

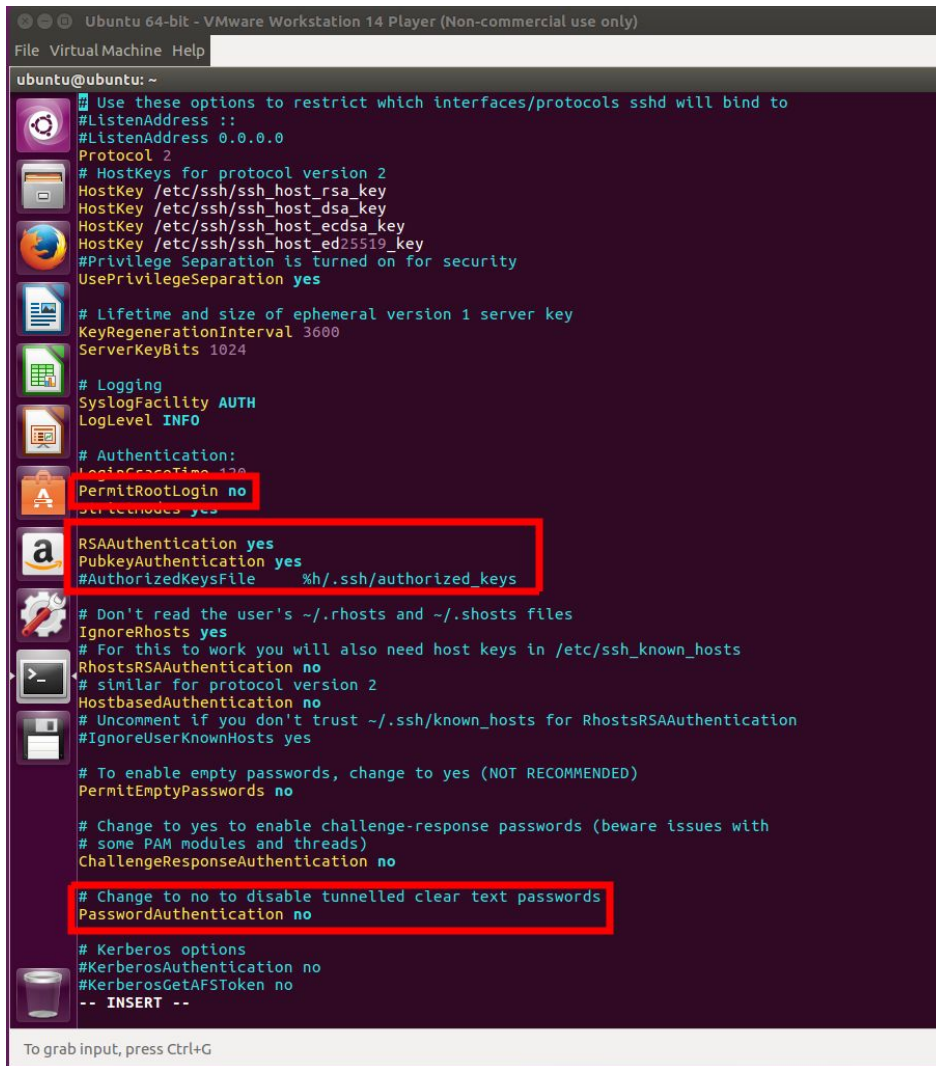
Computer Network & Security - Assignment 1

