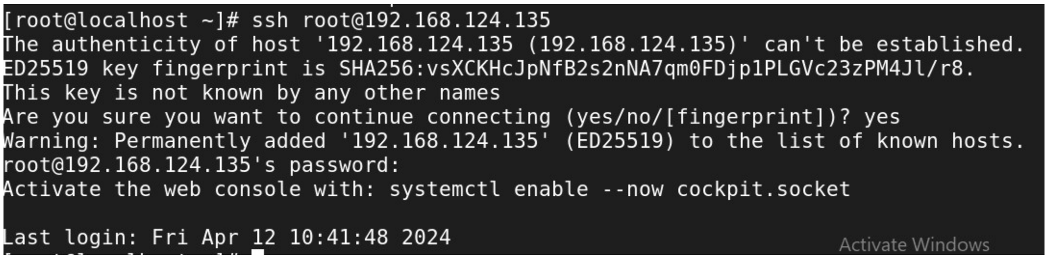
SSH

Step:1

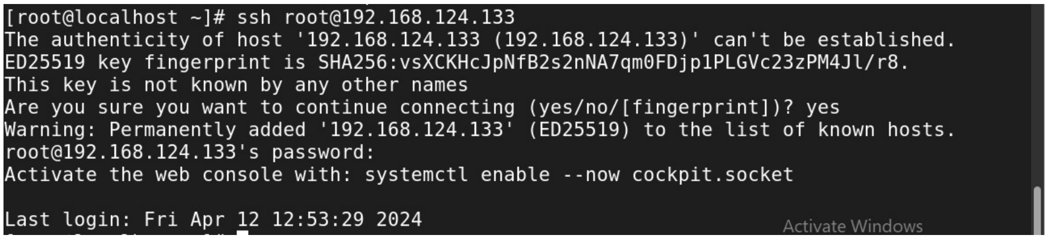
Passwd concept

For server side [client ip]



```
[root@localhost ~]# ssh root@192.168.124.135
The authenticity of host '192.168.124.135 (192.168.124.135)' can't be established.
ED25519 key fingerprint is SHA256:vsXCKHcJpNfB2s2nNA7qm0FDjp1PLGVc23zPM4Jl/r8.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.124.135' (ED25519) to the list of known hosts.
root@192.168.124.135's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Fri Apr 12 10:41:48 2024
```

For client side [serve ip]



```
[root@localhost ~]# ssh root@192.168.124.133
The authenticity of host '192.168.124.133 (192.168.124.133)' can't be established.
ED25519 key fingerprint is SHA256:vsXCKHcJpNfB2s2nNA7qm0FDjp1PLGVc23zPM4Jl/r8.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.124.133' (ED25519) to the list of known hosts.
root@192.168.124.133's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Fri Apr 12 12:53:29 2024
```

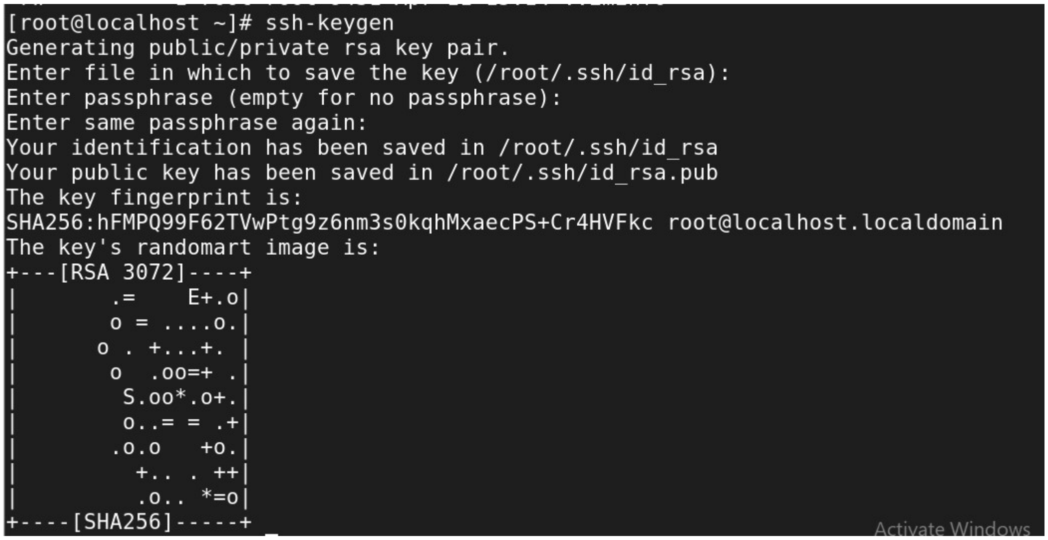
Step: 2

For server side [client ip]

