# Indian Institute of Technology Jodhpur

CSL6010 – Cyber Security
LAB 4 Report

**Name- Aman Srivastava**
**Roll No.- B20CS100**

Date-5th Mar 2023

## 1) Establishing a secure connection between two machines

To connect two machines, we can utilize the "ssh" command, which requires the username and IP address of the remote machine. However, in this scenario, both the client and server are on the same laptop, so we will use the local username and IP address. It's possible that the password of the remote machine will be prompted for entry. Once entered, the SSH connection will be established, allowing us to execute commands on the remote machine as if we were physically present.

```
aman@linux:~$ ssh aman@192.168.137.64
The authenticity of host '192.168.137.64 (192.168.137.64)' can't be established.
ECDSA key fingerprint is SHA256:bfLpIGwusSw+GZWhSlTFLVxwWxE+MnM3XdgpLF9stWM.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.137.64' (ECDSA) to the list of known hosts.
aman@192.168.137.64's password:
Welcome to Zorin OS 16.1 (GNU/Linux 5.15.0-48-generic x86_64)

 * Website:     https://zorin.com
 * Help:        https://help.zorin.com

200 updates can be applied immediately.
112 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.

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

Zorin OS comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

---

To ensure a secure connection, we can use a technique called key generation. To begin, we must enter "**ssh-keygen -t rsa**" into the terminal, which will prompt us to choose a file name and create a passphrase for encrypting the private key file. Next, we can enter "**ssh-copy-id username@hostname**" in the terminal, which will copy the public key and add it to the authorized key file we have created. To establish a secure SSH connection, we must enter "**ssh -i ~/.ssh/id_rsa username@hostname**" and provide the passphrase for the private key. This will establish a secure connection. A screenshot has been provided to demonstrate the process.

```
Your identification has been saved in key
Your public key has been saved in key.pub
The key fingerprint is:
SHA256:qOuHr5dOHeSLvycLEF3A7uNH7O66A7MzEsy0RnOhFS8 aman@linux
The key's randomart image is:
+---[RSA 3072]----+
|     .o...       |
|     oo..        |
|    oEoo .       |
|   = .o.+        |
|  = +....S       |
|   * oooooo      |
|  . ..*+=o       |
|   . =o*o+ .     |
|    o+O=B*=      |
+----[SHA256]-----+
```

```
aman@linux:~$ ssh-copy-id aman@192.168.137.64
```

**Allow remote administration of the server.**

```
aman@linux:~$ sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /lib/systemd/s
ystemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable ssh
```

**Use to transfer files.**

To transfer a file from a local machine to a remote machine via the terminal, we can use the "scp" command. First, we need to open the terminal and enter the command **"scp /path/to/local/file username@IP address:/path/to/remote/directory".** We should replace "/path/to/local/file" with the path of the file to be transferred and "username" with the username on the remote machine. Additionally, we should replace **"/path/to/remote/directory**" with the directory's path on the remote machine where we want the file to be transferred. In this scenario, the server and client are on the same machine, and the goal is to transfer a file called **"trial.txt"** from the "Documents" directory to the "Desktop" directory.

```
aman@linux:~$ scp /home/aman/Desktop/TXT.txt aman@192.168.137.64:/home/aman/doc
ument
aman@192.168.137.64's password:
TXT.txt                                       100%    0     0.0KB/s   00:00
```

**2) List the files in the directory**

To view the files within a directory, we can use the command **"ls /path/to/remote/directory".** Once we have established an SSH

connection, we can use this command to check the files in the remote "Desktop" directory.

```
aman@linux:~$ ls Desktop
TXT.txt
```

Occasionally, an error may arise, indicating that permission has been denied. To address this issue, we can grant full disk access via Remote Access or check individual permissions by going to Settings, selecting Sharing, choosing Remote Management, and selecting Options. From there, we can choose the appropriate options to resolve the problem.

### 3) To list the text files only

After establishing an SSH connection and navigating to a specific directory using the "cd" command, we can use the command "**ls -l *.txt**" to list only the text files within that directory. In this scenario, the goal was to check for text files in the "Desktop" directory.

```
aman@linux:~/Desktop$ ls -l *.txt
-rw-r--r-- 1 aman aman 0 Mar  5 23:08 TXT.txt
```

### 4) To list the name of the files that contain the string “it” in their name

Assuming that the user has already navigated to the "Desktop" directory using the **"cd Desktop"** command, they can use the command **"find . -name "it.txt" -print"** to retrieve a list of directories that contain the string "it" in their name. Specifically, this command searches for all files with names containing the string "it" and the ".txt" extension within the current directory and its subdirectories and prints their names.

```
aman@linux:~/Desktop$ ls it
ls: cannot access 'it': No such file or directory
```

### 5) To copy style.txt from one directory to another

To copy a file from one directory to another, we can use the "scp" command followed by the name of the file and the destination directory's path. In this scenario, the file **"style.txt"** was initially located in the "Documents" directory and needed to be copied to the "Desktop" directory. To achieve this, we can use the command **"scp style.txt /path/to/otherdirectory/"**, replacing **"/path/to/otherdirectory"** with the path of the destination directory where we want to copy the file.

```
aman@linux:~/Documents$ scp style.txt /home/aman/Desktop
```

### 6) Copying all the text files

To copy all text files from one directory to another, we can use the "scp" command followed by the wildcard symbol (*) and the destination directory's path. In this example, the user wanted to copy all text files from the "Documents" directory to the "Downloads" directory. To achieve this, we can use the command **"scp *.txt /path/to/otherdirectory**/", replacing **"/path/to/otherdirectory"** with the path of the destination directory where we want to copy the files.

```
aman@linux:~/Documents$ cp /home/aman/Documents/*.txt /home/aman/Desktop
```

7) **Copying all .txt files from the first directory and .dat files from the second directory**

Similar to the previous question, we can copy files from multiple directories using the "scp" command. This time, we need to include both the file type and the directory path in the command.

The format for the command is **"scp /path/to/firstdirectory/.txt /path/to/seconddirectory/.dat /path/to/thirddirectory/"**. This command copies all .txt files from the first directory and all .dat files from the second directory to the third directory. In this specific case, the user copied all .txt files from the "Documents" directory and all .dat files from the "Desktop" directory to the "Downloads" directory.

```
aman@linux:~/Documents$ cp /home/aman/Document/*.txt /home/aman/Desktop/*.dat /home/aman/Downloads
```