Design of Secure Computer Systems

Lab 03

Telnet & SSH

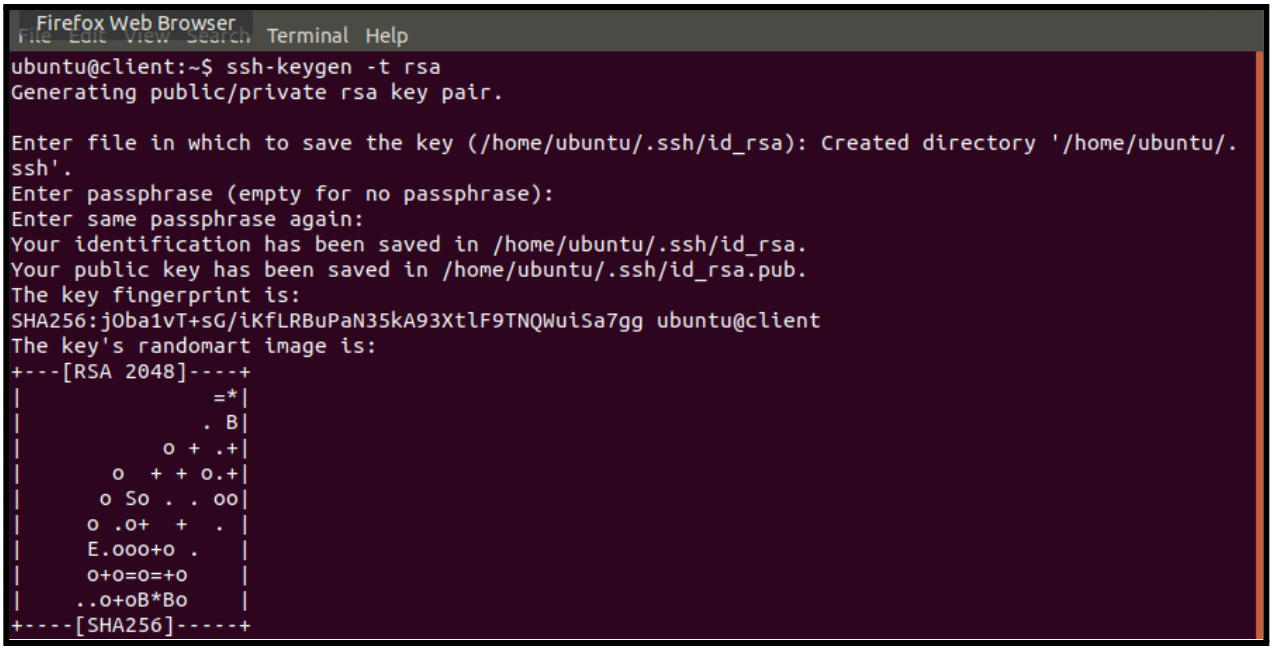
These LABs will focus on Telnet & SSH clients to access resources on a server. These two are simple labs intended to illustrate basic client-server networking and the password issue.

Name: Rakshita Mathur

SSH Lab

1. Generate authentication keys (public/private RSA key pair) on the client computer input:

Command used: **ssh-keygen -t rsa**
This will create a private key and its corresponding public key and place them in your .ssh directory.



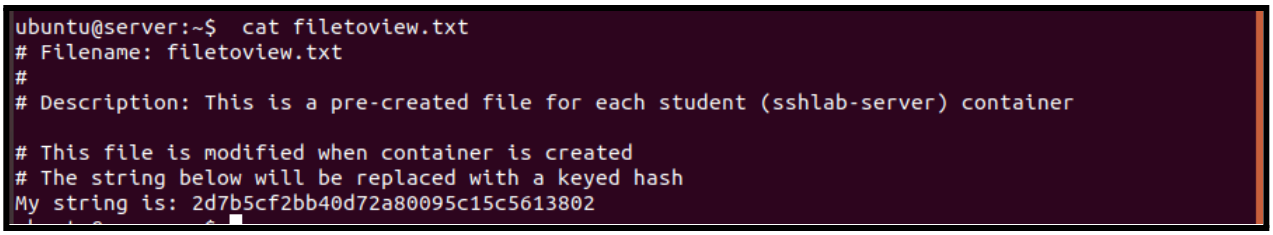
2. Setup SSH on the server for the user to use their authentication keys

The server's IP address is 172.20.0.3. The user is "ubuntu", and the user's password is also "ubuntu".
On the client computer:
- Use this command: **ssh-copy-id -i ~/.ssh/id_rsa.pub 172.20.0.3**
-When prompted to "...continue connecting (yes/no):, type "yes".
- Provided the user password when prompted.