Keygen concept

Step :1

ssh-keygen

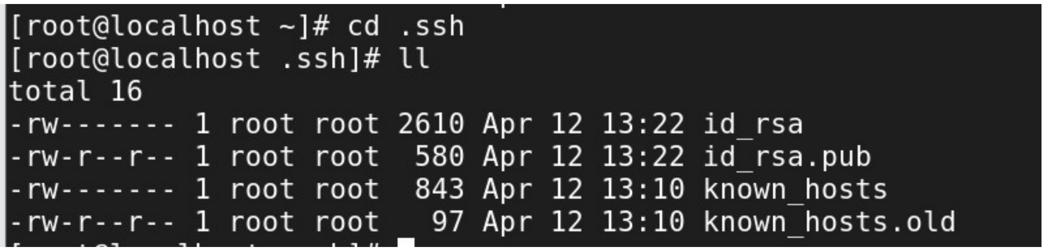


```
[root@localhost ~]# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:hFMPQ99F62TVwPtg9z6nm3s0kqhMxaecPS+Cr4HVFkc root@localhost.localdomain
The key's randomart image is:
+---[RSA 3072]----+
|       .=    E+.o|
|       o = ....o.|
|      o . +...+. |
|       o  .oo=+ .|
|        S.oo*.o+.|
|        o..= = .+|
|       .o.o   +o.|
|         +.. . ++|
|         .o.. *=o|
+----[SHA256]-----+
```

Step 2

cd .ssh

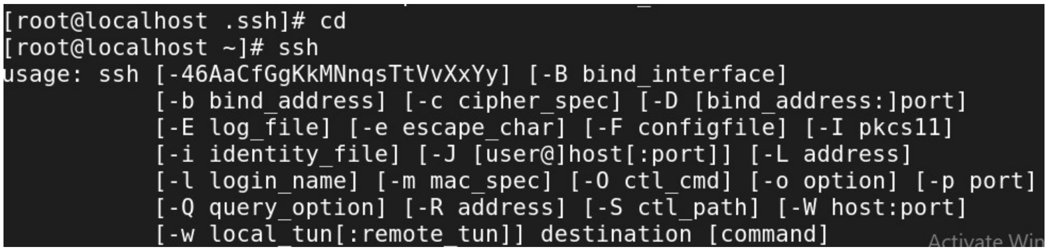
ll



```
[root@localhost ~]# cd .ssh
[root@localhost .ssh]# ll
total 16
-rw------- 1 root root 2610 Apr 12 13:22 id_rsa
-rw-r--r-- 1 root root  580 Apr 12 13:22 id_rsa.pub
-rw------- 1 root root  843 Apr 12 13:10 known_hosts
-rw-r--r-- 1 root root   97 Apr 12 13:10 known_hosts.old
```

cd

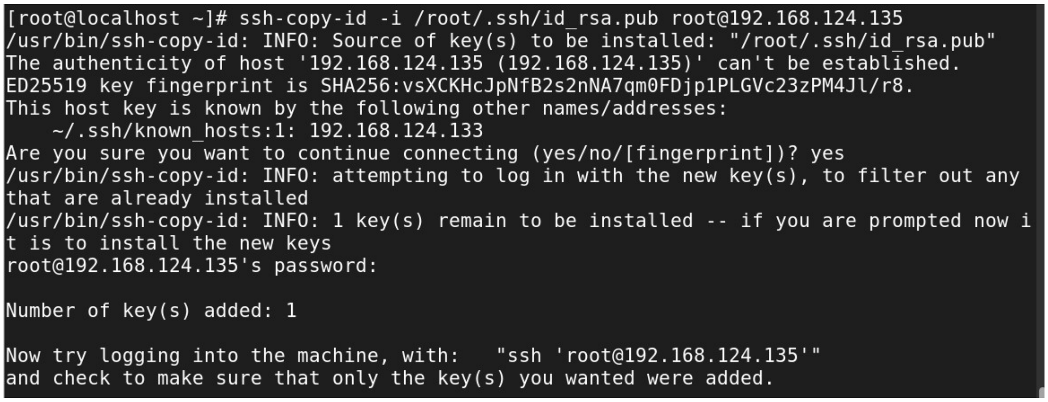
ssh



```
[root@localhost .ssh]# cd
[root@localhost ~]# ssh
usage: ssh [-46AaCfGgKkMNnqsTtVvXxYy] [-B bind_interface]
           [-b bind_address] [-c cipher_spec] [-D [bind_address:]port]
           [-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]
           [-i identity_file] [-J [user@]host[:port]] [-L address]
           [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
           [-Q query_option] [-R address] [-S ctl_path] [-W host:port]
           [-w local_tun[:remote_tun]] destination [command]
```

