VPM'S B.N.BANDODKAR COLLEGE OF SCIENCE THANE(W)
DEPARTMENT OF IT
TYBSc IT Sem5 LINUX SYSTEM ADMINISTRATION PRACTICAL MANUAL

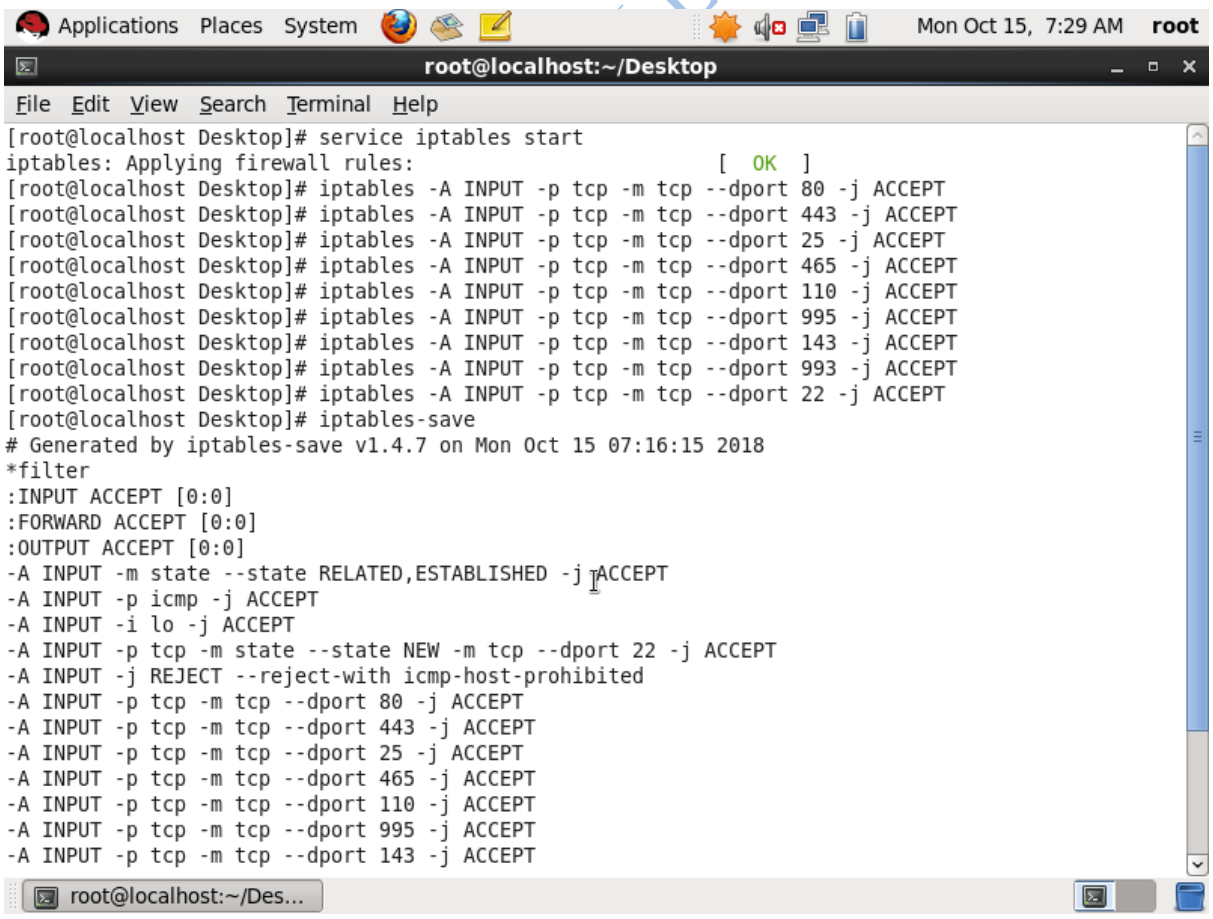
Practical 5

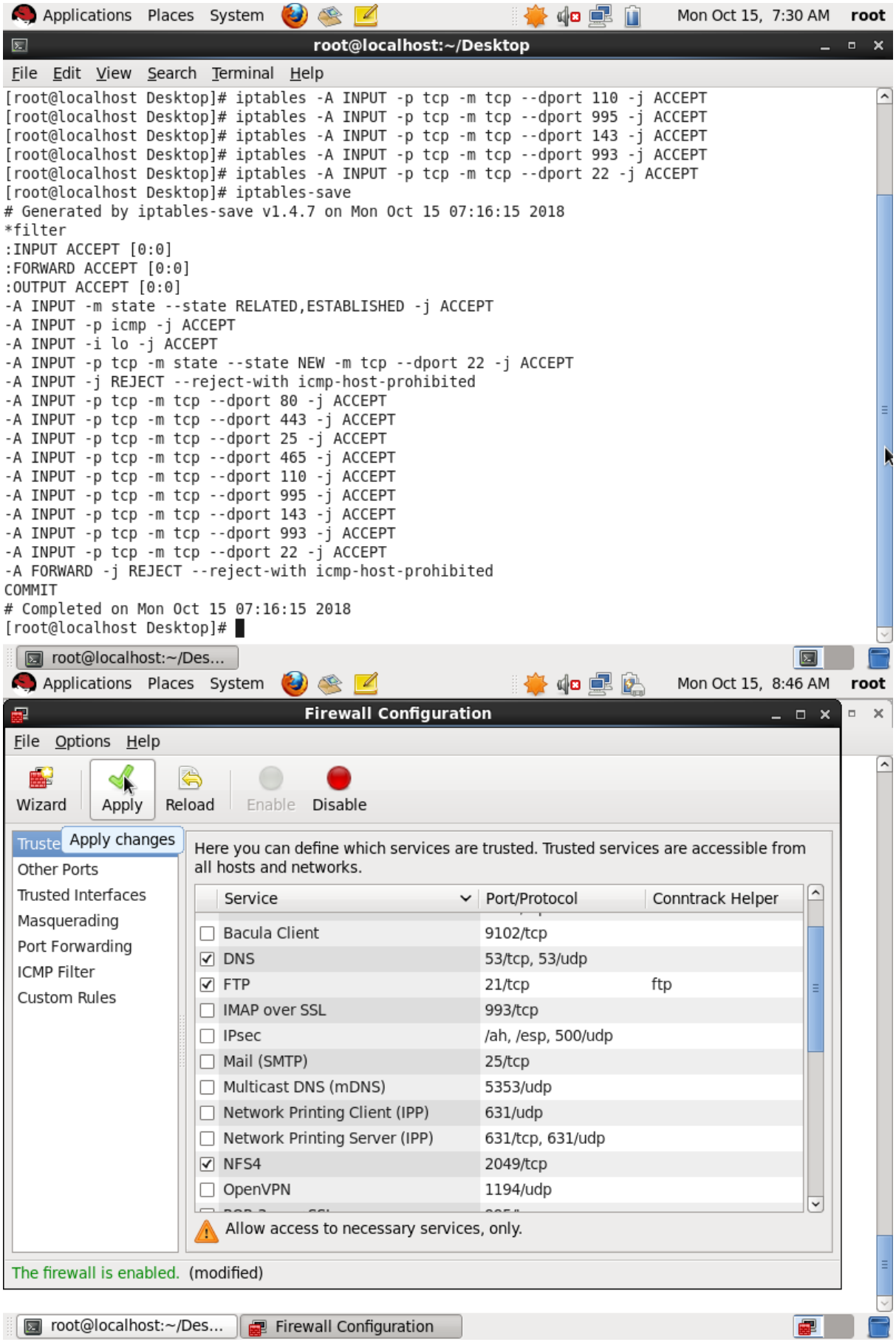
5A) Securing Server with iptables

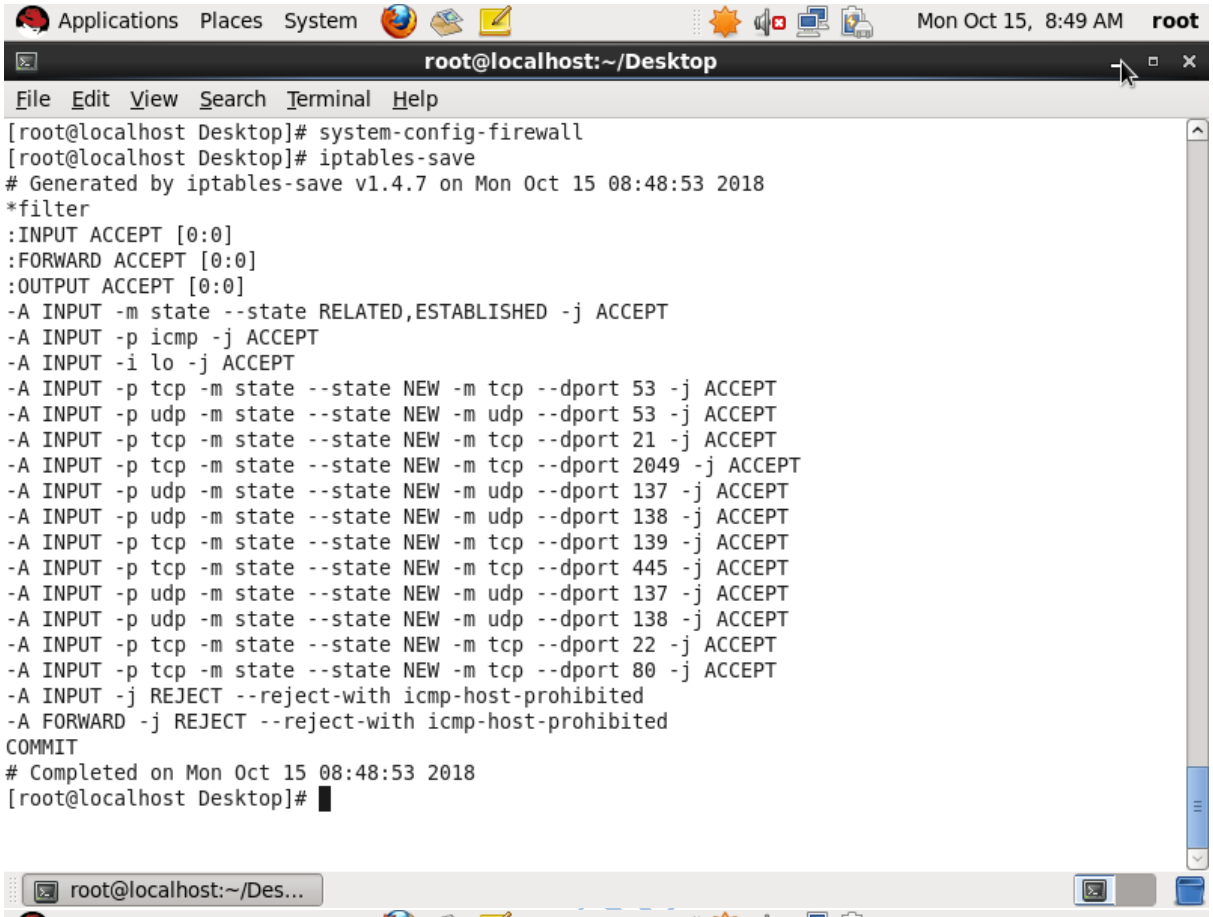
Run following command

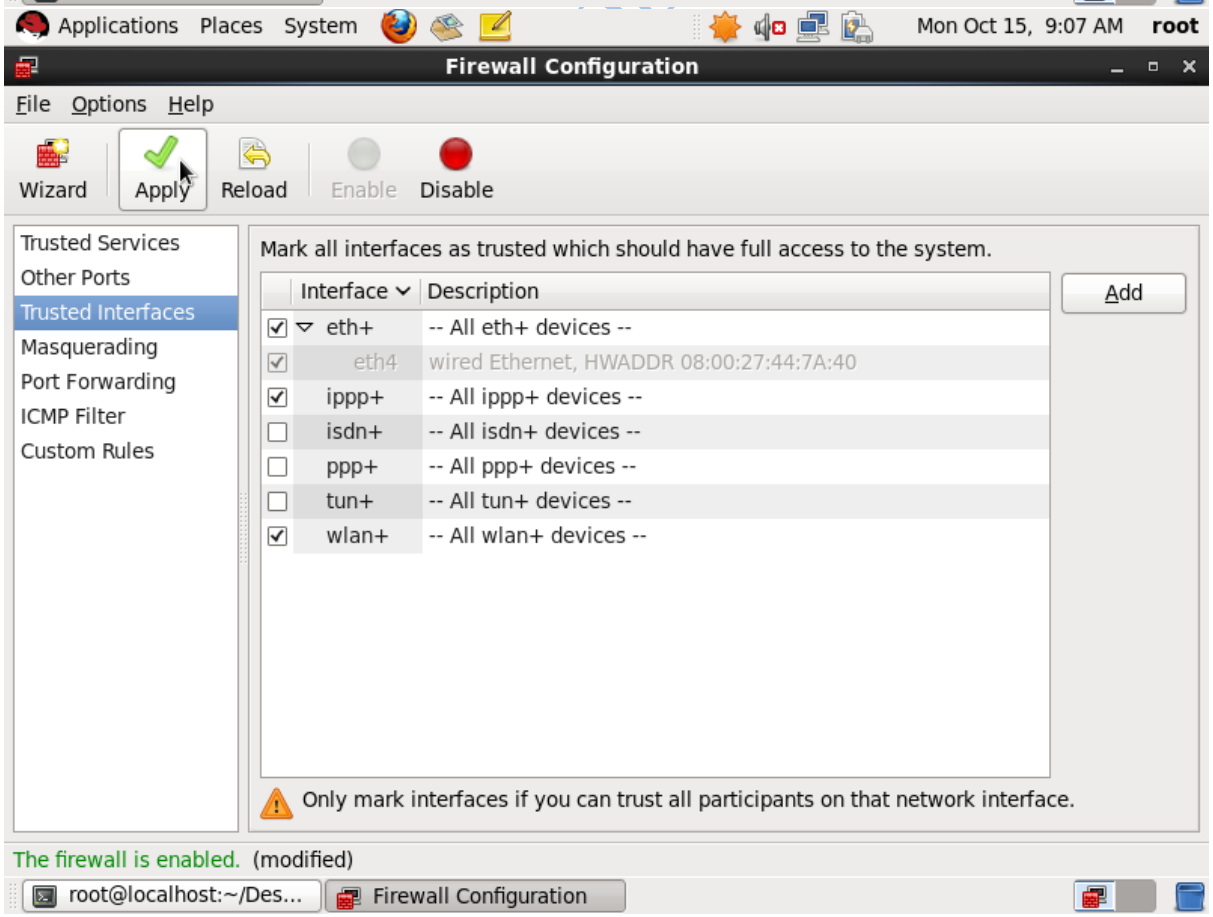
service iptables start

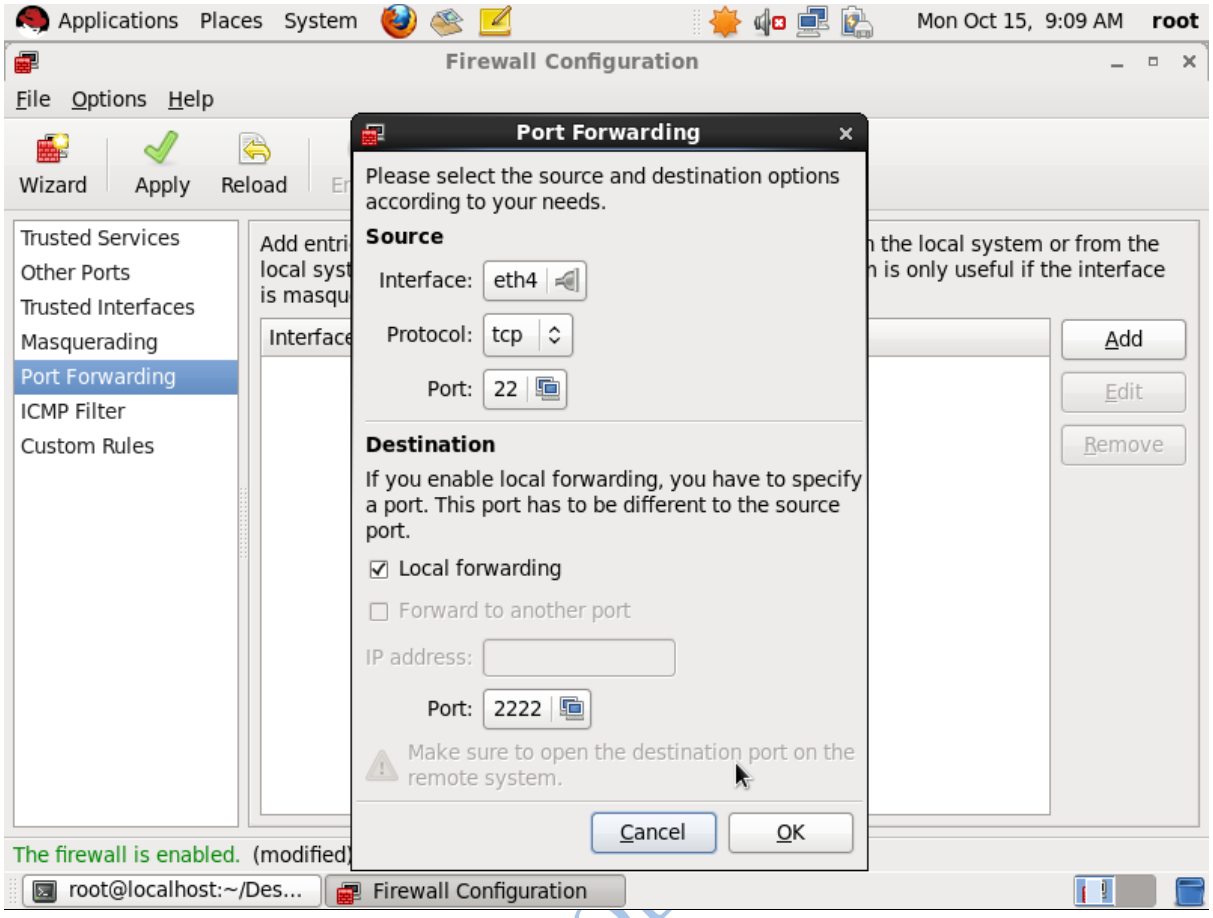
Add rules to iptables and save them using "iptables-save" command
To view iptables rules , use "iptables -L -n"




Applications Places System
Mon Oct 15, 7:30 AM root
root@localhost:~/Desktop
File Edit View Search Terminal Help
[root@localhost Desktop]# iptables -A INPUT -p tcp -m tcp --dport 110 -j ACCEPT
[root@localhost Desktop]# iptables -A INPUT -p tcp -m tcp --dport 995 -j ACCEPT
[root@localhost Desktop]# iptables -A INPUT -p tcp -m tcp --dport 143 -j ACCEPT
[root@localhost Desktop]# iptables -A INPUT -p tcp -m tcp --dport 993 -j ACCEPT
[root@localhost Desktop]# iptables -A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
[root@localhost Desktop]# iptables-save
Generated by iptables-save v1.4.7 on Mon Oct 15 07:16:15 2018
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 443 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 25 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 465 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 110 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 995 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 143 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 993 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
Completed on Mon Oct 15 07:16:15 2018
[root@localhost Desktop]#
root@localhost:~/Des...
Applications Places System
Mon Oct 15, 8:46 AM root
Firewall Configuration
File Options Help
Wizard
Apply
Reload
Enable
Disable
Apply changes
Other Ports
Trusted Interfaces
Masquerading
Port Forwarding
ICMP Filter
Custom Rules
Here you can define which services are trusted. Trusted services are accessible from all hosts and networks.
Service
Port/Protocol
Conntrack Helper
Bacula Client 9102/tcp
DNS 53/tcp, 53/udp
