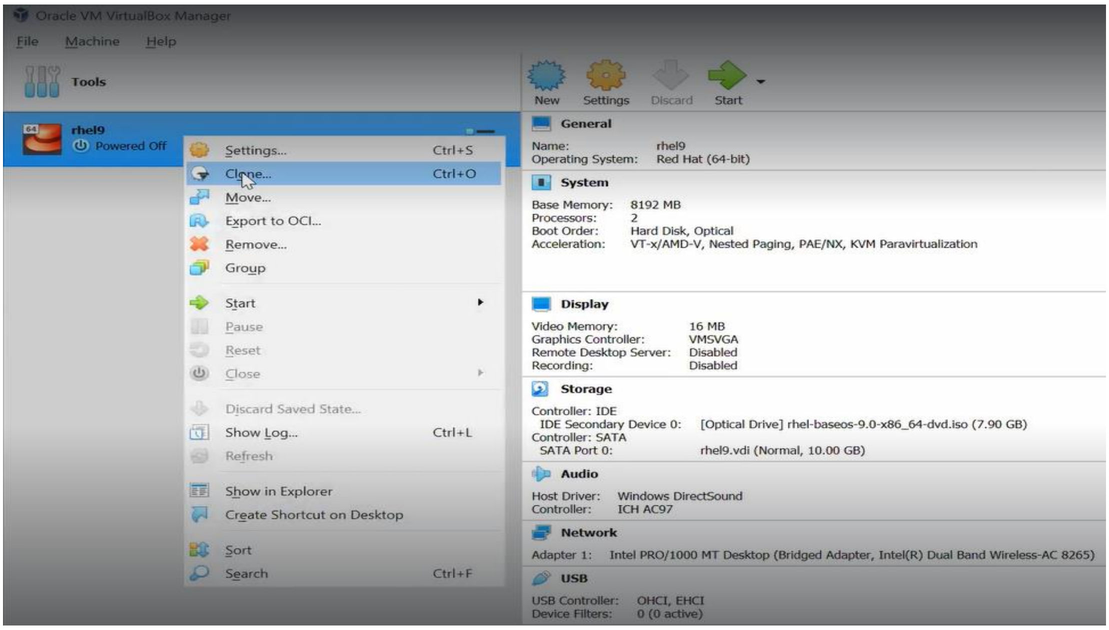
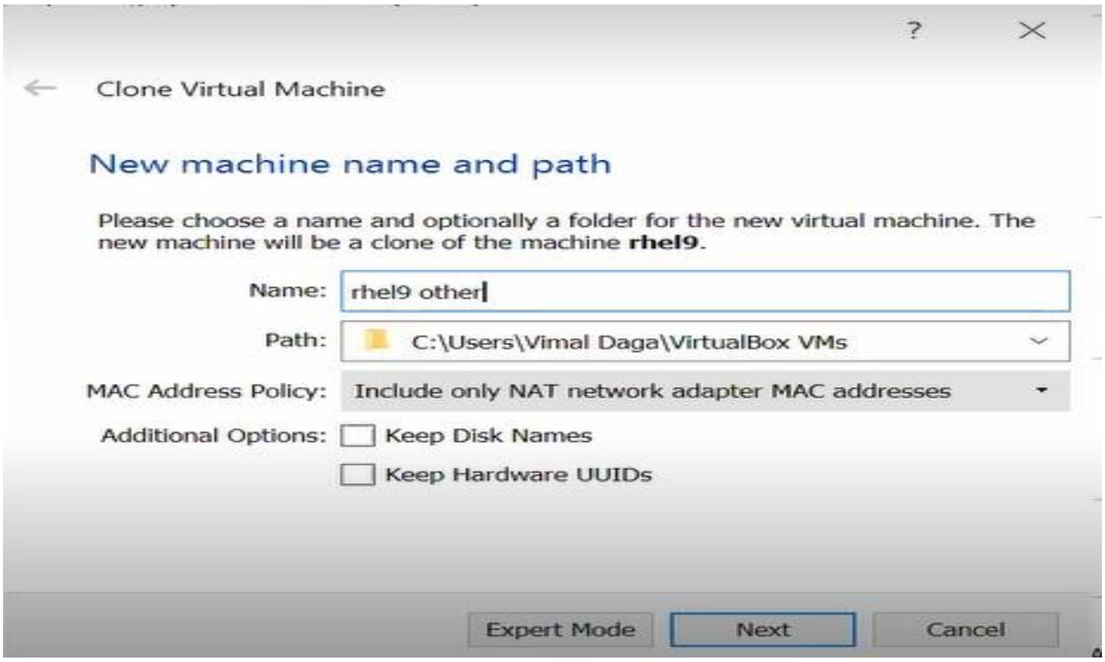
RHEL9

Session 6 – 30th October 2022 Summary

- To create a clone of a Virtual Machine- Right Click →Clone



```
General
Name:               rhel9
Operating System:   Red Hat (64-bit)

System
Base Memory:   8192 MB
Processors:    2
Boot Order:    Hard Disk, Optical
Acceleration:  VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization

Display
Video Memory:            16 MB
Graphics Controller:     VMSVGA
Remote Desktop Server:   Disabled
Recording:               Disabled

Storage
Controller: IDE
  IDE Secondary Device 0:   [Optical Drive] rhel-baseos-9.0-x86_64-dvd.iso (7.90 GB)
Controller: SATA
  SATA Port 0:              rhel9.vdi (Normal, 10.00 GB)

Audio
Host Driver:   Windows DirectSound
Controller:    ICH AC97

Network
Adapter 1:   Intel PRO/1000 MT Desktop (Bridged Adapter, Intel(R) Dual Band Wireless-AC 8265)

USB
USB Controller:   OHCI, EHCI
Device Filters:   0 (0 active)
```



New machine name and path

Please choose a name and optionally a folder for the new virtual machine. The new machine will be a clone of the machine **rhel9**.

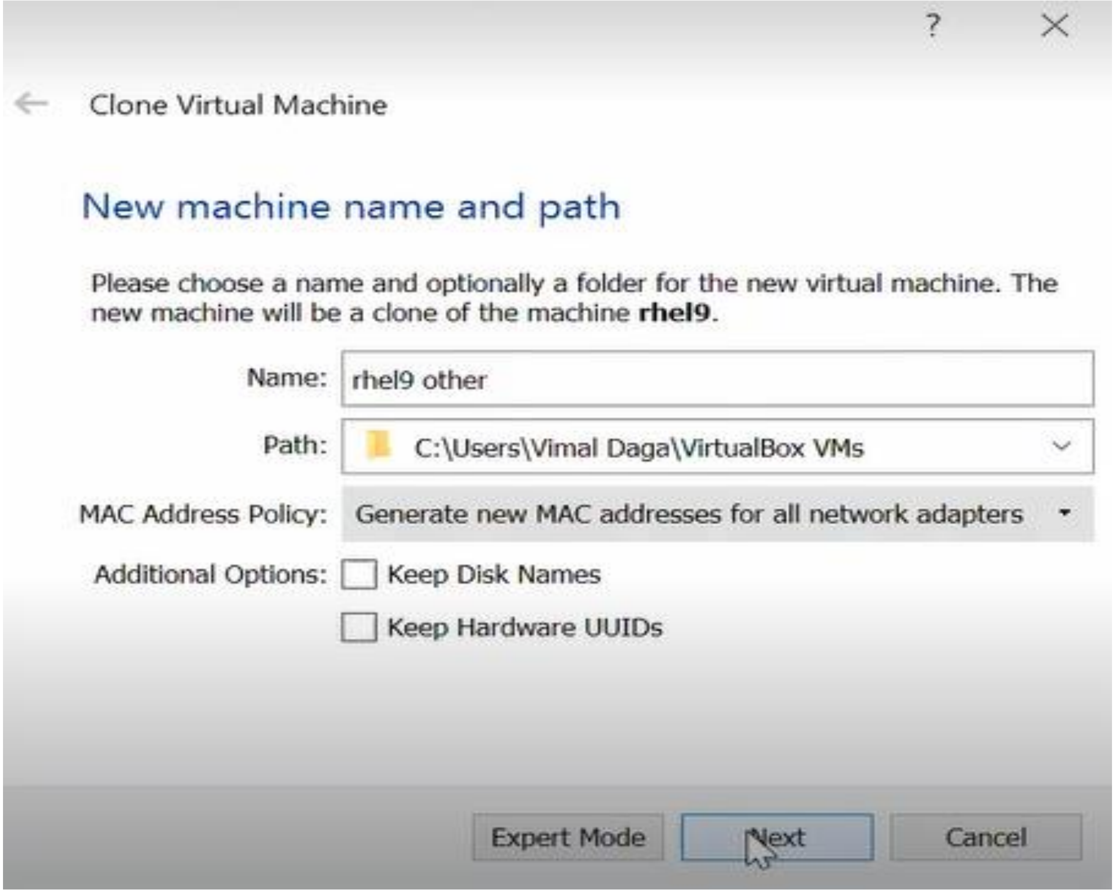
Name: rhel9 other

Path: C:\Users\Vimal Daga\VirtualBox VMs

MAC Address Policy: Include only NAT network adapter MAC addresses

Additional Options: □ Keep Disk Names

□ Keep Hardware UUIDs



Clone Virtual Machine

New machine name and path

Please choose a name and optionally a folder for the new virtual machine. The new machine will be a clone of the machine **rhel9**.

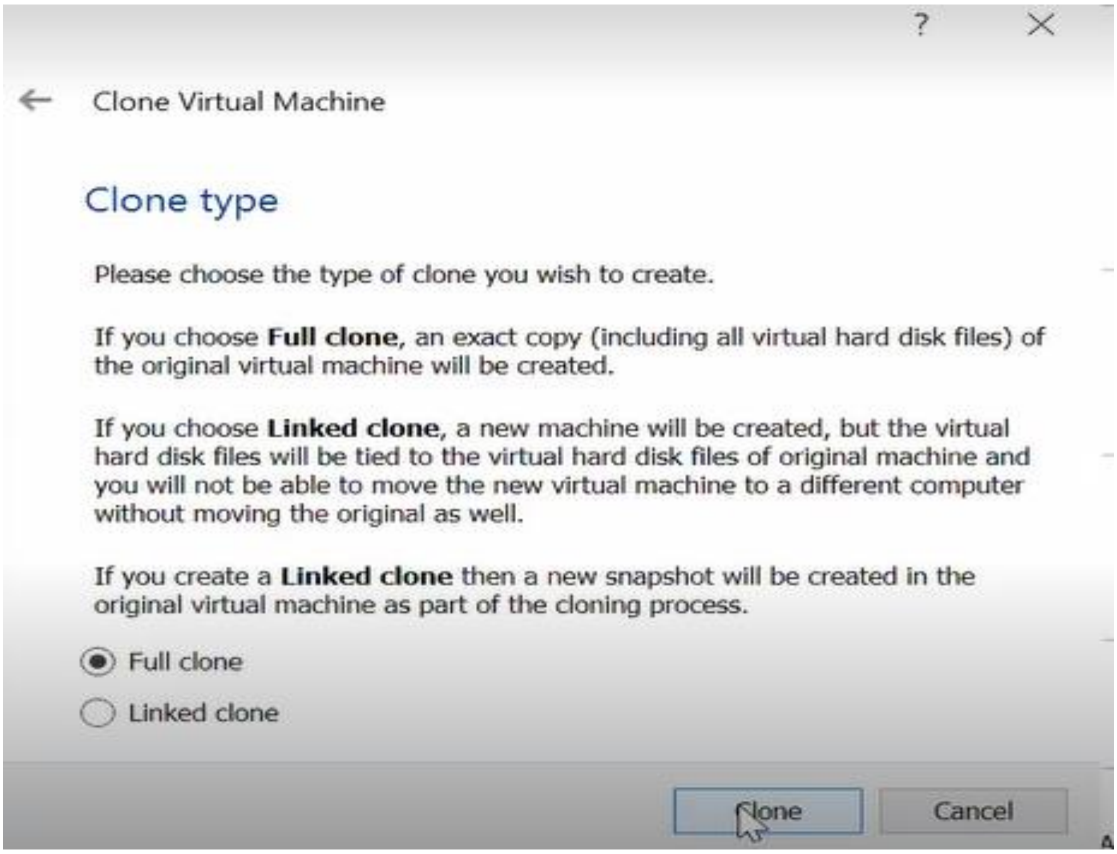
Name: rhel9 other

Path: C:\Users\Vimal Daga\VirtualBox VMs

MAC Address Policy: Generate new MAC addresses for all network adapters

Additional Options: □ Keep Disk Names

□ Keep Hardware UUIDs



Clone Virtual Machine

Clone type

Please choose the type of clone you wish to create.

If you choose **Full clone**, an exact copy (including all virtual hard disk files) of the original virtual machine will be created.

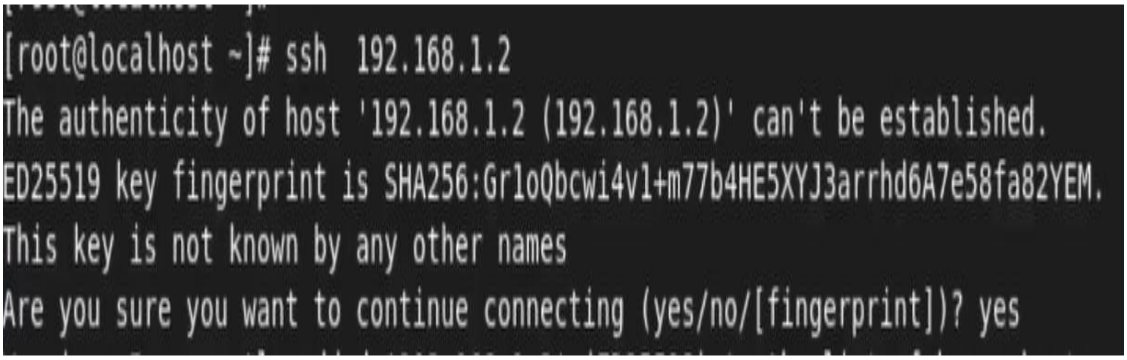
If you choose **Linked clone**, a new machine will be created, but the virtual hard disk files will be tied to the virtual hard disk files of original machine and you will not be able to move the new virtual machine to a different computer without moving the original as well.

If you create a **Linked clone** then a new snapshot will be created in the original virtual machine as part of the cloning process.