Step :3

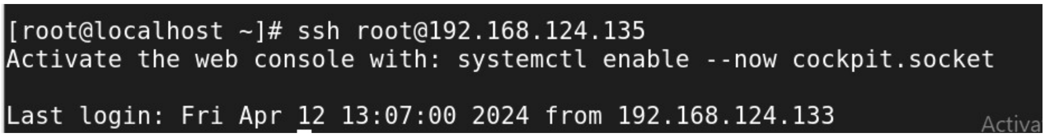
ssh-copy-id -i /root/.ssh/id_rsa.pub root@192.168.124.135



```
[root@localhost ~]# ssh-copy-id -i /root/.ssh/id_rsa.pub root@192.168.124.135
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
The authenticity of host '192.168.124.135 (192.168.124.135)' can't be established.
ED25519 key fingerprint is SHA256:vsXCKHcJpNfB2s2nNA7qm0FDjp1PLGVc23zPM4Jl/r8.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: 192.168.124.133
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 i
t is to install the new keys
root@192.168.124.135's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'root@192.168.124.135'"
and check to make sure that only the key(s) you wanted were added.
```

Step:4

ssh root@192.168.124.135

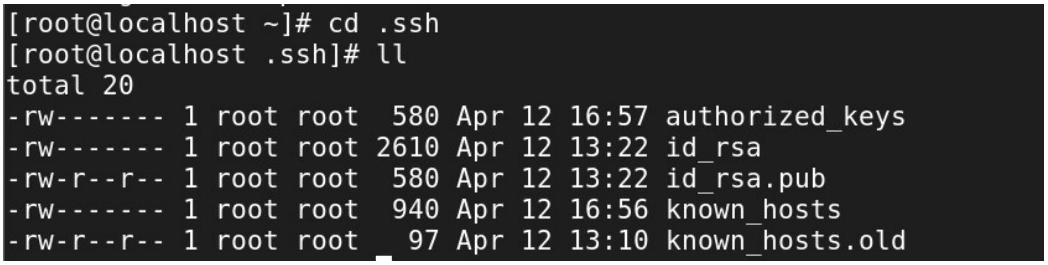


```
[root@localhost ~]# ssh root@192.168.124.135
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Fri Apr 12 13:07:00 2024 from 192.168.124.133
```

Step :5

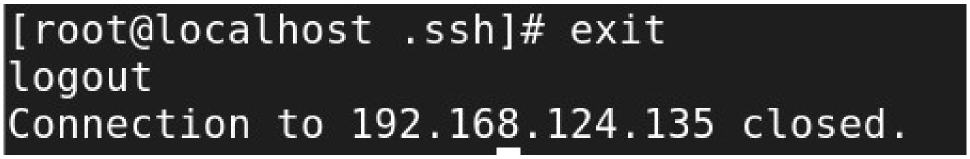
cd .ssh

ll



```
[root@localhost ~]# cd .ssh
[root@localhost .ssh]# ll
total 20
-rw------- 1 root root  580 Apr 12 16:57 authorized_keys
-rw------- 1 root root 2610 Apr 12 13:22 id_rsa
-rw-r--r-- 1 root root  580 Apr 12 13:22 id_rsa.pub
-rw------- 1 root root  940 Apr 12 16:56 known_hosts
-rw-r--r-- 1 root root   97 Apr 12 13:10 known_hosts.old
```

Exit



```
[root@localhost .ssh]# exit
logout
Connection to 192.168.124.135 closed.
```

