Ganpat University
(2CSE204) Basics of Operating System and Shell Scripting

Name: Jaymin Gondaliya

Enrollment No: 23162171007

Sem - 2

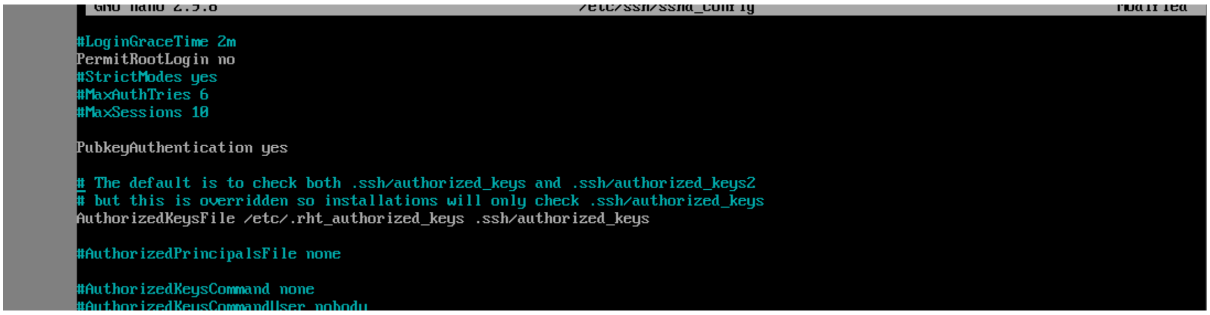
Branch: CS

Class: B

Batch: 25

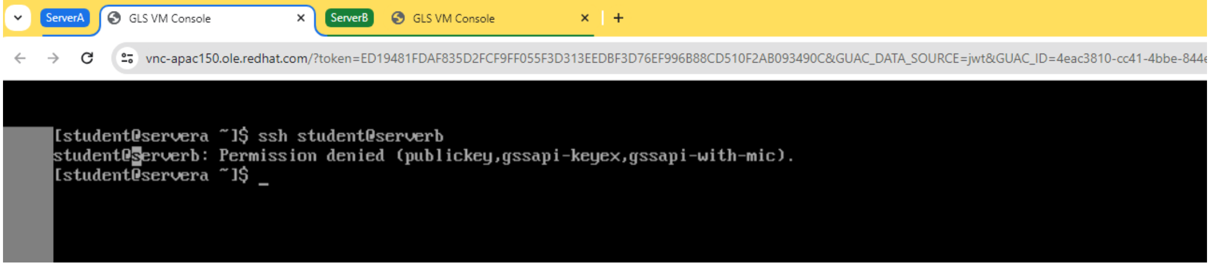
Practical-9

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 – serverb - sudo /etc/ssh/sshd_config (change pubkeyauthentication to yes)



```
  GNU nano 2.9.8                  /etc/ssh/sshd_config                  Modified
#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

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody
```