● Full clone

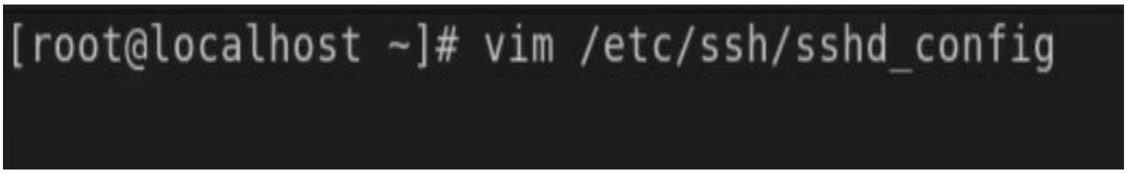
○ Linked clone

- To manage the server remotely – we have to configure as ssh server – we can use two VM – one as ssh server and other as ssh client
- First we can check the connectivity between the systems using "ping" command
- When we try to remote login for the first time

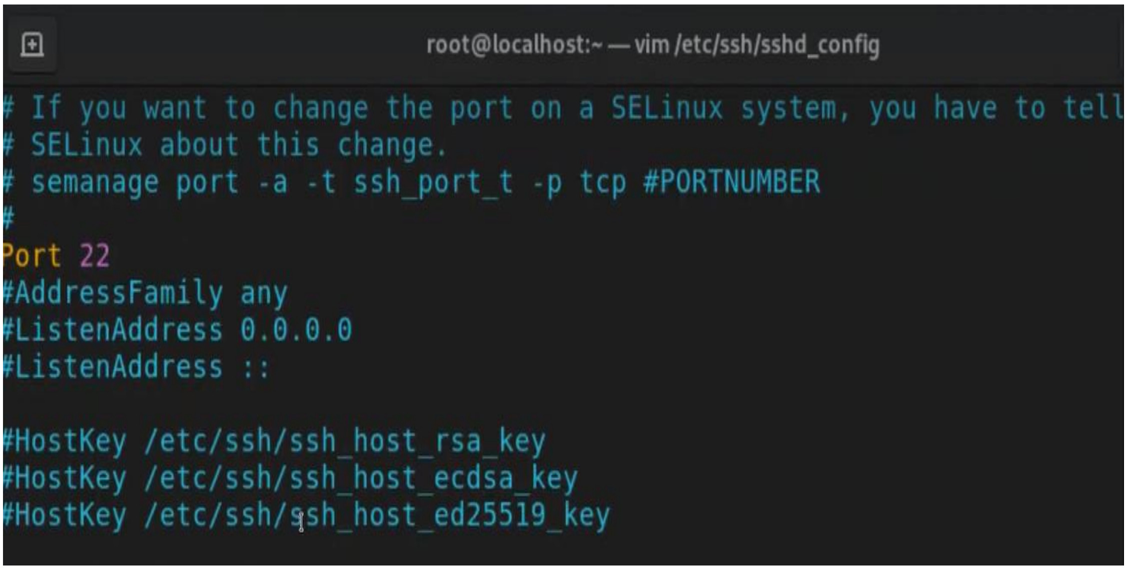


```
[root@localhost ~]# ssh  192.168.1.2
The authenticity of host '192.168.1.2 (192.168.1.2)' can't be established.
ED25519 key fingerprint is SHA256:Gr1oQbcwi4v1+m77b4HE5XYJ3arrhd6A7e58fa82YEM.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

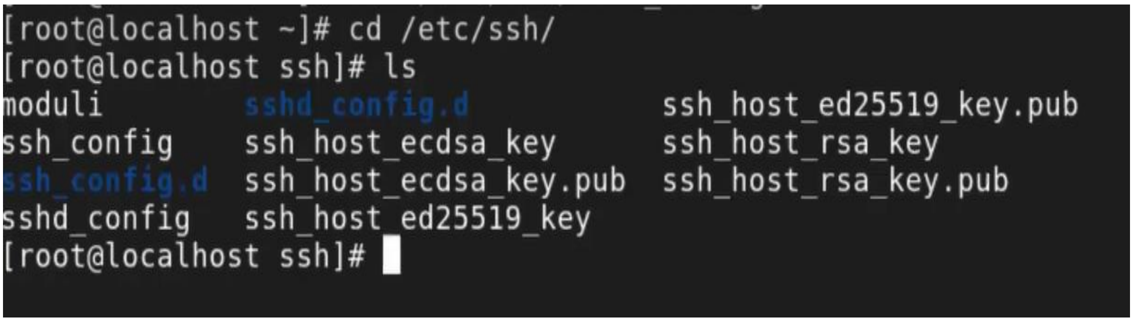
- The ssh will create a private and public key pair



```
[root@localhost ~]# vim /etc/ssh/sshd_config
```

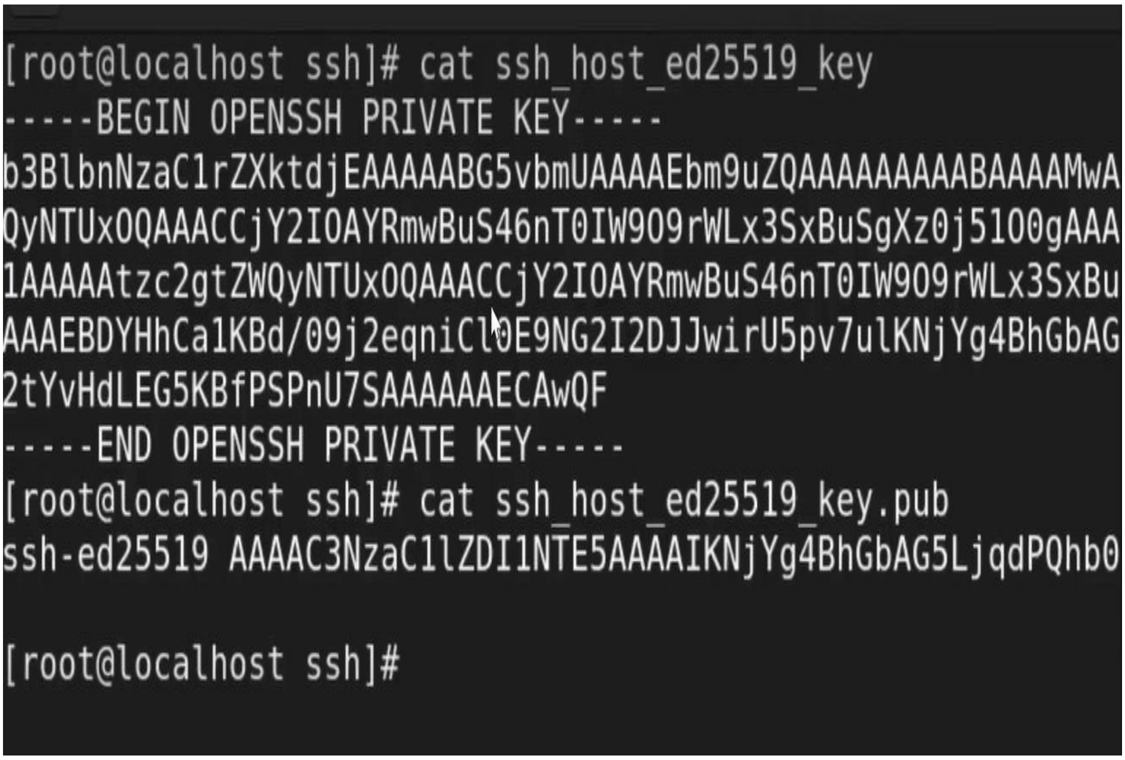


```
# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key
```



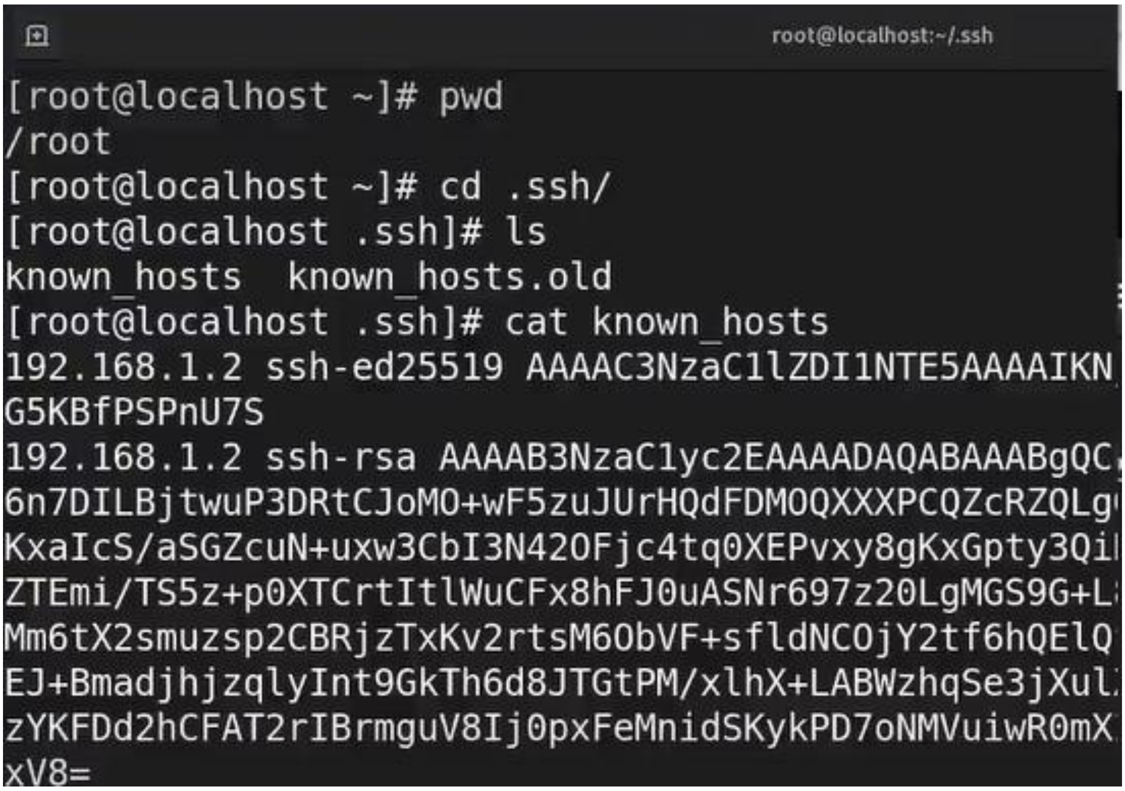
```
[root@localhost ~]# cd /etc/ssh/
[root@localhost ssh]# ls
moduli          sshd_config.d          ssh_host_ed25519_key.pub
ssh_config      ssh_host_ecdsa_key     ssh_host_rsa_key
ssh_config.d    ssh_host_ecdsa_key.pub ssh_host_rsa_key.pub
sshd_config     ssh_host_ed25519_key
[root@localhost ssh]# 
```

- The private and public key – when client connects to the server, server sends the public key to the client



```
[root@localhost ssh]# cat ssh_host_ed25519_key
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwA
QyNTUxOQAAACCjY2IOAYRmwBuS46nT0IW909rWLx3SxBuSgXz0j51O0gAAA
1AAAAAtzc2gtZWQyNTUxOQAAACCjY2IOAYRmwBuS46nT0IW909rWLx3SxBu
AAAEBDYHhCa1KBd/09j2eqniCl0E9NG2I2DJJwirU5pv7ulKNjYg4BhGbAG
2tYvHdLEG5KBfPSPnU7SAAAAAAECAwQF
-----END OPENSSH PRIVATE KEY-----
[root@localhost ssh]# cat ssh_host_ed25519_key.pub
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKNjYg4BhGbAG5LjqdPQhb0