FTP 21/tcp ftp
IMAP over SSL 993/tcp
IPsec /ah, /esp, 500/udp
Mail (SMTP) 25/tcp
Multicast DNS (mDNS) 5353/udp
Network Printing Client (IPP) 631/udp
Network Printing Server (IPP) 631/tcp, 631/udp
NFS4 2049/tcp
OpenVPN 1194/udp
Allow access to necessary services, only.
The firewall is enabled. (modified)
root@localhost:~/Des...
Firewall Configuration


Applications Places System
Mon Oct 15, 8:49 AM root
root@localhost:~/Desktop
File Edit View Search Terminal Help
[root@localhost Desktop]# system-config-firewall
[root@localhost Desktop]# iptables-save
Generated by iptables-save v1.4.7 on Mon Oct 15 08:48:53 2018
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 53 -j ACCEPT
-A INPUT -p udp -m state --state NEW -m udp --dport 53 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 21 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 2049 -j ACCEPT
-A INPUT -p udp -m state --state NEW -m udp --dport 137 -j ACCEPT
-A INPUT -p udp -m state --state NEW -m udp --dport 138 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 139 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 445 -j ACCEPT
-A INPUT -p udp -m state --state NEW -m udp --dport 137 -j ACCEPT
-A INPUT -p udp -m state --state NEW -m udp --dport 138 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
Completed on Mon Oct 15 08:48:53 2018
[root@localhost Desktop]#
root@localhost:~/Des...

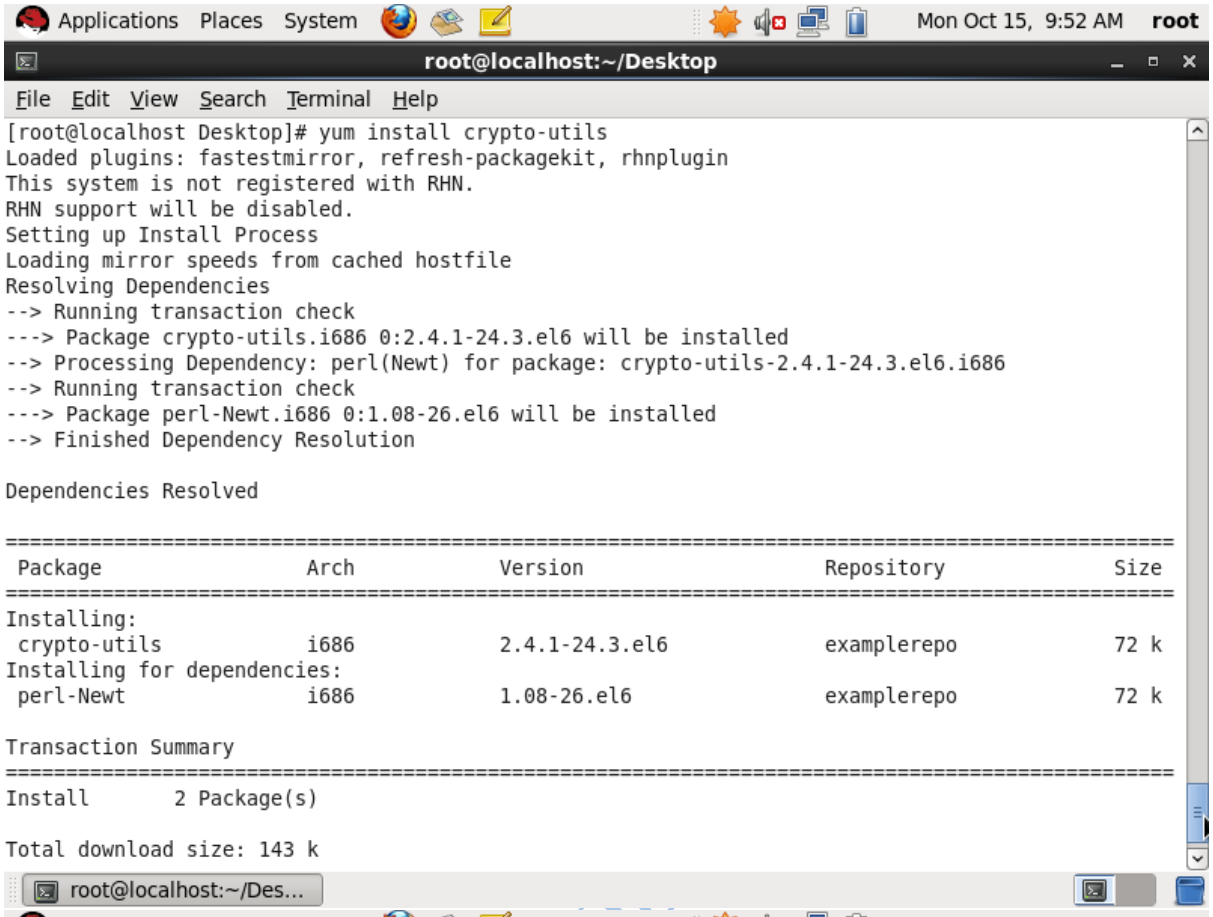

Applications Places System
Mon Oct 15, 9:07 AM root
Firewall Configuration
File Options Help
Wizard
Apply
Reload
Enable
Disable
Trusted Services
Other Ports
Trusted Interfaces
Masquerading
Port Forwarding
ICMP Filter
Custom Rules
Mark all interfaces as trusted which should have full access to the system.
Interface
Description
Add
eth+ -- All eth+ devices --
eth4 wired Ethernet, HWADDR 08:00:27:44:7A:40
ippp+ -- All ippp+ devices --
isdn+ -- All isdn+ devices --
ppp+ -- All ppp+ devices --
tun+ -- All tun+ devices --
wlan+ -- All wlan+ devices --
Only mark interfaces if you can trust all participants on that network interface.
The firewall is enabled. (modified)
root@localhost:~/Des...
Firewall Configuration

