Strategies For Securing a Linux System

Donald Buchan
malak@malak.ca

May/August 2009

Translated & Updated January 2011

Overview

- Use a router
- All users should have their own account
- Manage Passwords
- Control Access to Your Desktop
- Perform Updates Regularly
- Install Software From Repositories
- Activate Your Firewall and Tune Appropriately
- Turn Off Unneeded Services
- Limit SSH Access to only the users you allow, and exclude the root user
- Install DenyHosts
- Other Strategies
    - Install SELinux and Operate it in enforcing mode
    - Use NoScript
    - Encrypt your filesystem
    - Remove accumulated junk
    - Don't automount devices
    - Close root sessions at the command line

-Protect your system's physical integrity

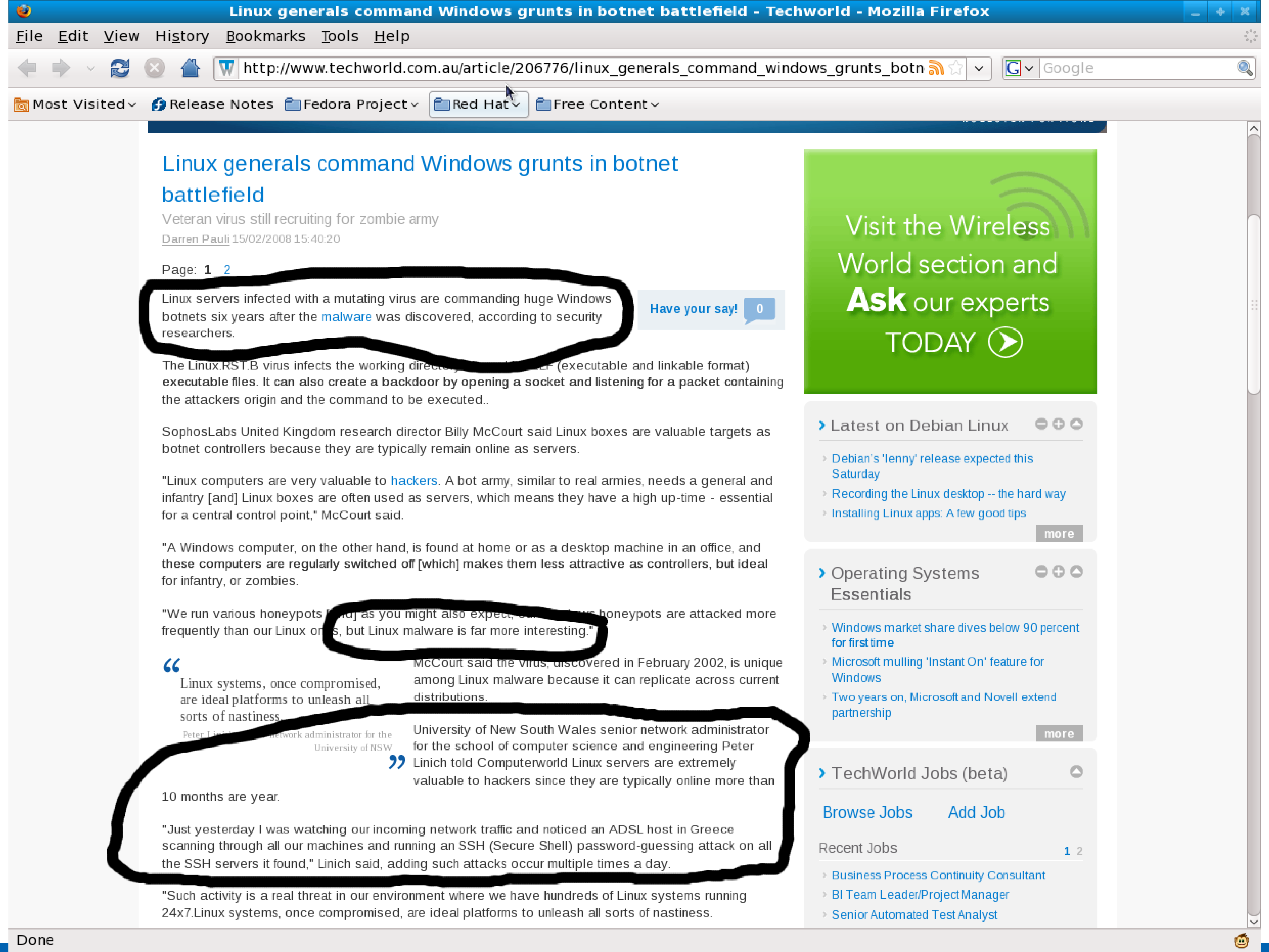
Why should you protect your system?