[root@localhost ssh]#
```

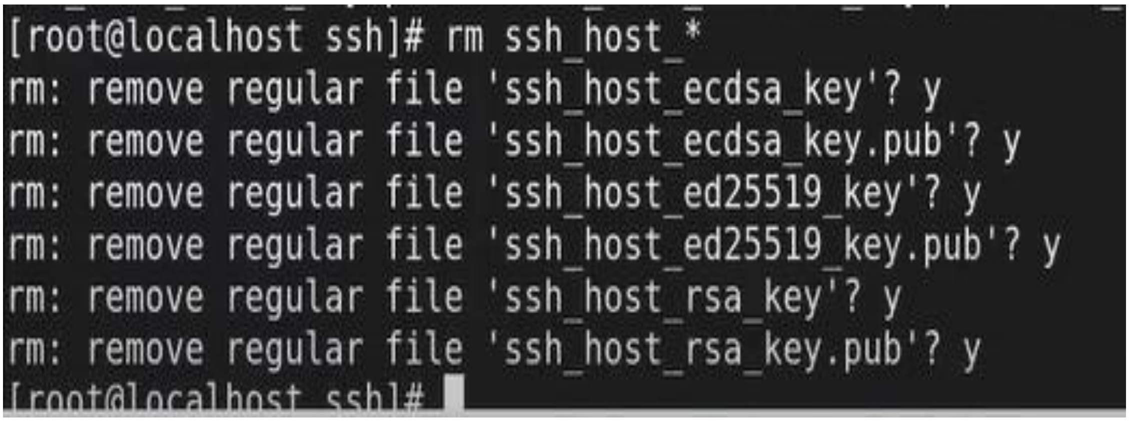
- In client system the public key is downloaded – this public key is same as the public key generated by ssh server



root@localhost:~/.ssh

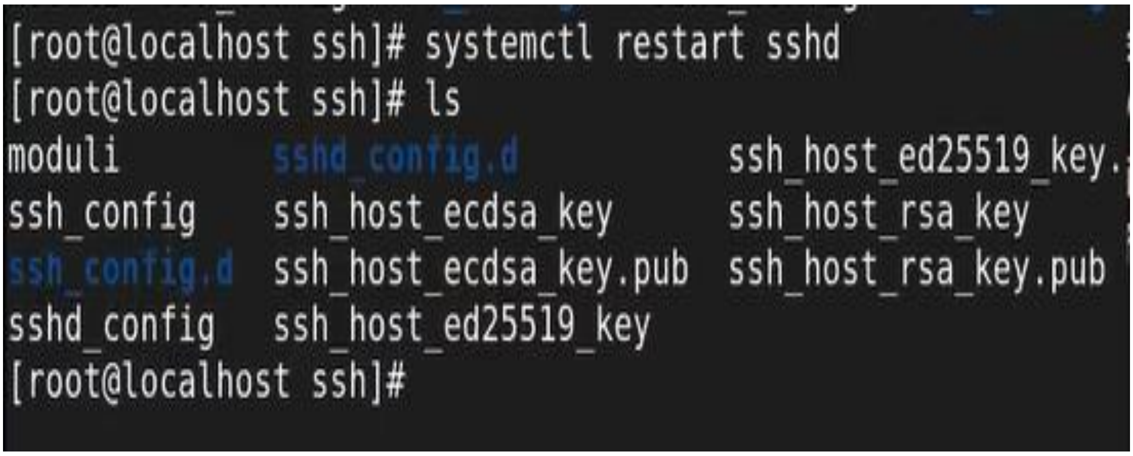
```
[root@localhost ~]# pwd
/root
[root@localhost ~]# cd .ssh/
[root@localhost .ssh]# ls
known_hosts  known_hosts.old
[root@localhost .ssh]# cat known_hosts
192.168.1.2 ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKN
G5KBfPSPnU7S
192.168.1.2 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC
6n7DILBjtwuP3DRtCJoMO+wF5zuJUrHQdFDMOQXXXPCQZcRZQLg
KxaIcS/aSGZcuN+uxw3CbI3N42OFjc4tq0XEPvxy8gKxGpty3Qi
ZTEmi/TS5z+p0XTCrtItlWuCFx8hFJ0uASNr697z20LgMGS9G+L
Mm6tX2smuzsp2CBRjzTxKv2rtsM6ObVF+sfldNCOjY2tf6hQElQ
EJ+BmadjhjzqlyInt9GkTh6d8JTGtPM/xlhX+LABWzhqSe3jXul
zYKFDd2hCFAT2rIBrmguV8Ij0pxFeMnidSKykPD7oNMVuiwR0mX
xV8=
```

- In server if all keys deleted –



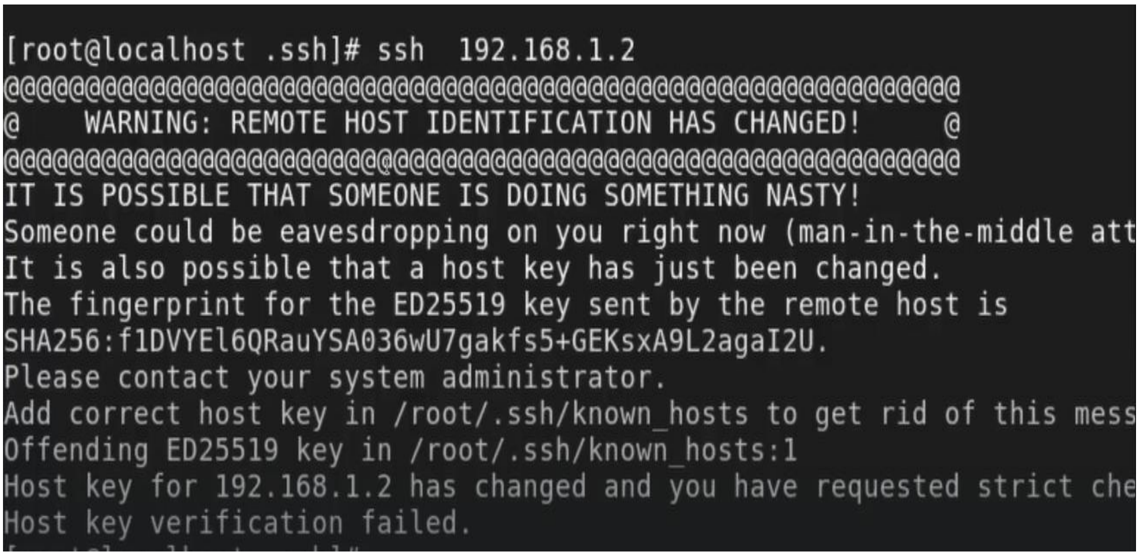
```
[root@localhost ssh]# rm ssh_host_*
rm: remove regular file 'ssh_host_ecdsa_key'? y
rm: remove regular file 'ssh_host_ecdsa_key.pub'? y
rm: remove regular file 'ssh_host_ed25519_key'? y
rm: remove regular file 'ssh_host_ed25519_key.pub'? y
rm: remove regular file 'ssh_host_rsa_key'? y
rm: remove regular file 'ssh_host_rsa_key.pub'? y
[root@localhost ssh]#
```

- Once we restart the service – private and public keys are automatically created



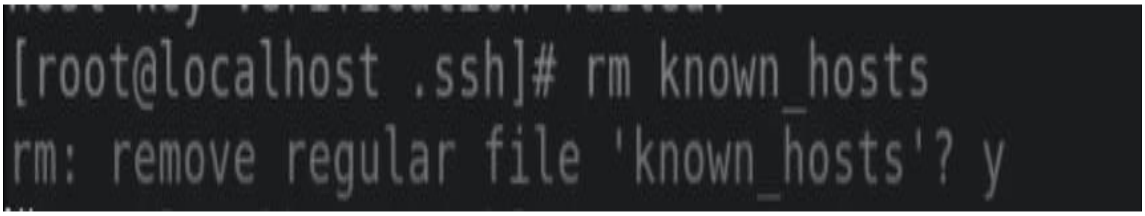
```
[root@localhost ssh]# systemctl restart sshd
[root@localhost ssh]# ls
moduli        sshd_config.d           ssh_host_ed25519_key.
ssh_config    ssh_host_ecdsa_key      ssh_host_rsa_key
ssh_config.d  ssh_host_ecdsa_key.pub  ssh_host_rsa_key.pub
sshd_config   ssh_host_ed25519_key
[root@localhost ssh]#
```

- Now when client tries to login-

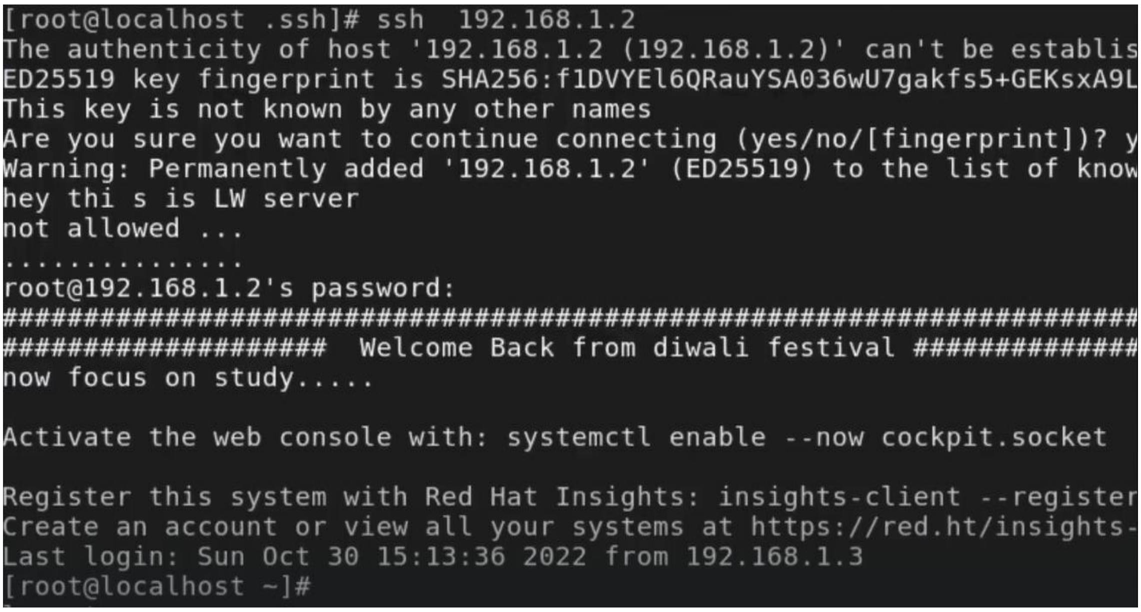


```
[root@localhost .ssh]# ssh  192.168.1.2
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle att
It is also possible that a host key has just been changed.
The fingerprint for the ED25519 key sent by the remote host is
SHA256:f1DVYEl6QRauYSA036wU7gakfs5+GEKsxA9L2agaI2U.
Please contact your system administrator.
Add correct host key in /root/.ssh/known_hosts to get rid of this mess
Offending ED25519 key in /root/.ssh/known_hosts:1
Host key for 192.168.1.2 has changed and you have requested strict che
Host key verification failed.
```

- The client has older key – so remove it and connect again

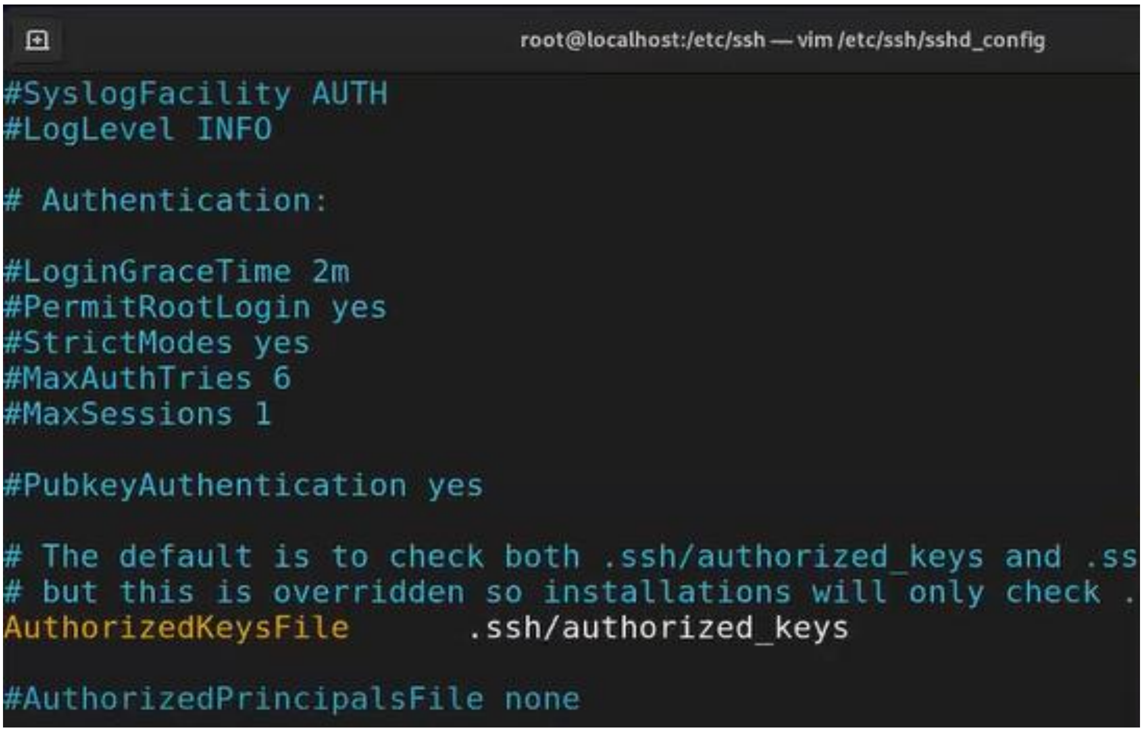


```
[root@localhost .ssh]# rm known_hosts
rm: remove regular file 'known_hosts'? y
```



```
[root@localhost .ssh]# ssh  192.168.1.2
The authenticity of host '192.168.1.2 (192.168.1.2)' can't be establis
ED25519 key fingerprint is SHA256:f1DVYEl6QRauYSA036wU7gakfs5+GEKsxA9L
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Warning: Permanently added '192.168.1.2' (ED25519) to the list of know
hey thi s is LW server
not allowed ...
...............
root@192.168.1.2's password:
######################################################################
####################  Welcome Back from diwali festival ##############
now focus on study.....

Activate the web console with: systemctl enable --now cockpit.socket

Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-
Last login: Sun Oct 30 15:13:36 2022 from 192.168.1.3
[root@localhost ~]#
```

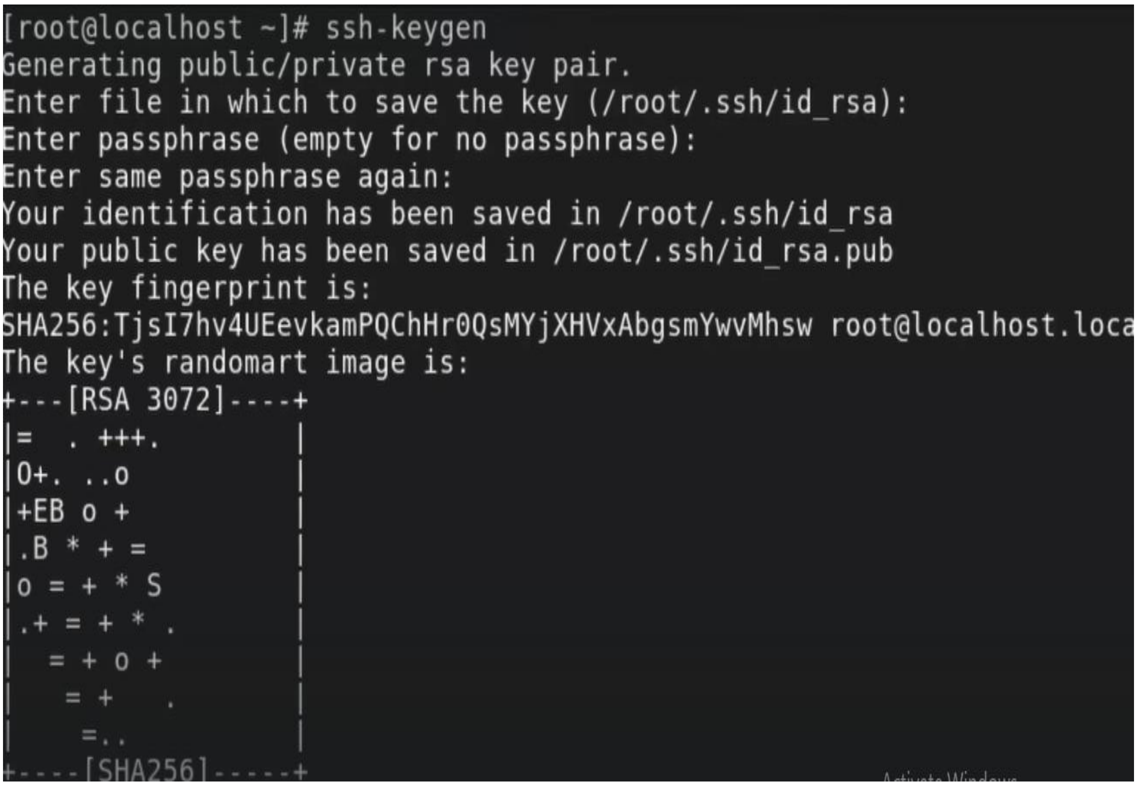
- For key based authentication – on server side its already enabled



root@localhost:/etc/ssh — vim /etc/ssh/sshd_config

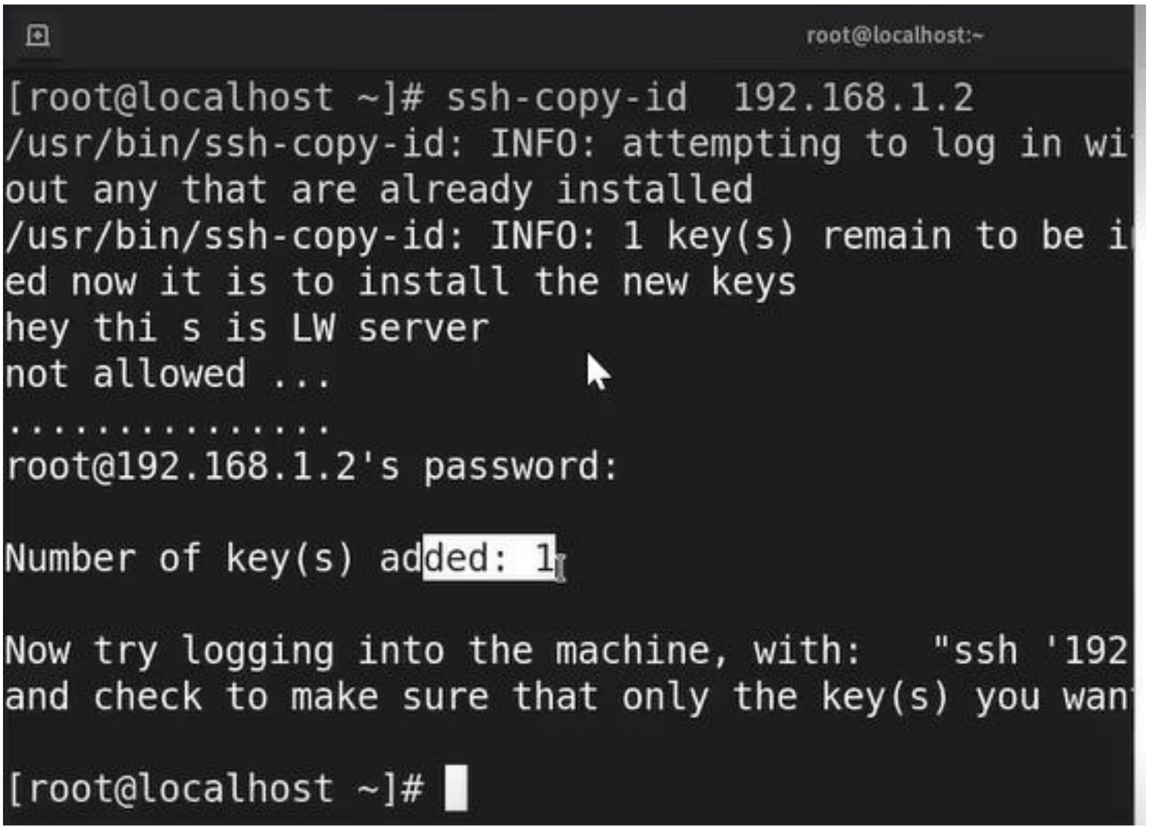
```
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 1