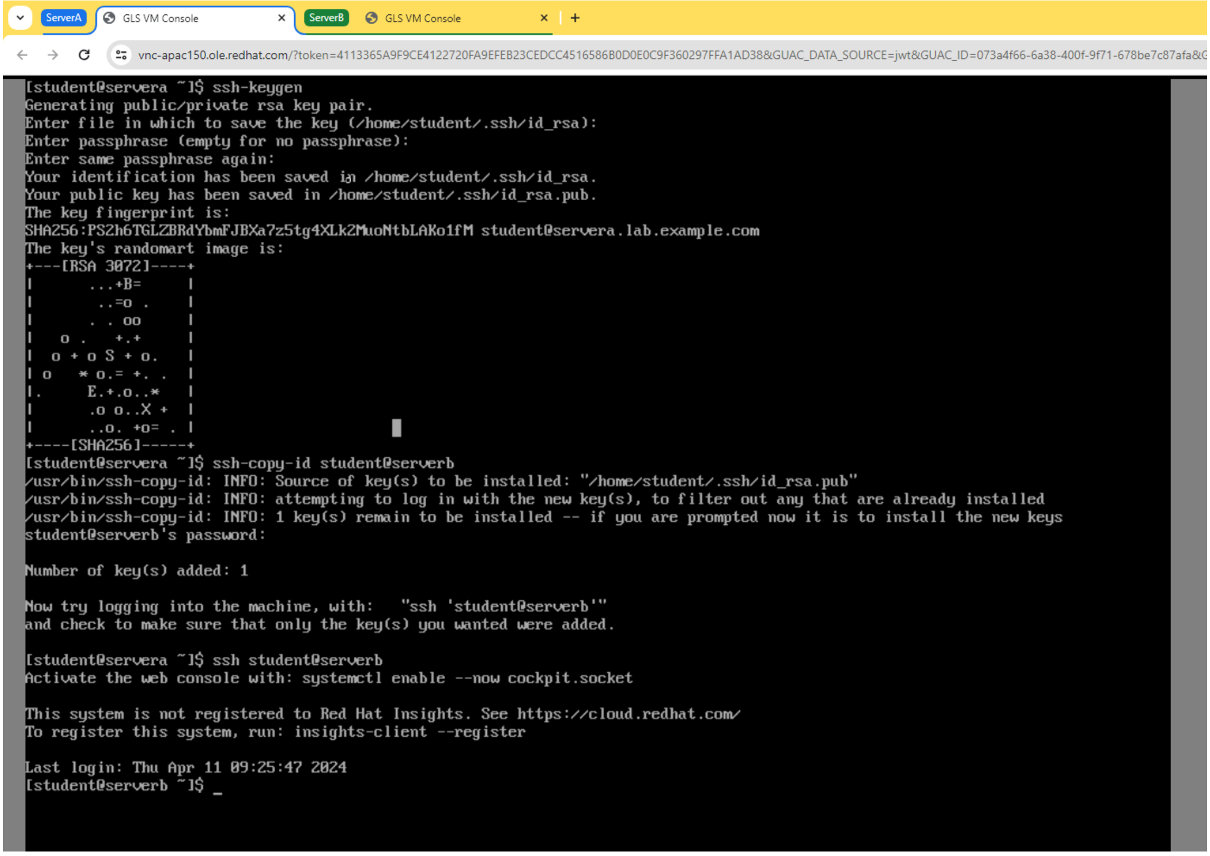
try logged in to serverb – ssh student@serverb



ServerA
GLS VM Console
ServerB
GLS VM Console
vnc-apac150.ole.redhat.com/?token=ED19481FDAF835D2FCF9FF055F3D313EEDBF3D76EF996B88CD510F2AB093490C&GUAC_DATA_SOURCE=jwt&GUAC_ID=4eac3810-cc41-4bbe-844

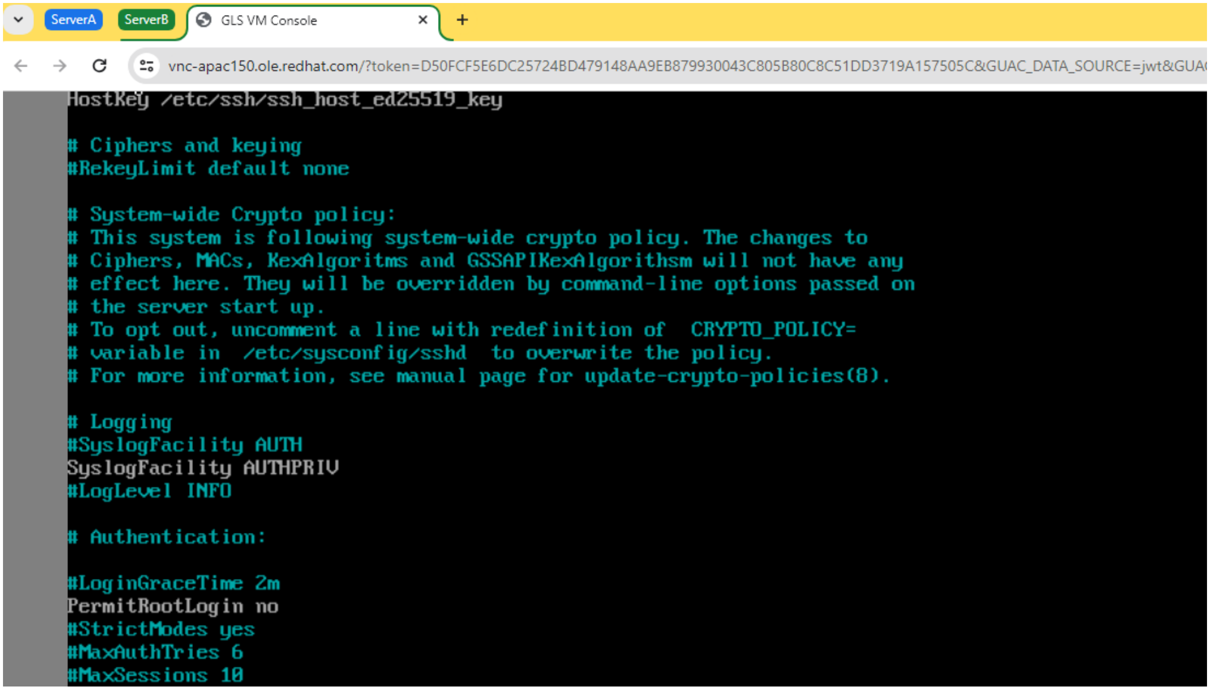
```
[student@servera ~]$ ssh student@serverb
student@serverb: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
[student@servera ~]$ _
```