Setup SSH server

Harsh Agarwal
CS15BTECH11019

Procedure Followed

1. I created an Ubuntu 16.04.3 Desktop Virtual Machine on VMWare.
2. After logging into the VM , I installed ssh server on it using the following command
sudo apt install openssh-server
3. I modified /etc/ssh/sshd_config to make the following changes
PermitRootLogin no
PasswordAuthentication no



```
Ubuntu 64-bit - VMware Workstation 14 Player (Non-commercial use only)
File Virtual Machine Help
ubuntu@ubuntu: ~
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 1024

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
PermitRootLogin no
StrictModes yes

RSAAuthentication yes
PubkeyAuthentication yes
#AuthorizedKeysFile %h/.ssh/authorized_keys

# Don't read the user's ~/.rhosts and ~/.shosts files
IgnoreRhosts yes
# For this to work you will also need host keys in /etc/ssh_known_hosts
RhostsRSAAuthentication no
# similar for protocol version 2
HostbasedAuthentication no
# Uncomment if you don't trust ~/.ssh/known_hosts for RhostsRSAAuthentication
#IgnoreUserKnownHosts yes

# To enable empty passwords, change to yes (NOT RECOMMENDED)
PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no

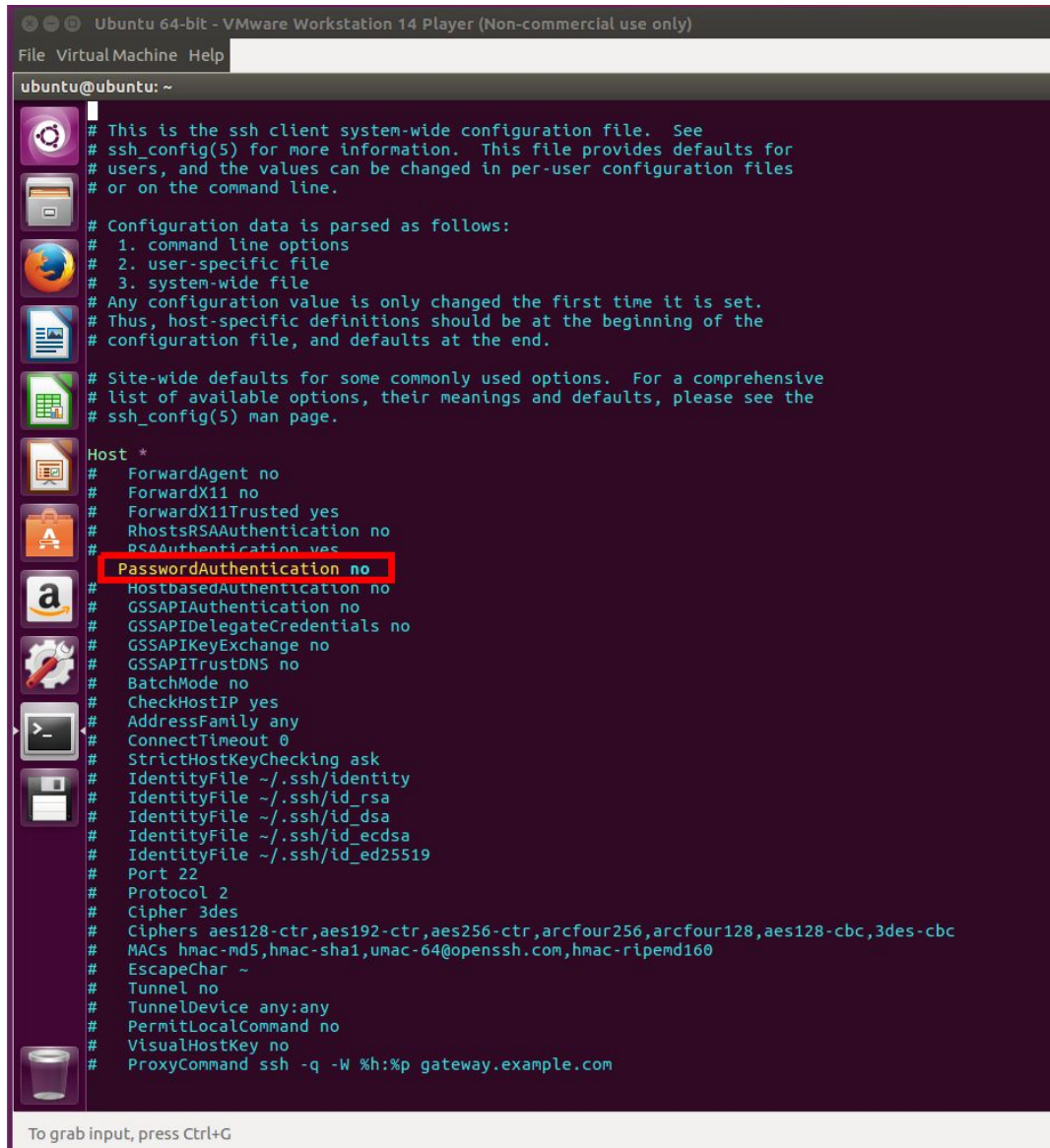
# Change to no to disable tunnelled clear text passwords
PasswordAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosGetAFSToken no
-- INSERT --

To grab input, press Ctrl+G
```

