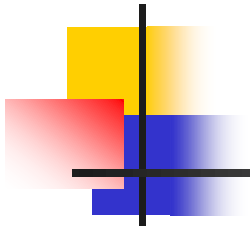
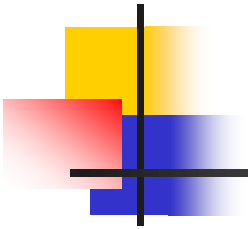
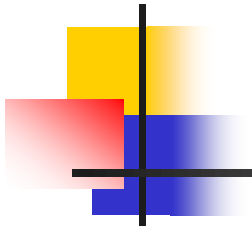


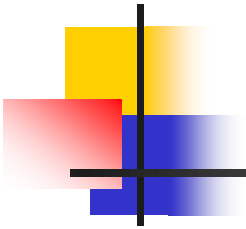
SSH
(SECURED SHELL)



- SSH stand for Secure Shell.
- SSH is a network protocol for secure data communication.
- SSH protocol allows remote command line login.
- SSH protocol enables remote command execution.
- Telnet, rlogin, and ftp transmit unencrypted data over internet.
- OpenSSH encrypt data before sending it over insecure network like internet.
- OpenSSH effectively eliminate eavesdropping, connection hijacking, and other attacks.



- OpenSSH provides secure tunneling and several authentication methods.
- OpenSSH replace Telnet and rlogin with SSH, rcp with scp, ftp with sftp.
-



SSH Tools

- **ssh**

  The ssh [Secure Shell command] is a secure way to log and execute commands in to SSH Server system.

- **sshd**

  The daemon service that implements the ssh server. By default it must be listening on port 22 TCP/IP.

- **scp**

  The Secure Copy command is a secure way to transfer files between computers using the private/public key encryption method.

SSH Packages

- we have to install two packages to configure ssh

1.Openssh

2.Openssh-server

#rpm -qa | grep –i ssh

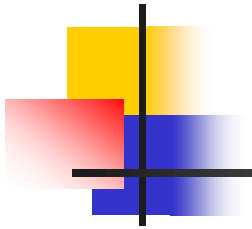
#rpm –qa | grep –i openssh

#yum install openssh* (if there are no packages)