3. Connect using SSH and display a file on the server

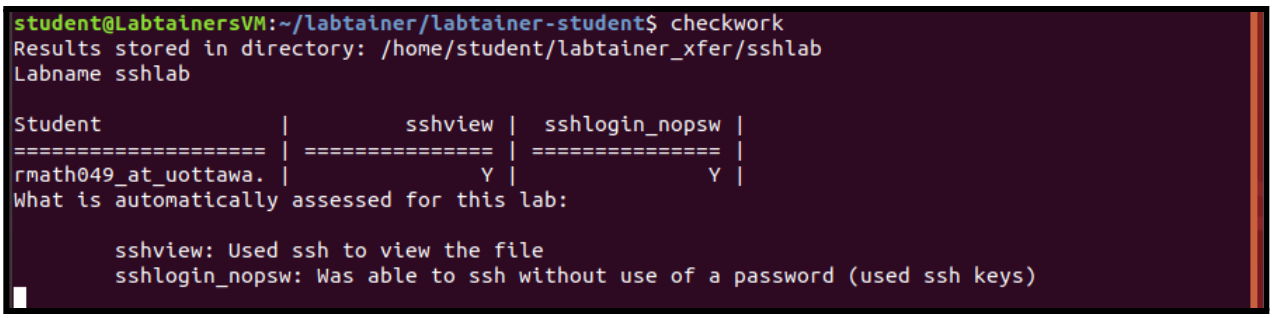
Connecting to the client sever.

Displaying file over a server.



Used the **exit** command to close the connection.

Used the **checkwork** command to check my lab.



Telnet lab

1. Determine the server IP address

Command Used**: ifconfig**
The server IP address will follow the “inet adddr:” label.

```
ubuntu@server:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 02:42:ac:14:00:03
          inet addr:172.20.0.3  Bcast:172.20.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:62 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:7717 (7.7 KB)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

2. Telnet to telnet server and display a file on the server

Using the telnet command to access the server using IP address
Command used: **telnet 172.20.0.3**
Login in using the password and the user login information and then seeing the file using **the cat filetoview.txt** command. Used **exit** command to come out of the connection.

```
ubuntu@client:~$ telnet 172.20.0.3
Trying 172.20.0.3...
Connected to 172.20.0.3.
Escape character is '^]'.
Ubuntu 16.04.4 LTS
server login: ubuntu
Password:
Last login: Sun Oct  3 06:53:52 UTC 2021 from 172.20.0.2 on pts/2
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.15.0-20-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
ubuntu@server:~$ cat filetoview.txt
# Filename: filetoview.txt
#
# Description: This is a pre-created file for each student (telnet-server) container

# This file is modified when container is created
# The string below will be replaced with a keyed hash
My string is: ffb757d8cc95efac3b5538cd727a7c2a
ubuntu@server:~$ exit
logout
Connection closed by foreign host.
ubuntu@client:~$
```

3. View plaintext passwords.

Started tcpdump to display the TCP network traffic.
The command used: **sudo tcpdump -i eth0 -X tcp**

