Lab b. Enable Key Based Authentication between VMs

Objectives

- Generate Private/Public Key pair using ssh-keygen command
- Copy Public key to the machine to which you want to connect without using password.
- Use ssh command to gain the access to a VM from other VM using key based authentication.
- Using Puttygen to convert Private Key to PPK Format
- Connect prom windows machine to a VM using PPK format Key

Pre-Requisite

- Two VMs one as "***server***" and other as "***tester1***"
- Networking between two machines using ***Host only Adaptor***.
- Root password of both machines. If you are using VM provided by instructor, the root password is "***oracle***"
- **Clear Existing Keys and folder on both VMs**
- Start both machines if not already running, login as root and delete ***.ssh*** folder from both machines by executing following commands on ***server*** and ***tester1.***

  # *cd ~*

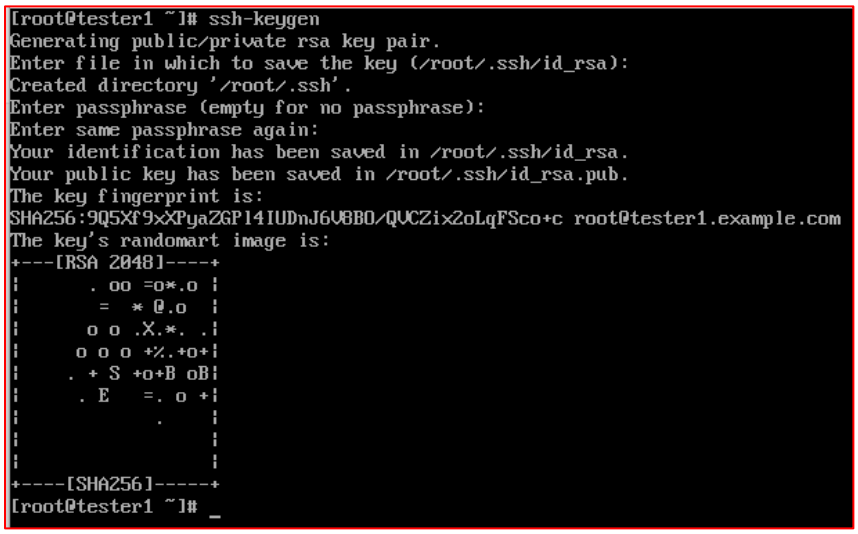
  # *rm -rf .ssh/*

Sequence 1. Create and use SSH Keys

Watch the video https://www.youtube.com/watch?v=A9CNbrwhcJs to know about SSH Key pair.

1. Start both machines if not already running, login as root and follow these steps to generate the SSH Key pairs
   a. On ***tester1***

      # ssh-keygen



b. On ***server***

ssh-keygen

```
[root@server ~]# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Created directory '/root/.ssh'.
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:z2t0m9++UZJIOv1Wf0l6iIEENIV5D/2Keuc2+ynl3jU root@server.example.com
```

2. Once the Keys are generated you need to copy your public key to other machine. Copy the public key in a notepad file. You will need this Key in Lab 4 also.
   # cat .ssh/id_rsa.pub
   Paste the contents of the output to a notepad file and save it for later use in Lab 4 and other labs.
3. Copy public key from ***server*** to ***tester1***

```
[root@server ~]# ssh-copy-id root@tester1
The authenticity of host 'tester1 (10.10.0.101)' can't be established.
ECDSA key fingerprint is SHA256:pUFGCoi69FdDrgVe5h2LyqgaxWHzwF4eYbTKDZner0Y.
ECDSA key fingerprint is MD5:69:56:98:b0:55:2d:83:d7:f2:ad:93:fd:6f:21:e4:c8.
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 filt
out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are pro
ed now it is to install the new keys
root@tester1's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'root@tester1'"
and check to make sure that only the key(s) you wanted were added.

[root@server ~]#
```

4. Copy public key from ***tester1*** to ***server***

```
[root@tester1 ~]# ssh-copy-id root@server
/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
The authenticity of host 'server (10.10.0.100)' can't be established.
ECDSA key fingerprint is SHA256:LE9tPxfj9UoZHnhm0dURulyZUDTQI9B9hlrr6SORo8Y.
ECDSA key fingerprint is MD5:ef:ca:27:db:c4:8f:24:4c:bd:1b:c8:3b:0e:10:40:4c.
Are you sure you want to continue connecting (yes/no)? yes
/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out a
 installed
/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted no
the new keys
root@server's password:

Number of key(s) added: 1

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

5. Now try to ssh from both machines to connect to other machine.
   a. SSH from ***tester1*** to ***server***

 # ssh server