#yum install ssh*

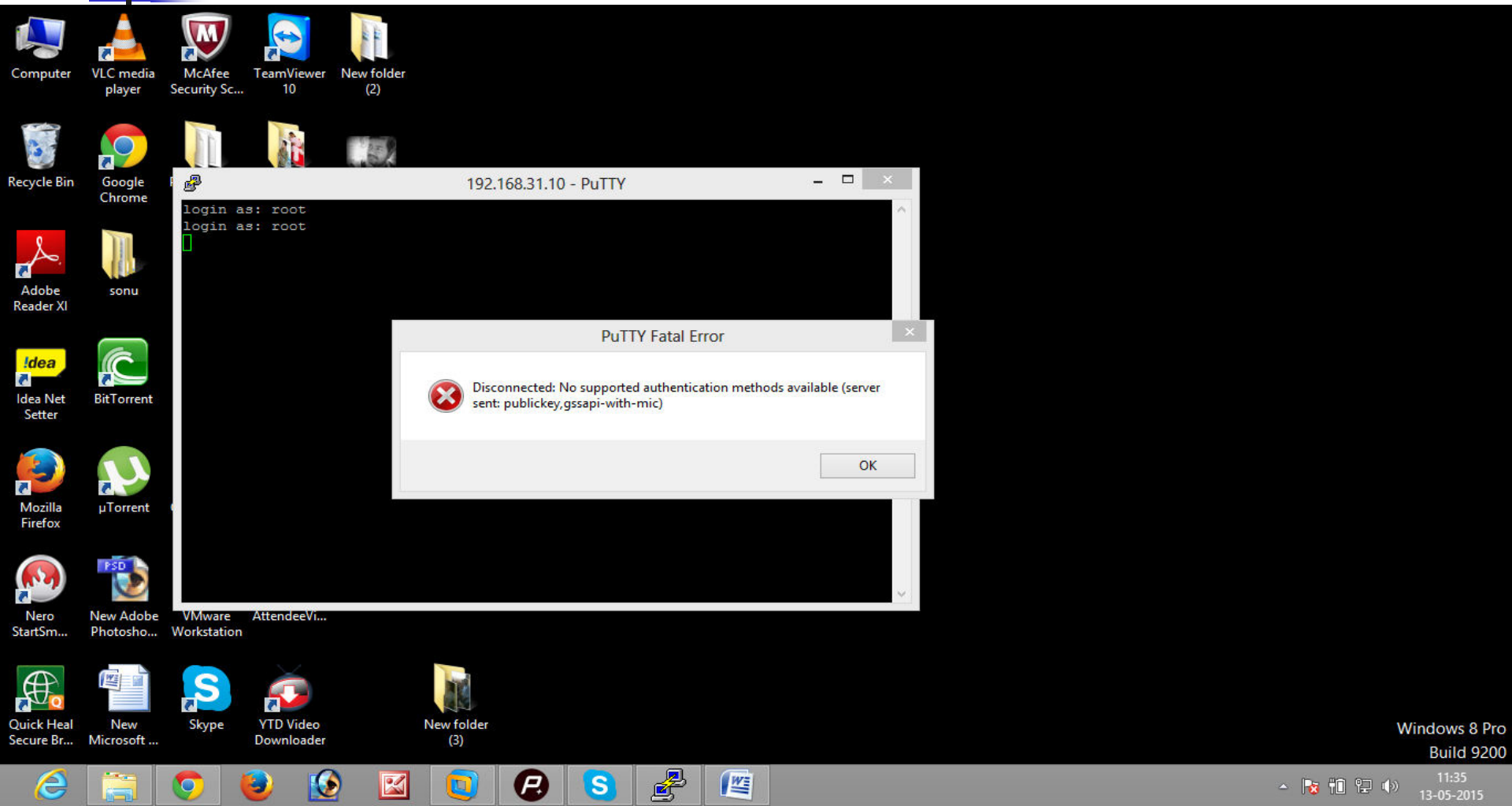
SSH Configuration

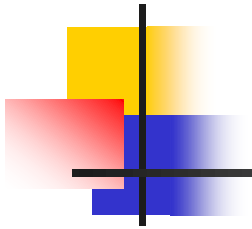
- create two users and assign individual passwords
  useradd user1
  useradd user2
- ssh configuration file
  vi /etc/ssh/sshd_config
- Edit the configuration setting and restart the service
  service network restart



- Check the value of **PasswordAuthentication** directive.
- In order to accept local user password base authentication it must be set to **yes**.
- Set it to **yes** if it is set to **no** and save the file.
- Restart the service if you have made any change in **sshd_config**

  service sshd restart


Computer
VLC media player
McAfee Security Sc...
TeamViewer 10
New folder (2)
Recycle Bin
Google Chrome
Adobe Reader XI
sonu
Idea Net Setter
BitTorrent
Mozilla Firefox
µTorrent
Nero StartSm...
New Adobe Photosho...
VMware Workstation
AttendeeVi...
Quick Heal Secure Br...
New Microsoft ...
Skype
YTD Video Downloader
New folder (3)
192.168.31.10 - PuTTY
login as: root
login as: root
PuTTY Fatal Error
Disconnected: No supported authentication methods available (server sent: publickey,gssapi-with-mic)
OK
Windows 8 Pro
Build 9200
11:35
13-05-2015