Why should you protect your linux system?

- Crackers want to compromise your system to do nefarious things, or just for the challenge;
- You don't want your system to be used for illicit or illegal activities (spam, porn, or financial or identity theft);
- A compromised Linux system is worth more than a compromised Windows system.

Why should you protect your linux system?

- You have personal files to protect – it's no one's business but yours that you like wine, nature walks, or Barbie dolls – unless, of course, you wish to share that information!
- ***Simply put, it's your computer, to be used for your purposes as you see fit.***


Linux generals command Windows grunts in botnet battlefield - Techworld - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.techworld.com.au/article/206776/linux_generals_command_windows_grunts_botn
Google
Most Visited
Release Notes
Fedora Project
Red Hat
Free Content

Linux generals command Windows grunts in botnet battlefield

Veteran virus still recruiting for zombie army

Darren Pauli 15/02/2008 15:40:20

Page: 1 2

Linux servers infected with a mutating virus are commanding huge Windows botnets six years after the malware was discovered, according to security researchers.

Have your say! 0

The Linux.RST.B virus infects the working direct[illegible] ELF (executable and linkable format) executable files. It can also create a backdoor by opening a socket and listening for a packet containing the attackers origin and the command to be executed..

SophosLabs United Kingdom research director Billy McCourt said Linux boxes are valuable targets as botnet controllers because they are typically remain online as servers.

"Linux computers are very valuable to hackers. A bot army, similar to real armies, needs a general and infantry [and] Linux boxes are often used as servers, which means they have a high up-time - essential for a central control point," McCourt said.

"A Windows computer, on the other hand, is found at home or as a desktop machine in an office, and these computers are regularly switched off [which] makes them less attractive as controllers, but ideal for infantry, or zombies.

"We run various honeypots [illegible] as you might also expect, [illegible] honeypots are attacked more frequently than our Linux ones, but Linux malware is far more interesting."

McCourt said the virus, discovered in February 2002, is unique among Linux malware because it can replicate across current distributions.

University of New South Wales senior network administrator for the school of computer science and engineering Peter Linich told Computerworld Linux servers are extremely valuable to hackers since they are typically online more than 10 months are year.

> “Linux systems, once compromised, are ideal platforms to unleash all sorts of nastiness.”
>
> Peter [illegible] network administrator for the University of NSW

"Just yesterday I was watching our incoming network traffic and noticed an ADSL host in Greece scanning through all our machines and running an SSH (Secure Shell) password-guessing attack on all the SSH servers it found," Linich said, adding such attacks occur multiple times a day.

"Such activity is a real threat in our environment where we have hundreds of Linux systems running 24x7.Linux systems, once compromised, are ideal platforms to unleash all sorts of nastiness.

Latest on Debian Linux

- Debian's 'lenny' release expected this Saturday
- Recording the Linux desktop -- the hard way
- Installing Linux apps: A few good tips

more

Operating Systems Essentials

- Windows market share dives below 90 percent for first time
- Microsoft mulling 'Instant On' feature for Windows
- Two years on, Microsoft and Novell extend partnership

more

TechWorld Jobs (beta)

