TCP Reset Attack on Telnet

Naser Anjum , 1505099

1 Introduction

TCP Reset Attack breaks an existing connection between two victim hosts with the use of a single spoofed RST packet. RST is important for the TCP protocol as it is often used in emergency situations to close connection as FIN Protocol takes more time, but it makes it useful for attacks too.

2 Topology Diagram

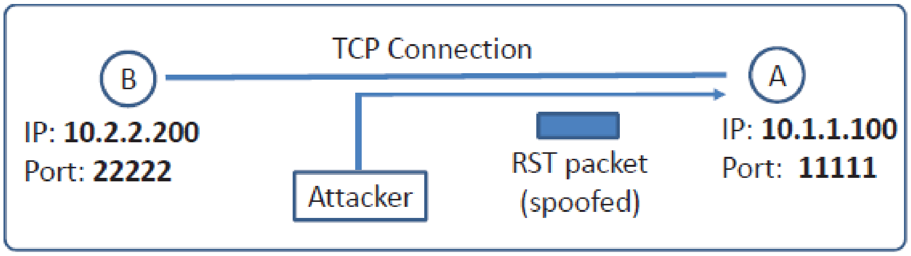


Figure 1: Topology of TCP Reset Attack

3 Attacking Strategy

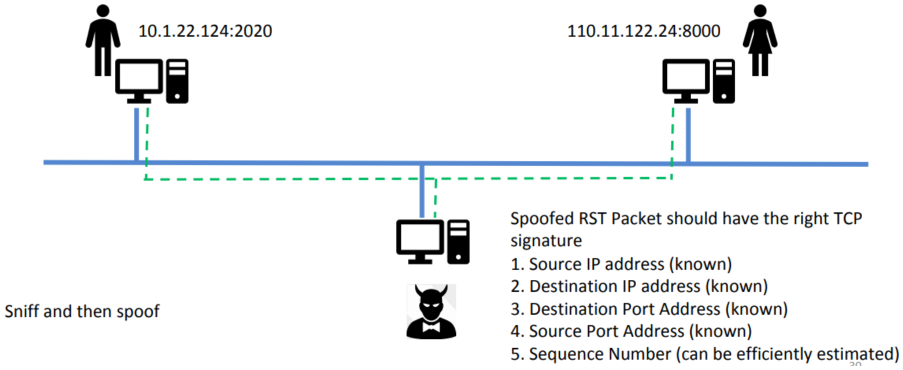
If we, the attacker, send out an RST packet to either A or B of Figure 1, the connection will be closed. For the attack to be successful, few fields of the IP and TCP headers need to be filled out appropriately. Four fields differentiate a connection from others:

- Source IP address
- Source port
- Destination IP address
- Destination port

These fields in the spoofed packet need to be same as the connection. Also, for the receiver to not discard the packet, the **Sequence Number** needs to be correct (within receiver's window or stricter restrictions in some cases).

To get these fields, we will sniff using the tool Wireshark from the same network. We will observe the last packet sent between the two users who will be using Telnet.

With these information collected, we can write a program to generate a spoofed RST packet. We hope to write the program on Python.



Spoofed RST Packet should have the right TCP signature

1. Source IP address (known)
2. Destination IP address (known)
3. Destination Port Address (known)
4. Source Port Address (known)
5. Sequence Number (can be efficiently estimated)

Figure 2: Attacking Strategy - Sniff and Spoof

4 Timing Diagram

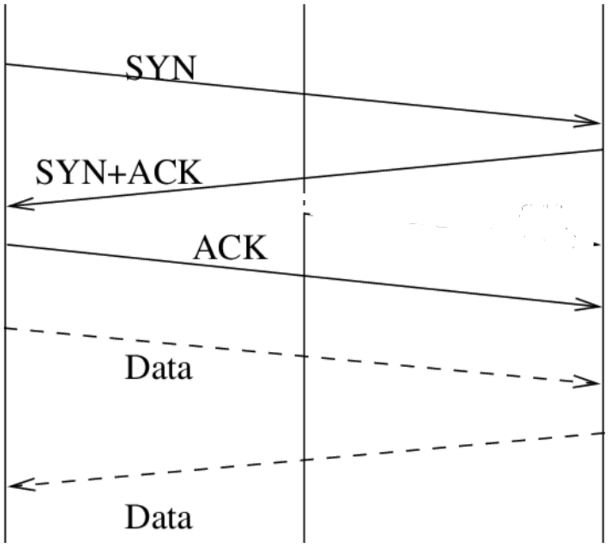


Figure 3: Original protocol timing diagram

Originally, the TCP protocol gets initiated by a SYN packet. Then upon receiving the other side sends a SYN+ACK packet and the first sender returns ACK packet to establish the connection. After that they exchange data accordingly. In case of closing connections they use FIN or RST packet.