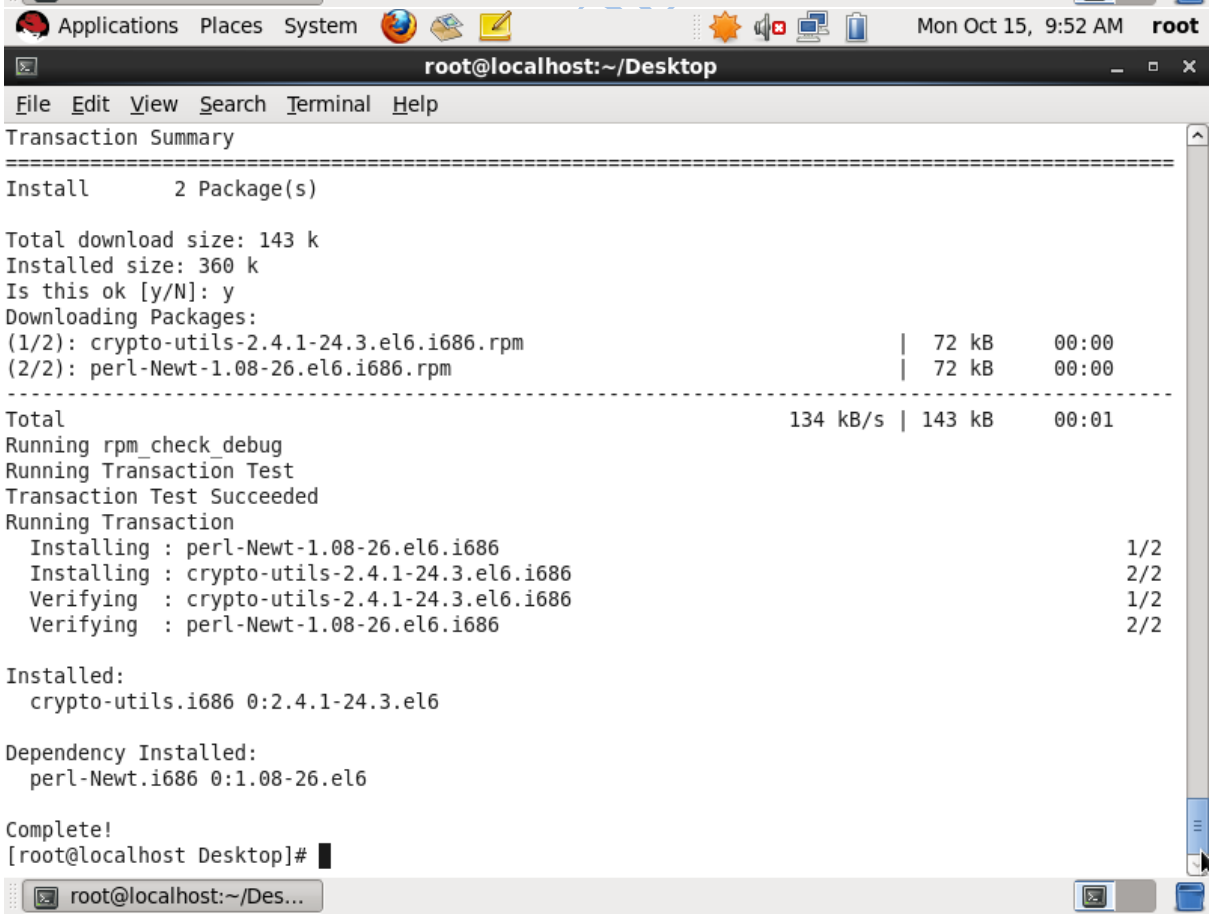


5B) Setting Up Cryptographic Services

Run following commands

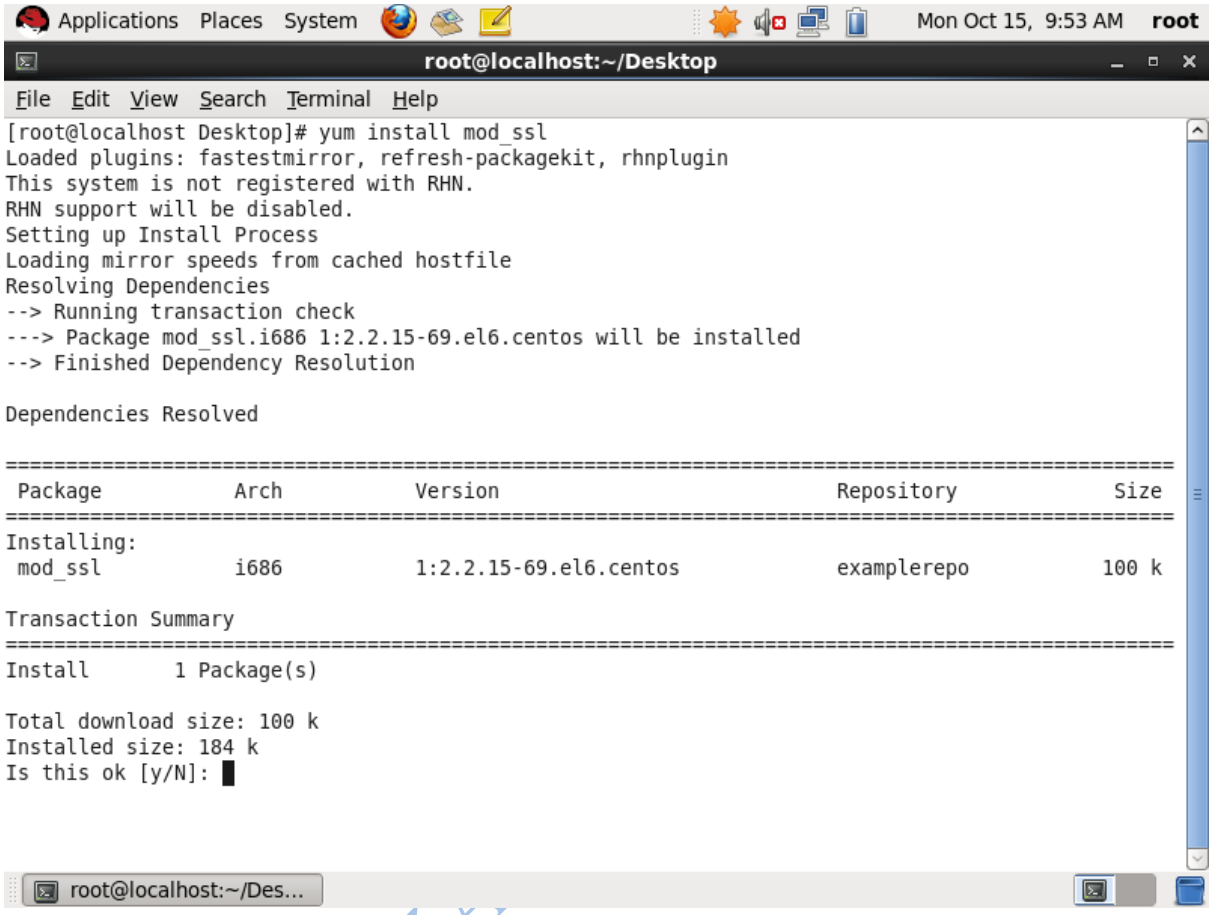
yum install crypto-utils

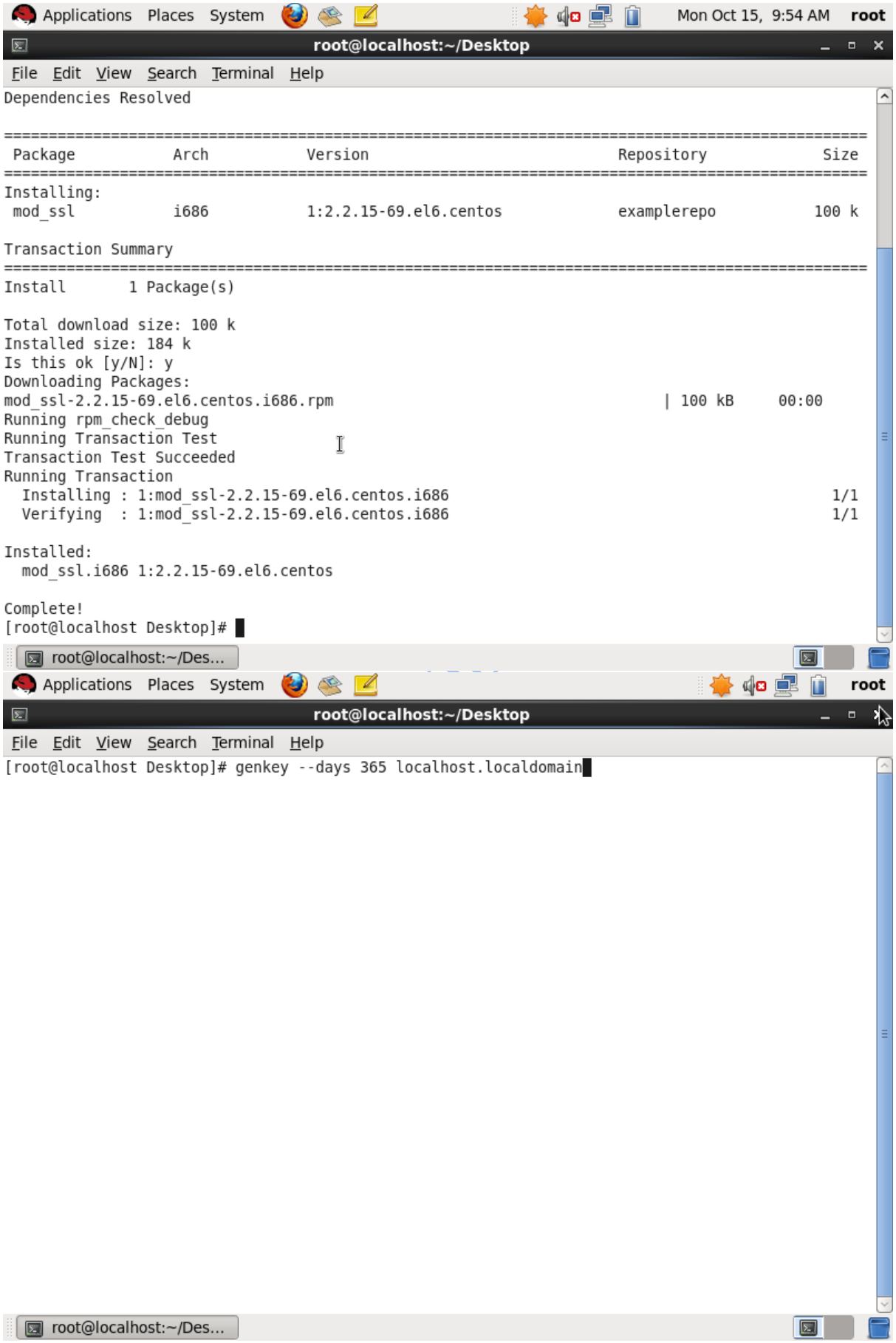

Applications Places System
Mon Oct 15, 9:52 AM root
root@localhost:~/Desktop
File Edit View Search Terminal Help
[root@localhost Desktop]# yum install crypto-utils
Loaded plugins: fastestmirror, refresh-packagekit, rhnplugin
This system is not registered with RHN.
RHN support will be disabled.
Setting up Install Process
Loading mirror speeds from cached hostfile
Resolving Dependencies
--> Running transaction check
---> Package crypto-utils.i686 0:2.4.1-24.3.el6 will be installed
--> Processing Dependency: perl(Newt) for package: crypto-utils-2.4.1-24.3.el6.i686
--> Running transaction check
---> Package perl-Newt.i686 0:1.08-26.el6 will be installed
--> Finished Dependency Resolution
Dependencies Resolved
Package Arch Version Repository Size
Installing:
crypto-utils i686 2.4.1-24.3.el6 examplerepo 72 k
Installing for dependencies:
perl-Newt i686 1.08-26.el6 examplerepo 72 k
Transaction Summary
Install 2 Package(s)
Total download size: 143 k
root@localhost:~/Des...