2. Enable password-less authentication for the user to access remote server.
   Command- ssh-keygen (generate key) , ssh-copy-id student@serverb , ssh student@serverb (logged In without password)

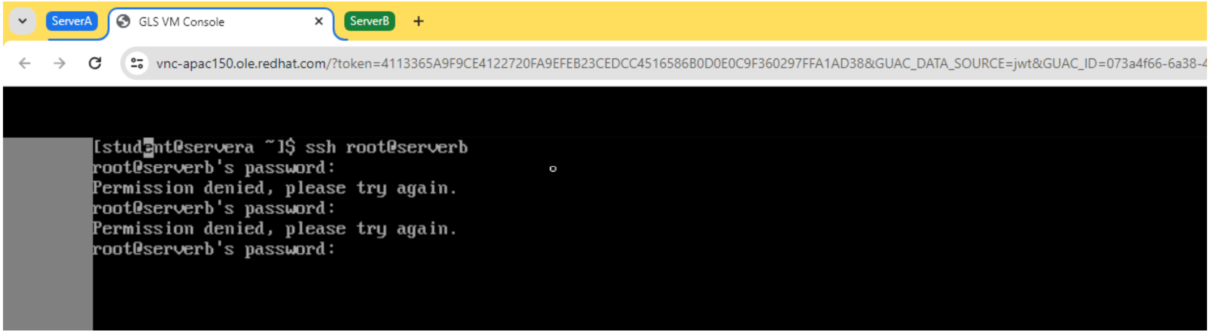

ServerA
GLS VM Console
ServerB
GLS VM Console
vnc-apac150.ole.redhat.com/?token=4113365A9F9CE4122720FA9EFEB23CEDCC4516586B0D0E0C9F360297FFA1AD38&GUAC_DATA_SOURCE=jwt&GUAC_ID=073a4f66-6a38-400f-9f71-678be7c87afa&G

```
[student@servera ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/student/.ssh/id_rsa):
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:PS2h6TGLZBRdYbmFJBXa7z5tg4XLk2MuoNtbLAKo1fM student@servera.lab.example.com
The key's randomart image is:
+---[RSA 3072]----+
|       ...+B=    |
|        ..=o .   |
|       . . oo    |
|   o .   +.+     |
|  o + o S + o.   |
| o   * o.= +. .  |
|.      E.+.o..*  |
|       .o o..X + |
|       ..o. +o= .|
+----[SHA256]-----+
[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 login: Thu Apr 11 09:25:47 2024
[student@serverb ~]$ _
```

3. On serverb, restrict root login to any system.
   Command – logged in serverb as a root user and change PermitRootLogin to No (nano /etc/ssh/sshd_config) , systemctl restart sshd


ServerA
ServerB
GLS VM Console
vnc-apac150.ole.redhat.com/?token=D50FCF5E6DC25724BD479148AA9EB879930043C805B80C8C51DD3719A157505C&GUAC_DATA_SOURCE=jwt&GUA

```
HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# System-wide Crypto policy:
# This system is following system-wide crypto policy. The changes to
# Ciphers, MACs, KexAlgoritms and GSSAPIKexAlgorithsm will not have any
# effect here. They will be overridden by command-line options passed on
# the server start up.
# To opt out, uncomment a line with redefinition of  CRYPTO_POLICY=
# variable in  /etc/sysconfig/sshd  to overwrite the policy.
# For more information, see manual page for update-crypto-policies(8).

# Logging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```


ServerA
GLS VM Console
ServerB
vnc-apac150.ole.redhat.com/?token=4113365A9F9CE4122720FA9EFEB23CEDCC4516586B0D0E0C9F360297FFA1AD38&GUAC_DATA_SOURCE=jwt&GUAC_ID=073a4f66-6a38-4

```
[student@servera ~]$ ssh root@serverb
root@serverb's password:
Permission denied, please try again.
root@serverb's password:
Permission denied, please try again.
root@serverb's password:
```