4. I modified /etc/ssh_config to make the following change

PasswordAuthentication no



```
Ubuntu 64-bit - VMware Workstation 14 Player (Non-commercial use only)
File VirtualMachine Help
ubuntu@ubuntu: ~
# This is the ssh client system-wide configuration file. See
# ssh_config(5) for more information. This file provides defaults for
# users, and the values can be changed in per-user configuration files
# or on the command line.
#
# Configuration data is parsed as follows:
# 1. command line options
# 2. user-specific file
# 3. system-wide file
# Any configuration value is only changed the first time it is set.
# Thus, host-specific definitions should be at the beginning of the
# configuration file, and defaults at the end.
#
# Site-wide defaults for some commonly used options. For a comprehensive
# list of available options, their meanings and defaults, please see the
# ssh_config(5) man page.
Host *
# ForwardAgent no
# ForwardX11 no
# ForwardX11Trusted yes
# RhostsRSAAuthentication no
# RSAAuthentication yes
# PasswordAuthentication no
# HostbasedAuthentication no
# GSSAPIAuthentication no
# GSSAPIDelegateCredentials no
# GSSAPIKeyExchange no
# GSSAPITrustDNS no
# BatchMode no
# CheckHostIP yes
# AddressFamily any
# ConnectTimeout 0
# StrictHostKeyChecking ask
# IdentityFile ~/.ssh/identity
# IdentityFile ~/.ssh/id_rsa
# IdentityFile ~/.ssh/id_dsa
# IdentityFile ~/.ssh/id_ecdsa
# IdentityFile ~/.ssh/id_ed25519
# Port 22
# Protocol 2
# Cipher 3des
# Ciphers aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc
# MACs hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160
# EscapeChar ~
# Tunnel no
# TunnelDevice any:any
# PermitLocalCommand no
# VisualHostKey no
# ProxyCommand ssh -q -W %h:%p gateway.example.com
```