#PubkeyAuthentication yes

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

#AuthorizedPrincipalsFile none
```

- On the client side we have to generate the private and public key



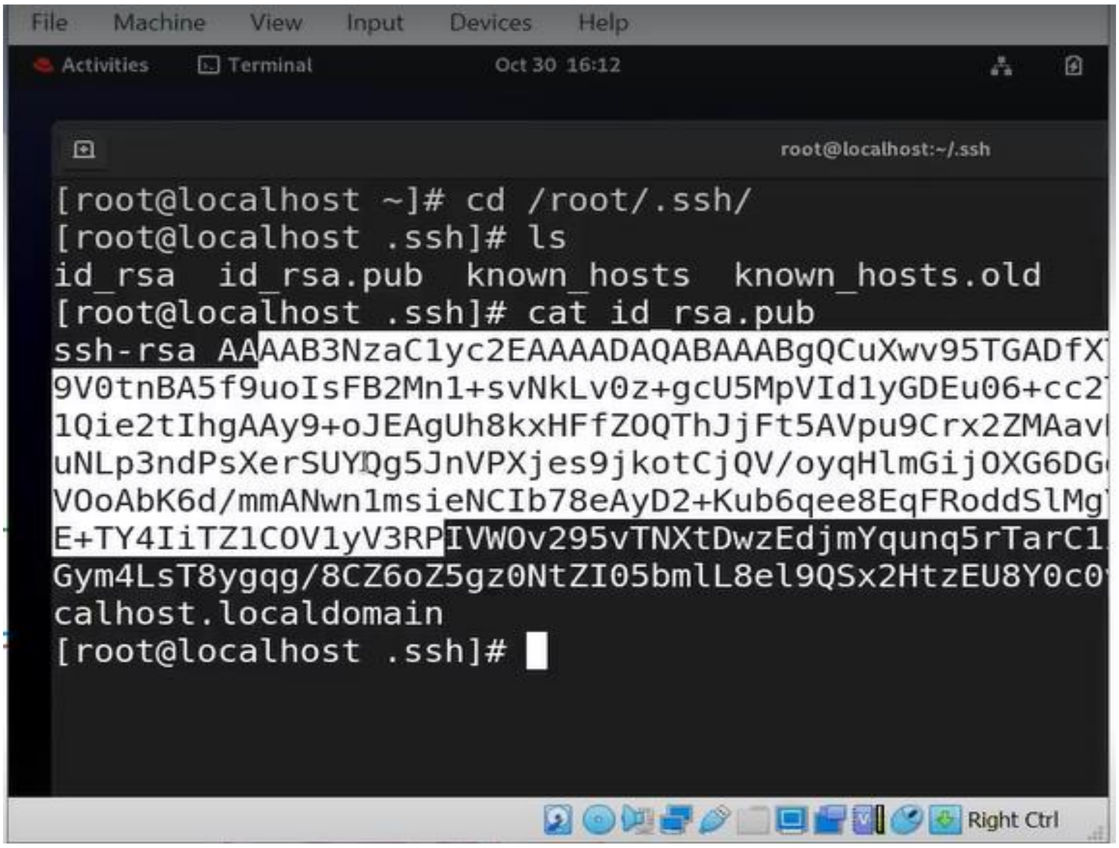
```
[root@localhost ~]# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:TjsI7hv4UEevkamPQChHr0QsMYjXHVxAbgsmYwvMhsw root@localhost.loca
The key's randomart image is:
+---[RSA 3072]----+
|=  . +++.        |
|O+. ..o          |
|+EB o +          |
|.B * + =         |
|o = + * S        |
|.+ = + * .       |
|  = + o +        |
|   = +   .       |
|    =..          |
+----[SHA256]-----+
```

- The client sends the public key to the server and authorized by server



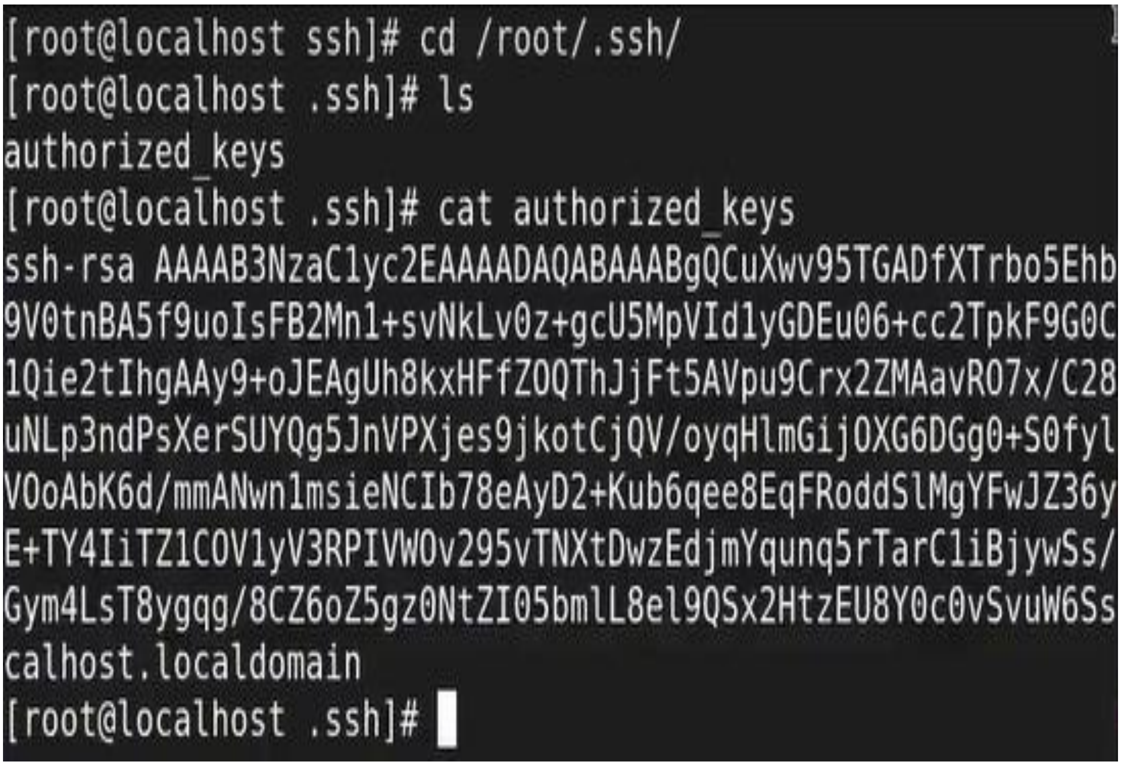
```
[root@localhost ~]# ssh-copy-id  192.168.1.2
/usr/bin/ssh-copy-id: INFO: attempting to log in wi
out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be i
ed now it is to install the new keys
hey thi s is LW server
not allowed ...
...............
root@192.168.1.2's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh '192
and check to make sure that only the key(s) you wan

[root@localhost ~]#
```

- At the client side the public key location



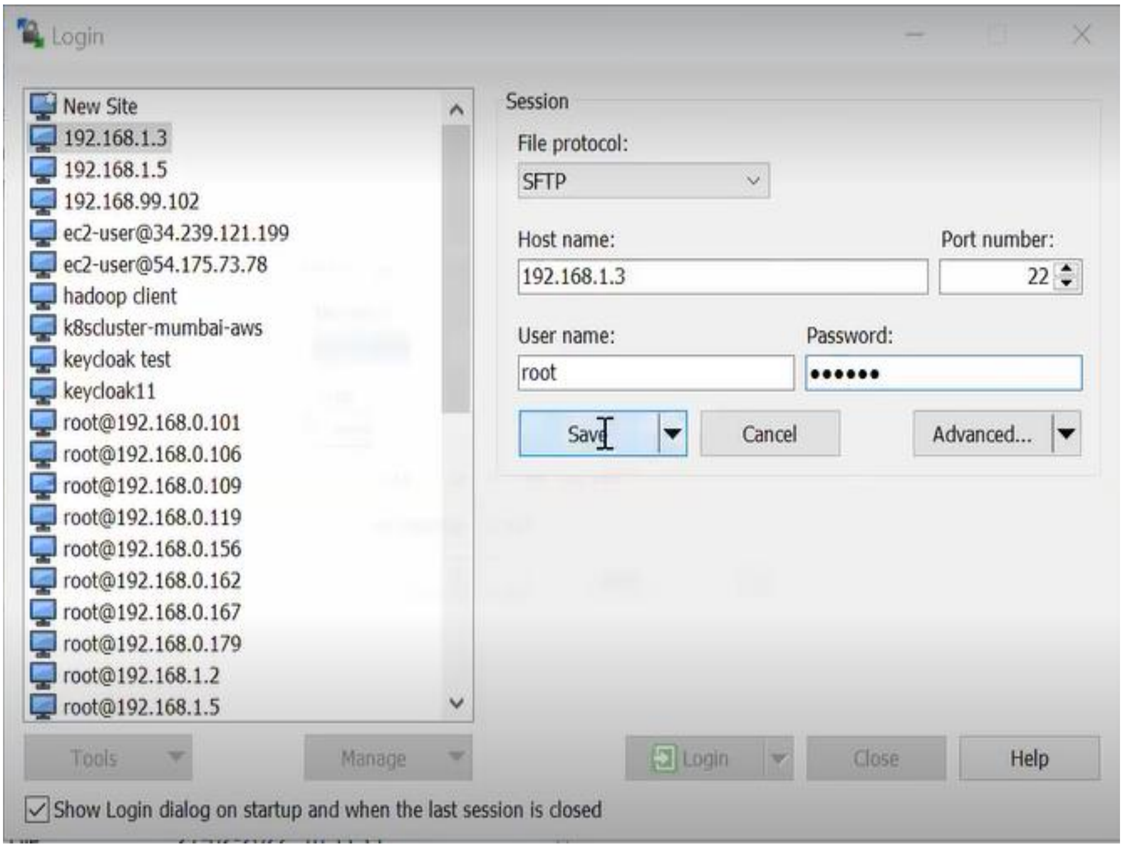
```
[root@localhost ~]# cd /root/.ssh/
[root@localhost .ssh]# ls
id_rsa  id_rsa.pub  known_hosts  known_hosts.old
[root@localhost .ssh]# cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCuXwv95TGADfX
9V0tnBA5f9uoIsFB2Mn1+svNkLv0z+gcU5MpVId1yGDEu06+cc2
1Qie2tIhgAAy9+oJEAgUh8kxHFfZ0QThJjFt5AVpu9Crx2ZMAav
uNLp3ndPsXerSUYQg5JnVPXjes9jkotCjQV/oyqHlmGijOXG6DG
VOoAbK6d/mmANwn1msieNCIb78eAyD2+Kub6qee8EqFRoddSlMg
E+TY4IiTZ1COV1yV3RPIVWOv295vTNXtDwzEdjmYqunq5rTarC1
Gym4LsT8ygqg/8CZ6oZ5gz0NtZI05bmlL8el9QSx2HtzEU8Y0c0
calhost.localdomain
[root@localhost .ssh]# 
```

- The public key of client is transferred to server-



