

Institute of Computer Technology
B. Tech Computer Science and Engineering
Subject: BOSS (2CSE204)
PRACTICAL-8

AIM: - To learn about configuring and securing SSH in linux.

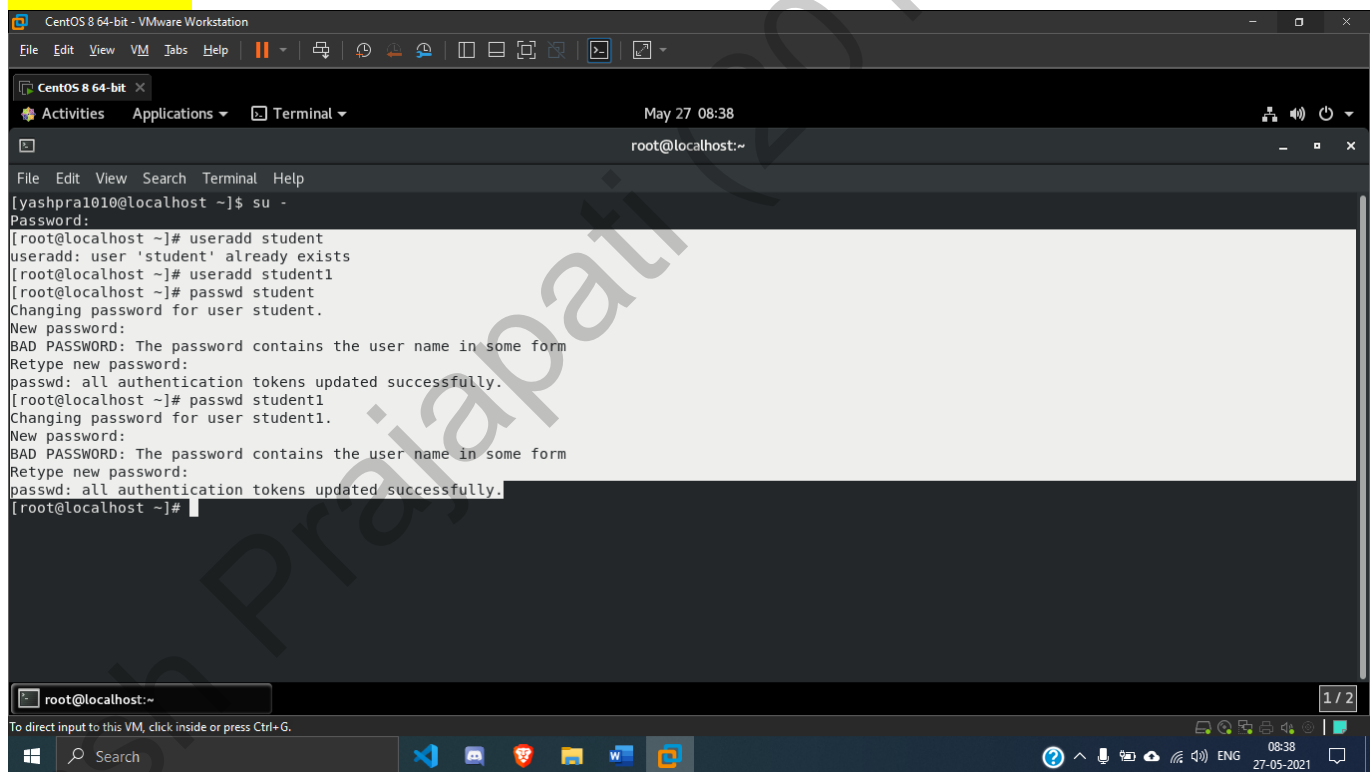
Commands:

- **ssh user@remotehost** – This command is used to create remote connections on remote users.
- **ssh-keygen** – To create public keygen of localhost.
- **ssh-copy-id** – To share public keygen to remote user.

Exercise:

1. Create two users student and student1. Set their passwords "student123".

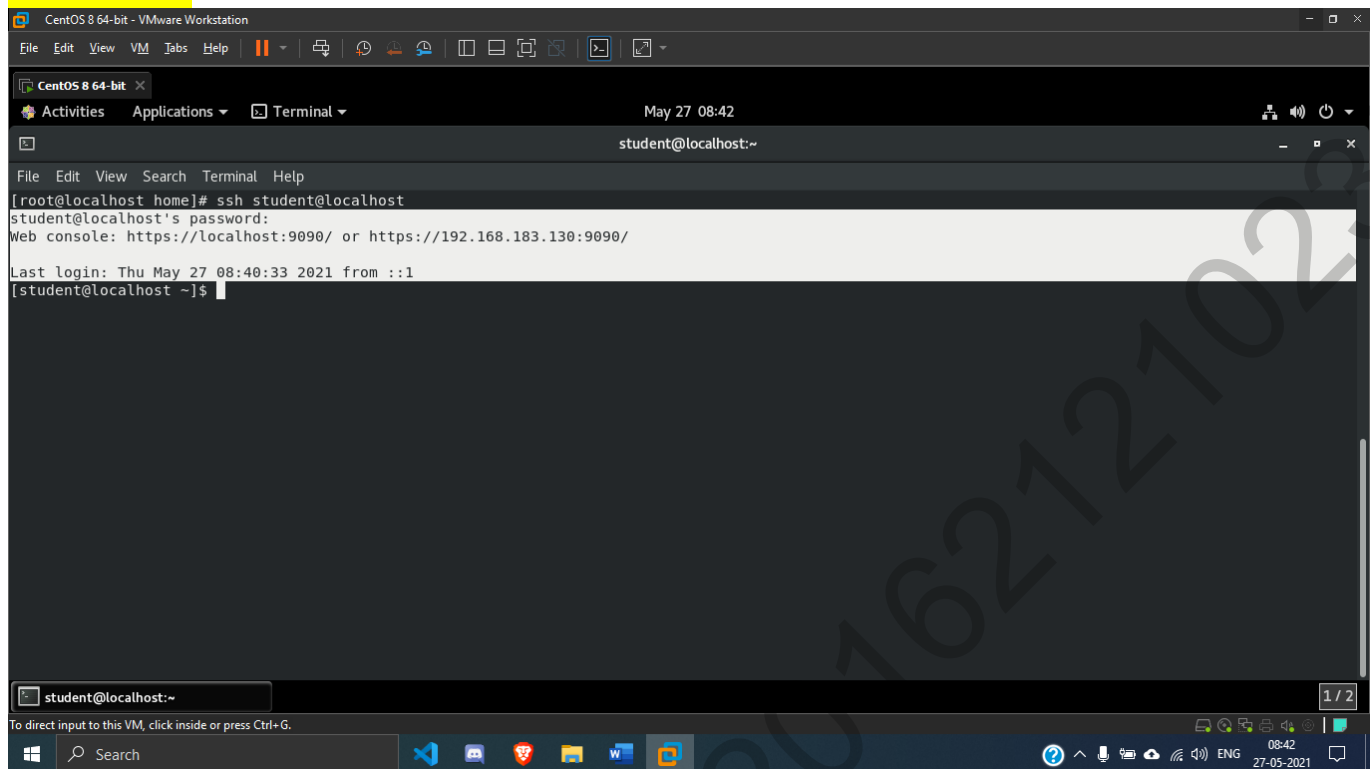
SOLUTION



```
CentOS 8 64-bit - VMware Workstation
File Edit View VM Tabs Help
CentOS 8 64-bit x
Activities Applications Terminal May 27 08:38
root@localhost:~
File Edit View Search Terminal Help
[yashpra1010@localhost ~]$ su -
Password:
[root@localhost ~]# useradd student
useradd: user 'student' already exists
[root@localhost ~]# useradd student1
[root@localhost ~]# passwd student
Changing password for user student.
New password:
BAD PASSWORD: The password contains the user name in some form
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost ~]# passwd student1
Changing password for user student1.
New password:
BAD PASSWORD: The password contains the user name in some form
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost ~]#
```