Browse Jobs Add Job

Recent Jobs 1 2

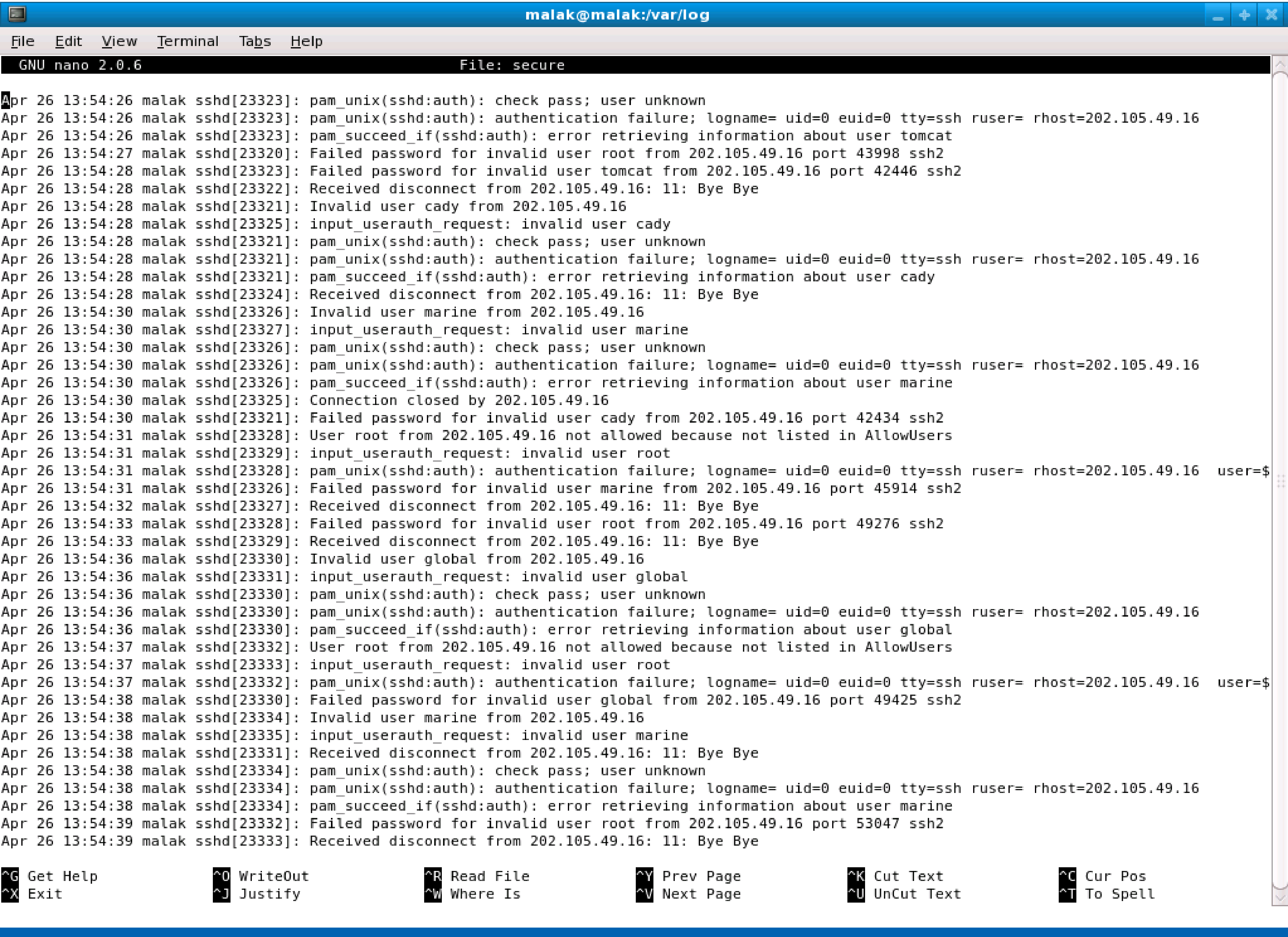
- Business Process Continuity Consultant
- BI Team Leader/Project Manager
- Senior Automated Test Analyst

Why should you protect your linux system?

The approach to take must be multi-faceted with different approaches which may or may not overlap. Some ways are automatic settings in your computer, some are habits you should adopt.