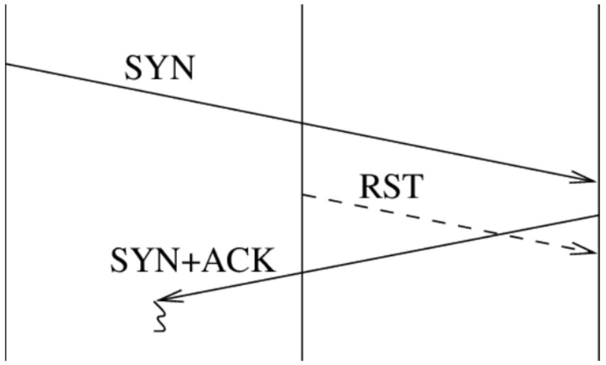


Figure 4: Attack timing diagram

In case of the attack, the attacker can send the RST packet with correct details at any point of connection. And this RST packet terminates the connection.

5 Packet Details

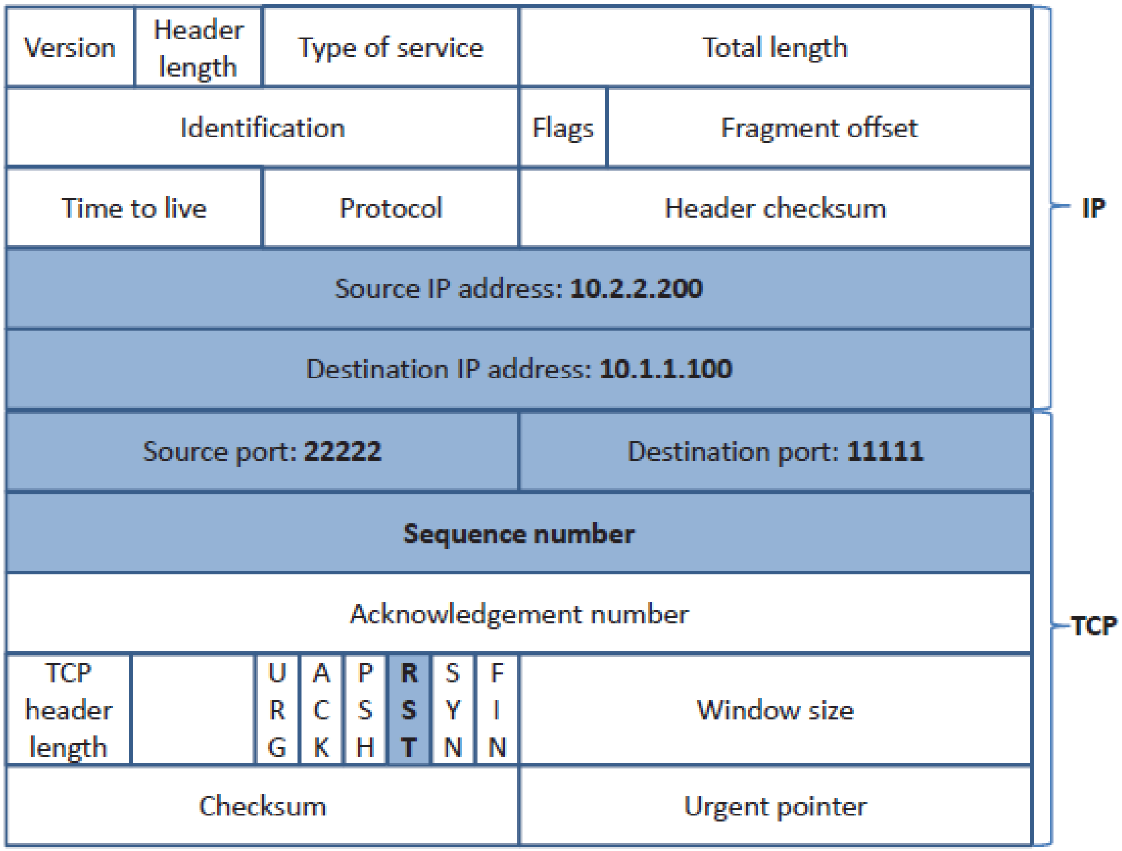


Figure 5: Packet Information

The Source and Destination IP address of the IP header needs to correctly given. The Source and Destination port, Sequence number should be filled out accordingly. And the RST bit needs to be set.

6 Justification

In the figure 1, If A and B can send out an RST packet to each other to break up the connection, an attacker could also send out exactly the same packet on behalf of A or B. The most significant part is the sequence number. If it is filled out correctly, the receiver will obviously accept it and looking at the RST bit on the packet from the same source destination and port, it will terminate the connection. Thus, making our attack successful.