```
[root@tester1 ~]# ssh server
Last login: Wed Feb  3 06:16:08 2021
[root@server ~]#
```

b. SSH from ***server*** to ***tester1***

 # ssh root@tester1

```
[root@server ~]# ssh root@tester1
Last login: Wed Feb  3 06:14:52 2021
[root@tester1 ~]#
```

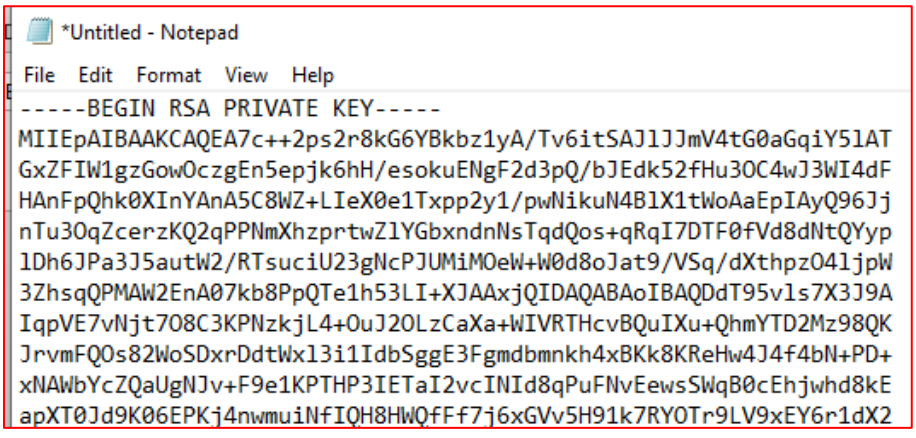
6. You should be able to use ***ssh*** command without password.
7. To use putty to connect any of the VM, you first have to convert the Private Key of that machine to PPK format. For example to connect to ***tester1***, login to ***server*** VM where you have the private key which you have used to connect to ***tester1***. Use cat command to copy the content of the ***private key*** as follows

cd

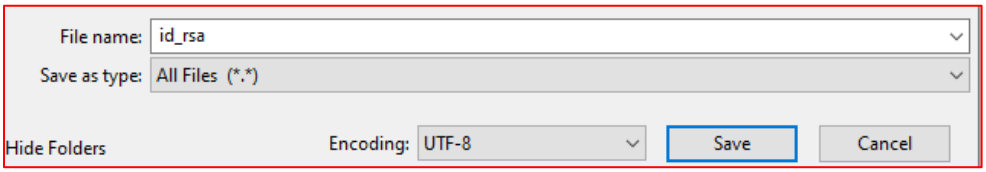
cat .ssh/id_rsa