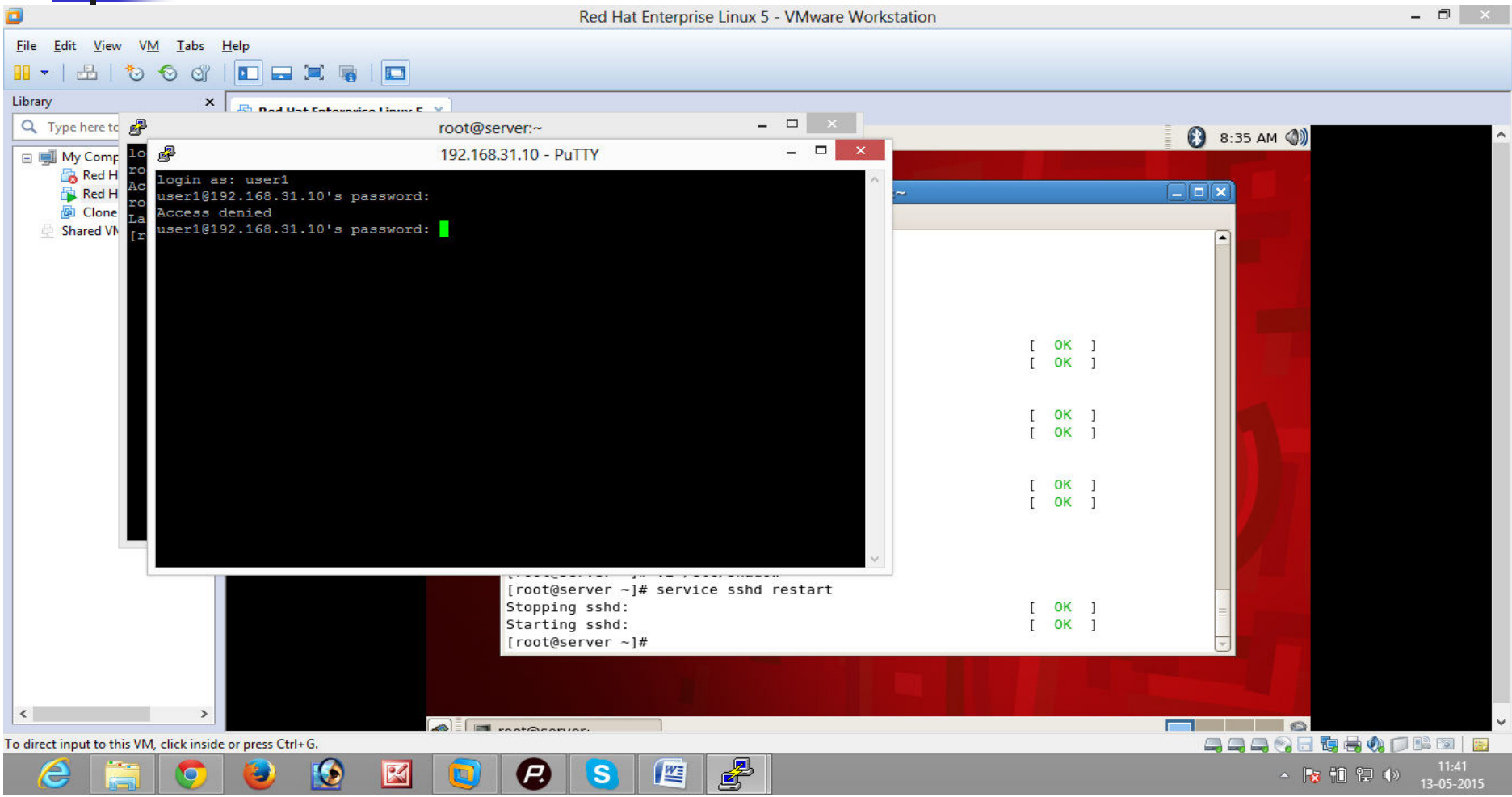


- Following additional directives can be added to **/etc/sshd/sshd_config** file in order to make the ssh server more restrictive.
- **Block empty passwords**

