DIGITAL ASSIGNMENT – 6

Information Security Management (CSE3502)

NAME: AMRITANSHI SAXENA

REG. NO: 18BCE2524

WORKING REMOTELY WITH LINUX SYSTEMS

STEPS-

SSH PROTOCOL-

First of all, you need to install the OpenSSH SSH server on your host. By default, OpenSSH may be installed depending on your distribution, but you will have to make sure that this is the case. First, for safety purposes, make sure to update the packages on your system.

```
amy99@ubuntu:~$ sudo apt-get update
[sudo] password for amy99:
Hit:1 http://us.archive.ubuntu.com/ubuntu focal InRelease
Get:2 http://security.ubuntu.com/ubuntu focal-security InRelease [109 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu focal-backports InRelease [101 kB]
Get:5 http://security.ubuntu.com/ubuntu focal-security/main amd64 Packages [598 kB]
Get:6 http://us.archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [943 kB]
Get:7 http://security.ubuntu.com/ubuntu focal-security/main i386 Packages [215 kB]
Get:8 http://security.ubuntu.com/ubuntu focal-security/main Translation-en [124 kB]
Get:9 http://us.archive.ubuntu.com/ubuntu focal-updates/main i386 Packages [459 kB]
Get:10 http://security.ubuntu.com/ubuntu focal-security/main amd64 DEP-11 Metadata [24.3 kB]
Get:11 http://security.ubuntu.com/ubuntu focal-security/main amd64 c-n-f Metadata [7,436 B]
Get:12 http://security.ubuntu.com/ubuntu focal-security/restricted amd64 Packages [165 kB]
Get:13 http://security.ubuntu.com/ubuntu focal-security/restricted i386 Packages [14.9 kB]
Get:14 http://security.ubuntu.com/ubuntu focal-security/restricted Translation-en [24.4 kB]
Get:15 http://security.ubuntu.com/ubuntu focal-security/restricted amd64 c-n-f Metadata [396 B]
Get:16 http://security.ubuntu.com/ubuntu focal-security/universe i386 Packages [436 kB]
Get:17 http://us.archive.ubuntu.com/ubuntu focal-updates/main Translation-en [216 kB]
Get:18 http://us.archive.ubuntu.com/ubuntu focal-updates/main amd64 DEP-11 Metadata [264 kB]
Get:19 http://us.archive.ubuntu.com/ubuntu focal-updates/main DEP-11 48x48 Icons [55.6 kB]
Get:20 http://us.archive.ubuntu.com/ubuntu focal-updates/main DEP-11 64x64 Icons [87.9 kB]
Get:21 http://us.archive.ubuntu.com/ubuntu focal-updates/main amd64 c-n-f Metadata [13.1 kB]
Get:22 http://us.archive.ubuntu.com/ubuntu focal-updates/restricted i386 Packages [16.2 kB]
Get:23 http://us.archive.ubuntu.com/ubuntu focal-updates/restricted amd64 Packages [204 kB]
Get:24 http://us.archive.ubuntu.com/ubuntu focal-updates/restricted Translation-en [30.4 kB]
Get:25 http://us.archive.ubuntu.com/ubuntu focal-updates/restricted amd64 c-n-f Metadata [440 B]
Get:26 http://security.ubuntu.com/ubuntu focal-security/universe amd64 Packages [551 kB]
Get:27 http://security.ubuntu.com/ubuntu focal-security/universe Translation-en [82.1 kB]
Get:28 http://us.archive.ubuntu.com/ubuntu focal-updates/universe amd64 Packages [759 kB]
Get:29 http://security.ubuntu.com/ubuntu focal-security/universe amd64 DEP-11 Metadata [58.2 kB]
Get:30 http://security.ubuntu.com/ubuntu focal-security/universe amd64 c-n-f Metadata [10.7 kB]
Get:31 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 Packages [14.8 kB]
Get:32 http://security.ubuntu.com/ubuntu focal-security/multiverse i386 Packages [2,536 B]
Get:33 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 c-n-f Metadata [340 B]
Get:34 http://us.archive.ubuntu.com/ubuntu focal-updates/universe i386 Packages [562 kB]
Get:35 http://us.archive.ubuntu.com/ubuntu focal-updates/universe Translation-en [162 kB]
Get:36 http://us.archive.ubuntu.com/ubuntu focal-updates/universe amd64 DEP-11 Metadata [303 kB]
Get:37 http://us.archive.ubuntu.com/ubuntu focal-updates/universe DEP-11 48x48 Icons [200 kB]
Get:38 http://us.archive.ubuntu.com/ubuntu focal-updates/universe DEP-11 64x64 Icons [356 kB]
Get:39 http://us.archive.ubuntu.com/ubuntu focal-updates/universe amd64 c-n-f Metadata [17.0 kB]
Get:40 http://us.archive.ubuntu.com/ubuntu focal-updates/multiverse i386 Packages [6,132 B]
Get:41 http://us.archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 Packages [21.6 kB]
```

```
Get:42 http://us.archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 DEP-11 Metadata [2,468 B]
Get:43 http://us.archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 c-n-f Metadata [600 B]
Get:44 http://us.archive.ubuntu.com/ubuntu focal-backports/universe amd64 DEP-11 Metadata [1,768 B]
Fetched 7,334 kB in 5s (1,566 kB/s)
Reading package lists... Done
amy99@ubuntu:~$ sudo apt-get install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
openssh-server is already the newest version (1:8.2p1-4ubuntu0.2).
0 upgraded, 0 newly installed, 0 to remove and 127 not upgraded.
amy99@ubuntu:~$ sudo apt install ssh
Reading package lists... Done
Building dependency tree
Reading state information... Done
ssh is already the newest version (1:8.2p1-4ubuntu0.2).
0 upgraded, 0 newly installed, 0 to remove and 127 not upgraded.
```

