Step

Establish passwordless Secure Shell (SSH) and Secure Copy (SCP) access from a Windows machine to virtual machines.

Objective: This task requires you to establish passwordless Secure Shell (SSH) and Secure Copy (SCP) access from a Windows machine to virtual machines.

Scenario: You need to manage virtual machines (VMs) remotely from a Windows machine. This task focuses on setting up passwordless SSH and SCP access for efficient and secure management.

Constraints: - You should be able to take a SSH access of both VM's root user without entering password from Windows (Base Machine). - You can use RSA keys if needed.

Completion Criteria: - You can establish SSH connections and transfer files using SCP between your Windows machine and VMs without entering passwords.

SSH (Secure Shell) is a network communication protocol that enables secure communication and data exchange between two computers. It provides a secure channel over an unsecured network, much like HTTP facilitates web page transfer.

Methods of SSH Authentication:

1. **Password Authentication**: Users authenticate with a username and password.
2. **Public Key-Based Authentication**: Users generate a pair of keys (public and private). The public key is placed on the server, while the private key remains on the client for secure authentication.

ssh-keygen is a tool used to generate SSH key pairs. Users create a new public-private key pair and then securely copy the public key to the server using SSH and their login credentials.

ssh-copy-id installs an SSH public key on a server's ~/.ssh/authorized_keys file. This allows for passwordless authentication using SSH keys.

SCP (Secure Copy Protocol) is a command-line utility for securely transferring files and directories between Unix or Linux systems. It operates over SSH, ensuring data encryption during transmission.

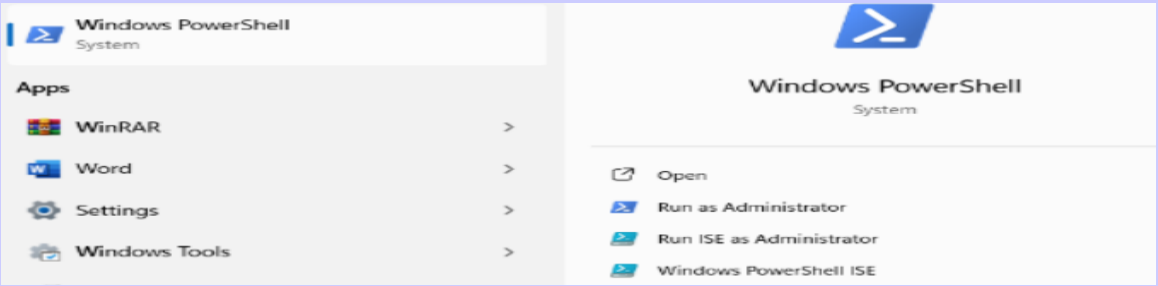
Prerequisites for Ubuntu and OpenSUSE VMs:

1. Ensure Ubuntu 20.04 minimal and OpenSUSE Leap 15 minimal are installed.
2. Check that SSH service (sshd) is running on both systems with **systemctl status sshd.**
3. Make necessary changes in /etc/ssh/sshd_config, including setting PermitRootLogin yes and PasswordAuthentication yes.
4. Add SSH service and allow port 22/tcp in the firewall settings to enable SSH connections securely.

These steps ensure SSH is properly configured for secure remote access between Ubuntu and OpenSUSE virtual machines.

Prerequisites for Windows machine

1. Run Windows Powershell as an administrat



The `ssh-keygen` command is used to generate SSH keys on a Windows machine. The generated keys are stored in the `\.ssh` directory.

Step

```
PS C:\Users\ASUS> ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\ASUS/.ssh/id_rsa):
C:\Users\ASUS/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\ASUS/.ssh/id_rsa
Your public key has been saved in C:\Users\ASUS/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:iT0BV6VFEvPzS/tud82osp9Sv4W1yUMOx4/Uy3Oktb4 asus@Bhole
The key's randomart image is:
+---[RSA 3072]----+
|      . ..=++    |
|       o   *     |
|        . . o    |
|       o o   o.. |
|      . S    .++=|
|         .  .oBX*|
|           . .*&=|
|          o  .+oX|
|           .=+..E*|
+----[SHA256]-----+
PS C:\Users\ASUS>
```

copy public key from windows machine which is id_rsa.pub and send it to OpenSUSE virtual machine and you get passwordless SSH access of suse machine.

```
PS C:\Users\ASUS> ssh root@192.168.202.148
(root@192.168.202.148) Password:
Last login: Mon Jul 15 13:40:06 2024 from 192.168.202.187
Have a lot of fun...
opensuse:~ #
```