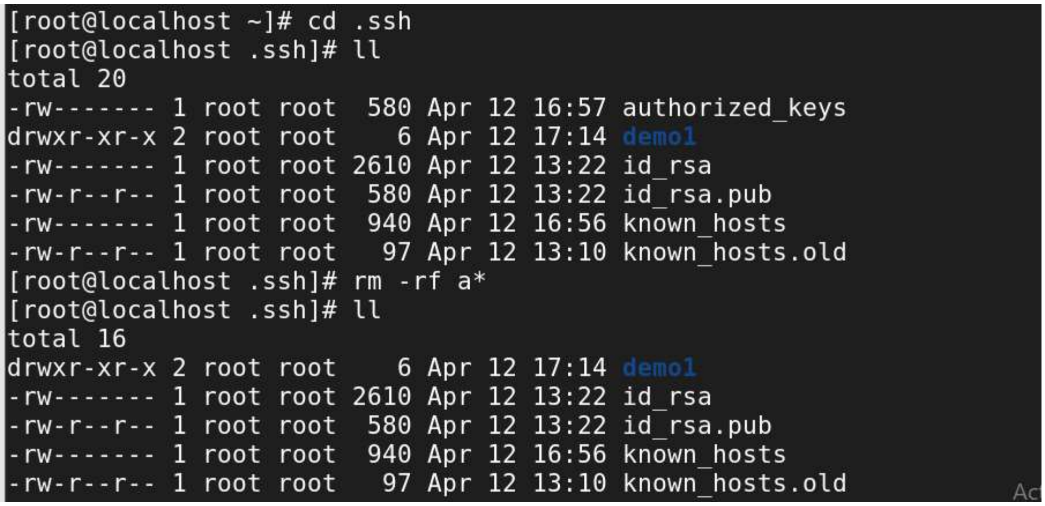
Step:6

Ls -la

Then you delete Authorised keys

rm –rf authorized keys

rm –rf x*

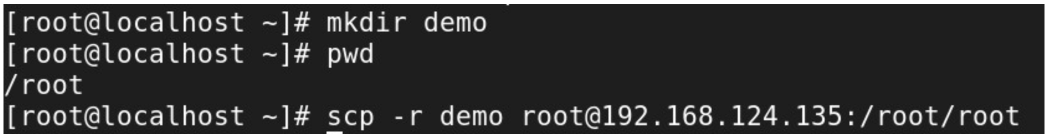


```
[root@localhost ~]# cd .ssh
[root@localhost .ssh]# ll
total 20
-rw------- 1 root root  580 Apr 12 16:57 authorized_keys
drwxr-xr-x 2 root root    6 Apr 12 17:14 demo1
-rw------- 1 root root 2610 Apr 12 13:22 id_rsa
-rw-r--r-- 1 root root  580 Apr 12 13:22 id_rsa.pub
-rw------- 1 root root  940 Apr 12 16:56 known_hosts
-rw-r--r-- 1 root root   97 Apr 12 13:10 known_hosts.old
[root@localhost .ssh]# rm -rf a*
[root@localhost .ssh]# ll
total 16
drwxr-xr-x 2 root root    6 Apr 12 17:14 demo1
-rw------- 1 root root 2610 Apr 12 13:22 id_rsa
-rw-r--r-- 1 root root  580 Apr 12 13:22 id_rsa.pub
-rw------- 1 root root  940 Apr 12 16:56 known_hosts
-rw-r--r-- 1 root root   97 Apr 12 13:10 known_hosts.old
```

Step :7

mkdir demo

scp -r demo root@192.168.124.135:/root/root

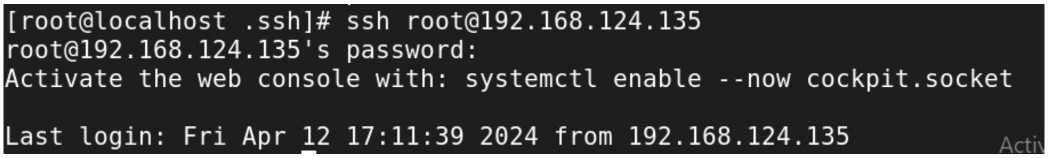


```
[root@localhost ~]# mkdir demo
[root@localhost ~]# pwd
/root
[root@localhost ~]# scp -r demo root@192.168.124.135:/root/root
```