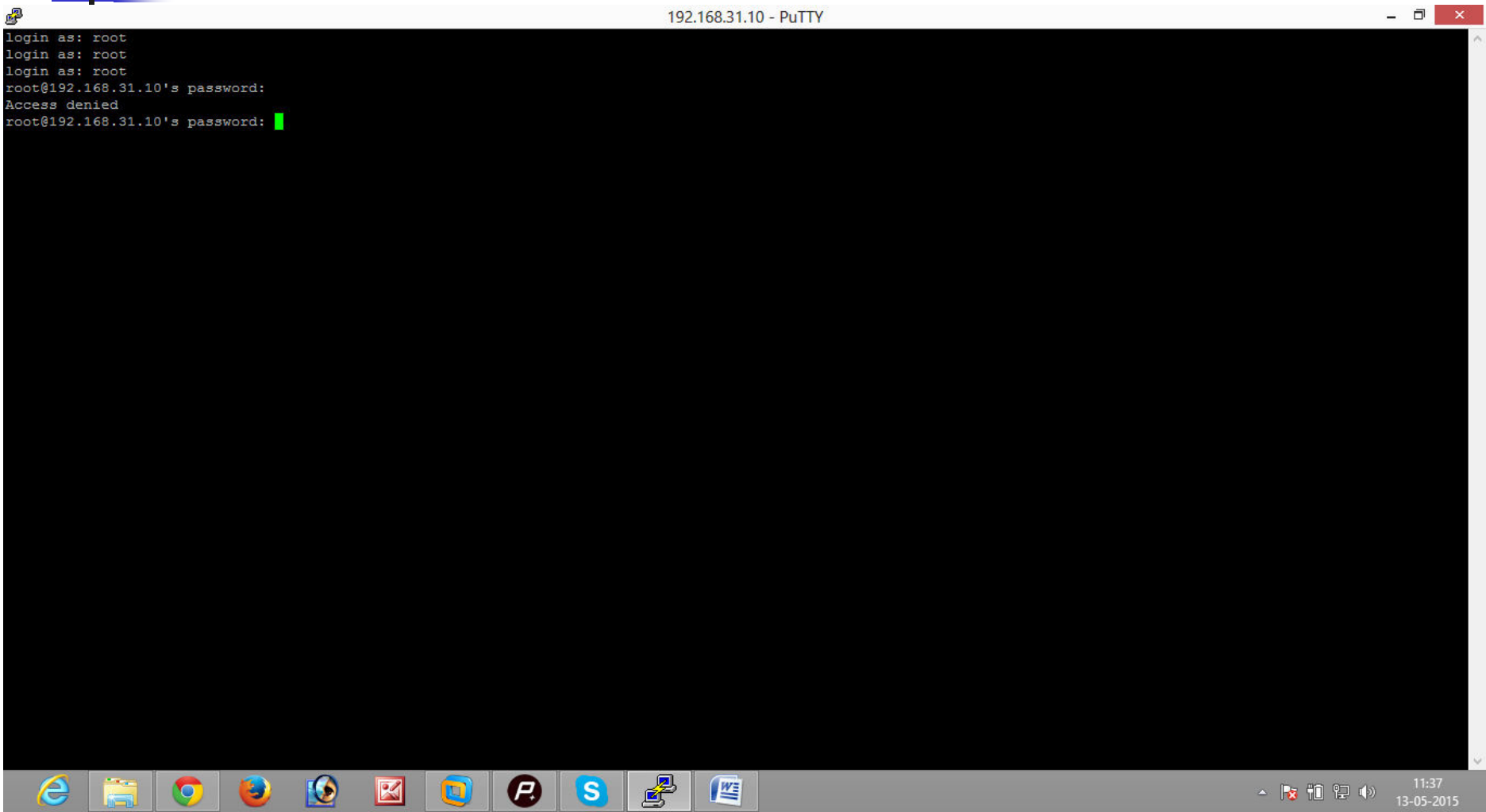
  PermitEmptyPasswords no
- service sshd restart
- **Block root user to log on the system using ssh**.

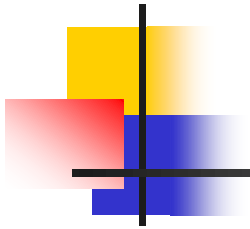
  #PermitRootLogin no

Block empty passwords



Block root user to log on the system using ssh.

