Disabling password logins for SSH is a crucial step in securing your remote server.
Instead of passwords, SSH keys, which are a form of public key encryption, should be used.
SSH keys consist of the public key, theoretically similar to the concept of usernames, and a private key, something resembling a 2048 character-long password.
SSH private keys are generated on the respective user's device and are encrypted with a passphrase and ssh-agent.
SSH-agents take charge of establishing a connection with the SSH server, forwarding your keys.

Disable SSH password login

```
ubuntuSERVER$ sudo nano /etc/ssh/sshd_config
>>>
PasswordAuthentication no
(PubkeyAuthentication no) by default
>>>
ubuntuSERVER$ sudo systemctl restart ssh
```

Password login attempt(even with correct password) :

```
┌──(deusxmachina㉿pwner3000)-[~]
└─$ sudo ssh ubuntu@10.0.2.7
+-+-+-+-+-+-+-+-+-+-+-+-+-++-+-+-+-+-+-+-+-+-+-+-+-+-+-+-++-+-+-+
                        LINUXVMIMAGES.COM
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                    User Name: ubuntu
                    Password:  ubuntu (sudo su -)
ubuntu@10.0.2.7's password:
Permission denied, please try again.
ubuntu@10.0.2.7's password:
Permission denied, please try again.
ubuntu@10.0.2.7's password:
ubuntu@10.0.2.7: Permission denied ().
```

*optional : outright reject all other methods of login attempts and force public key-based authentication

```
ubuntuSERVER$ sudo nano /etc/ssh/sshd_config
>>>
PasswordAuthentication no
AuthenticationMethods publickey
PubkeyAuthentication yes
>>>
```

Password login attempt :

```
┌──(deusxmachina㉿pwner3000)-[~]
└─$ sudo ssh ubuntu@10.0.2.7
+-+-+-+-+-+-+-+-+-+-+-+-+-++-+-+-+-+-+-+-+-+-+-+-+-+-+-+-++-+-+-+
                        LINUXVMIMAGES.COM
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                    User Name: ubuntu
                    Password:  ubuntu (sudo su -)
ubuntu@10.0.2.7: Permission denied (publickey).
```

Generate SSH keys

Use the command ‘ssh-keygen’ on Unix devices to create SSH keys. The passphrase that is asked is to encrypt the local key file, not for authentication with the SSH server.
The private key is saved by default as ~/.ssh/id_rsa
The public key is saved by default as ~/.ssh/id_rsa.pub

remoteDEVICE$ ssh-keygen

```
Generating public/private rsa key pair.
Enter file in which to save the key (/home/deusxmachina/.ssh/id_rsa):
Enter passphrase (empty for no passphrase): P@ssw0rd
Enter same passphrase again: P@ssw0rd
Your identification has been saved in /home/deusxmachina/.ssh/id_rsa
Your public key has been saved in /home/deusxmachina/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:3CsWo3CiDjt+z6Ld/yHiD47eSPMtWNFPc9a7z246+G0 deusxmachina@pwner3000
The key's randomart image is:
+---[RSA 3072]----+
|                 |
|                 |
|      .     .    |
|     . o + o .   |
|    o o S =   .  |
|   . = . + . .   |
|. .ooo..o..  . . |
|.+o+@.+..... ooE |
|o+=oO++..   .oB= |
+----[SHA256]-----+
```

While the private key resides on the connecting device, the public key must be uploaded to the server so that they can verify your identity. *You will need to have password login enabled one last time to upload said public key.*
SSH servers usually keeps a list of authorized users in ~/.ssh/authorized_keys
We can upload our public key manually using the ‘ssh-copy-id’ command :

remoteDEVICE$ ssh-copy-id -i ~/.ssh/id_rsa.pub user@host

```
┌──(deusxmachina㉿pwner3000)-[~]
└─$ ssh-copy-id -i ~/.ssh/id_rsa.pub ubuntu@10.0.2.7
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/deusxmachina/.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 key
s
+-+-+-+-+-+-+-+-+-+-+-+-++-+-+-+-+-+-+-+-+-+-+-+-++-+-+-+
                     LINUXVMIMAGES.COM
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                User Name: ubuntu
                Password:  ubuntu (sudo su -)
ubuntu@10.0.2.7's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'ubuntu@10.0.2.7'"
and check to make sure that only the key(s) you wanted were added.
```

Check our uploaded public key in the SSH server

ubuntuSERVER$ cat ~/.ssh/authorized_keys

```
ubuntu@ubunu2004:~/.ssh$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC2F0O8btuWJlmy4GkgkmdAgTdbYqBSScWTSrVmI2RN
t694WlcezIe/YyR2YWT5HPRxUAKSsIUuByoojcPkwIEN+BfIR52+CP0fRe4w8YuNKjJEqq87CbunXhM7
51aGCa1nKxx2NpcezEcq1hjTlzELSFHKajk5pUusx4Rx7SBM0vfB9Lrkl3vL7DRwBlrvuhZaeBXMDgHv
D25fKLIWluBg+1BEf96kp5DpQ6RD4qa1gBYUBhwGDF0jLa8t9ceBReRBrx7f64OLwMGGEaWbU9bLe8Ft
F8prPE08ZFSvIxgg5WRxGmcf3f3+7uK8NomR2xEERAwwmZ8SIrRYo9OEAL9CEzMk1dPkhp7WHkrZ4bOU
Xj6T26AklmT1XSMHZMTvqvAyPWidEnxCKgGur5EUxXqXnxHVrAhTAhI87vW9CSYjiKYoGjKjK4r/XAUY
XXvjzz689FxTvK1xPUI+Mo9ZajMZukrLICJXoLhS9g5fDdU3y4NwLXQqdLxZGOcZ/RBybZ0= deusxma
china@pwner3000
```

SSH key login

remoteDEVICE$ ssh -i ~/.ssh/id_rsa user@host

```
┌──(deusxmachina㉿pwner3000)-[~]
└─$ ssh -i ~/.ssh/id_rsa ubuntu@10.0.2.7
+-+-+-+-+-+-+-+-+-+-+-+-++-+-+-+-+-+-+-+-+-+-+-+-+-+-++-+-+-+
                    LINUXVMIMAGES.COM
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                  User Name: ubuntu
                  Password:  ubuntu (sudo su -)
Enter passphrase for key '/home/deusxmachina/.ssh/id_rsa': P@ssw0rd
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-26-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


0 updates can be installed immediately.
0 of these updates are security updates.

Your Hardware Enablement Stack (HWE) is supported until April 2025.
+-+-+-+-+-+-+-+-+-+-+-+-++-+-+-+-+-+-+-+-+-+-+-+-+-+-++-+-+-+
                    LINUXVMIMAGES.COM
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                  User Name: ubuntu
                  Password:  ubuntu (sudo su -)
Last login: Fri Apr 24 00:39:01 2020 from 192.168.0.240
ubuntu@ubunu2004:~$
```