```
[root@localhost ssh]# cd /root/.ssh/
[root@localhost .ssh]# ls
authorized_keys
[root@localhost .ssh]# cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCuXwv95TGADfXTrbo5Ehb
9V0tnBA5f9uoIsFB2Mn1+svNkLv0z+gcU5MpVId1yGDEu06+cc2TpkF9G0C
1Qie2tIhgAAy9+oJEAgUh8kxHFfZOQThJjFt5AVpu9Crx2ZMAavRO7x/C28
uNLp3ndPsXerSUYQg5JnVPXjes9jkotCjQV/oyqHlmGijOXG6DGg0+S0fyl
VOoAbK6d/mmANwn1msieNCIb78eAyD2+Kub6qee8EqFRoddSlMgYFwJZ36y
E+TY4IiTZ1COV1yV3RPIVWOv295vTNXtDwzEdjmYqunq5rTarC1iBjywSs/
Gym4LsT8ygqg/8CZ6oZ5gz0NtZI05bmlL8el9QSx2HtzEU8Y0c0vSvuW6Ss
calhost.localdomain
[root@localhost .ssh]# 
```

- Use winscp to transfer files – transfer private key from .ssh folder to windows – to login to ssh server without password



New Site
192.168.1.3
192.168.1.5
192.168.99.102
ec2-user@34.239.121.199
ec2-user@54.175.73.78
hadoop client
k8scluster-mumbai-aws
keycloak test
keycloak11
root@192.168.0.101
root@192.168.0.106
root@192.168.0.109
root@192.168.0.119
root@192.168.0.156
root@192.168.0.162
root@192.168.0.167
root@192.168.0.179
root@192.168.1.2
root@192.168.1.5

Session

File protocol: SFTP

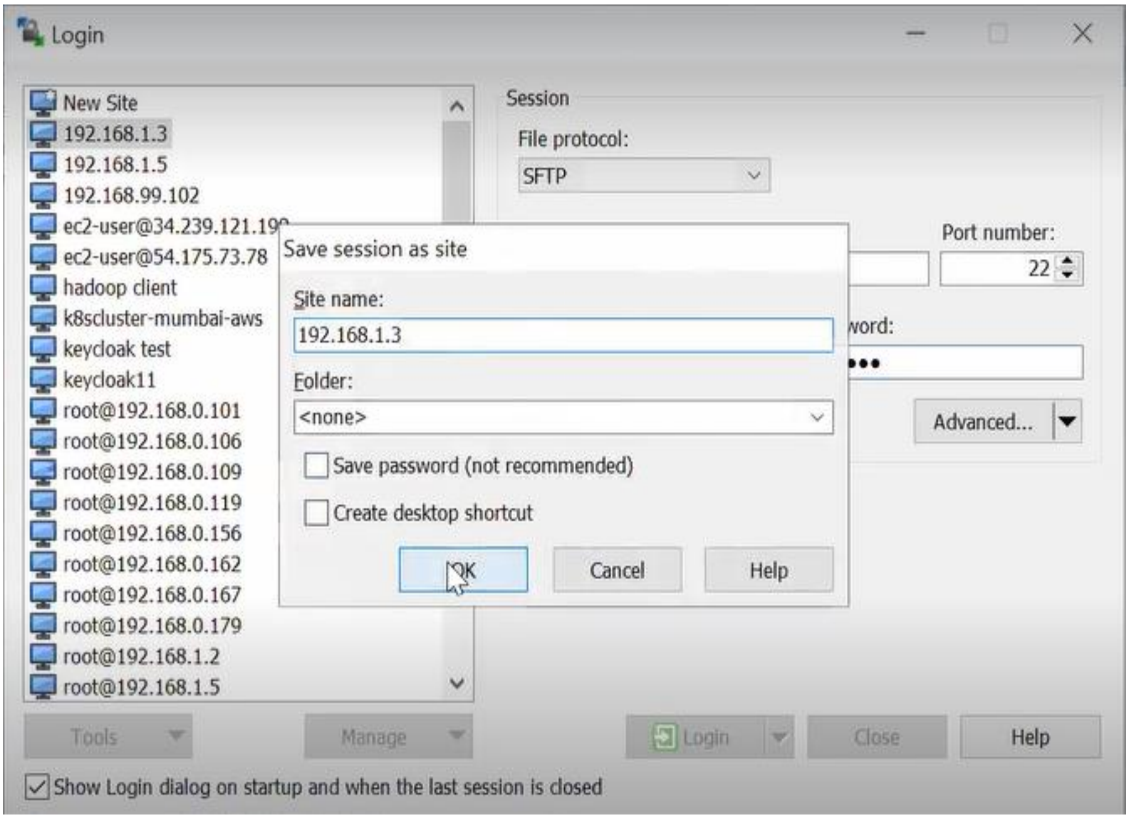
Host name: 192.168.1.3

Port number: 22

User name: root

Password: ••••••

☑ Show Login dialog on startup and when the last session is closed



New Site
192.168.1.3
192.168.1.5
192.168.99.102
ec2-user@34.239.121.19
ec2-user@54.175.73.78
hadoop client
k8scluster-mumbai-aws
keycloak test
keycloak11
root@192.168.0.101
root@192.168.0.106
root@192.168.0.109
root@192.168.0.119
root@192.168.0.156
root@192.168.0.162
root@192.168.0.167
root@192.168.0.179
root@192.168.1.2
root@192.168.1.5

Session

File protocol: SFTP

Port number: 22

Save session as site

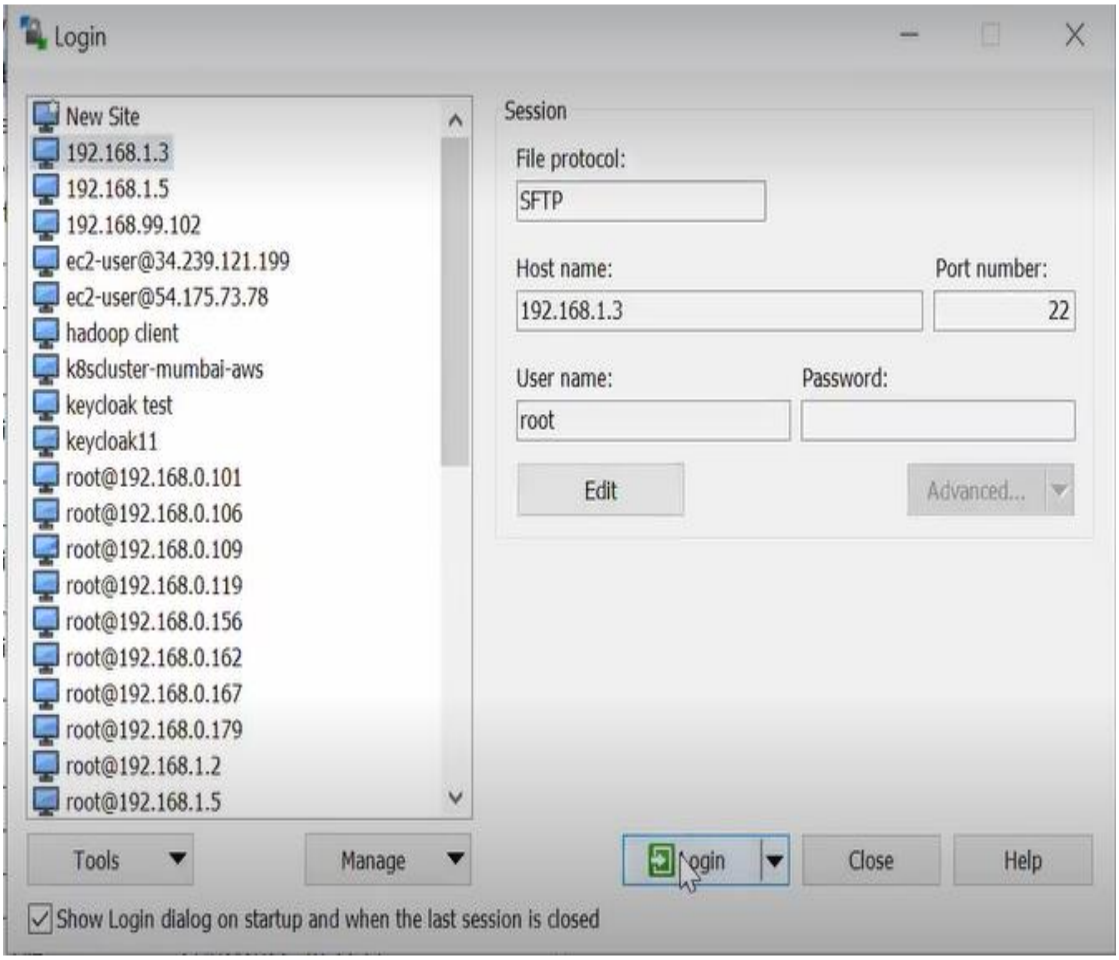
Site name: 192.168.1.3

Folder: <none>

□ Save password (not recommended)

□ Create desktop shortcut

☑ Show Login dialog on startup and when the last session is closed



File protocol: SFTP

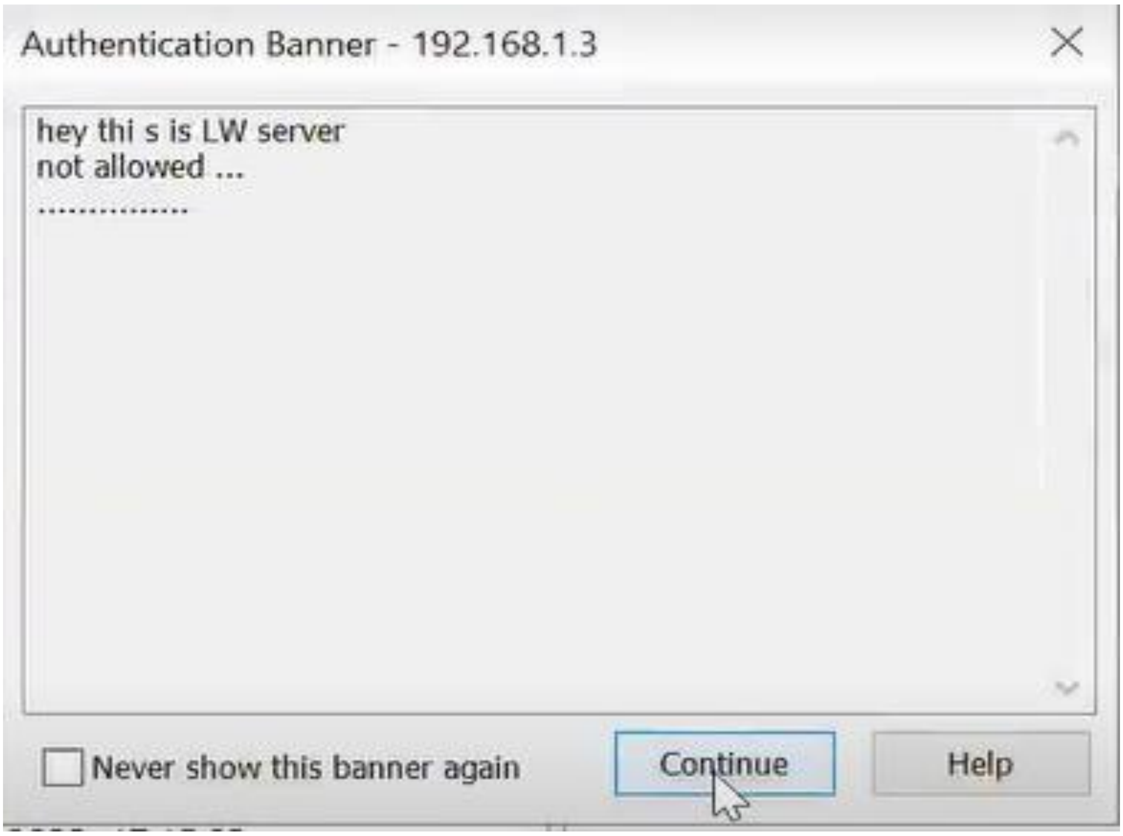
Host name: 192.168.1.3

Port number: 22

User name: root

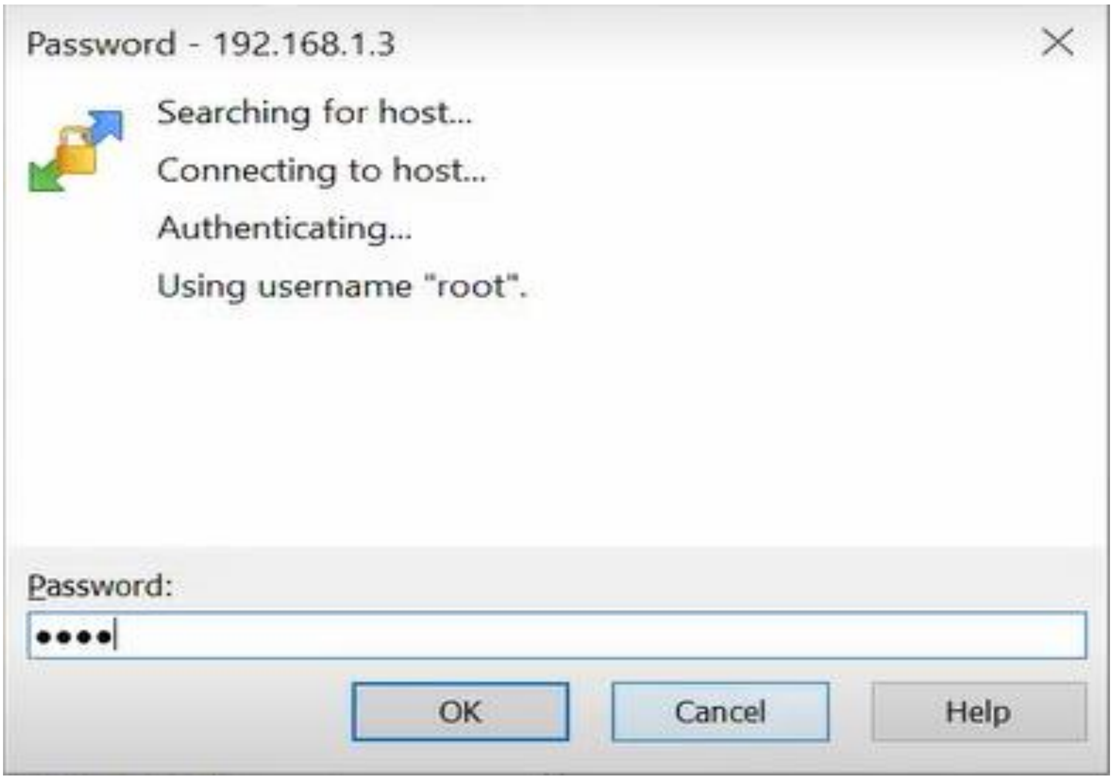
Password:

☑ Show Login dialog on startup and when the last session is closed


Authentication Banner - 192.168.1.3

hey thi s is LW server
not allowed ...
....

□ Never show this banner again



Password - 192.168.1.3

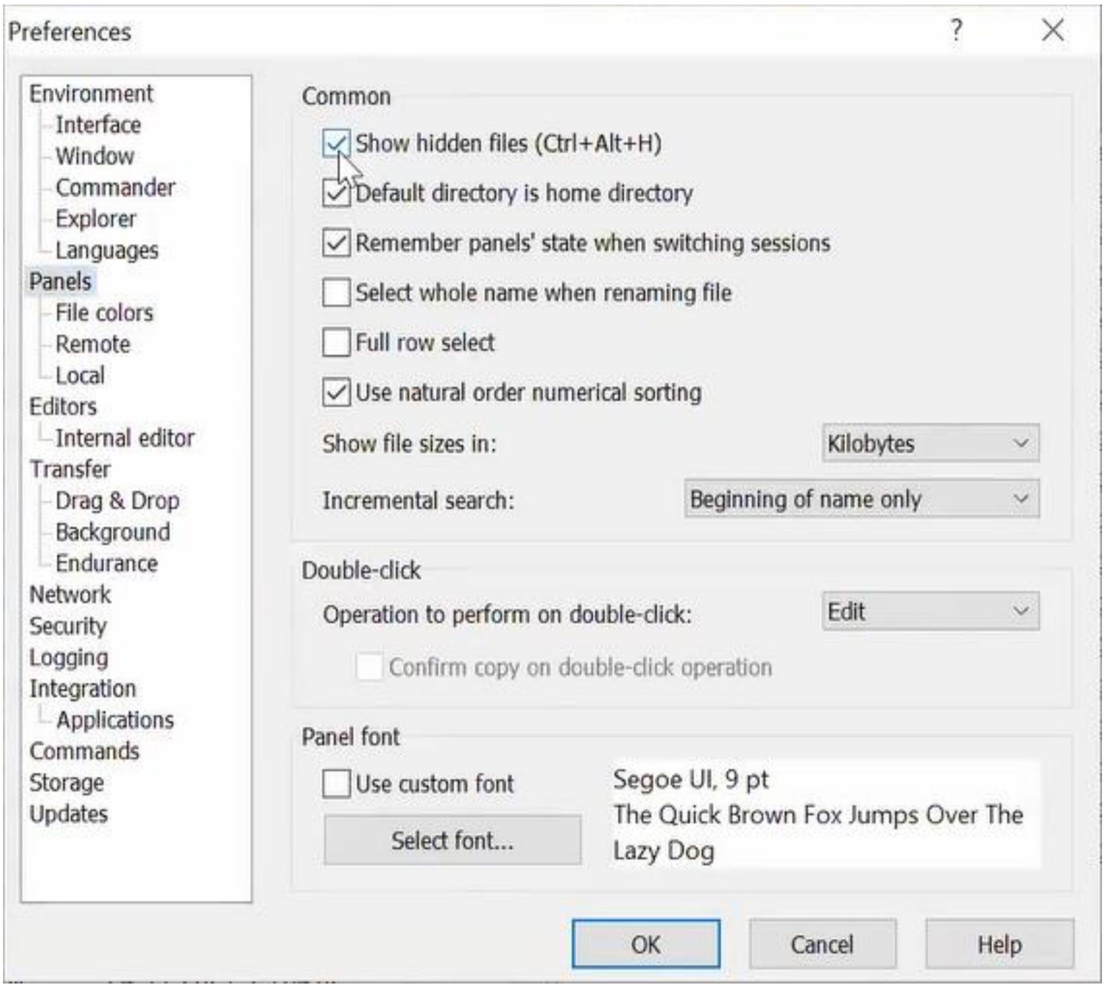
Searching for host...

Connecting to host...

Authenticating...

Using username "root".

Password: ●●●●



Preferences

Common

☑ Show hidden files (Ctrl+Alt+H)

☑ Default directory is home directory

☑ Remember panels' state when switching sessions

☐ Select whole name when renaming file

☐ Full row select