```
[root@server ~]# cat .ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAubTGDBl0AftFKTC6TiMith7jpoSr2mIAPhTDdPqTbDnfL7PA
p1CDy4xB1VjiB/GZYGG0eSjs6dbaoiuykMoNB6i5ddqqlJ/QTcrz+YduFjpxkcmO
F+NZ9jUAZdinZRej4l0lEdYI3F7g9vWoZb+KVv3jk1aJdW4vINULz9Sv337//pLF
69DmGFrEbHFQ4hsQEmjqkY7d/GU01HSdl05LDzDVC4JHHVORz2HimHj8gcUToC/T
4C6AwlWHZRFpHhDlgv+5NKoLbxCkTA+WZ8jOtV6BksgmYmYivxHAKK5SPIZJ3SHp
XZjEeqrvrIGC+zrm2X/soEaxq2m2ud4M8W/+AQIDAQABAoIBADLLlZhdpfOczTAV
GgChb68tB8vWYkNbpwFUIJpwp75knf2oRzv8s/ALLz6yDzFpDjDkyL6TSSo1EJxn
I3KjMak0p3XrF9mLVSjSKKXKO3xtA/+CiBFUqJjFqpQxDKiELNmP7MHSL55HfXVP
gH5FBAzDaWo1s2ehedabL53raSfSV7nxILJHFPAQLdq8RZzibo+0iarwc2Y/5HZh
```

8. Now select the entire Key from ***"---- BEGIN"*** to end and past it in a notepad file. If you are not able to paste it, then you have to enable ***Bidirectional Clipboard*** on your Virtual Box (***Devices -> Shared Clipboard -> Bidirectional***). This is possible only for server VM.

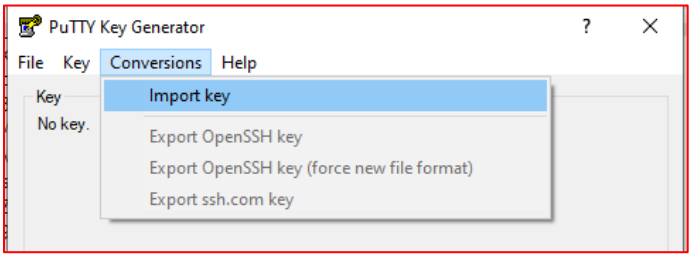


9. Save this File in your windows machine.

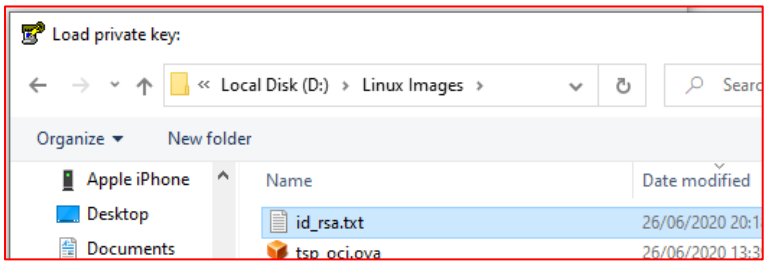


10. Start Puttygen Program to convert the Private key to PPK format.

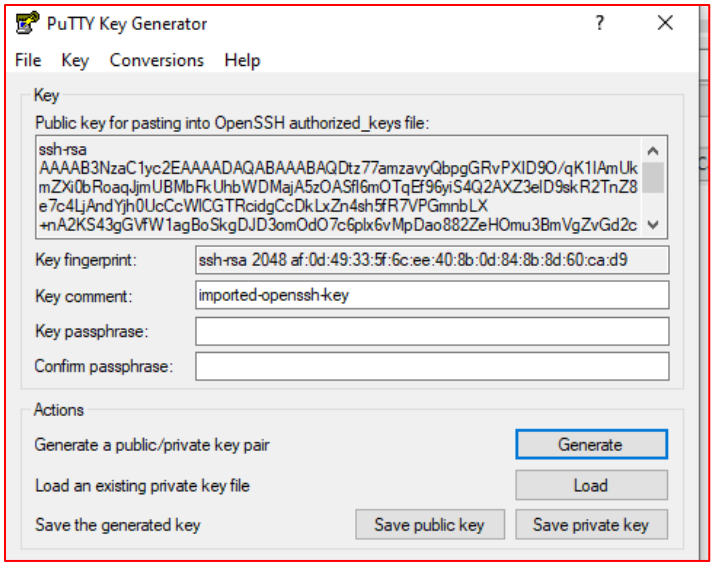
11. Open ***Conversions -> Import Key***



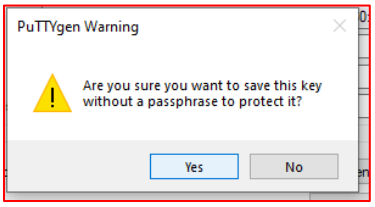
12. Select the text file you saved earlier



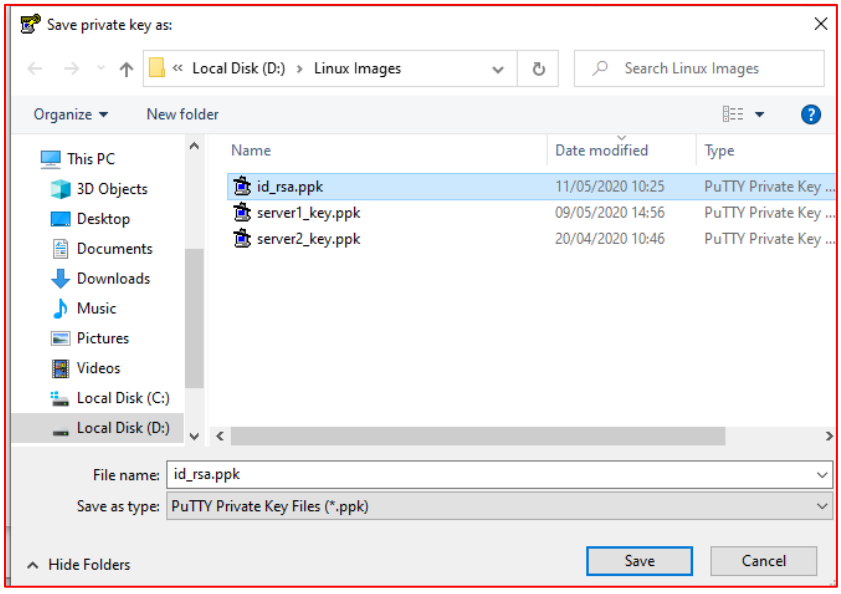
13. It will import the Private Key to Puttygen