Now send file from windows machine to SUSE using Secure Copy (SCP)

The scp (Secure Copy) command is used to securely transfer files between a local host and a remote host or between two remote hosts. This command utilizes the SSH protocol to ensure that the data is encrypted during transfer, providing a secure method for file copying.

Command: scp filename user@ip:destination

Scp: command is used to securely transfer files

.\windowsfile.txt: source file located on windows machine

root@192.168.202.148:/ : root@ip indicates the file should copied to host and should be placed in root users home directory.

```
PS C:\Users\ASUS> echo "Hello" > windowfile.txt
PS C:\Users\ASUS> cat windowfile.txt
Hello
PS C:\Users\ASUS> scp .\windowfile.txt root@192.168.202.148
        1 file(s) copied.
PS C:\Users\ASUS> ssh root@192.168.202.148
(root@192.168.202.148) Password:
Last login: Mon Jul 15 13:33:25 2024 from 192.168.202.187
Have a lot of fun...
opensuse:~ # ls
.bash_history  .gnupg    .ssh      .wget-hsts  bin
.cache         .lesshst  .viminfo  Task1       inst-sys
opensuse:~ # logout
Connection to 192.168.202.148 closed.
PS C:\Users\ASUS> scp .\windowfile.txt root@192.168.202.148:/
(root@192.168.202.148) Password:
windowfile.txt                                100%   16     2.0KB/s   00:00
PS C:\Users\ASUS> ssh root@192.168.202.148
(root@192.168.202.148) Password:
Last login: Mon Jul 15 13:39:29 2024 from 192.168.202.187
Have a lot of fun...
opensuse:~ # ls
.bash_history  .gnupg    .ssh      .wget-hsts  bin
.cache         .lesshst  .viminfo  Task1       inst-sys
opensuse:~ # cd /
opensuse:/ # ls
.snapshots  dev   lib    mnt   root  selinux  tmp  windowfile.txt
bin         etc   lib64  opt   run   srv      usr
boot        home  media  proc  sbin  sys      var
opensuse:/ # cat windowfile.txt
◆◆Hello
opensuse:/ #
```

Follow same process for Ubuntu:

ssh-keygen : using this command keys get generate on windows machine. Which is stored on \.ssh location.

1> copy public key from windows machine which is id_rsa.pub and send it to ubuntu virtual machine.

2> Give password of ubuntu root and then key will send successfully.

3> Now copy public key from windows machine which is id_rsa.pub and send it to ubuntu virtual machine.

4> Give password of ubuntu root and then key will send successfully.

5> Now you get passwordless SSH access of Ubuntu machin.

Step

```
root@ubuntu:~# ls
mytest  mytest.c  snap  Task2  Task2.1  Task2.2
root@ubuntu:~#
```

Send file from windows machine to SUSE using Secure Copy (SCP)

```
echo " hello from Window" > windowsfile.txt
ls
```

Scp filename user@ip:destination

Scp: command is used to securely transfer files

.\windowsfile.txt: source file located on windows machine

root@192.168.225.133:/ : root@ip indicates the file should copied to host and should be placed in root users home directory.

```
root@ubuntu:~# cd /
root@ubuntu:/# ls
bin   etc   lib32   lost+found  mydata    proc  sbin  swap.img  usr
boot  home  lib64   media       nodocker  root  snap  sys       var
dev   lib   libx32  mnt         opt       run   srv   tmp       windowsfile.txt
root@ubuntu:/# cat windowsfile.txt
 hello from Window
```

check that file came on ubuntu successfully

```
root@ubuntu:/# cat windowsfile.txt
 hello from Window
```

Thank you

dasaremahir333@gmail.com