☑ Use natural order numerical sorting

Show file sizes in: Kilobytes

Incremental search: Beginning of name only

Double-click

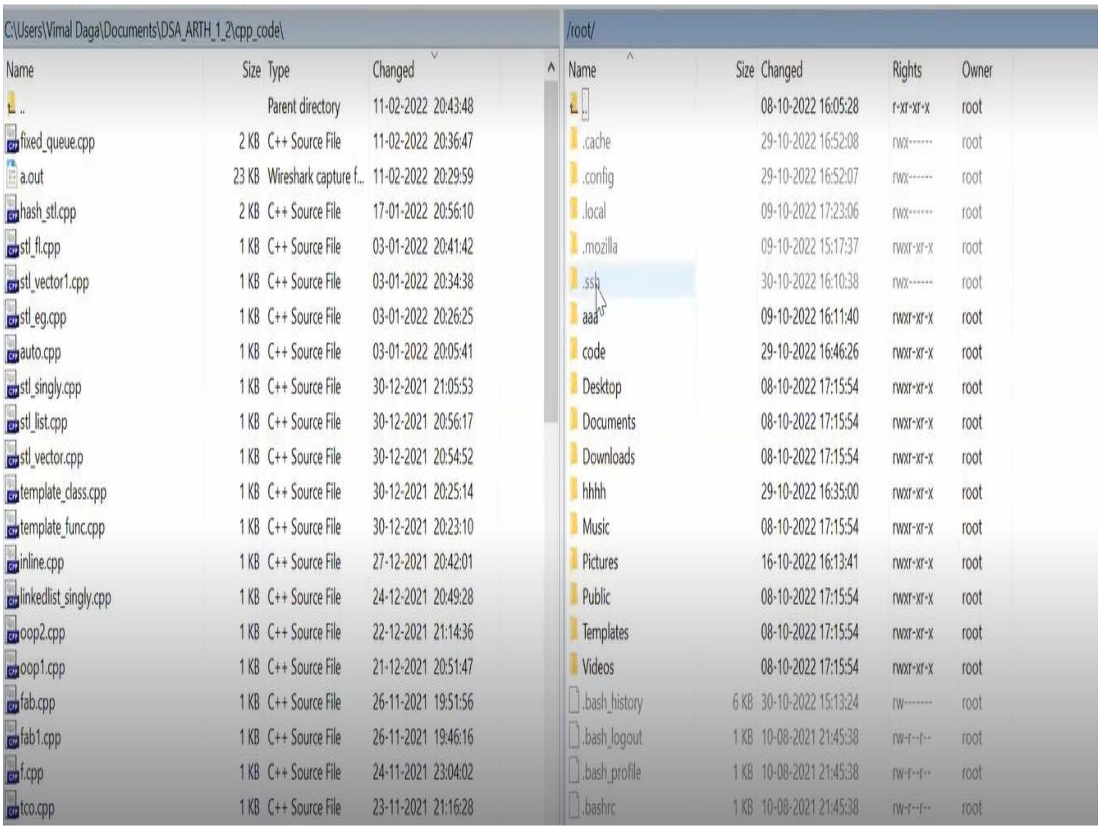
Operation to perform on double-click: Edit

☐ Confirm copy on double-click operation

Panel font

☐ Use custom font

Segoe UI, 9 pt
The Quick Brown Fox Jumps Over The Lazy Dog

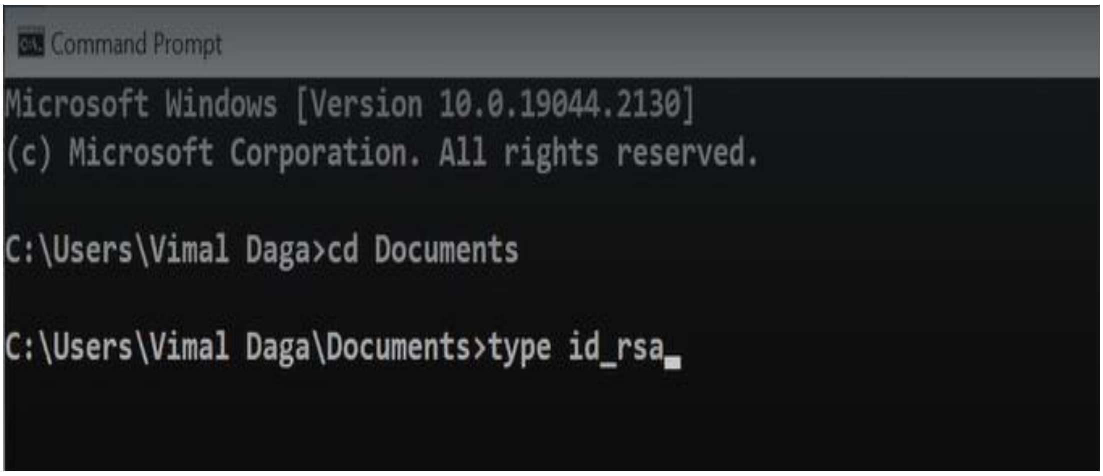


C:\Users\Vimal Daga\Documents\DSA_ARTH_1_2\cpp_code\

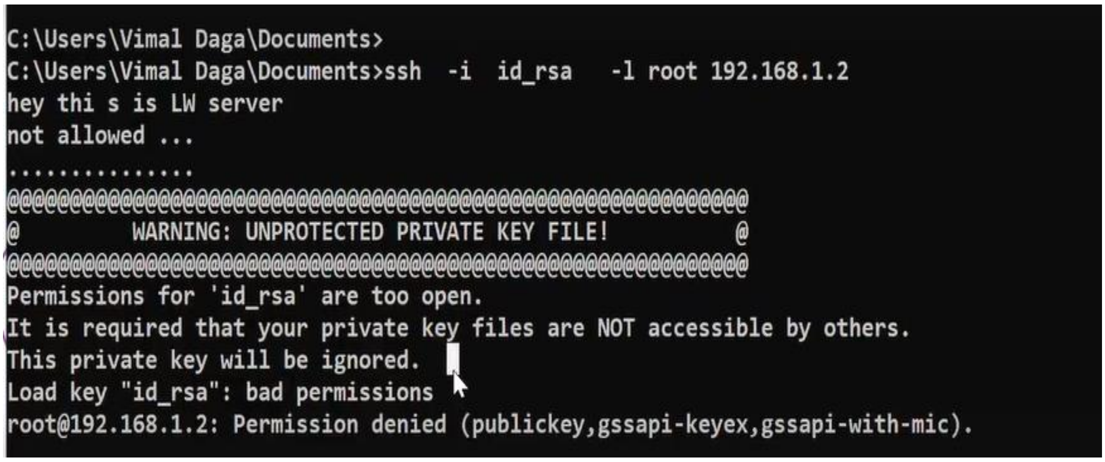
Name	Size	Type	Changed
..		Parent directory	11-02-2022 20:43:48
fixed_queue.cpp	2 KB	C++ Source File	11-02-2022 20:36:47
a.out	23 KB	Wireshark capture f...	11-02-2022 20:29:59
hash_stl.cpp	2 KB	C++ Source File	17-01-2022 20:56:10
stl_fl.cpp	1 KB	C++ Source File	03-01-2022 20:41:42
stl_vector1.cpp	1 KB	C++ Source File	03-01-2022 20:34:38
stl_eg.cpp	1 KB	C++ Source File	03-01-2022 20:26:25
auto.cpp	1 KB	C++ Source File	03-01-2022 20:05:41
stl_singly.cpp	1 KB	C++ Source File	30-12-2021 21:05:53
stl_list.cpp	1 KB	C++ Source File	30-12-2021 20:56:17
stl_vector.cpp	1 KB	C++ Source File	30-12-2021 20:54:52
template_class.cpp	1 KB	C++ Source File	30-12-2021 20:25:14
template_func.cpp	1 KB	C++ Source File	30-12-2021 20:23:10
inline.cpp	1 KB	C++ Source File	27-12-2021 20:42:01
linkedlist_singly.cpp	1 KB	C++ Source File	24-12-2021 20:49:28
oop2.cpp	1 KB	C++ Source File	22-12-2021 21:14:36
oop1.cpp	1 KB	C++ Source File	21-12-2021 20:51:47
fab.cpp	1 KB	C++ Source File	26-11-2021 19:51:56
fab1.cpp	1 KB	C++ Source File	26-11-2021 19:46:16
f.cpp	1 KB	C++ Source File	24-11-2021 23:04:02
tco.cpp	1 KB	C++ Source File	23-11-2021 21:16:28

/root/

Name	Size	Changed	Rights	Owner
..		08-10-2022 16:05:28	r-xr-xr-x	root
.cache		29-10-2022 16:52:08	rwx------	root
.config		29-10-2022 16:52:07	rwx------	root
.local		09-10-2022 17:23:06	rwx------	root
.mozilla		09-10-2022 15:17:37	rwxr-xr-x	root
.ssh		30-10-2022 16:10:38	rwx------	root
aaa		09-10-2022 16:11:40	rwxr-xr-x	root
code		29-10-2022 16:46:26	rwxr-xr-x	root
Desktop		08-10-2022 17:15:54	rwxr-xr-x	root
Documents		08-10-2022 17:15:54	rwxr-xr-x	root
Downloads		08-10-2022 17:15:54	rwxr-xr-x	root
hhhh		29-10-2022 16:35:00	rwxr-xr-x	root
Music		08-10-2022 17:15:54	rwxr-xr-x	root
Pictures		16-10-2022 16:13:41	rwxr-xr-x	root
Public		08-10-2022 17:15:54	rwxr-xr-x	root
Templates		08-10-2022 17:15:54	rwxr-xr-x	root
Videos		08-10-2022 17:15:54	rwxr-xr-x	root
.bash_history	6 KB	30-10-2022 15:13:24	rw-------	root
.bash_logout	1 KB	10-08-2021 21:45:38	rw-r--r--	root
.bash_profile	1 KB	10-08-2021 21:45:38	rw-r--r--	root
.bashrc	1 KB	10-08-2021 21:45:38	rw-r--r--	root

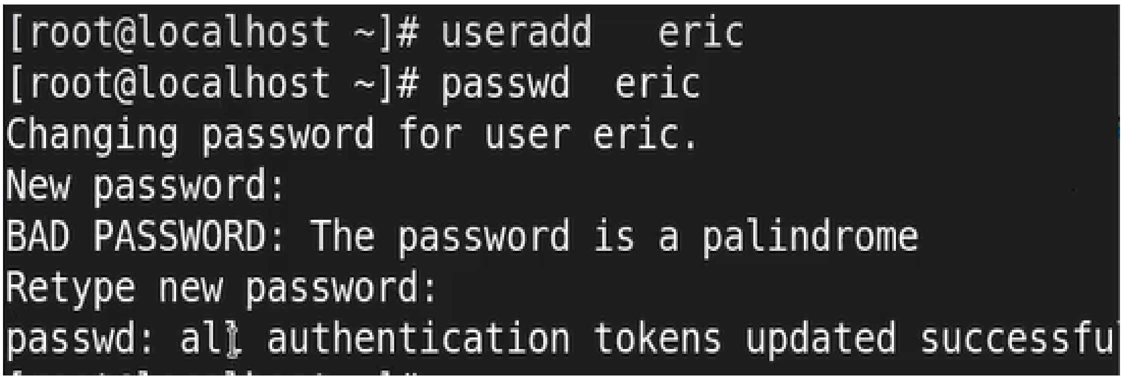


