

Ganpat University
Faculty of Engineering & Technology
Computer Science & Engineering
(2CSE204) Basics of Operating System and Shell Scripting

Name:- Dwij Vatsal Desai

Sem:- 2

Sub: - BOSS

Enrollment No.:- 23162121027

Prac:- 9

Date:- 14/4/2024

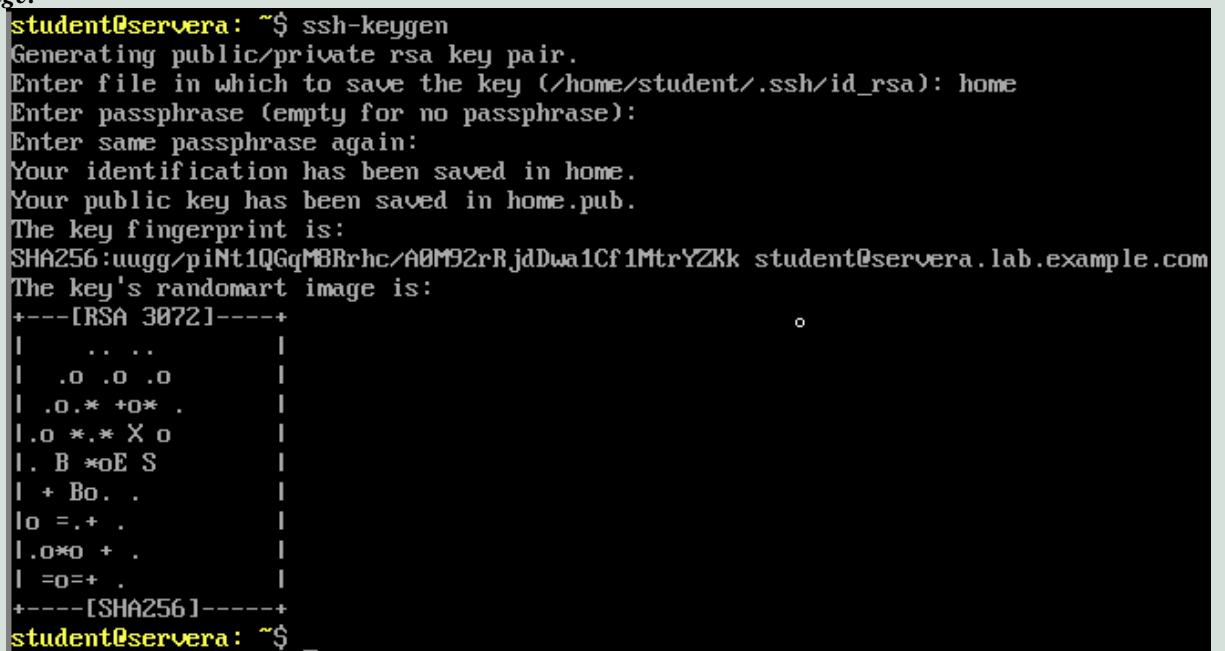
Practical 9

1. Configure one machine (servera) in such a way that if the public key of a remote user is modified then login is restricted.

Command:-

In servera:-
ssh-keygen (Phase: dwij)

Image:-



```
student@servera: ~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/student/.ssh/id_rsa): home
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in home.
Your public key has been saved in home.pub.
The key fingerprint is:
SHA256:uugg/piNt1QGqM8RrhC/A0M92rRjdDwa1Cf1MtrYZKk student@servera.lab.example.com
The key's randomart image is:
+---[RSA 3072]-----+
|      .. ..      |
|    .o .o .o    |
|  .o.* +o* .    |
|.o *.* X o     |
|. B *oE S      |
| + Bo. .       |
|o =.+ .        |
|.o*o + .       |
| =o=+ .        |
+---[SHA256]-----+
student@servera: ~$ _
```

Now in serverb:-

```
student@serverb: ~$ systemctl reload sshd
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to reload 'sshd.service'.
Authenticating as: Student User (student)
Password:
==== AUTHENTICATION COMPLETE ====
^[[student@serverb: ~$
```

```
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication yes
#PermitEmptyPasswords no
PasswordAuthentication no

# Change to no to disable s/key passwords
#ChallengeResponseAuthentication yes
ChallengeResponseAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
```

```
#MaxAuthTries 6
#MaxSessions 10

PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile /etc/.rht_authorized_keys .ssh/authorized_keys

#AuthorizedPrincipalsFile none
```

2. Enable password-less authentication for the user to access remote server.

Command:-

In servera:-

- i. ssh-keygen
- ii. ssh-copy-id student@serverb
- iii. ssh student@serverb

Image:-

```
student@servera: ~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/student/.ssh/id_rsa):
/home/student/.ssh/id_rsa already exists.
Overwrite (y/n)? y
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:Sk6ldikHBURrsNWYbgh65iBBcuUDlLr01TBWJISRAc student@servera.lab.example.com
The key's randomart image is:
+---[RSA 3072]-----+
| .*Eo+*0+. |
| |=0++=0.o |
| |*00+=0+ . |
| 00.B. + . |
| |+= o * $ |
| 0 .. = = |
|   o |
|   | |
|   | |
+---[SHA256]-----+
student@servera: ~$
student@servera: ~$ ssh-copy-id student@serverb
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/student/.ssh/id_rsa.pub"
/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
student@serverb's password:

Number of key(s) added: 1

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

student@servera: ~$ ssh student@serverb
Activate the web console with: systemctl enable --now cockpit.socket

This system is not registered to Red Hat Insights. See https://cloud.redhat.com/
To register this system, run: insights-client --register

Last failed login: Sun Apr 14 09:18:07 EDT 2024 from 172.25.250.10 on ssh:notty
There were 4 failed login attempts since the last successful login.
Last login: Sun Apr 14 09:16:38 2024 from 172.25.250.10
[student@serverb ~]$
```

3. On serverb, restrict root login to any system.

Command:-

In servera:-

```
ssh root@serverb
```

In serverb:-

```
nano /etc/ssh/sshd_config
```

```
systemctl reload sshd
```

PermitRootLogin no (edit this in known_hosts)

Image:-

```
student@servera: ~$ ssh root@serverb
root@serverb's password:
Activate the web console with: systemctl enable --now cockpit.socket

This system is not registered to Red Hat Insights. See https://cloud.redhat.com/
To register this system, run: insights-client --register

Last login: Thu Mar 28 00:25:26 2024 from 172.25.250.10
[root@serverb ~]#
```

Now in serverb:-

```
# Logging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no_
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

# PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile /etc/.rht_authorized_keys .ssh/authorized_keys
```

```
student@serverb: ~/.ssh$ systemctl reload sshd
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to reload 'sshd.service'.
Authenticating as: Student User (student)
Password:
==== AUTHENTICATION COMPLETE ====
student@serverb: ~/.ssh$
```