Running those commands, the OpenSSH server will be installed on your computer.

```
amy99@ubuntu:~$ sudo service ssh start
amy99@ubuntu:~$ sudo systemctl status sshd
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2021-04-16 02:03:21 IST; 4min 54s ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 6943 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 6944 (sshd)
      Tasks: 1 (limit: 2280)
     Memory: 2.3M
     CGroup: /system.slice/ssh.service
             └─6944 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Apr 16 02:03:21 ubuntu systemd[1]: Starting OpenBSD Secure Shell server...
Apr 16 02:03:21 ubuntu sshd[6944]: Server listening on 0.0.0.0 port 22.
Apr 16 02:03:21 ubuntu sshd[6944]: Server listening on :: port 22.
Apr 16 02:03:21 ubuntu systemd[1]: Started OpenBSD Secure Shell server.
Apr 16 02:03:37 ubuntu sshd[6948]: Accepted password for amy99 from 192.168.29.170 port 5448 ssh2
Apr 16 02:03:37 ubuntu sshd[6948]: pam_unix(sshd:session): session opened for user amy99 by (uid=0)
```

By default, the SSH server is listening to connections on port 22 as described in the previous sections. In order to verify that this is the case, run the “netstat” command to list open ports.

```
amy99@ubuntu:~$ sudo netstat -tulpn|grep 22
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      6944/sshd: /usr/sbi
tcp6       0      0 :::22                   :::*                    LISTEN      6944/sshd: /usr/sbi
```

Connecting to your SSH server

Now that your SSH server is up and running and that traffic is allowed on port 22, it is time for your client to connect. On your client machine, make sure that you have the SSH utility.

```
┌──(amritanshi㉿kali)-[~]
└─$ ssh -V
OpenSSH_8.4p1 Debian-5, OpenSSL 1.1.1k  25 Mar 2021
```

In order to connect to your SSH server, simply use “ssh” followed by your username and the IP address (or hostname if it is configured) of your SSH server.

```
┌──(amritanshi㉿kali)-[~]
└─$ ssh amy99@192.168.29.137
amy99@192.168.29.137's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.8.0-48-generic x86_64)

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

70 updates can be installed immediately.
36 of these updates are security updates.
To see these additional updates run: apt list --upgradable

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Fri Apr 16 02:03:37 2021 from 192.168.29.170
```

As a consequence, the server identify will be added to your known_hosts file located in the .ssh directory.

```
amy99@ubuntu:~$ cat ~/.ssh/known_hosts
|1|cUJPW0rdKDZoYYsoePNiCEQ9e4o=|5pBO87xWu5yxlBBwxvpr5c86Gq8= ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBGCoCKJ2Orpec6XH2uPVWCdqVqhbtXz85CzobwTajwLVSA90x
Kbp/HTDOM=
|1|YTww1r3WheMTEah5CqcwlLlr9rg=|w7GgqQ/6TE5r02Tel9AtNSsxVjU= ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBDbc2ccC+GmNdVvSuhaaLz/wyqbgFsnCrzjdGuYbFTyLTwLB1
O+PAe9F/A=
|1|epCqEMbckSmAQL4oNOyPmvRLoYo=|gs1triTfYfRUDhvP4xZZe0ZWWOg= ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBDbc2ccC+GmNdVvSuhaaLz/wyqbgFsnCrzjdGuYbFTyLTwLB1
O+PAe9F/A=
```