```
Microsoft Windows [Version 10.0.19044.2130]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Vimal Daga>cd Documents

C:\Users\Vimal Daga\Documents>type id_rsa
```



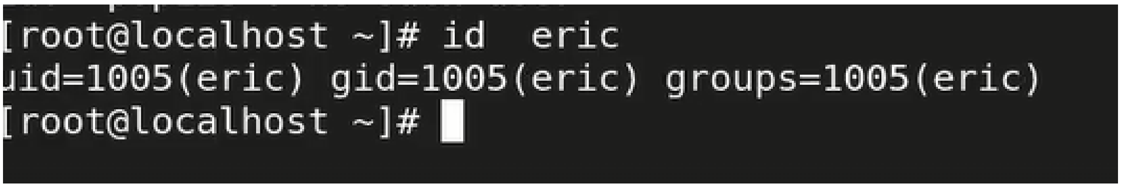
```
C:\Users\Vimal Daga\Documents>
C:\Users\Vimal Daga\Documents>ssh  -i  id_rsa   -l root 192.168.1.2
hey thi s is LW server
not allowed ...
...............
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions for 'id_rsa' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "id_rsa": bad permissions
root@192.168.1.2: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
```

- To use OS we have to login- for login we need account(user name and password)
- By default account the Linux OS create is root account
- Command to create user account



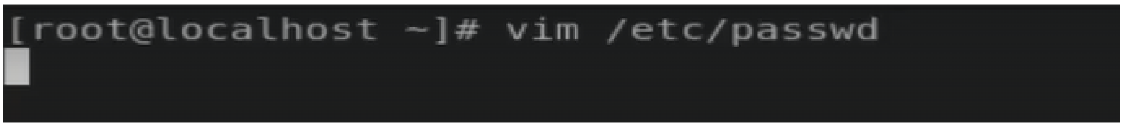
```
[root@localhost ~]# useradd   eric
[root@localhost ~]# passwd  eric
Changing password for user eric.
New password:
BAD PASSWORD: The password is a palindrome
Retype new password:
passwd: all authentication tokens updated successfu
```

- To verify account has been created

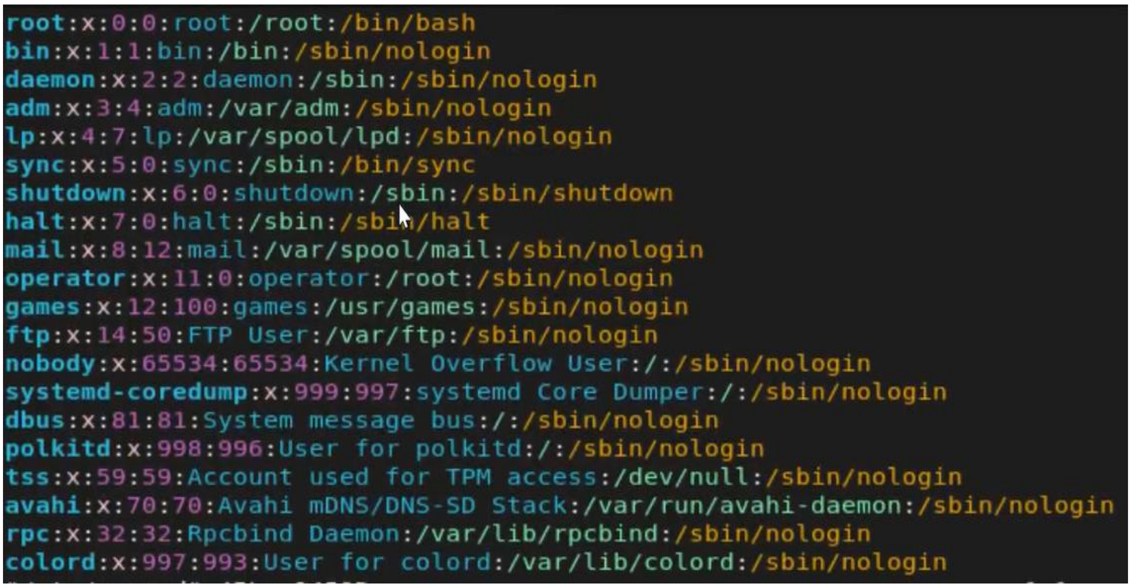


```
[root@localhost ~]# id  eric
uid=1005(eric) gid=1005(eric) groups=1005(eric)
[root@localhost ~]# 
```

- When "Useradd" command is used to create a user, it updates the "/etc/passwd"
- The "/etc/passwd" file contains all the user accounts in the system

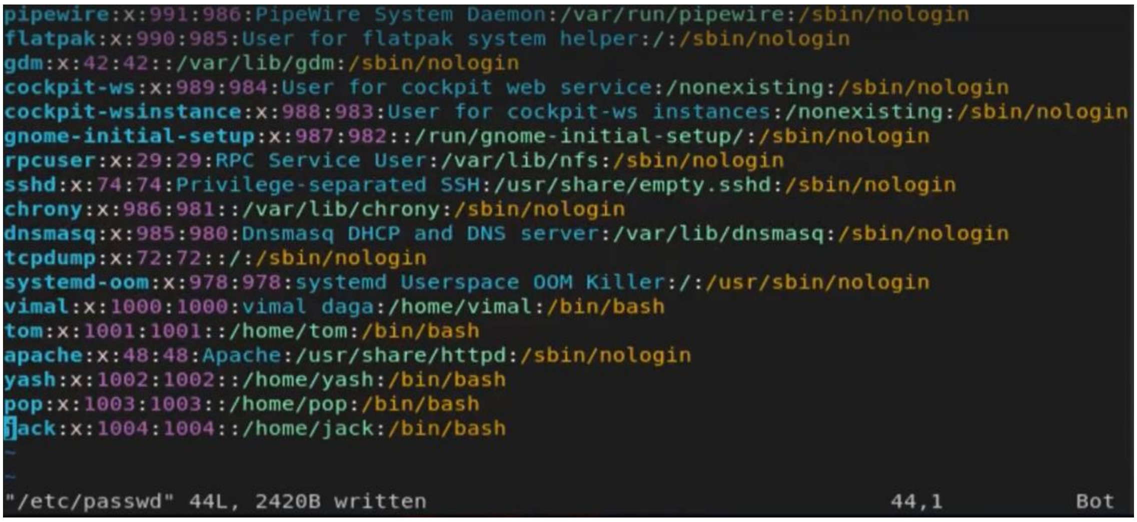


```
[root@localhost ~]# vim /etc/passwd
```

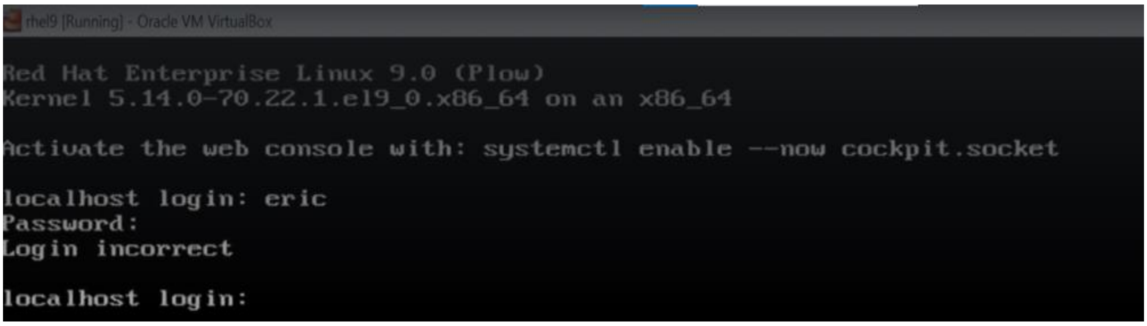


```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin
systemd-coredump:x:999:997:systemd Core Dumper:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:998:996:User for polkitd:/:/sbin/nologin
tss:x:59:59:Account used for TPM access:/dev/null:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
colord:x:997:993:User for colord:/var/lib/colord:/sbin/nologin
```

- ➢ Each line in the “/etc/passwd” file contains the record of one user – it contains seven fields
- ➢ If we delete an entry from this file – that is like to delete an user account



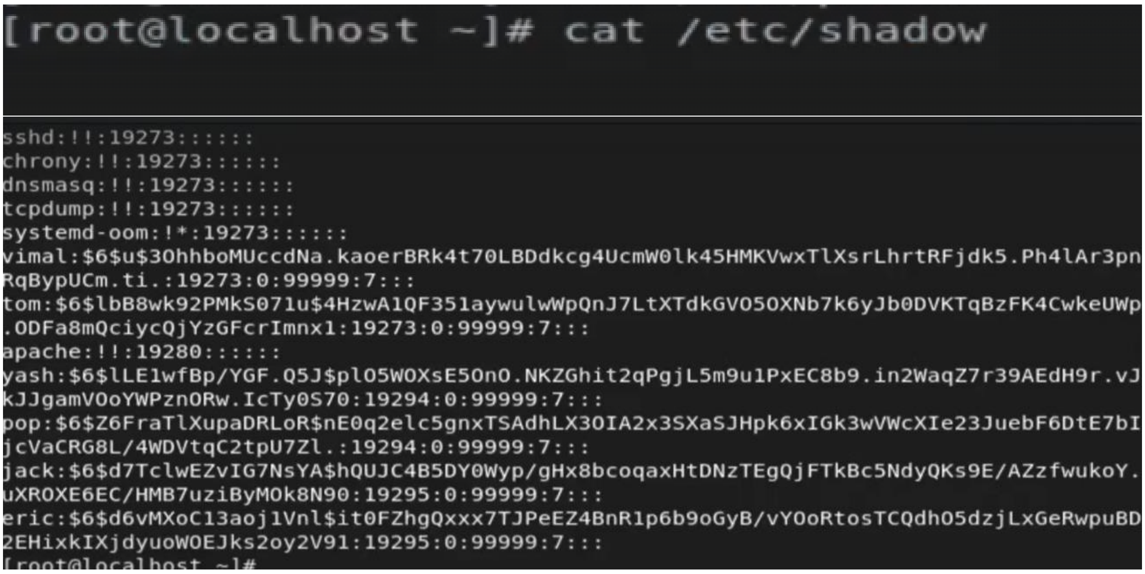
```
pipewire:x:991:986:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
flatpak:x:990:985:User for flatpak system helper:/:/sbin/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
cockpit-ws:x:989:984:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:988:983:User for cockpit-ws instances:/nonexisting:/sbin/nologin
gnome-initial-setup:x:987:982::/run/gnome-initial-setup/:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
chrony:x:986:981::/var/lib/chrony:/sbin/nologin
dnsmasq:x:985:980:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
systemd-oom:x:978:978:systemd Userspace OOM Killer:/:/usr/sbin/nologin
vimal:x:1000:1000:vimal daga:/home/vimal:/bin/bash
tom:x:1001:1001::/home/tom:/bin/bash
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
yash:x:1002:1002::/home/yash:/bin/bash
pop:x:1003:1003::/home/pop:/bin/bash
jack:x:1004:1004::/home/jack:/bin/bash
~
~
"/etc/passwd" 44L, 2420B written                                  44,1          Bot
```



rhel9 [Running] - Oracle VM VirtualBox

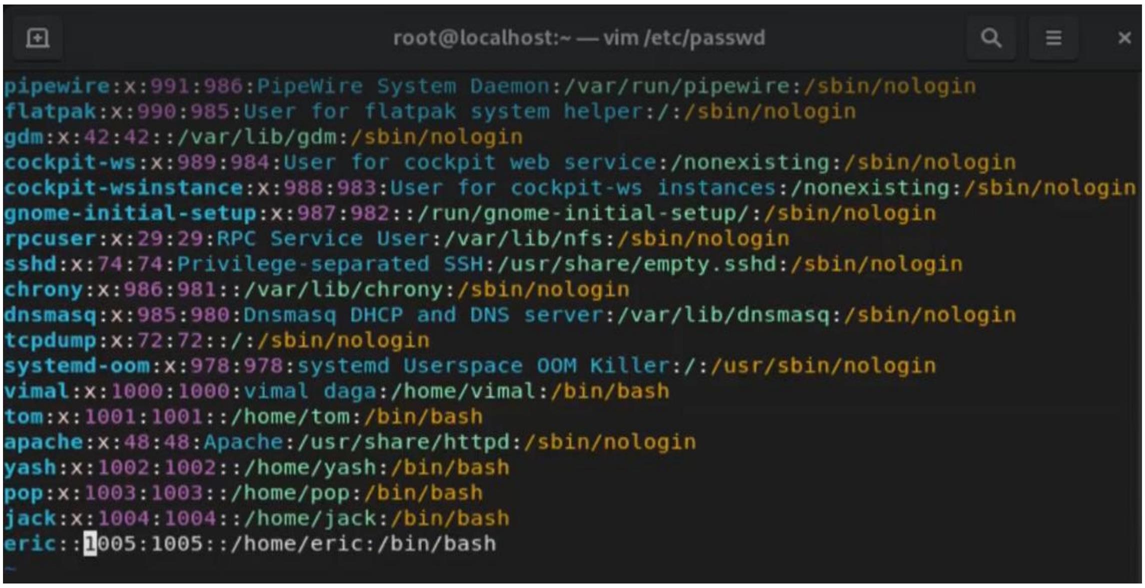
```
Red Hat Enterprise Linux 9.0 (Plow)
Kernel 5.14.0-70.22.1.el9_0.x86_64 on an x86_64

Activate the web console with: systemctl enable --now cockpit.socket

localhost login: eric
Password:
Login incorrect

localhost login:
```

- ➢ The first field is the user/login name
- ➢ The second field is the password field (x) – it links to other file “/etc/shadow”



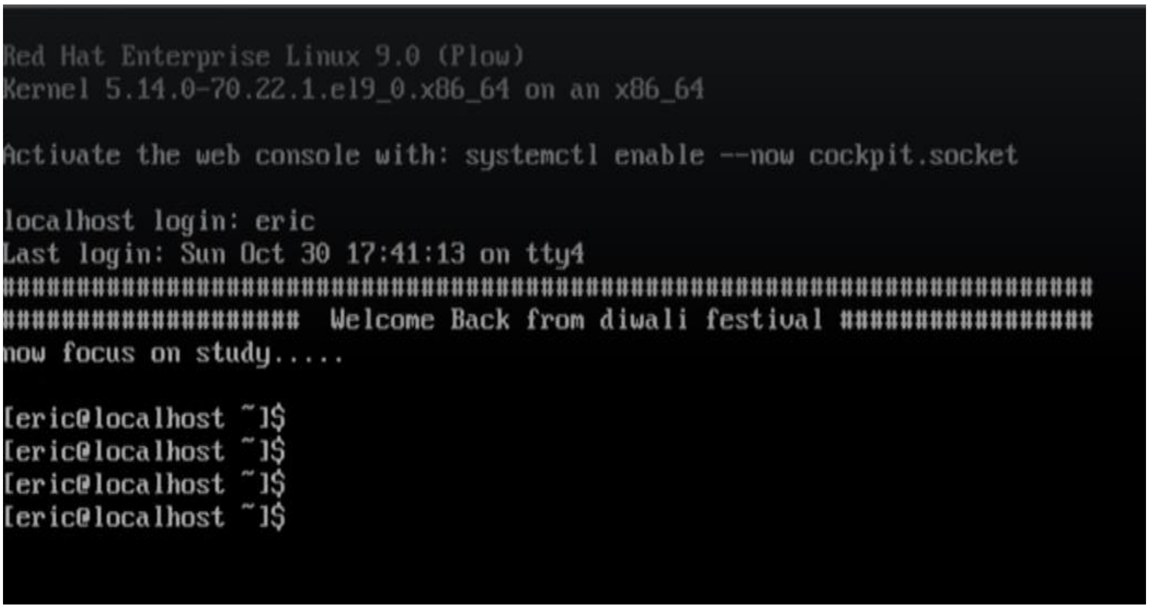
```
[root@localhost ~]# cat /etc/shadow