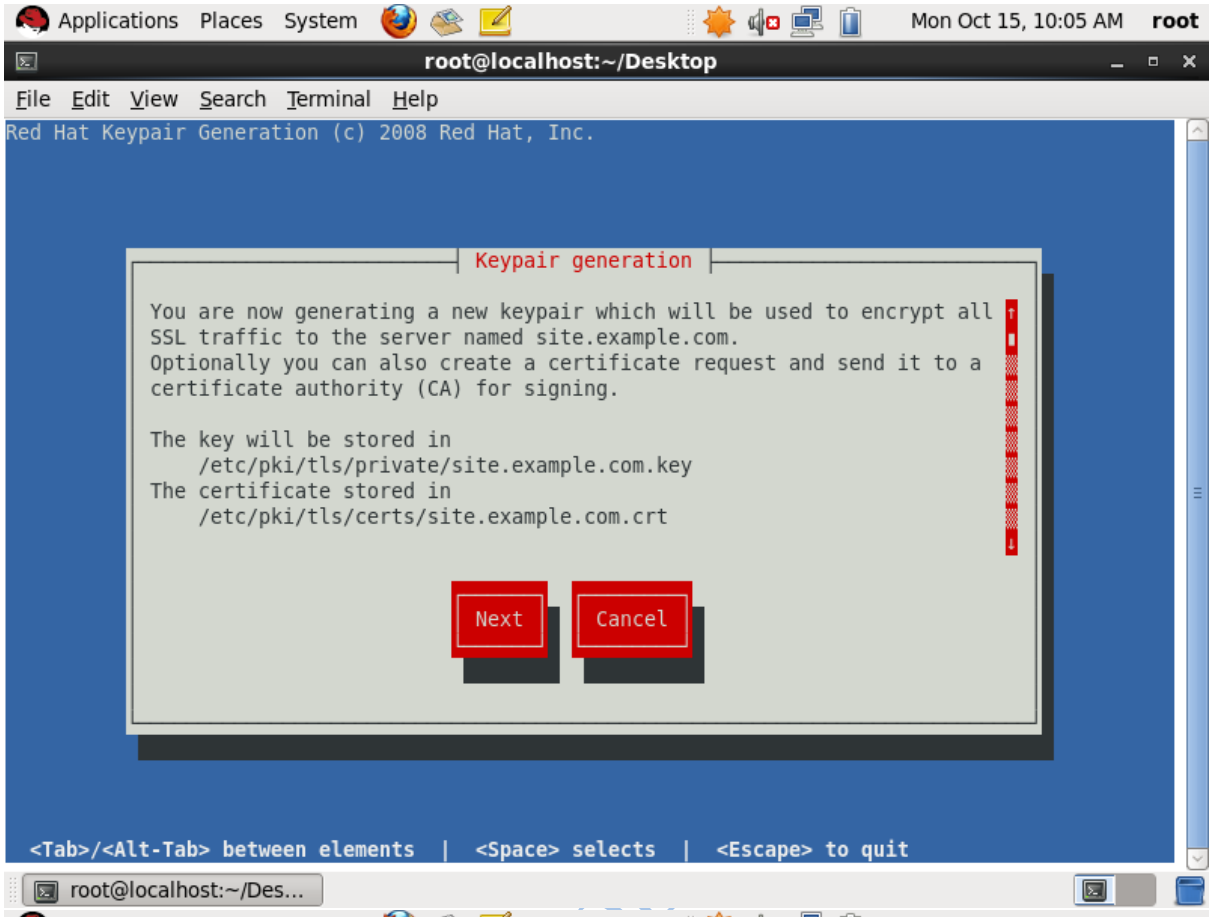

Applications Places System
Mon Oct 15, 9:52 AM root
root@localhost:~/Desktop
File Edit View Search Terminal Help
Transaction Summary
Install 2 Package(s)
Total download size: 143 k
Installed size: 360 k
Is this ok [y/N]: y
Downloading Packages:
(1/2): crypto-utils-2.4.1-24.3.el6.i686.rpm | 72 kB 00:00
(2/2): perl-Newt-1.08-26.el6.i686.rpm | 72 kB 00:00
Total 134 kB/s | 143 kB 00:01
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
Installing : perl-Newt-1.08-26.el6.i686 1/2
Installing : crypto-utils-2.4.1-24.3.el6.i686 2/2
Verifying : crypto-utils-2.4.1-24.3.el6.i686 1/2
Verifying : perl-Newt-1.08-26.el6.i686 2/2
Installed:
crypto-utils.i686 0:2.4.1-24.3.el6
Dependency Installed:
perl-Newt.i686 0:1.08-26.el6
Complete!
[root@localhost Desktop]#
root@localhost:~/Des...