2. Open an SSH session to localhost as student.

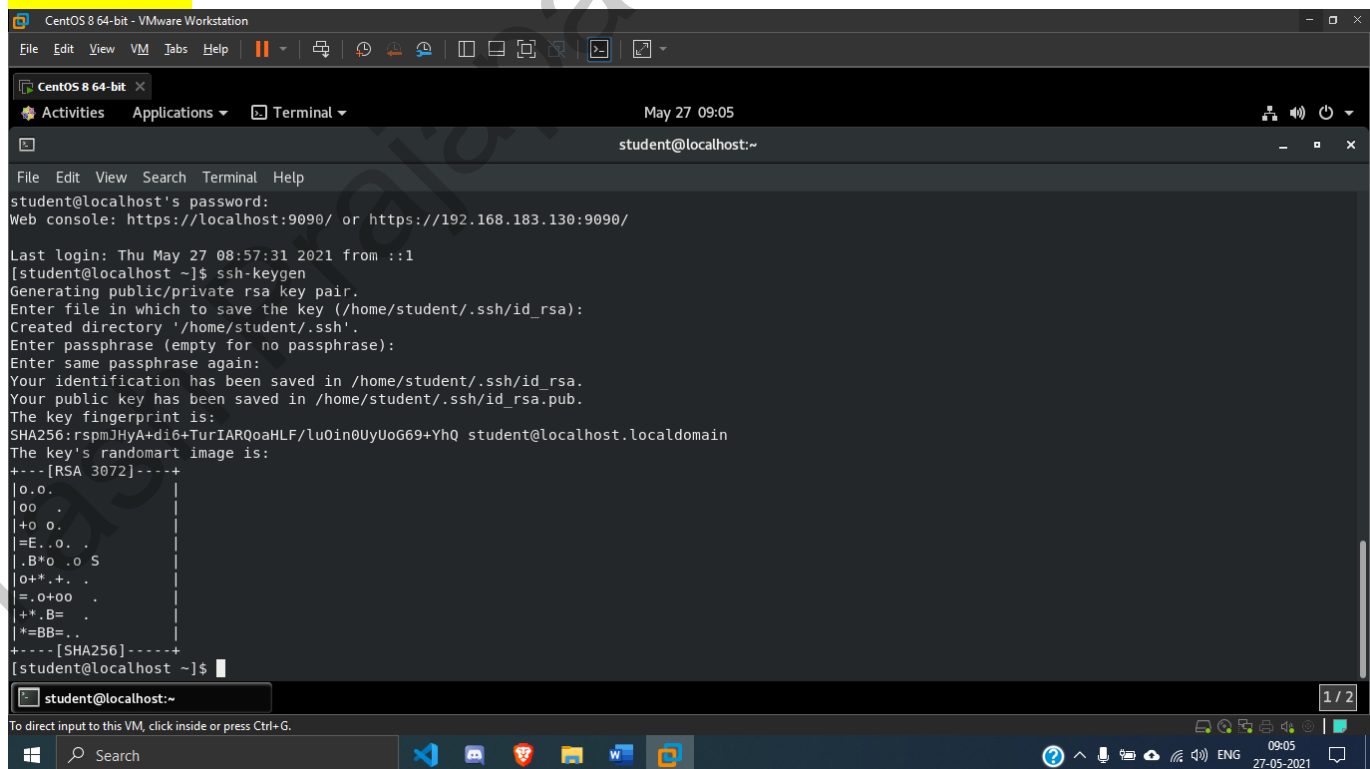
SOLUTION



```
CentOS 8 64-bit - VMware Workstation
File Edit View VM Tabs Help
CentOS 8 64-bit x
Activities Applications Terminal May 27 08:42
student@localhost:~
File Edit View Search Terminal Help
[root@localhost home]# ssh student@localhost
student@localhost's password:
Web console: https://localhost:9090/ or https://192.168.183.130:9090/
Last login: Thu May 27 08:40:33 2021 from ::1
[student@localhost ~]$
```

3. Use the ssh-keygen command to generate SSH keys for student on localhost.

SOLUTION



```
CentOS 8 64-bit - VMware Workstation
File Edit View VM Tabs Help
CentOS 8 64-bit x
Activities Applications Terminal May 27 09:05
student@localhost:~
File Edit View Search Terminal Help
student@localhost's password:
Web console: https://localhost:9090/ or https://192.168.183.130:9090/
Last login: Thu May 27 08:57:31 2021 from ::1
[student@localhost ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/student/.ssh/id_rsa):
Created directory '/home/student/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/student/.ssh/id_rsa.
Your public key has been saved in /home/student/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:rspmJHyA+di6+TurIARQoaHLf/Lu0in0UyUoG69+YhQ student@localhost.localdomain
The key's randomart image is:
+---[RSA 3072]-----+
|o.o. |
|oo . |
|+o o. |
|=E.o. . |
|.B*o .o S |
|O+*.+. . |
|=..O+oo . |
|+..B= . |
|*=BB=.. |
+---[SHA256]-----+
[student@localhost ~]$
```

4. Use the ssh-copy-id command to send the public key of the SSH key pair to student1 on localhost.

SOLUTION

```

CentOS 8 64-bit - VMware Workstation
File Edit View VM Tabs Help
CentOS 8 64-bit
Activities Applications Terminal
May 27 09:10
student@localhost:~

File Edit View Search Terminal Help
The key's randomart image is:
+---[RSA 3072]-----+
|o.o.
|oo
|+o o.
|=E..o.
|.B*o .o S
|O+*.+.
|=..o+oo
|+..B=
|*=BB=..
+---[SHA256]-----+
[student@localhost ~]$ ssh-copy-id student1@localhost
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/student/.ssh/id_rsa.pub"
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is SHA256:rEd9RHg9/UH0thBayLZhWpkstmfAtDelHvngPPDyE.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
student1@localhost's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'student1@localhost'"
and check to make sure that only the key(s) you wanted were added.

[student@localhost ~]$
student@localhost:~

```

5. Confirm that student can successfully log in to student1 using the SSH keys.

SOLUTION

```

CentOS 8 64-bit - VMware Workstation
File Edit View VM Tabs Help
CentOS 8 64-bit
Activities Applications Terminal
May 27 09:14
student1@localhost:~

File Edit View Search Terminal Help
|oo
|+o o.
|=E..o.
|.B*o .o S
|O+*.+.
|=..o+oo
|+..B=
|*=BB=..
+---[SHA256]-----+
[student@localhost ~]$ ssh-copy-id student1@localhost
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/student/.ssh/id_rsa.pub"
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is SHA256:rEd9RHg9/UH0thBayLZhWpkstmfAtDelHvngPPDyE.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
student1@localhost's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'student1@localhost'"
and check to make sure that only the key(s) you wanted were added.

[student@localhost ~]$ ssh student1@localhost
Web console: https://localhost:9090/ or https://192.168.183.130:9090/

[student1@localhost ~]$
student1@localhost:~

```