sshd:!!:19273::::::
chrony:!!:19273::::::
dnsmasq:!!:19273::::::
tcpdump:!!:19273::::::
systemd-oom:!*:19273::::::
vimal:$6$u$3OhhboMUccdNa.kaoerBRk4t70LBDdkcg4UcmW0lk45HMKVwxTlXsrLhrtRFjdk5.Ph4lAr3pn
RqBypUCm.ti.:19273:0:99999:7:::
tom:$6$lbB8wk92PMkS071u$4HzwA1QF351aywulwWpQnJ7LtXTdkGVO5OXNb7k6yJb0DVKTqBzFK4CwkeUWp
.ODFa8mQciycQjYzGFcrImnx1:19273:0:99999:7:::
apache:!!:19280::::::
yash:$6$lLE1wfBp/YGF.Q5J$plO5WOXsE5OnO.NKZGhit2qPgjL5m9u1PxEC8b9.in2WaqZ7r39AEdH9r.vJ
kJJgamVOoYWPznORw.IcTy0S70:19294:0:99999:7:::
pop:$6$Z6FraTlXupaDRLoR$nE0q2elc5gnxTSAdhLX3OIA2x3SXaSJHpk6xIGk3wVWcXIe23JuebF6DtE7bI
jcVaCRG8L/4WDVtqC2tpU7Zl.:19294:0:99999:7:::
jack:$6$d7TclwEZvIG7NsYA$hQUJC4B5DY0Wyp/gHx8bcoqaxHtDNzTEgQjFTkBc5NdyQKs9E/AZzfwukoY.
uXROXE6EC/HMB7uziByMOk8N90:19295:0:99999:7:::
eric:$6$d6vMXoC13aoj1Vnl$it0FZhgQxxx7TJPeEZ4BnR1p6b9oGyB/vYOoRtosTCQdhO5dzjLxGeRwpuBD
2EHixkIXjdyuoWOEJks2oy2V91:19295:0:99999:7:::
[root@localhost ~]#
```

- If we delete the “x” from “/etc/passwd” file of “eric” account



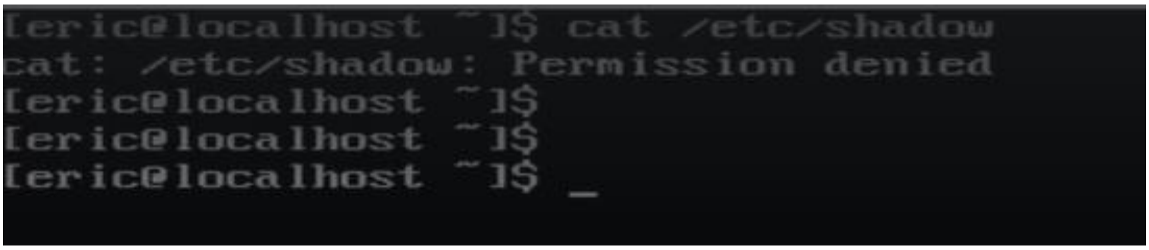
```
pipewire:x:991:986:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
flatpak:x:990:985:User for flatpak system helper:/:/sbin/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
cockpit-ws:x:989:984:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:988:983:User for cockpit-ws instances:/nonexisting:/sbin/nologin
gnome-initial-setup:x:987:982::/run/gnome-initial-setup/:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
chrony:x:986:981::/var/lib/chrony:/sbin/nologin
dnsmasq:x:985:980:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
systemd-oom:x:978:978:systemd Userspace OOM Killer:/:/usr/sbin/nologin
vimal:x:1000:1000:vimal daga:/home/vimal:/bin/bash
tom:x:1001:1001::/home/tom:/bin/bash
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
yash:x:1002:1002::/home/yash:/bin/bash
pop:x:1003:1003::/home/pop:/bin/bash
jack:x:1004:1004::/home/jack:/bin/bash
eric::1005:1005::/home/eric:/bin/bash
~
```

- Now if we try to login to eric account- we can login without password



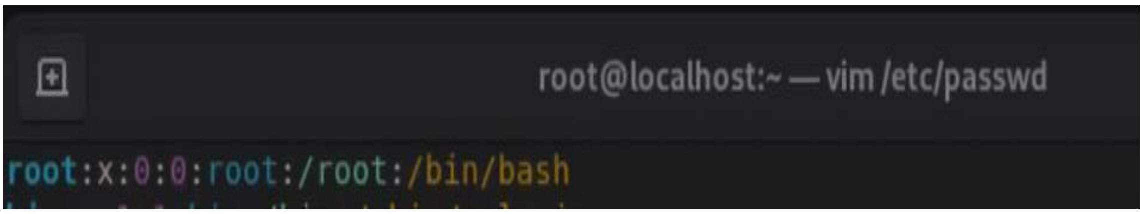
```
Red Hat Enterprise Linux 9.0 (Plow)
Kernel 5.14.0-70.22.1.el9_0.x86_64 on an x86_64

Activate the web console with: systemctl enable --now cockpit.socket

localhost login: eric
Last login: Sun Oct 30 17:41:13 on tty4
###########################################################################
#####################  Welcome Back from diwali festival ##################
now focus on study.....

[eric@localhost ~]$
[eric@localhost ~]$
[eric@localhost ~]$
[eric@localhost ~]$
```

- The “/etc/passwd” file is readable by all the accounts
- The “/etc/shadow” file is not readable by all the accounts – so password is stored here due to security reasons



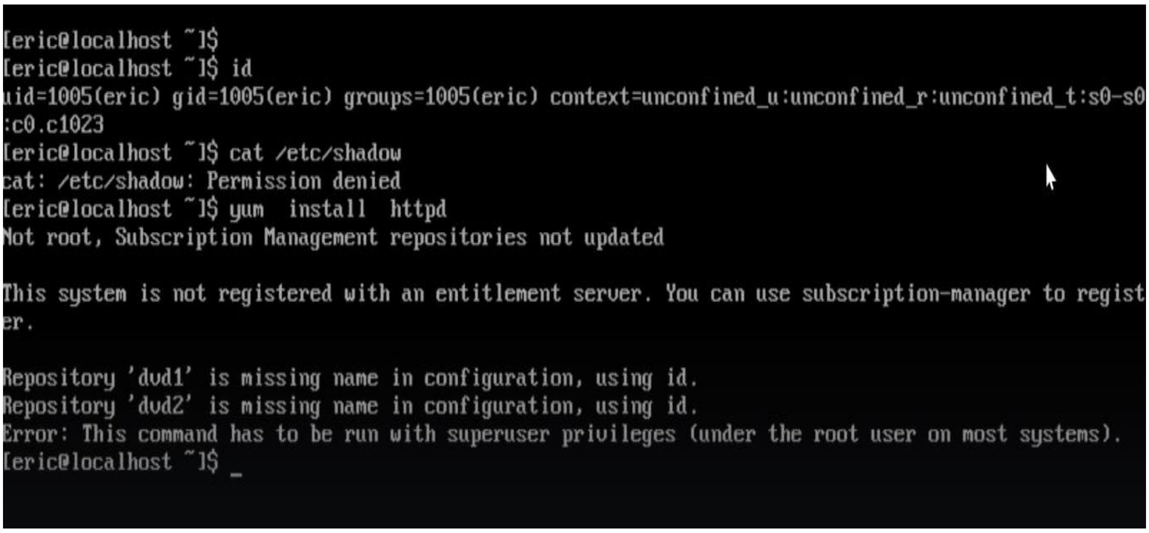
```
[eric@localhost ~]$ cat /etc/shadow
cat: /etc/shadow: Permission denied
[eric@localhost ~]$
[eric@localhost ~]$
[eric@localhost ~]$ _
```

- The third field is the UID- every user has been given a user ID – system recognizes with UID
- The root has the UID “0”



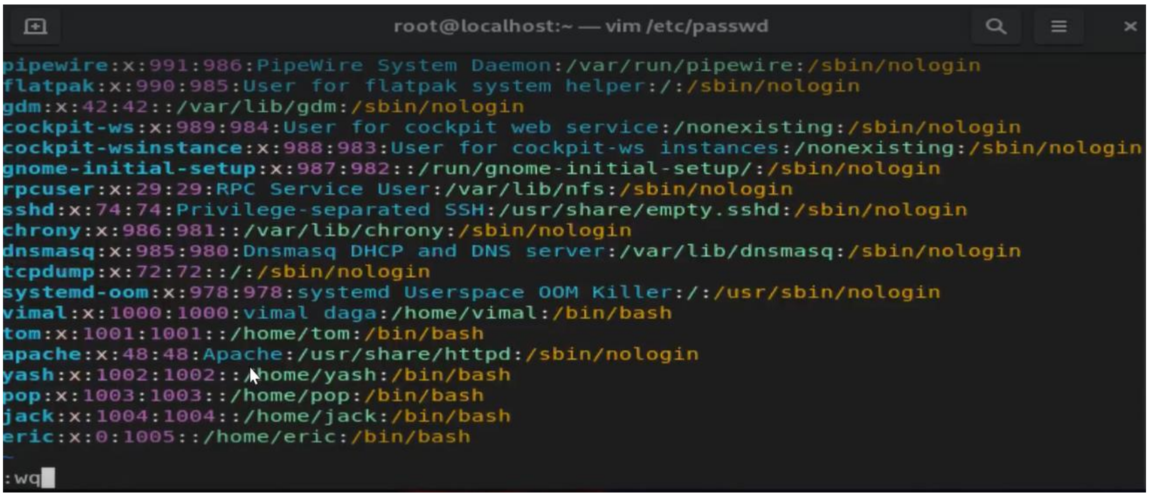
```
root:x:0:0:root:/root:/bin/bash
```

- Any user with ID “0” is the super user – power has come from the UID not from the name “root”
- With UID other than “0” has no power to install a software, create other user accounts etc

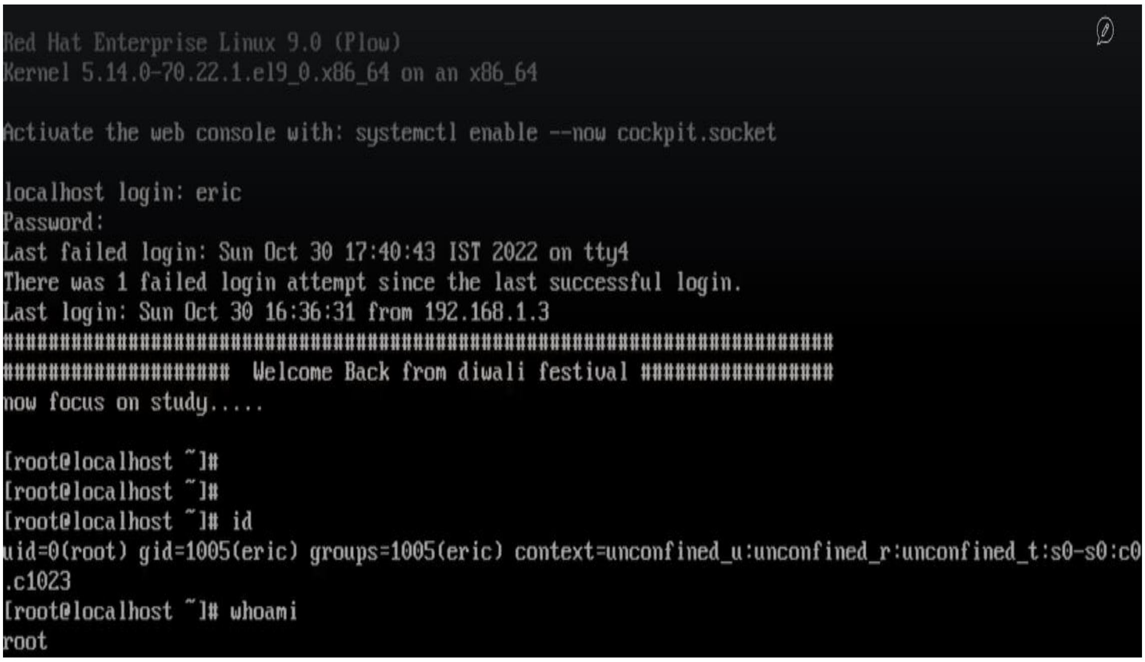


```
[eric@localhost ~]$
[eric@localhost ~]$ id
uid=1005(eric) gid=1005(eric) groups=1005(eric) context=unconfined_u:unconfined_r:unconfined_t:s0-s0
:c0.c1023
[eric@localhost ~]$ cat /etc/shadow
cat: /etc/shadow: Permission denied
[eric@localhost ~]$ yum  install  httpd
Not root, Subscription Management repositories not updated

This system is not registered with an entitlement server. You can use subscription-manager to regist
er.

Repository 'dvd1' is missing name in configuration, using id.
Repository 'dvd2' is missing name in configuration, using id.
Error: This command has to be run with superuser privileges (under the root user on most systems).
[eric@localhost ~]$ _
```

- If the UID of user eric has changed to “0” – the user get unlimited power



```
pipewire:x:991:986:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
flatpak:x:990:985:User for flatpak system helper:/:/sbin/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
cockpit-ws:x:989:984:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:988:983:User for cockpit-ws instances:/nonexisting:/sbin/nologin
gnome-initial-setup:x:987:982::/run/gnome-initial-setup/:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
chrony:x:986:981::/var/lib/chrony:/sbin/nologin
dnsmasq:x:985:980:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
systemd-oom:x:978:978:systemd Userspace OOM Killer:/:/usr/sbin/nologin
vimal:x:1000:1000:vimal daga:/home/vimal:/bin/bash
tom:x:1001:1001::/home/tom:/bin/bash
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
yash:x:1002:1002::/home/yash:/bin/bash
pop:x:1003:1003::/home/pop:/bin/bash
jack:x:1004:1004::/home/jack:/bin/bash
eric:x:0:1005::/home/eric:/bin/bash
~
:wq
```



```
Red Hat Enterprise Linux 9.0 (Plow)
Kernel 5.14.0-70.22.1.el9_0.x86_64 on an x86_64

Activate the web console with: systemctl enable --now cockpit.socket

localhost login: eric
Password:
Last failed login: Sun Oct 30 17:40:43 IST 2022 on tty4
There was 1 failed login attempt since the last successful login.
Last login: Sun Oct 30 16:36:31 from 192.168.1.3
#########################################################################
####################  Welcome Back from diwali festival #################
now focus on study.....

[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# id
uid=0(root) gid=1005(eric) groups=1005(eric) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0
.c1023
[root@localhost ~]# whoami
root
```