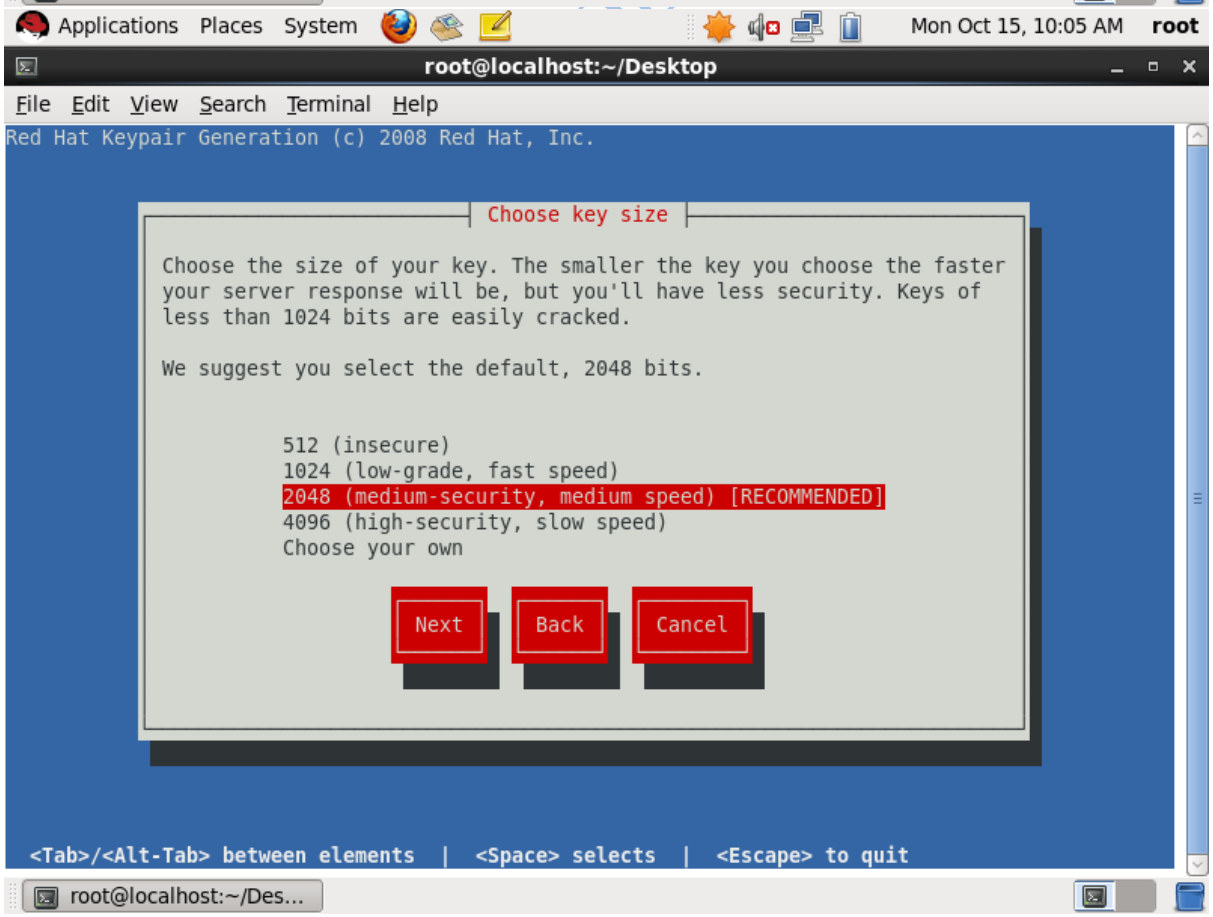
Run following command

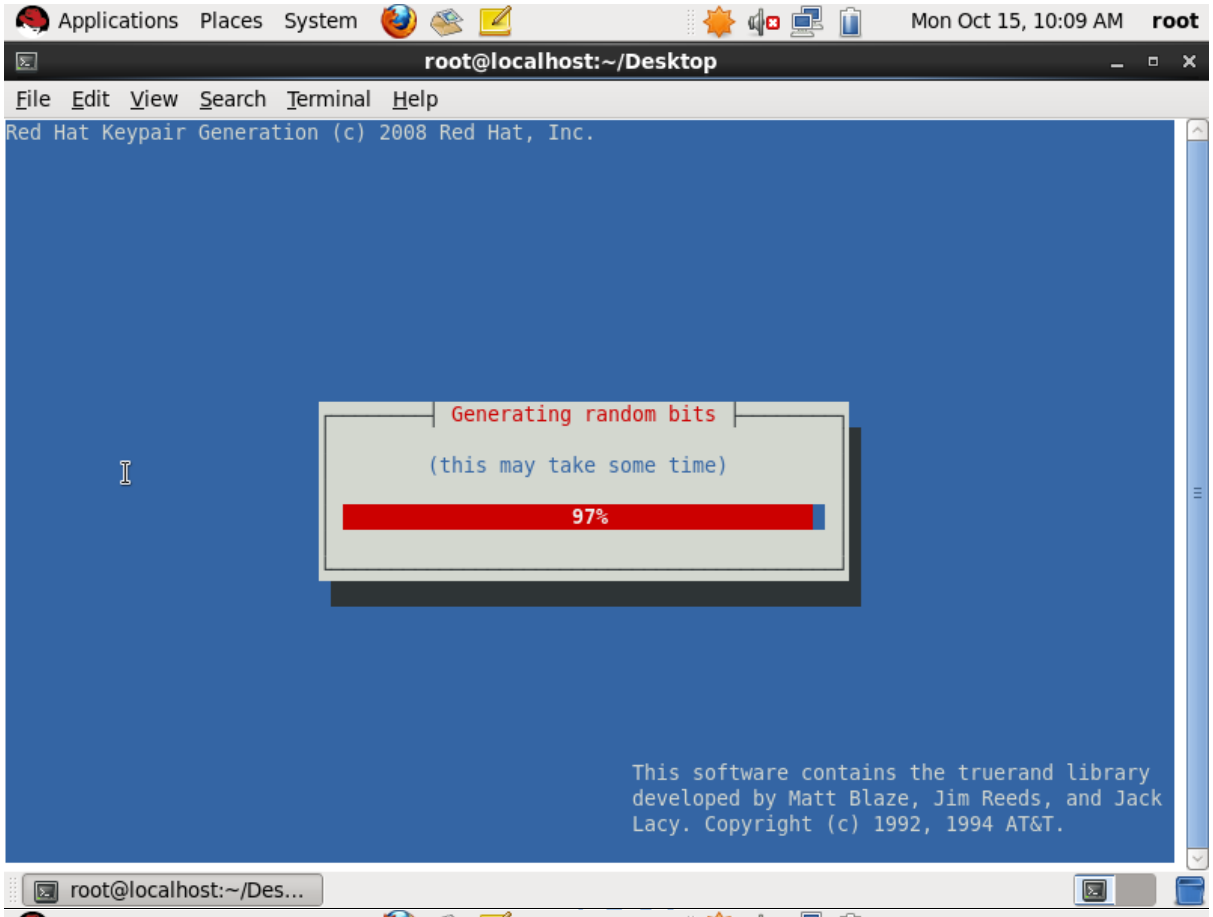
yum install mod_ssl

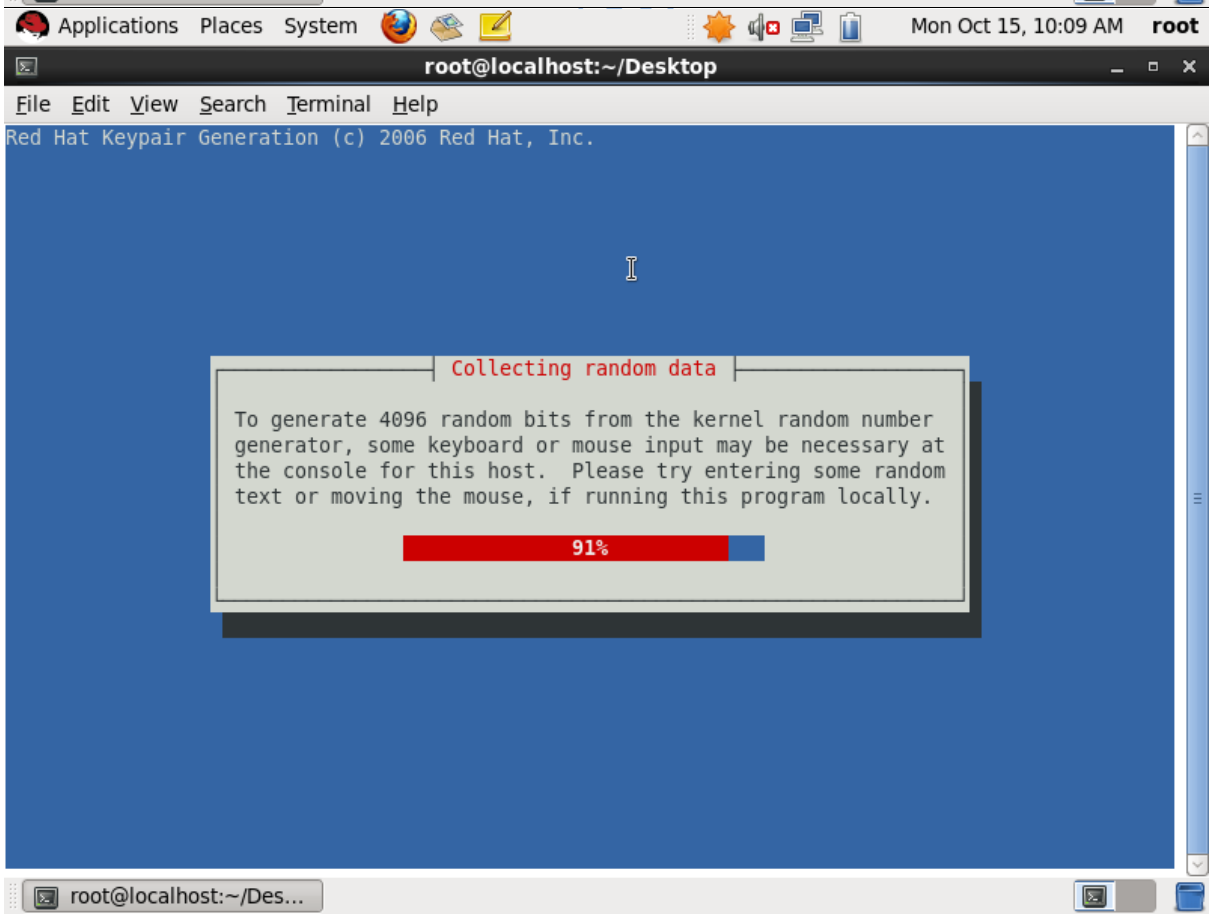


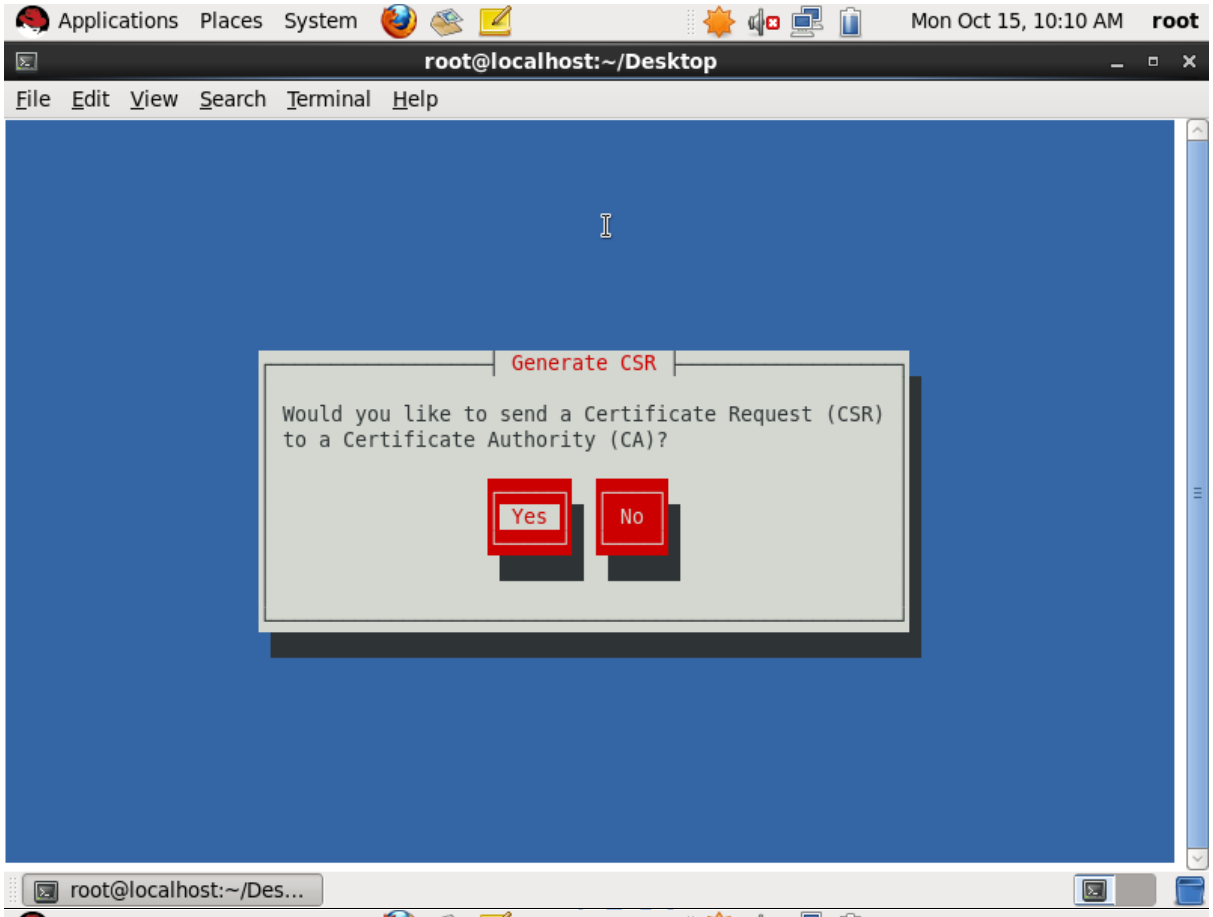

Applications Places System
Mon Oct 15, 9:54 AM root
root@localhost:~/Desktop
File Edit View Search Terminal Help
Dependencies Resolved
Package Arch Version Repository Size
Installing:
mod_ssl i686 1:2.2.15-69.el6.centos examplerepo 100 k
Transaction Summary
Install 1 Package(s)
Total download size: 100 k
Installed size: 184 k
Is this ok [y/N]: y
Downloading Packages:
mod_ssl-2.2.15-69.el6.centos.i686.rpm | 100 kB 00:00
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
Installing : 1:mod_ssl-2.2.15-69.el6.centos.i686 1/1
Verifying : 1:mod_ssl-2.2.15-69.el6.centos.i686 1/1
Installed:
mod_ssl.i686 1:2.2.15-69.el6.centos
Complete!
[root@localhost Desktop]#
root@localhost:~/Des...
Applications Places System
root
root@localhost:~/Desktop
File Edit View Search Terminal Help
[root@localhost Desktop]# genkey --days 365 localhost.localdomain
root@localhost:~/Des...


Applications Places System
Mon Oct 15, 10:05 AM root
root@localhost:~/Desktop
File Edit View Search Terminal Help
Red Hat Keypair Generation (c) 2008 Red Hat, Inc.
Keypair generation
You are now generating a new keypair which will be used to encrypt all SSL traffic to the server named site.example.com.
Optionally you can also create a certificate request and send it to a certificate authority (CA) for signing.
The key will be stored in
/etc/pki/tls/private/site.example.com.key
The certificate stored in
/etc/pki/tls/certs/site.example.com.crt
Next
Cancel
<Tab>/<Alt-Tab> between elements | <Space> selects | <Escape> to quit
root@localhost:~/Des...

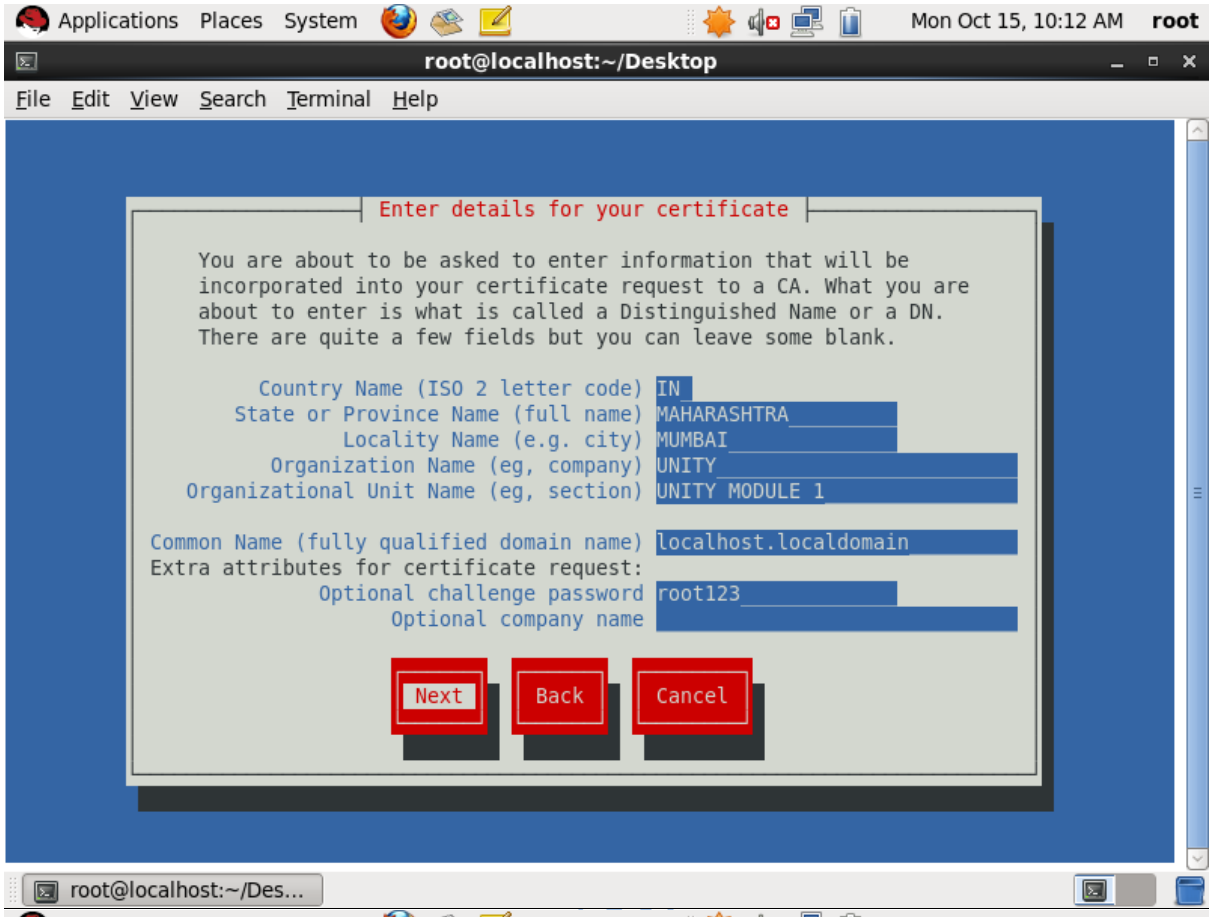

Applications Places System
Mon Oct 15, 10:05 AM root
root@localhost:~/Desktop
File Edit View Search Terminal Help
Red Hat Keypair Generation (c) 2008 Red Hat, Inc.
Choose key size
Choose the size of your key. The smaller the key you choose the faster your server response will be, but you'll have less security. Keys of less than 1024 bits are easily cracked.
We suggest you select the default, 2048 bits.
512 (insecure)
1024 (low-grade, fast speed)
2048 (medium-security, medium speed) [RECOMMENDED]
4096 (high-security, slow speed)
Choose your own
Next
Back
Cancel
<Tab>/<Alt-Tab> between elements | <Space> selects | <Escape> to quit
root@localhost:~/Des...

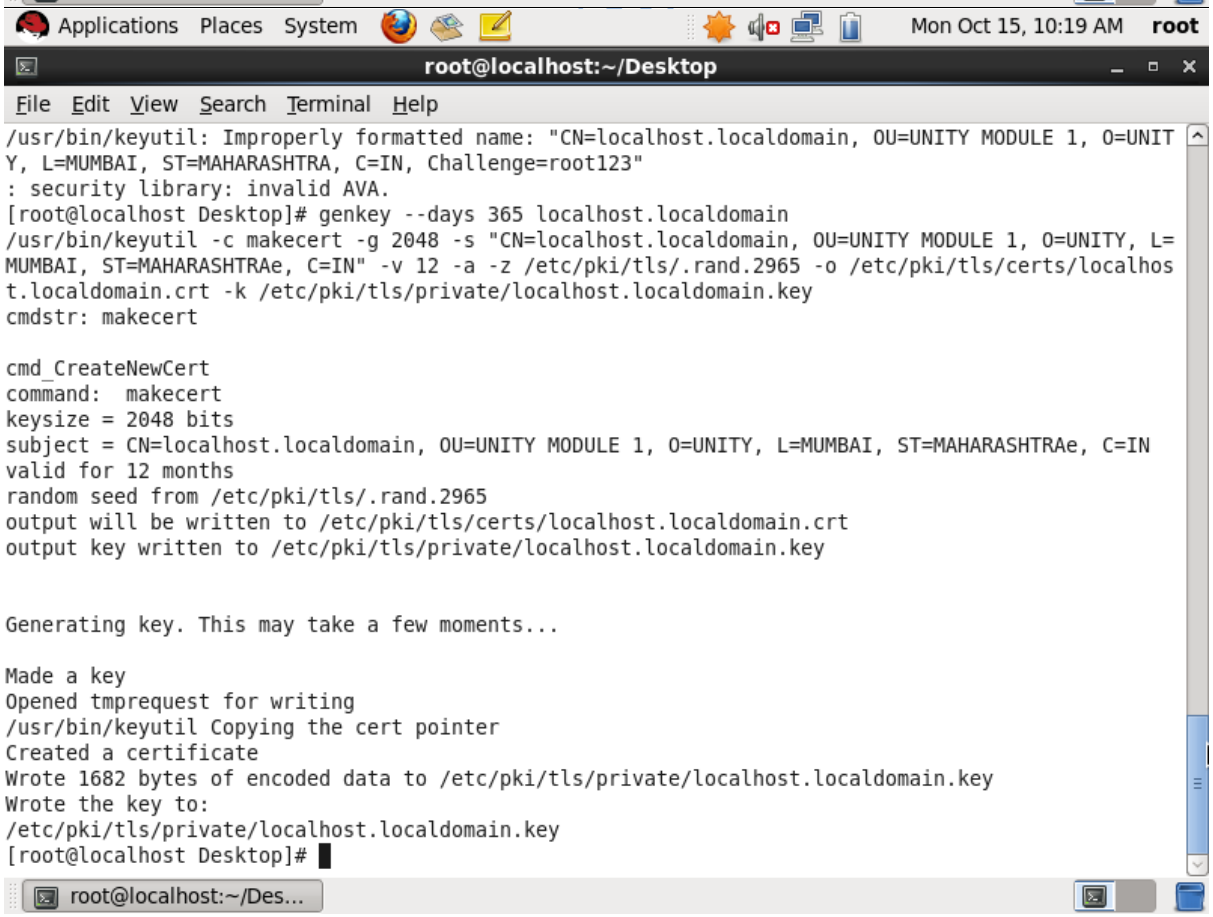

Applications Places System
Mon Oct 15, 10:09 AM root
root@localhost:~/Desktop
File Edit View Search Terminal Help
Red Hat Keypair Generation (c) 2008 Red Hat, Inc.
Generating random bits
(this may take some time)
97%
This software contains the truerand library
developed by Matt Blaze, Jim Reeds, and Jack
Lacy. Copyright (c) 1992, 1994 AT&T.
root@localhost:~/Des...

