Passwordless Authentication using ssh

Pre request:

1. Have two machines one will be ssh client and the other will be ssh server or remote server
2. ssh needs to be installed in ssh remote server

Steps:

3. Login to your ssh client as root user and generate public & private key using the command "ssh-keygen"
4. Click enter to save the key in default location
5. In enter the passphrase just click enter that is empty passphrase(if you wish to make your key secure you can provide the passphrase)
6. Now your keys should be generated
7. Now copy the public key to your remote server using the command "ssh-copy-id -i /root/.ssh/id_rsa.pub root@"your remote ip"
8. Now public key should have been added now
9. Now try to login remote server using ssh root@"youripaddress" it should not prompt for the password you should be logged in successfully

The local server is **root@192.168.56.103**
The remote server is **root@192.168.56.101**

```
root@192.168.56.103's password:
Last login: Sat Aug 12 14:58:19 2023
[root@localhost ~]# cd .ssh
[root@localhost .ssh]# ls
[root@localhost .ssh]# cd
[root@localhost ~]# cd .ssh
[root@localhost .ssh]# ls
[root@localhost .ssh]# cd
[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:KUYM+LnhGStXGaqRBLe4HJ9a0xNUP9Q2gjV/jLyhw4U root@localhost.localdomain
The key's randomart image is:
+---[RSA 2048]----+
|........o+.      |
| oo..o..o.=+o    |
|.o.o +oo Eo*.o   |
|..= O.+ ..+ +    |
|.. O Xo S+ .     |
|  = B            |
```

```
[root@localhost .ssh]# ssh-copy-id -i /root/.ssh/id_rsa.pub root@192.168.56.101
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
The authenticity of host '192.168.56.101 (192.168.56.101)' can't be established.
ECDSA key fingerprint is SHA256:krhF3z6WR+DSpCMaLbVJUgbVDS3CJc70R0uyGyPNw3E.
ECDSA key fingerprint is MD5:be:10:33:f2:4c:a7:86:f0:32:25:ce:87:50:e8:1f:82.
Are you sure you want to continue connecting (yes/no)? 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 it is to install the new keys
root@192.168.56.101's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'root@192.168.56.101'"
and check to make sure that only the key(s) you wanted were added.

[root@localhost .ssh]# ssh root@192.168.56.101
Last login: Sat Aug 12 20:37:53 2023 from 192.168.56.1
[root@localhost ~]#
```