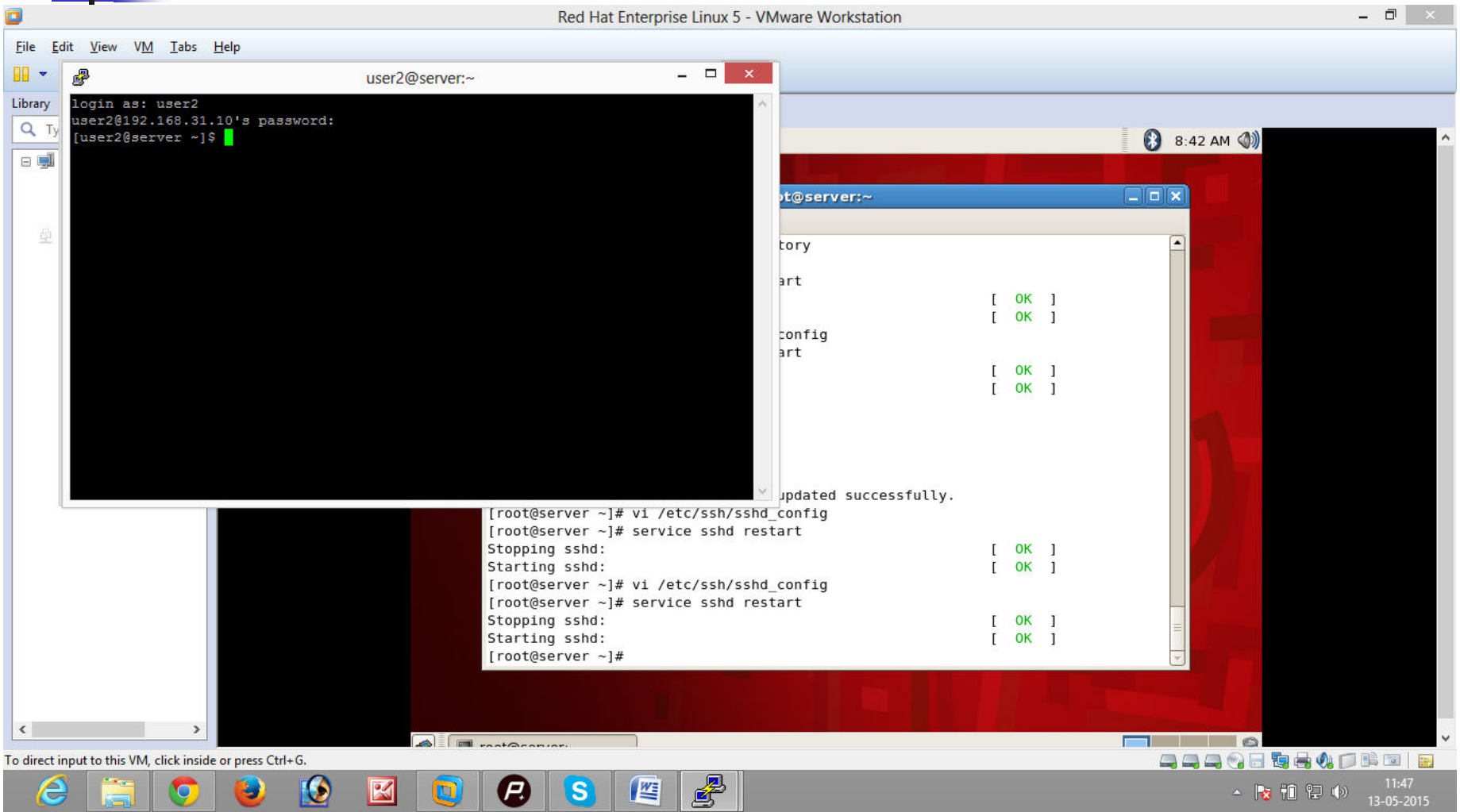




- In addition you can restrict the access to users. In this case all users except ‘nitin' are allowed to connect to the SSH server.
- add in /etc/ssh/sshd_config

  DenyUsers nitin sukesh
- Restart ssh service
- #service sshd restart

Deny users


Red Hat Enterprise Linux 5 - VMware Workstation
File Edit View VM Tabs Help
Library
user2@server:~
login as: user2
user2@192.168.31.10's password:
[user2@server ~]$
8:42 AM
[root@server ~]# vi /etc/ssh/sshd_config
[root@server ~]# service sshd restart
Stopping sshd: [OK]
Starting sshd: [OK]
[root@server ~]# vi /etc/ssh/sshd_config
[root@server ~]# service sshd restart
Stopping sshd: [OK]
Starting sshd: [OK]
[root@server ~]#
To direct input to this VM, click inside or press Ctrl+G.
11:47
13-05-2015