Executing commands

Now that you are connecting to your SSH server, you can start executing remote tasks on your server.

```
amy99@ubuntu:~$ ls -al
total 92
drwxr-xr-x 17 amy99 amy99 4096 Apr 16 02:03 .
drwxr-xr-x  3 root  root  4096 Apr 10 16:51 ..
-rw-------  1 amy99 amy99 1945 Apr 16 02:06 .bash_history
-rw-r--r--  1 amy99 amy99  220 Apr 10 16:51 .bash_logout
-rw-r--r--  1 amy99 amy99 3771 Apr 10 16:51 .bashrc
drwx------ 13 amy99 amy99 4096 Apr 16 01:54 .cache
drwx------ 12 amy99 amy99 4096 Apr 16 00:02 .config
drwxr-xr-x  2 amy99 amy99 4096 Apr 10 17:06 Desktop
drwxr-xr-x  2 amy99 amy99 4096 Apr 10 17:06 Documents
drwxr-xr-x  2 amy99 amy99 4096 Apr 10 17:06 Downloads
drwx------  3 amy99 amy99 4096 Apr 10 17:06 .gnupg
drwxr-xr-x  3 amy99 amy99 4096 Apr 10 17:05 .local
drwx------  5 amy99 amy99 4096 Apr 10 17:12 .mozilla
drwxr-xr-x  2 amy99 amy99 4096 Apr 10 17:06 Music
-rw-r--r--  1 amy99 amy99  306 Apr 10 17:24 .pam_environment
drwxr-xr-x  2 amy99 amy99 4096 Apr 10 17:06 Pictures
-rw-r--r--  1 amy99 amy99  807 Apr 10 16:51 .profile
drwxr-xr-x  2 amy99 amy99 4096 Apr 10 17:06 Public
drwxr-xr-x  3 amy99 amy99 4096 Apr 10 17:07 snap
drwx------  2 amy99 amy99 4096 Apr 15 19:00 .ssh
-rw-r--r--  1 amy99 amy99    0 Apr 10 17:07 .sudo_as_admin_successful
drwxr-xr-x  2 amy99 amy99 4096 Apr 10 17:06 Templates
drwxr-xr-x  2 amy99 amy99 4096 Apr 10 17:06 Videos
-rw-------  1 amy99 amy99  156 Apr 16 02:03 .Xauthority
```

Your commands are not executed on your local machine but they are executed on the remote machine. To verify it, run a command that is simply sleeping for an extended period of time on the client.

```
amy99@ubuntu:~$ sleep 100
^Z
[1]+  Stopped                 sleep 100
```

Back on the server, you can actually verify that the command is actually running on the server.

```
amy99@ubuntu:~$ ps aux | grep sleep
amy99       7842  0.0  0.0  16716   524 pts/1    S+   02:12   0:00 sleep 100
amy99       7844  0.0  0.0  17676   656 pts/0    S+   02:13   0:00 grep --color=auto sleep
```

But what if you wanted to execute a graphical application, like Firefox for example?

```
amy99@ubuntu:~$ firefox
Error: no DISPLAY environment variable specified
```

In order to know where the graphical interface needs to be drawn, your session has a DISPLAY environment variable that details the output device.

```
amy99@ubuntu:~$ echo $DISPLAY
:0
```

The xrandr command can be used in order to see screens connected to a Linux system.

```
:0
amy99@ubuntu:~$ xrandr --query
Screen 0: minimum 1 x 1, current 1718 x 851, maximum 16384 x 16384
Virtual1 connected primary 1718x851+0+0 (normal left inverted right x axis y axis) 0mm x 0mm
   1718x851      60.00*+
   2560x1600     59.99
   1920x1440     60.00
   1856x1392     60.00
   1792x1344     60.00
   1920x1200     59.88
   1600x1200     60.00
   1680x1050     59.95
   1400x1050     59.98
   1280x1024     60.02
   1440x900      59.89
   1280x960      60.00
   1360x768      60.02
   1280x800      59.81
   1152x864      75.00
   1280x768      59.87
   1024x768      60.00
   800x600       60.32
   640x480       59.94
Virtual2 disconnected (normal left inverted right x axis y axis)
Virtual3 disconnected (normal left inverted right x axis y axis)
Virtual4 disconnected (normal left inverted right x axis y axis)
Virtual5 disconnected (normal left inverted right x axis y axis)
Virtual6 disconnected (normal left inverted right x axis y axis)
Virtual7 disconnected (normal left inverted right x axis y axis)
Virtual8 disconnected (normal left inverted right x axis y axis)
```

When using the SSH client, you can append the “-x” option in order to redirect X11 traffic to your local machine. As a consequence, the application will run on the server but it will be displayed on your client.

```
amy99@ubuntu:~$ ssh amy99@192.168.29.137 -X
amy99@192.168.29.137's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.8.0-48-generic x86_64)

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

70 updates can be installed immediately.
36 of these updates are security updates.
To see these additional updates run: apt list --upgradable

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Fri Apr 16 02:22:02 2021 from 192.168.29.137
amy99@ubuntu:~$ echo $DISPLAY
localhost:10.0
```

In this case, the device number is not actually connected to a real piece of hardware on the server but it is mapped to a remote connection on the server. To illustrate that, try listing the open connections on your server starting with 60.

```
amy99@ubuntu:~$ netstat -tulpn | grep 60
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
tcp        0      0 127.0.0.1:6010          0.0.0.0:*               LISTEN      -
tcp6       0      0 ::1:6010                :::*                    LISTEN      -
```

On the client, while being connected to a SSH session, try running Firefox.