```
ubuntu@server:~$ sudo tcpdump -i eth0 -X tcp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
06:47:32.570763 IP telnetlab.client.student.some_network.59840 > server.telnet: Flags [S], seq 13
71665251, win 29200, options [mss 1460,sackOK,TS val 1758255888 ecr 0,nop,wscale 7], length 0
        0x0000:  4510 003c 7d5e 4000 4006 6520 ac14 0002  E..<}^@.@.e.....
        0x0010:  ac14 0003 e9c0 0017 51c1 f363 0000 0000  ........Q..c....
        0x0020:  a002 7210 585c 0000 0204 05b4 0402 080a  ..r.X\..........
        0x0030:  68cc db10 0000 0000 0103 0307            h...........
06:47:32.570791 IP server.telnet > telnetlab.client.student.some_network.59840: Flags [S.], seq 2
534070588, ack 1371665252, win 28960, options [mss 1460,sackOK,TS val 2572330676 ecr 1758255888,n
op,wscale 7], length 0
        0x0000:  4500 003c 0000 4000 4006 e28e ac14 0003  E..<..@.@.......
        0x0010:  ac14 0002 0017 e9c0 970a d93c 51c1 f364  ...........<Q..d
        0x0020:  a012 7120 585c 0000 0204 05b4 0402 080a  ..q.X\..........
        0x0030:  9952 a6b4 68cc db10 0103 0307            .R..h.......
06:47:32.570817 IP telnetlab.client.student.some_network.59840 > server.telnet: Flags [.], ack 1,
 win 229, options [nop,nop,TS val 1758255888 ecr 2572330676], length 0
        0x0000:  4510 0034 7d5f 4000 4006 6527 ac14 0002  E..4}_@.@.e'....
        0x0010:  ac14 0003 e9c0 0017 51c1 f364 970a d93d  ........Q..d...=
        0x0020:  8010 00e5 5854 0000 0101 080a 68cc db10  ....XT......h...
        0x0030:  9952 a6b4                                .R..
06:47:32.571558 IP telnetlab.client.student.some_network.59840 > server.telnet: Flags [P.], seq 1
:28, ack 1, win 229, options [nop,nop,TS val 1758255889 ecr 2572330676], length 27 [telnet DO SUP
PRESS GO AHEAD, WILL TERMINAL TYPE, WILL NAWS, WILL TSPEED, WILL LFLOW, WILL LINEMODE, WILL NEW-E
NVIRON, DO STATUS, WILL XDISPLOC [|telnet]
        0x0000:  4510 004f 7d60 4000 4006 650b ac14 0002  E..O}`@.@.e.....
        0x0010:  ac14 0003 e9c0 0017 51c1 f364 970a d93d  ........Q..d...=
        0x0020:  8018 00e5 586f 0000 0101 080a 68cc db11  ....Xo......h...
        0x0030:  9952 a6b4 fffd 03ff fb18 fffb 1fff fb20  .R.............
        0x0040:  fffb 21ff fb22 fffb 27ff fd05 fffb 23    ..!.."..'.....#
06:47:32.571570 IP server.telnet > telnetlab.client.student.some_network.59840: Flags [.], ack 28
, win 227, options [nop,nop,TS val 2572330677 ecr 1758255889], length 0
        0x0000:  4500 0034 5700 4000 4006 8b96 ac14 0003  E..4W.@.@.......
        0x0010:  ac14 0002 0017 e9c0 970a d93d 51c1 f37f  ...........=Q...
        0x0020:  8010 00e3 5854 0000 0101 080a 9952 a6b5  ....XT.......R..
        0x0030:  68cc db11                                h...
06:47:32.574410 IP server.telnet > telnetlab.client.student.some_network.59840: Flags [P.], seq 1
:13, ack 28, win 227, options [nop,nop,TS val 2572330680 ecr 1758255889], length 12 [telnet DO TE
RMINAL TYPE, DO TSPEED, DO XDISPLOC, DO NEW-ENVIRON [|telnet]
        0x0000:  4510 0040 5701 4000 4006 8b79 ac14 0003  E..@W.@.@..y....
        0x0010:  ac14 0002 0017 e9c0 970a d93d 51c1 f37f  ...........=Q...
        0x0020:  8018 00e3 5860 0000 0101 080a 9952 a6b8  ....X`.......R..
        0x0030:  68cc db11 fffd 18ff fd20 fffd 23ff fd27  h..........#..'
```

4. Use SSH to protect communications with the server

From the client computer, used the SSH command to access the server using its IP address: **ssh 172.20.0.3**
After authenticating, I viewed the file content by typing: **cat filetoview.txt**

```
ubuntu@client:~$ ssh 172.20.0.3
The authenticity of host '172.20.0.3 (172.20.0.3)' can't be established.
ECDSA key fingerprint is SHA256:nFDnpYXdisAGpF1ZxOBv8Xc83CDp5qYU2frYQvB7Pt8.
Are you sure you want to continue connecting (yes/no)? yes
yes
Warning: Permanently added '172.20.0.3' (ECDSA) to the list of known hosts.
ubuntu@172.20.0.3's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.15.0-20-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Last login: Sun Oct  3 06:43:49 2021 from telnetlab.client.student.some_network
ubuntu@server:~$ cat filetoview.txt
# Filename: filetoview.txt
#
# Description: This is a pre-created file for each student (telnet-server) container

# This file is modified when container is created
# The string below will be replaced with a keyed hash
My string is: ffb757d8cc95efac3b5538cd727a7c2a
ubuntu@server:~$
```

Used the **checkwork** command to check my lab.

```
student@LabtainersVM:~/labtainer/labtainer-student$ checkwork
Results stored in directory: /home/student/labtainer_xfer/telnetlab
Labname telnetlab

Student              |      telnetview |         sshview |    failed_login |
==================== | =============== | =============== | =============== |
rmath049_at_uottawa. |               Y |               Y |               Y |
What is automatically assessed for this lab:
        failed_login: Failed login as expected.
        telnetview: viewed file from telnet
        sshview: viewed file from ssh
```