

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.
```

```
kali@kali: ~/.ssh
(kali@kali)~[~/.ssh]
$ ls
authorized_keys  known_hosts  known_hosts.old
```

```
Link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
    valid_lft forever preferred_lft forever

(kali@kali)~[~/.ssh]
$ ls
authorized_keys  known_hosts  known_hosts.old

(kali@kali)~[~/.ssh]
$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCSqGFRcw5Lrr8yUeVAiGL+sdYUbcKp35Eg7+4gkqhQ5vcbS
MPs90sWRi2v+gyNYCC00KSBWx9IRzhKajbL7J+C2pH9HY1PnUvX7Vq1Sd817/9er0Jt96W1vE
4ImgdwFduV2oWqCfmDRfGIobnAePQy83t10xouGHLDRsJr6vZnJ7v7sDopSIQ2JCxzBrCayJ/aID9JY
o7Cxrs25ET5gRRBcEB9d36iSE8yP7zr1Vd29Sy2SHTf2YtRwxEXo2vu4L0H359Wq8Sbd2XdL8U7nB1B
1XovfotVadTcEB6ZSw10/IM5mns/UnHkQcJgGag8U9YC8AFWHZuDbTMDnyPU6ipxvd/dYud5L9vt9M
9EMFHOvnj6kesg2bToDh3FR2a+VdadSiCUue3s2XnKauByys9t1+vseoLmfAd7HDW/AoWxZmdrLaKe6
hjXzkNnPI5MNV5nsJ3aNCwp+OSxcDHAXX1eVxEZgI/gN7vC+6amw1rwL4qdGIwwqFF+mPNC= osboxes
@osboxes

osboxes@osboxes: ~/.ssh$ ls
id_rsa  id_rsa.pub  known_hosts  known_hosts.old
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

```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)~[~/Desktop]
$ ssh-copy-id oxboxes@192.168.20.139
/usr/bin/ssh-copy-id: ERROR: No identities found
```

- 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) 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 12:23:57 2022 from 192.168.20.139
└─(kali@kali)-[~]
```