step :8

ssh root@192.168.124.135

ll



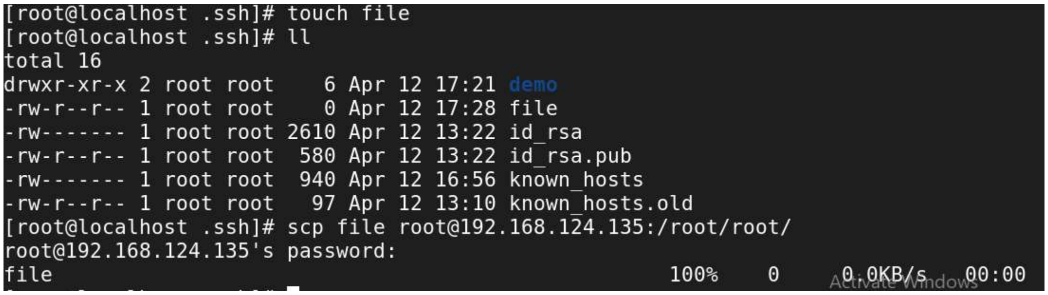
```
[root@localhost .ssh]# ssh root@192.168.124.135
root@192.168.124.135's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Fri Apr 12 17:11:39 2024 from 192.168.124.135
```

Step :8

touch file

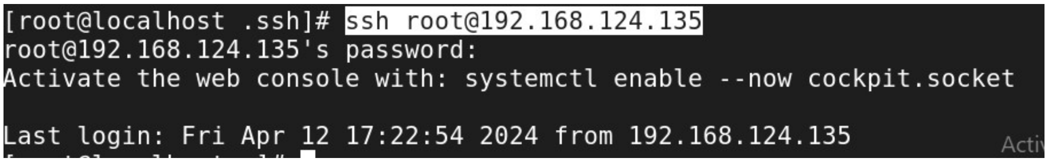
ll

scp file root@192.168.124.135:/root/root



```
[root@localhost .ssh]# touch file
[root@localhost .ssh]# ll
total 16
drwxr-xr-x 2 root root    6 Apr 12 17:21 demo
-rw-r--r-- 1 root root    0 Apr 12 17:28 file
-rw------- 1 root root 2610 Apr 12 13:22 id_rsa
-rw-r--r-- 1 root root  580 Apr 12 13:22 id_rsa.pub
-rw------- 1 root root  940 Apr 12 16:56 known_hosts
-rw-r--r-- 1 root root   97 Apr 12 13:10 known_hosts.old
[root@localhost .ssh]# scp file root@192.168.124.135:/root/root/
root@192.168.124.135's password:
file                                                  100%    0     0.0KB/s   00:00
```

ssh root@192.168.124.135

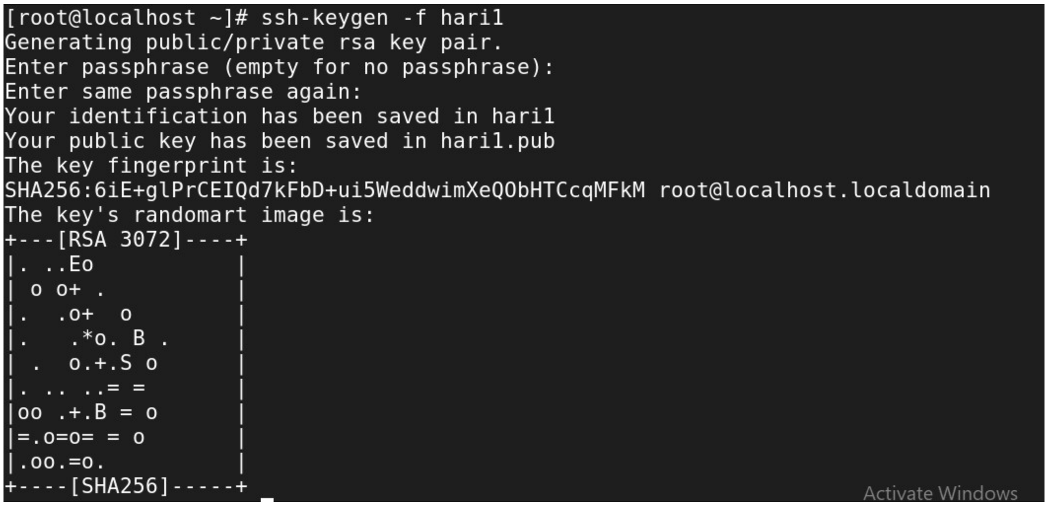


```
[root@localhost .ssh]# ssh root@192.168.124.135
root@192.168.124.135's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Fri Apr 12 17:22:54 2024 from 192.168.124.135
```