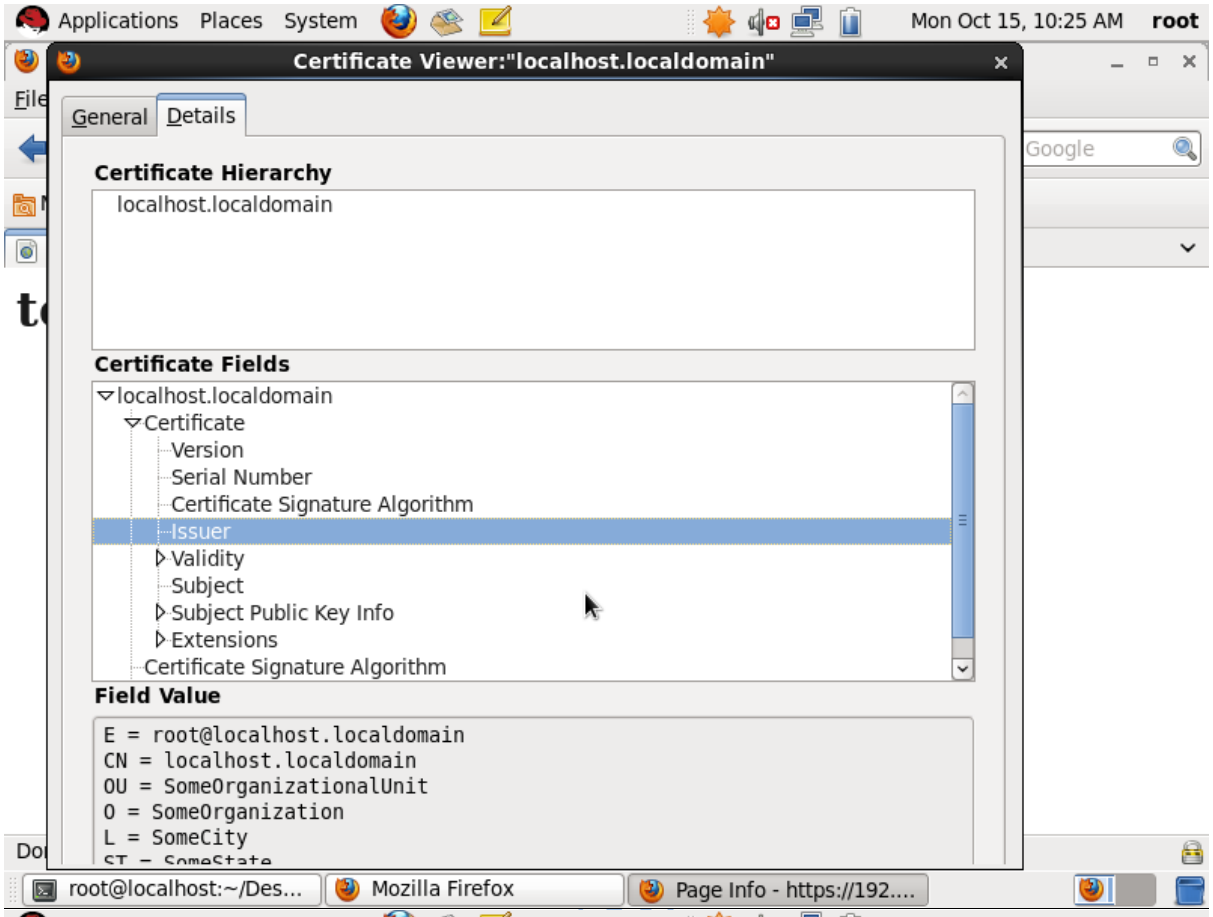

Applications Places System
Mon Oct 15, 10:09 AM root
root@localhost:~/Desktop
File Edit View Search Terminal Help
Red Hat Keypair Generation (c) 2006 Red Hat, Inc.
Collecting random data
To generate 4096 random bits from the kernel random number
generator, some keyboard or mouse input may be necessary at
the console for this host. Please try entering some random
text or moving the mouse, if running this program locally.
91%
root@localhost:~/Des...

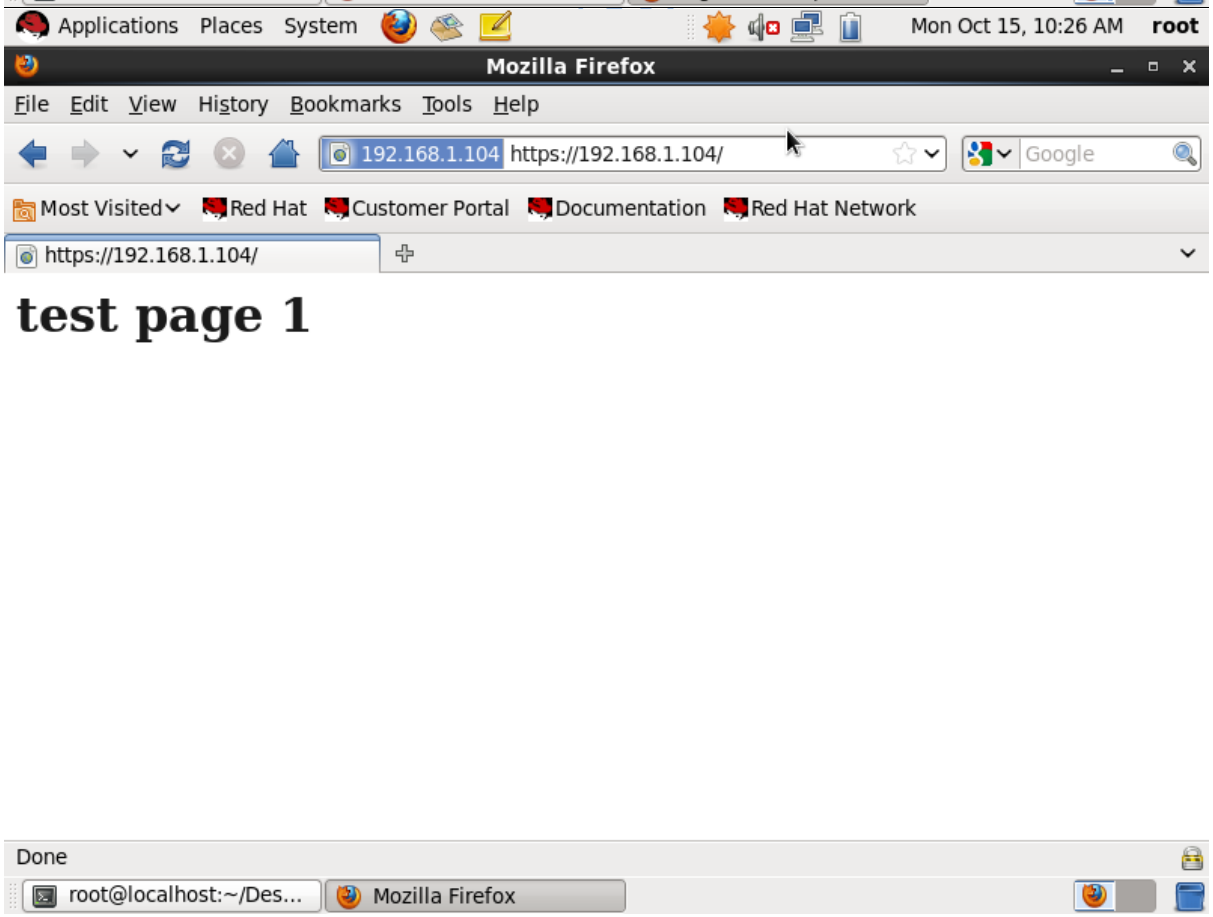

Applications Places System
Mon Oct 15, 10:10 AM root
root@localhost:~/Desktop
File Edit View Search Terminal Help
Generate CSR
Would you like to send a Certificate Request (CSR)
to a Certificate Authority (CA)?
Yes
No
root@localhost:~/Des...


Applications Places System
Mon Oct 15, 10:10 AM root
root@localhost:~/Desktop
File Edit View Search Terminal Help
Protecting your private key
At this stage you can set the passphrase on your private key. If you
set the passphrase you will have to enter it every time the server
starts. The passphrase you use to encrypt your key must be the same
for all the keys used by the same server installation.
If you do not encrypt your key, then if someone breaks into your
server and grabs the file containing your key, they will be able to
decrypt all communications to and from the server that were negotiated
using that key. If your key is encrypted it would be much more
work for someone to retrieve the private key.
[ ] Encrypt the private key
Next
Back
Cancel
root@localhost:~/Des...


Applications Places System
Mon Oct 15, 10:12 AM root
root@localhost:~/Desktop
File Edit View Search Terminal Help
Enter details for your certificate
You are about to be asked to enter information that will be
incorporated into your certificate request to a CA. What you are
about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank.
Country Name (ISO 2 letter code) IN
State or Province Name (full name) MAHARASHTRA
Locality Name (e.g. city) MUMBAI
Organization Name (eg, company) UNITY
Organizational Unit Name (eg, section) UNITY MODULE 1
Common Name (fully qualified domain name) localhost.localdomain
Extra attributes for certificate request:
Optional challenge password root123
Optional company name
Next
Back
Cancel
root@localhost:~/Des...


Applications Places System
Mon Oct 15, 10:19 AM root
root@localhost:~/Desktop
File Edit View Search Terminal Help
/usr/bin/keyutil: Improperly formatted name: "CN=localhost.localdomain, OU=UNITY MODULE 1, O=UNIT
Y, L=MUMBAI, ST=MAHARASHTRA, C=IN, Challenge=root123"
: security library: invalid AVA.
[root@localhost Desktop]# genkey --days 365 localhost.localdomain
/usr/bin/keyutil -c makecert -g 2048 -s "CN=localhost.localdomain, OU=UNITY MODULE 1, O=UNITY, L=
MUMBAI, ST=MAHARASHTRAe, C=IN" -v 12 -a -z /etc/pki/tls/.rand.2965 -o /etc/pki/tls/certs/localhos
t.localdomain.crt -k /etc/pki/tls/private/localhost.localdomain.key
cmdstr: makecert
cmd_CreateNewCert
command: makecert
keysize = 2048 bits
subject = CN=localhost.localdomain, OU=UNITY MODULE 1, O=UNITY, L=MUMBAI, ST=MAHARASHTRAe, C=IN
valid for 12 months
random seed from /etc/pki/tls/.rand.2965
output will be written to /etc/pki/tls/certs/localhost.localdomain.crt
output key written to /etc/pki/tls/private/localhost.localdomain.key
Generating key. This may take a few moments...
Made a key
Opened tmprequest for writing
/usr/bin/keyutil Copying the cert pointer
Created a certificate
Wrote 1682 bytes of encoded data to /etc/pki/tls/private/localhost.localdomain.key
Wrote the key to:
/etc/pki/tls/private/localhost.localdomain.key
[root@localhost Desktop]#
root@localhost:~/Des...