5. I restarted ssh server in VM using the command

sudo systemctl restart ssh*

6. Then I created a new public private keypair on my host ubuntu machine using the command

ssh-keygen -t rsa -b 4096

And added a passphrase to it

```
Terminal File Edit View Search Terminal Tabs Help
cse@cse:~$ ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQADKJe9SpVuX1d64HE0IFRa5MFFfqK76F0T0jm52ZrQX6lqxNBbZlv3HERPKyCTfsas/0KqxG+TaYcLK1pCMKlYlCpNFY3Hd+lp75a4gY3r1IykiEer ssJwQ46KZRBmXbgoqqdYQmPus8sKKua4FEA6b00M5T3ITAjN/ywoqUxIOS6yMCaIG01v/wghDIpa2Wln078bBb4+2slnCs7rfuyuhIIi5N0wK1cbWVntg2beU155GjK3VSwt0x9Dx92S8+SnoUZJ4mLE56exeRQAFm+2fRm+LciuI9aNOVDHqQbB1LSuSp4NTJIBo9BhSJtDaegfVukQkaSE1xJNsFwNGLTkZY/B+KOFEH8R7RysTZDPzN9Za+S+UlnOqW6MLCgh+Qlu8MP7Vn7DiJnuuKZ1nDrF+t381p3Xxhkj5ztMo57bBXp++0PDcRFWynGsGZnHLT5KmZ9EnHEVvYEu2I2GzLDrIR2eseUVFnJA9+Mu3zDUnLwRoLKMxD9WQ05+u9lWZdfCzs4i/7Qpraz+0FmZ+GpTncZY142FL18zYMNZ2Jk+LB0G1PEcGqX9Qw9x+GLFseMIqjQkAnh8EarLUREmAXAwed5GI+LVrnpPqkyBhTiL+u0EjQHPXx2h0n09pKNL1myDoxNiawgz2reRQUZhpgeLNX7rDHMCawnWDLw4Q== harsh@harsh-Inspiron-5558
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: AES-128-CBC, 5ECA5305488718161840D8D31AEFF7E6E
qP33F6fzMEw0axdvq0Wk2dZeJp6f/gth/ChUo956hSE5F52xmvQu4RA5LSTN+caom+1R804E11/Zr/dlXft4lJvWmFZ4ltZgvjBP5a7CWFbZRBdcmfhdQUQ/Ckg9hwtAgHhAh+LKP+ssu9e5JBAGPE095KYX4BwAdS7+yQBWgw140G1Q4WWSHvR3CL54pAu4QcMgDqvduwUEPTXDPK+wos2eCwvltgF/x/KUXUmq3fuFdv918zhz1jKbFYNFy/M222T7VsYw2aaFYObTnR80X3hgZ0P6cV40Cxm0cBqUvrv/zIBi90IOLqvbfgaFCqKeJm7mKAbE99+9aeZ2tUysrj28pk0uJFV8Izhv0EaNXaGyGjV83vh7Q+eJWlrSEXqc0XX6u6ty+L8Ri1j4Ry81E7a941RYFmAAWmRdd14FWN16tqNdUYwmVrMULUfr7WpGdu6PABqZ5GZB9yVx8Mw2SWcy9MofysFN65v1Yx2KlB196mEKKt9qjXIVG1YUfrR4Fitxaf6QHGiyz6Vieg/80JuHpEsJI+Pb5s4+oa7kZBClnI+tcpt0g8BFIqgloC7rbA4V85PJGGVbdlDtg3vYn8GAbIZ+9kC67LxG7VZpDdtb0aDab+TM1ESRlB+ZhiNkg2Yx/T4U+KrJhMEyJvg3WENep6QeFv8GnIsaDt5FD22LM/LRC+OuXaV2uBXQRKgzIFg/uFyfo0sP6lLYeLM12fYmZCuPDJ2uoF3drNkdUHFuAprRLAmwxUuvnly71pPs7KXAxeouMzJLXStz4KdN0Gps20yIha092rxuePKPrfJdtEnNztjKfU7Vtdfcku/UT3W7GbQiprw3tC3bD1u+RcRIVJK/AkoukLjflRnNnnjEZ46gg7+0cu0u7VgnFAAU1iXmZog40oUoemjnyz72rLARb/P6ALWgZ7eCmDP5R44rWAJzjPfV10gTdmUAKKxaz4SD2G0tkCPkheJaV06hCCjYu/3cqWf6b+JBjYhnMp+trRarLXcgaF0C3SNYMP8xPFLX0D74yXH/LA4eb5Ug4frIaXJwRoSrFdxad4MAoK720V6I208RoMPTkWC8eEuwZRLGX1FTLRCec6decCm2wGhEJA9epj1SpW08T5D5piq0n81CY1LHMhoxP/6E7Ko3+MZsoyoU4uJE2JUH8213mEh68kHnlgj30617ddd1JWwjAgOrVxWXBbmXCLN0mMcByCGNQC0bfNqxWkRRd0rtzAhvux2N2bFhvVnBb2K0y8Fb8Zj6drizLZrd30x6t3K8o2WYNXYK8to4FCML0K4G3zKVb+pw8fGwDh/VyJjHMF2JH4nOWOL9FGafSg+AMrhXGVxyYJZ8awItjKLSkqsBXpr6eMkF2i439BM6Q5dA9zkebtXxqFNVp4D13XBTfzdvdCnx+X/Bjd2n0FuB1UNjNw76m2rBX18ApLJZUATX23sM+AuKEfcvnsG0UwlfMFH5kacoSpqpX1SaPnmg8Q1KbFzLLh25617rhaRra4IFVvV+TF+ddDhma5Gy3bEm/VU/07q358LQ6sf/vtn0j6MsL7+BuxImT7wprUD0wr769rLZXWDLmkrLLgbuGxWmjAMBft7n7sL1ATWg97uTejuJKA3yPLJuKN7ZL84+yyGu1l5rADoPvm9ILjKtbj2oGZD1TMwm30sCnuNugqERX9aDQogLA8PITE4Nno+JWR3b71Hy0jw7rns0IaewE1ixFLyn2Hyj688MT407Xn+ArtglbAmAh9a9gCXvqQGPNxln9e73Z7VGEPrI/RgR57nxyxjH5L11RVW6NDHOPP91F/g8NNLl170Fq8CLt0eUlrPMAcSUNBU3KY4WC06SfHx2eQSEwEvKN87s0J0Y578xV8K2T8mHGI4LxCcuh3vo2i6IRikG6PLo+KkAXK5F0+bmyQK50qFSBYZ+h1ldTrNF6i1vM1rdYEO0qa5w84BE0J2IWbKtASbI+6LERQPQINsT5o/Y9dj1ULq9tShgcJs9RuY+PMx0e08novhi0ks9aKICihFvH8KqVjgk8H0WgJ4vY6lyxz+pZiYQtAdIh+GU0ENyo7NCRZTWfSkwnb6/yvVhMIAmMqsY27HKBEIM0WtmPpX8tgDf31+1Mz/eSott896fJR7ZwDrq2t9LyX85aZbTLMkevYU2SVXSMGmPpMK0owp95VD8L1eotHnKcNMACv6m3R9BPhE26G7PR35J1oLZR
```