Step3method

Step:1

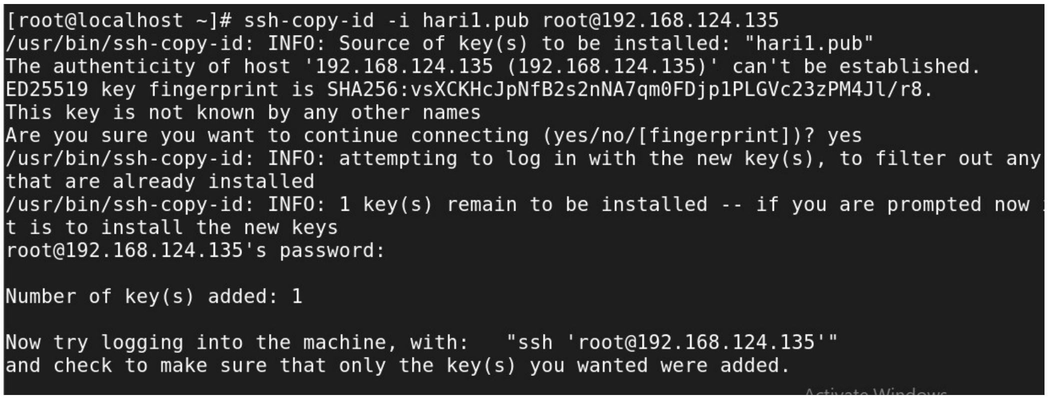
ssh-keygen –f hari1



```
[root@localhost ~]# ssh-keygen -f hari1
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in hari1
Your public key has been saved in hari1.pub
The key fingerprint is:
SHA256:6iE+glPrCEIQd7kFbD+ui5WeddwimXeQObHTCcqMFkM root@localhost.localdomain
The key's randomart image is:
+---[RSA 3072]----+
|. ..Eo           |
| o o+ .          |
|.  .o+  o        |
|.   .*o. B .     |
| .  o.+.S o      |
|. .. ..= =       |
|oo .+.B = o      |
|=.o=o= = o       |
|.oo.=o.          |
+----[SHA256]-----+
```

Step :2

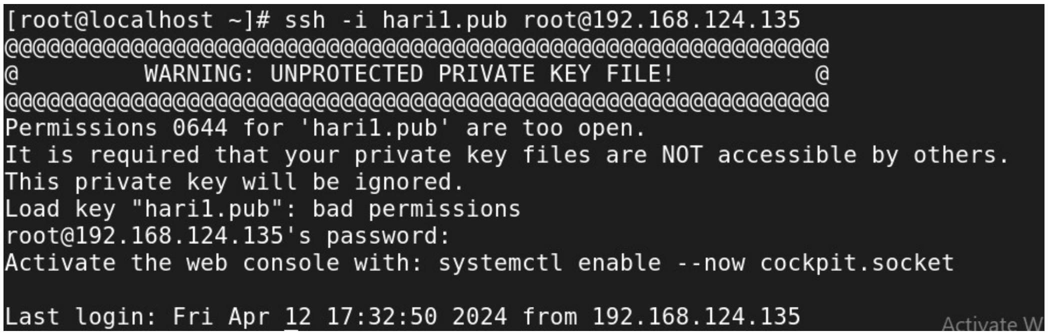
ssh-copy-id -i hari1.pub root@192.168.124.135



```
[root@localhost ~]# ssh-copy-id -i hari1.pub root@192.168.124.135
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "hari1.pub"
The authenticity of host '192.168.124.135 (192.168.124.135)' can't be established.
ED25519 key fingerprint is SHA256:vsXCKHcJpNfB2s2nNA7qm0FDjp1PLGVc23zPM4Jl/r8.
This key is not known by any other names
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
t is to install the new keys
root@192.168.124.135's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'root@192.168.124.135'"
and check to make sure that only the key(s) you wanted were added.
```

Step:3

ssh -i hari1.pub root@192.168.124.135



```
[root@localhost ~]# ssh -i hari1.pub root@192.168.124.135
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for 'hari1.pub' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "hari1.pub": bad permissions
root@192.168.124.135's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Fri Apr 12 17:32:50 2024 from 192.168.124.135
```