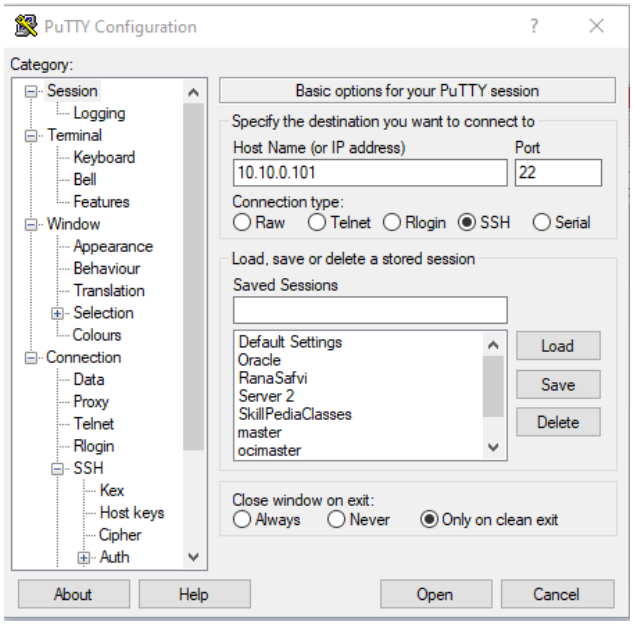
14. Click on ***Save Private Key*** and Confirm the ***Puttygen*** waring on saving this key without passphrase.



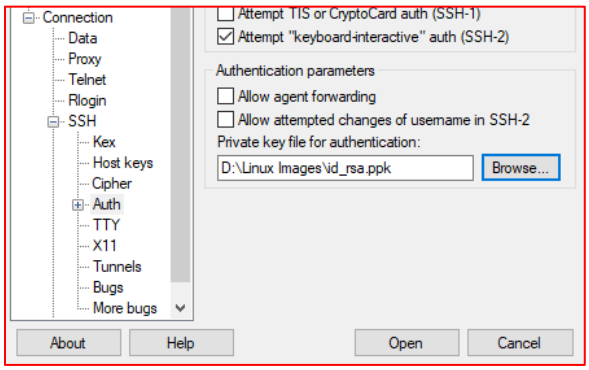
15. Specify a location and accept the default name. Save the PPK format Key on your Host machine.



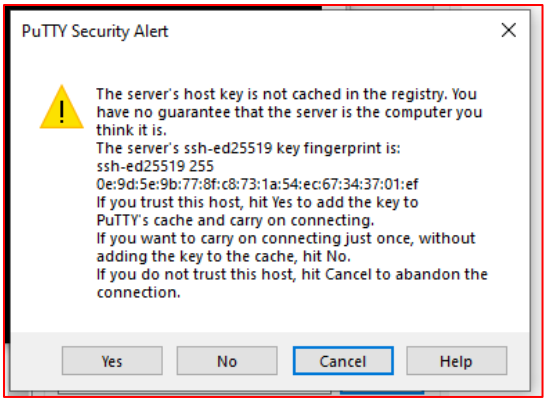
16. The Key you have converted is the private key of your ***server***. You have coped the corresponding public key to ***tester1*** VM. Hence you can now use this PPK format key to connect to your ***tester1*** VM. Launch Putty from your windows machine. Enter the IP address of ***tester1***.



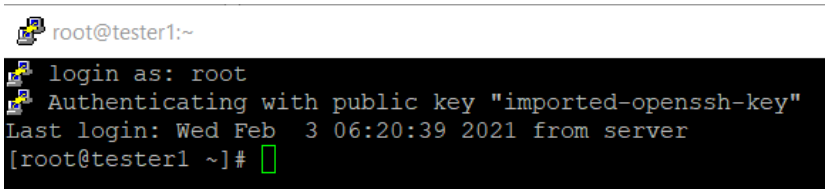
17. Expand ***SSH*** under ***Connection*** from Left part of the window and select ***Auth***. Now on the right part of the window, ***browse*** to the PPK format Key on your system



18. Click on ***Open*** to Connect. You will see a Security alert. Click on ***YES*** to accept.

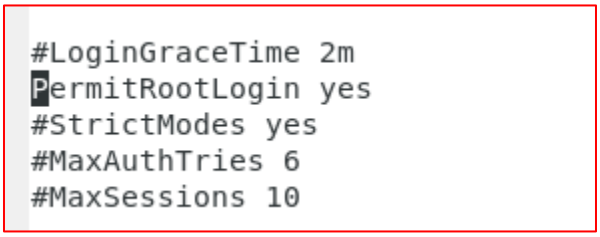


19. Enter the user name "***root***" and press enter key.



20. You are now logged into the ***tester1*** from putty using Key based authentication.

    Troubleshooting tip - Ensure that you have ***PermitRootLogin Yes*** in the file /etc/ssh/sshd_config



Repeat all the above steps as "oracle" user also so that you have key based authentication enabled for both users.