Applications Places System
Mon Oct 15, 10:25 AM root
Certificate Viewer:"localhost.localdomain"
General Details
Certificate Hierarchy
localhost.localdomain
Certificate Fields
localhost.localdomain
Certificate
Version
Serial Number
Certificate Signature Algorithm
Issuer
Validity
Subject
Subject Public Key Info
Extensions
Certificate Signature Algorithm
Field Value
E = root@localhost.localdomain
CN = localhost.localdomain
OU = SomeOrganizationalUnit
O = SomeOrganization
L = SomeCity
root@localhost:~/Des...
Mozilla Firefox
Page Info - https://192....

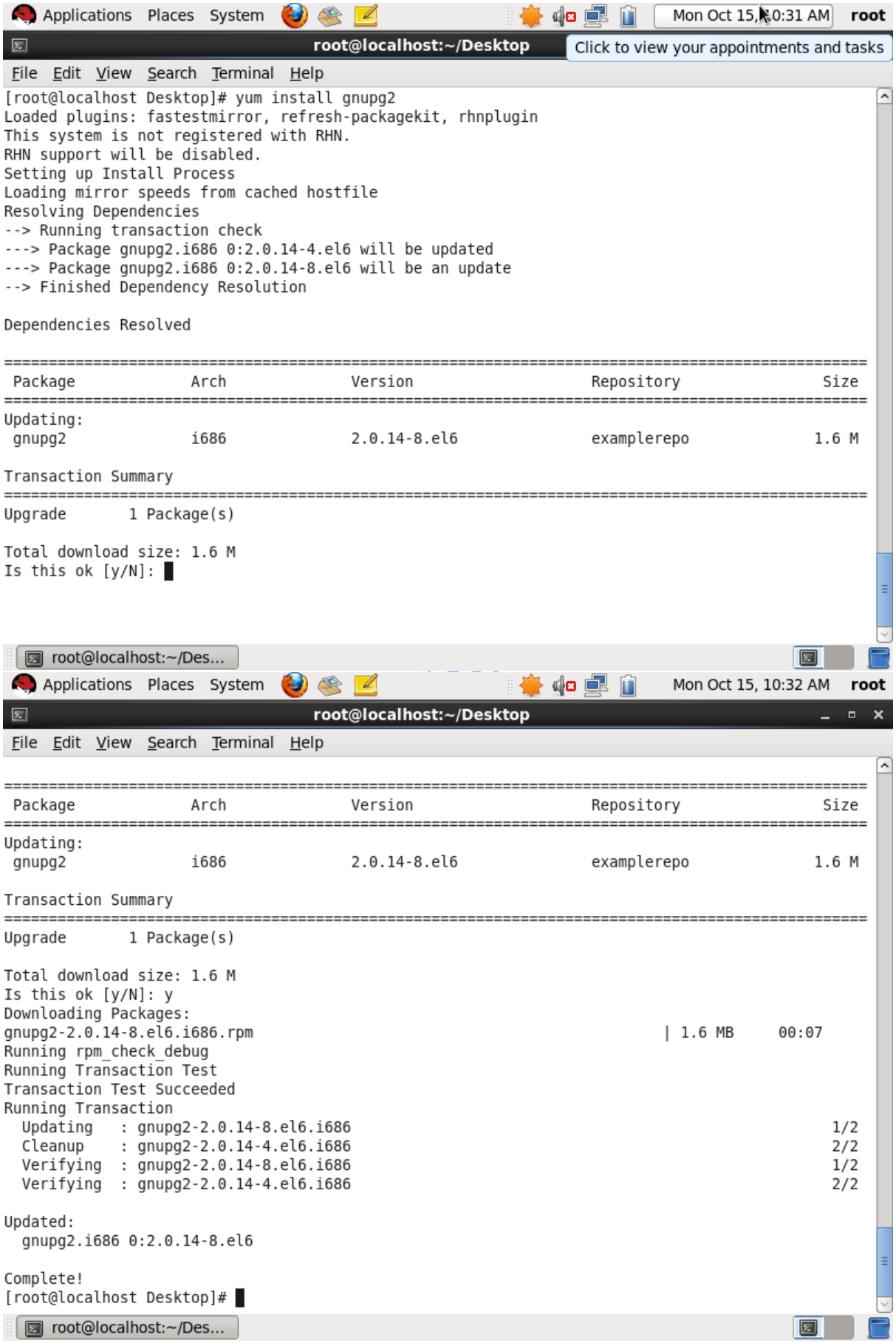

Applications Places System
Mon Oct 15, 10:26 AM root
Mozilla Firefox
File Edit View History Bookmarks Tools Help
192.168.1.104 https://192.168.1.104/
Google
Most Visited Red Hat Customer Portal Documentation Red Hat Network
https://192.168.1.104/
test page 1
Done
root@localhost:~/Des...
Mozilla Firefox

-

GPG Generation

Install gnupg2 package using command

yum install gnupg2

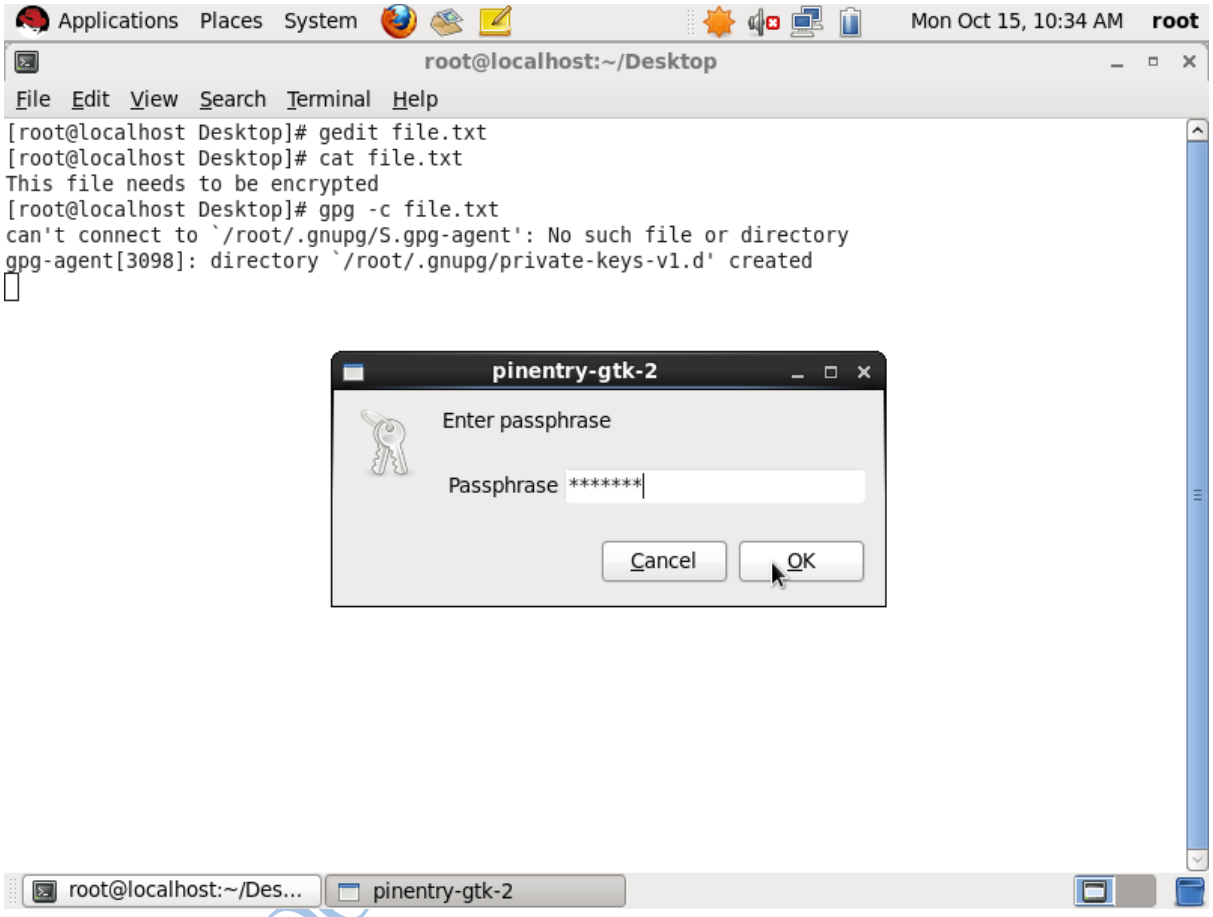

Applications Places System
Mon Oct 15, 10:31 AM root
root@localhost:~/Desktop
Click to view your appointments and tasks
File Edit View Search Terminal Help
[root@localhost Desktop]# yum install gnupg2
Loaded plugins: fastestmirror, refresh-packagekit, rhnplugin
This system is not registered with RHN.
RHN support will be disabled.
Setting up Install Process
Loading mirror speeds from cached hostfile
Resolving Dependencies
--> Running transaction check
---> Package gnupg2.i686 0:2.0.14-4.el6 will be updated
---> Package gnupg2.i686 0:2.0.14-8.el6 will be an update
--> Finished Dependency Resolution
Dependencies Resolved
Package Arch Version Repository Size
Updating:
gnupg2 i686 2.0.14-8.el6 examplerepo 1.6 M
Transaction Summary
Upgrade 1 Package(s)
Total download size: 1.6 M
Is this ok [y/N]:
root@localhost:~/Des...
Applications Places System
Mon Oct 15, 10:32 AM root
root@localhost:~/Desktop
File Edit View Search Terminal Help
Package Arch Version Repository Size
Updating:
gnupg2 i686 2.0.14-8.el6 examplerepo 1.6 M
Transaction Summary
Upgrade 1 Package(s)
Total download size: 1.6 M
Is this ok [y/N]: y
Downloading Packages:
gnupg2-2.0.14-8.el6.i686.rpm | 1.6 MB 00:07
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
Updating : gnupg2-2.0.14-8.el6.i686 1/2
Cleanup : gnupg2-2.0.14-4.el6.i686 2/2
Verifying : gnupg2-2.0.14-8.el6.i686 1/2
Verifying : gnupg2-2.0.14-4.el6.i686 2/2
Updated:
gnupg2.i686 0:2.0.14-8.el6
Complete!
[root@localhost Desktop]#
root@localhost:~/Des...