Then using

sudo ssh-copy-id -i id_rsa.pub harsh@192.168.244.128

I sent the public key to the VM

```
File Virtual Machine Help
harsh@ubuntu:~$ ssh
harsh@ubuntu:~/.ssh$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQADKJe9SpVuX1d64HE0IFRa5MFFfqK76F0T0jm52ZrQX6lqxNBbZlv3HERPKyCTfsas/0KqxG+TaYcLK1pCMKlYlCpNFY3Hd+lp75a4gY3r1IykiEer ssJwQ46KZRBmXbgoqqdYQmPus8sKKua4FEA6b00M5T3ITAjN/ywoqUxIOS6yMCaIG01v/wghDIpa2Wln078bBb4+2slnCs7rfuyuhIIi5N0wK1cbWVntg2beU155GjK3VSwt0x9Dx92S8+SnoUZJ4mLE56exeRQAFm+2fRm+LciuI9aNOVDHqQbB1LSuSp4NTJIBo9BhSJtDaegfVukQkaSE1xJNsFwNGLTkZY/B+KOFEH8R7RysTZDPzN9Za+S+UlnOqW6MLCgh+Qlu8MP7Vn7DiJnuuKZ1nDrF+t381p3Xxhkj5ztMo57bBXp++0PDcRFWynGsGZmHLT5KmZ9EnHEVvYEu2I2GzLDrIR2eseUVFnJA9+Mu3zDUnLwRoLKMxD9WQ05+u9lWZdfCzs4i/7Qpraz+0FmZ+GpTncZY142FL18zYMNZ2Jk+LB0G1PEcGqX9Qw9x+GLFseMIqjQkAnh8EarLUREmAXAwed5GI+LVrnpPqkyBhTiL+u0EjQHPXx2h0n09pKNL1myDoxNiawgz2reRQUZhpgeLNX7rDHMCawnWDLw4Q== harsh@harsh-Inspiron-5558
harsh@ubuntu:~/.ssh$
```


Demo

1. Root login is not permitted

```
Terminal File Edit View Search Terminal Help
harsh@harsh-Inspiron-5558:~$ ssh -i .ssh/id_rsa root@192.168.244.128
Permission denied (publickey).
harsh@harsh-Inspiron-5558:~$
```

2. SSH Login does not fall back to password mode on entering wrong passphrase

```
Terminal File Edit View Search Terminal Tabs Help
cse@cse: ~
harsh@harsh-Inspiron-5558: ~/.ssh
harsh@harsh-Inspiron-5558: ~/.ssh$ ssh -i id_rsa harsh@192.168.244.128
The authenticity of host '192.168.244.128 (192.168.244.128)' can't be established.
ECDSA key fingerprint is SHA256:JJsWeaG5oBJAqlqVogDgPxAAk9sFDRSbHoIhJ+JywnI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.244.128' (ECDSA) to the list of known hosts.
Enter passphrase for key 'id_rsa':
Enter passphrase for key 'id_rsa':
Enter passphrase for key 'id_rsa':
Permission denied (publickey).
harsh@harsh-Inspiron-5558:~/.ssh$
```

3. Successful login using Public Key based authentication

```
Terminal File Edit View Search Terminal Tabs Help
cse@cse: ~
harsh@ubuntu: ~
harsh@harsh-Inspiron-5558: ~/.ssh
harsh@harsh-Inspiron-5558: ~/.ssh$ ssh -i id_rsa harsh@192.168.244.128
Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.10.0-28-generic x86_64)

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

292 packages can be updated.
152 updates are security updates.

harsh@ubuntu:~$
```