SSH login to remoter server using private Key

1) Let's assume there are 2 servers a) Kali Linux and ubuntu server
2) To be able to access one server from another we must first setup openssh
3) **-Sudo apt install openssh-server** //this will install ssh server in your server
4) **-Service ssh start** // will start the ssh server
5) Now you will be able to connect to the server you have started the ssh from another
6) Using the command **-ssh kali_user@ipadress**, I can connect to kali linux from ubuntu

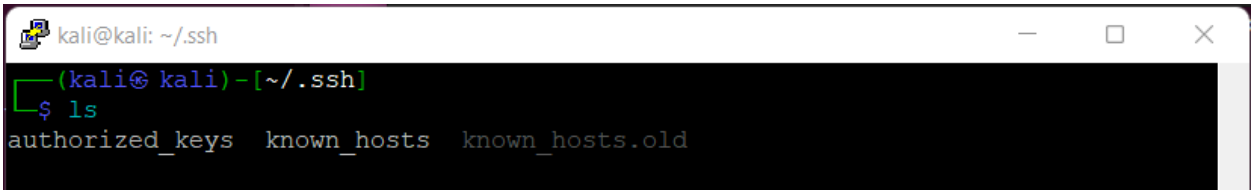
```
osboxes@osboxes:~/Desktop$ ssh kali@192.168.20.140
kali@192.168.20.140's password:
Linux kali 6.0.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.0.7-1kali1 (2022-11
-07) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Dec 24 12:23:22 2022 from 192.168.20.140
┌──(kali㉿kali)-[~]
└─$ whoami
kali
```

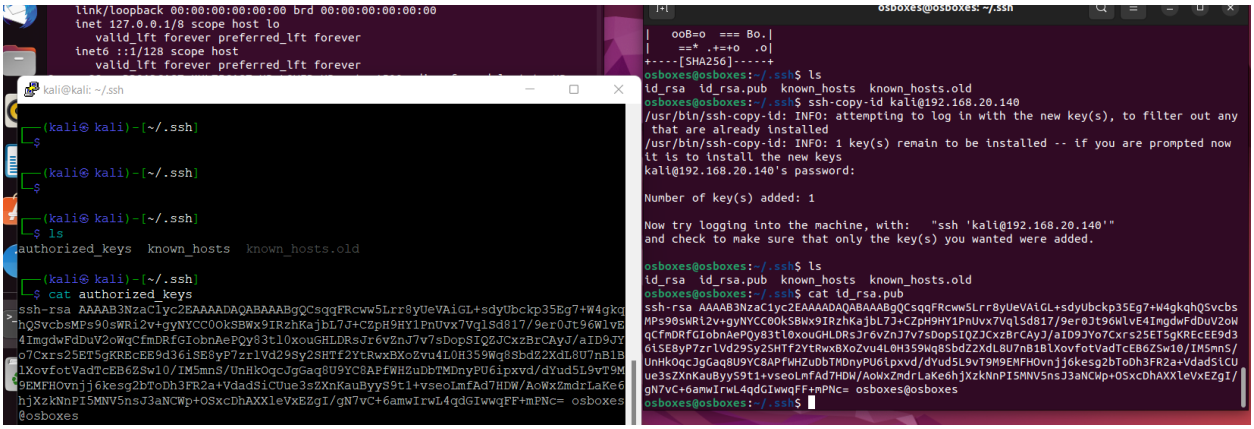
7) To login using private keys without knowing the password of kali Linux follow the below process
8) I have used **-ssh-keygen** command to generate both private and public keys in server1(ubuntu), generated id_rsa(private key) and id_rsa.pub(public key)

```
osboxes@osboxes:~/.ssh$ ls
known_hosts  known_hosts.old
osboxes@osboxes:~/.ssh$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/osboxes/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/osboxes/.ssh/id_rsa
Your public key has been saved in /home/osboxes/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:JL+qFLxvOM3pyI3lfe2YjT6WRzzPE9aG2eZPlmw4KXc osboxes@osboxes
The key's randomart image is:
+---[RSA 3072]----+
|                 |
|                 |
|      . .        |
|   .   +         |
|    o   S  .   = |
|     o   .  + O *|
|    o+...  = X Eo|
|   ooB=o  === Bo.|
|    ==* .+=+o  .o|
+----[SHA256]-----+
osboxes@osboxes:~/.ssh$ ls
id_rsa  id_rsa.pub  known_hosts  known_hosts.old
osboxes@osboxes:~/.ssh$
```

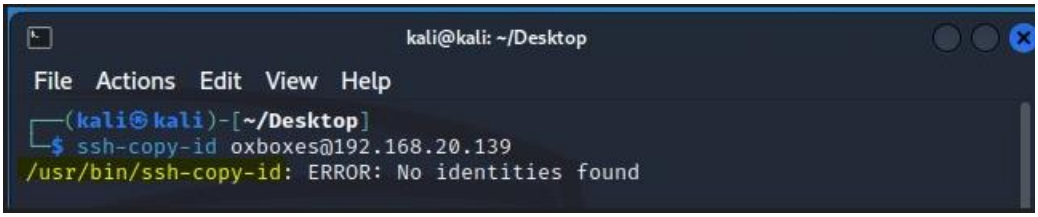
9) Now copy your public key id_rsa.pub to server2(kali linux) using the command **-ssh-copy-id username@remote_host** and if the public key existing in ubuntu then it will be copied to server2

```
osboxes@osboxes:~/.ssh$ ssh-copy-id kali@192.168.20.140
/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
kali@192.168.20.140's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'kali@192.168.20.140'"
and check to make sure that only the key(s) you wanted were added.
```





10) As you can see from the above images, we can see a new file name authorized_keys in server2 and it is the same
11) **Fun fact:** what happens if you try to copy the public key from server2 to server1? It won't work because we haven't generated public key yet in server2



12) Perfect we can login to server2(Kali Linux) from server1(ubuntu)

```
osboxes@osboxes:~/.ssh$ ssh kali@192.168.20.140
Linux kali 6.0.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.0.7-1kali1 (2022-11-07) x8
6_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Dec 24 12:23:57 2022 from 192.168.20.139
┌──(kali㉿kali)-[~]
```