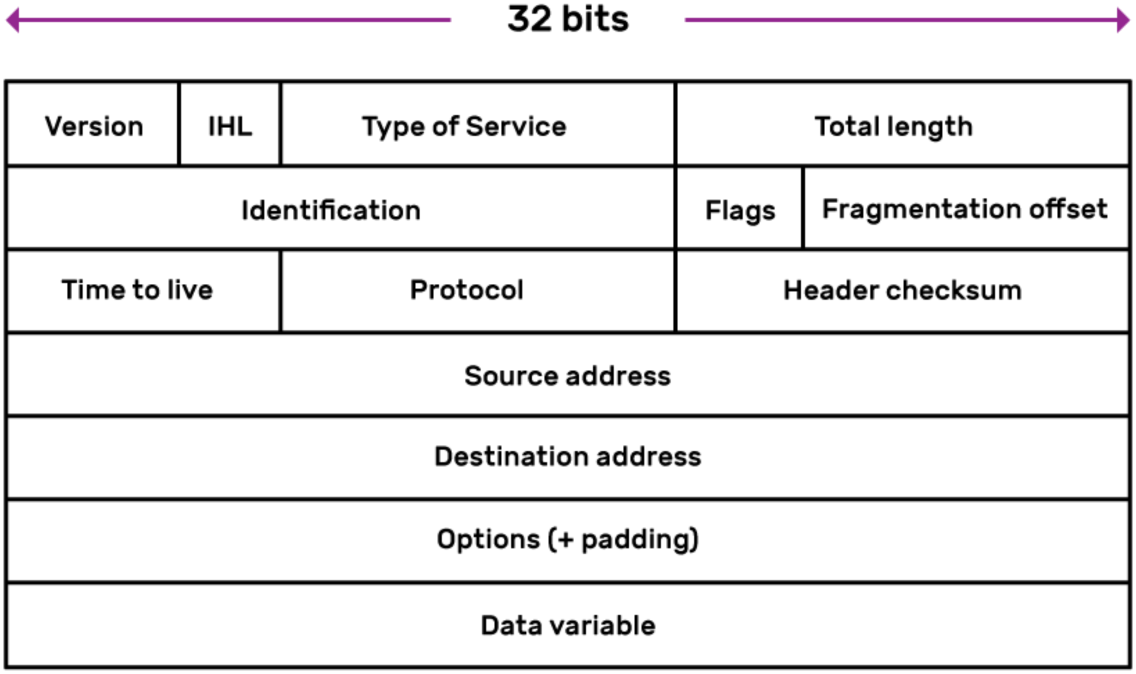

Fig: IP Header

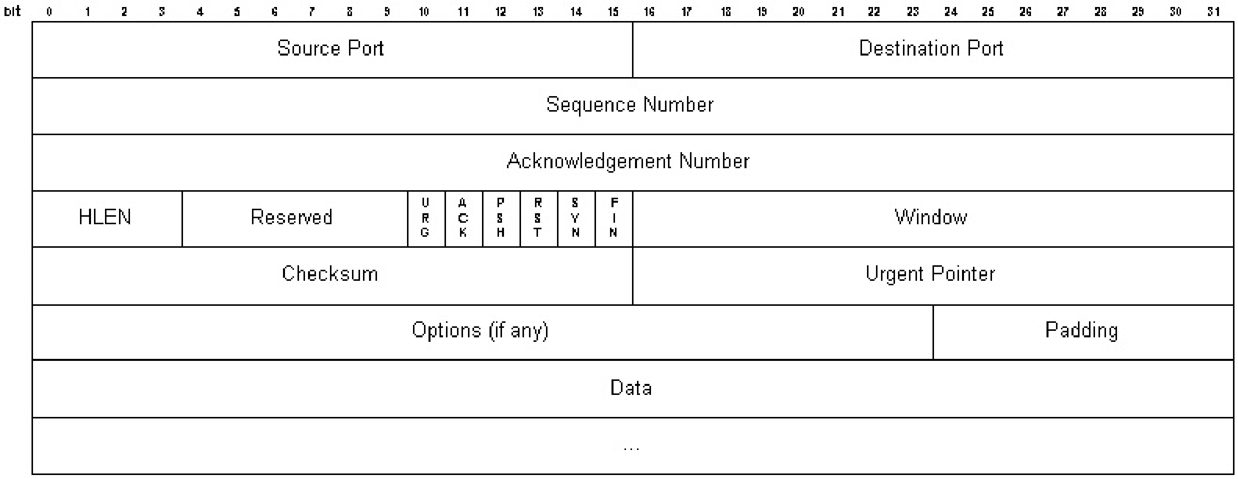

Fig: TCP Header

The attacker will sniff packets and retrieve IP address of source and victim from IP header and Source Port Number, Destination Port Number and Sequence Number from TCP header and then forge a packet following the above mentioned procedure.

6. Conclusion

As the attacker acts as a gateway for the victim, the victim has no way to differentiate between an actual **RST** packet and a forged **RST** packet. So it will terminate the connection regardless.

Hence the attack should be successful.