Create a file and Encrypt using command

gedit file.txt

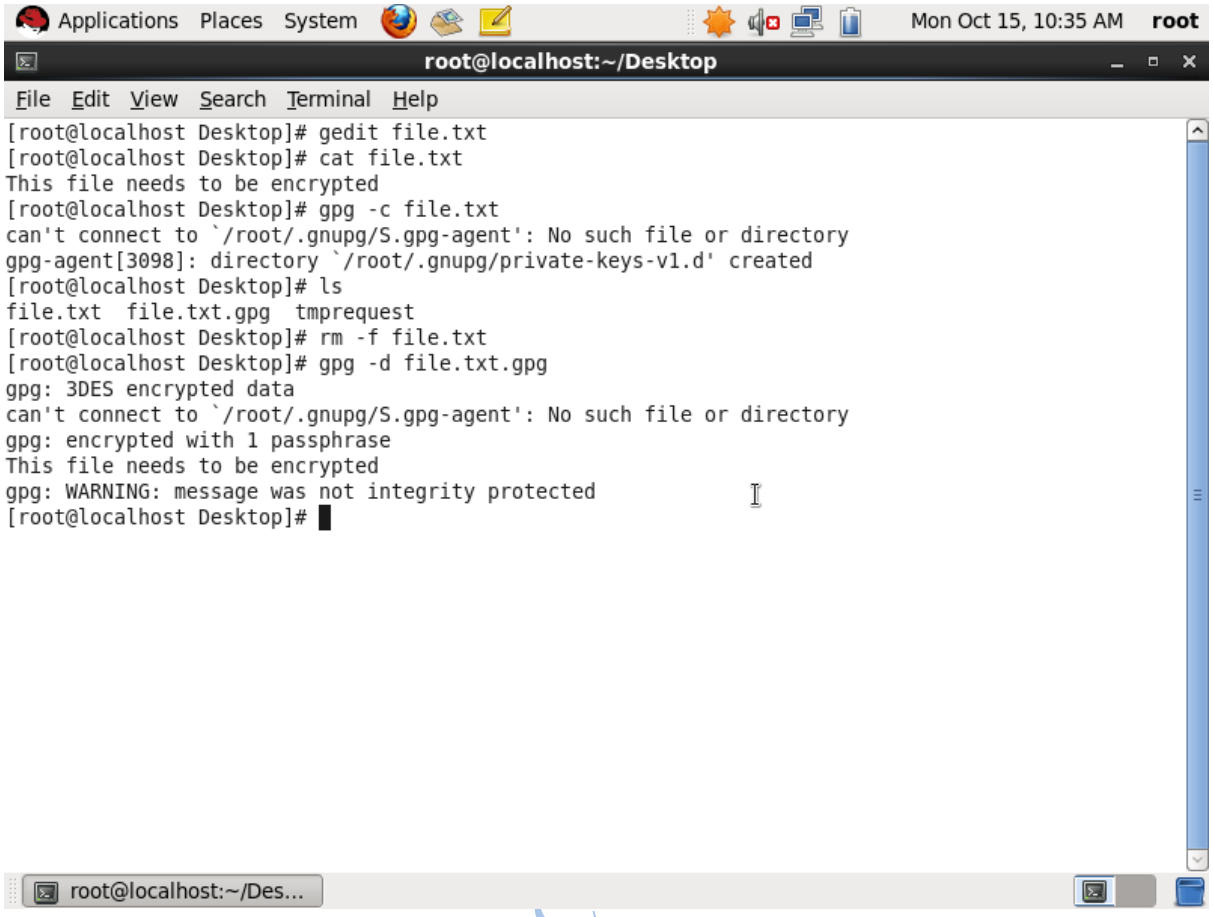
cat file.txt

gpg –c file.txt



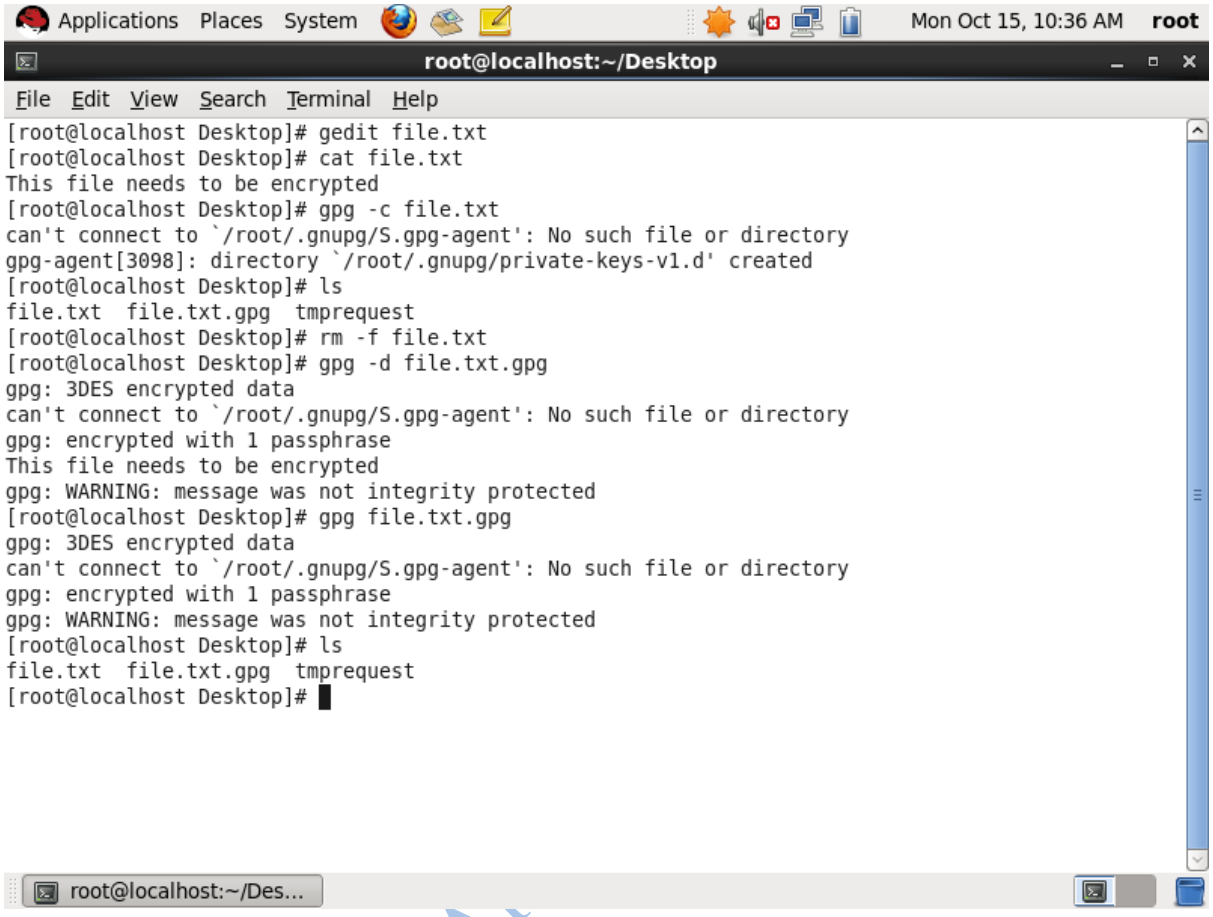
Decrypt to read

gpg –d file.txt.gpg

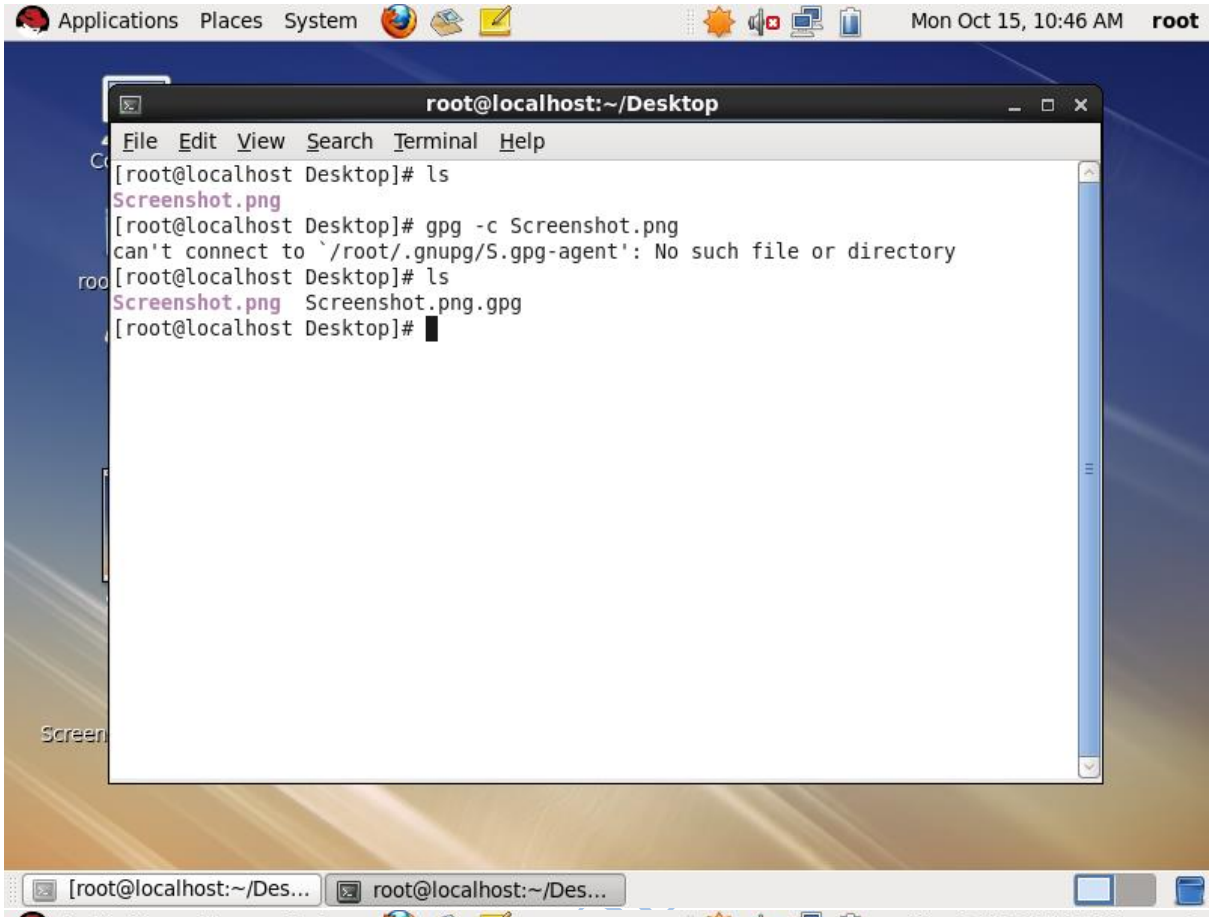


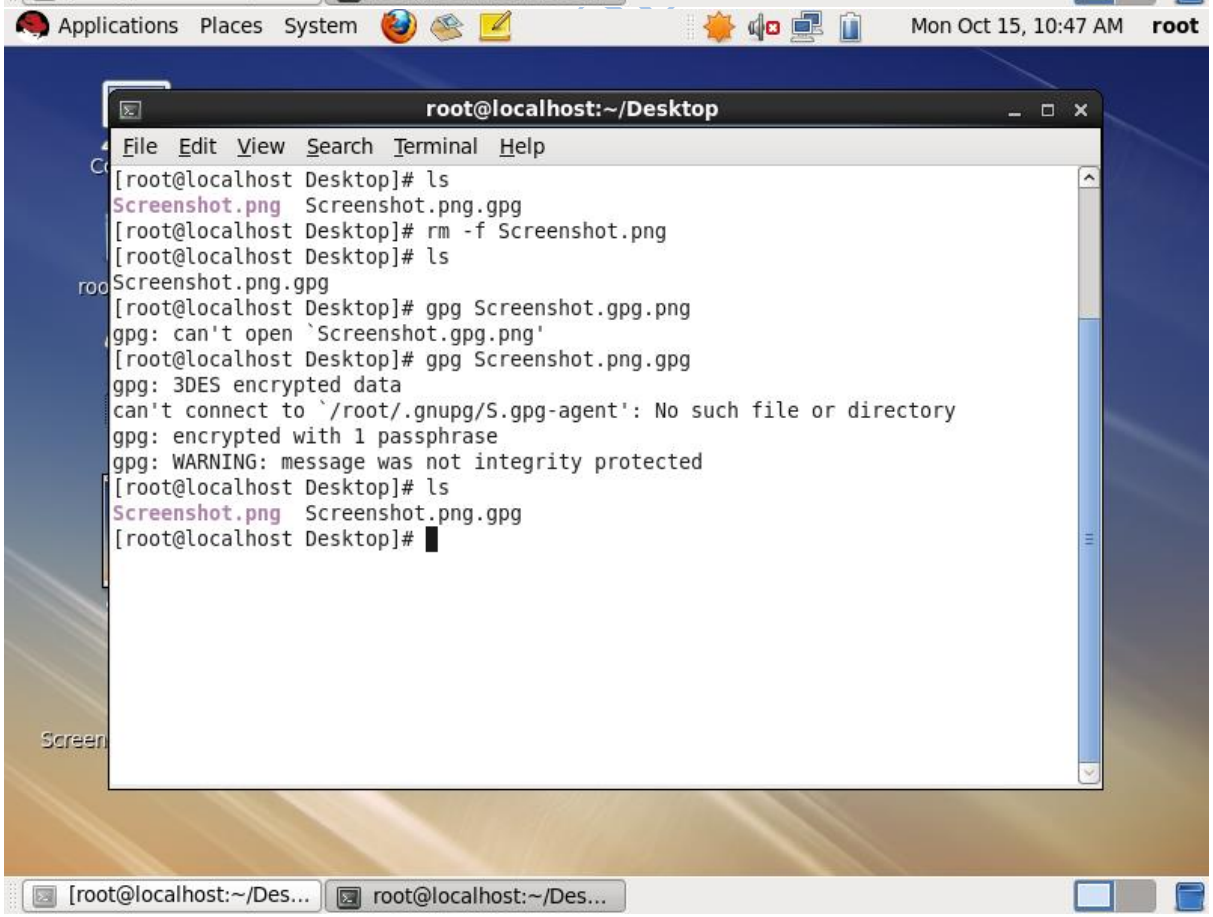
Permanent decrypt

Gpg file.txt.gpg



Encrypt and decrypt image also


Applications Places System
Mon Oct 15, 10:46 AM root
root@localhost:~/Desktop
File Edit View Search Terminal Help
[root@localhost Desktop]# ls
Screenshot.png
[root@localhost Desktop]# gpg -c Screenshot.png
can't connect to `/root/.gnupg/S.gpg-agent': No such file or directory
[root@localhost Desktop]# ls
Screenshot.png Screenshot.png.gpg
[root@localhost Desktop]#
[root@localhost:~/Des...
root@localhost:~/Des...


Applications Places System
Mon Oct 15, 10:47 AM root
root@localhost:~/Desktop
File Edit View Search Terminal Help
[root@localhost Desktop]# ls
Screenshot.png Screenshot.png.gpg
[root@localhost Desktop]# rm -f Screenshot.png
[root@localhost Desktop]# ls
Screenshot.png.gpg
[root@localhost Desktop]# gpg Screenshot.gpg.png
gpg: can't open `Screenshot.gpg.png'
[root@localhost Desktop]# gpg Screenshot.png.gpg
gpg: 3DES encrypted data
can't connect to `/root/.gnupg/S.gpg-agent': No such file or directory
gpg: encrypted with 1 passphrase
gpg: WARNING: message was not integrity protected
[root@localhost Desktop]# ls
Screenshot.png Screenshot.png.gpg
[root@localhost Desktop]#
[root@localhost:~/Des...
root@localhost:~/Des...