Remember: ***You have to win every day, but a cracker only has to win ONCE!***

A System Under Attack



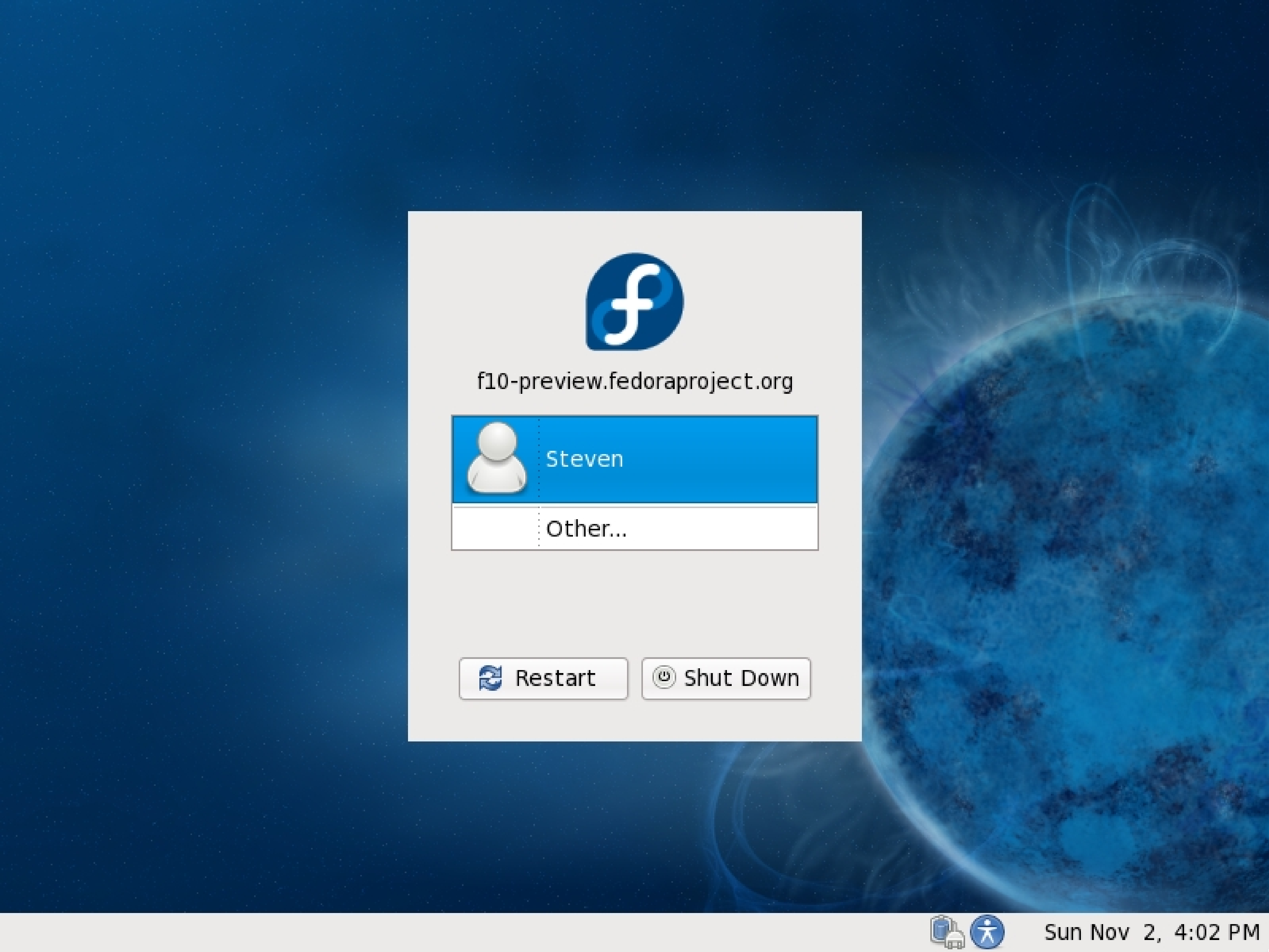
```
Apr 26 13:54:26 malak sshd[23323]: pam_unix(sshd:auth): check pass; user unknown
Apr 26 13:54:26 malak sshd[23323]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=202.105.49.16
Apr 26 13:54:26 malak sshd[23323]: pam_succeed_if(sshd:auth): error retrieving information about user tomcat
Apr 26 13:54:27 malak sshd[23320]: Failed password for invalid user root from 202.105.49.16 port 43998 ssh2
Apr 26 13:54:28 malak sshd[23323]: Failed password for invalid user tomcat from 202.105.49.16 port 42446 ssh2
Apr 26 13:54:28 malak sshd[23322]: Received disconnect from 202.105.49.16: 11: Bye Bye
Apr 26 13:54:28 malak sshd[23321]: Invalid user cady from 202.105.49.16
Apr 26 13:54:28 malak sshd[23325]: input_userauth_request: invalid user cady
Apr 26 13:54:28 malak sshd[23321]: pam_unix(sshd:auth): check pass; user unknown
Apr 26 13:54:28 malak sshd[23321]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=202.105.49.16
Apr 26 13:54:28 malak sshd[23321]: pam_succeed_if(sshd:auth): error retrieving information about user cady
Apr 26 13:54:28 malak sshd[23324]: Received disconnect from 202.105.49.16: 11: Bye Bye
Apr 26 13:54:30 malak sshd[23326]: Invalid user marine from 202.105.49.16
Apr 26 13:54:30 malak sshd[23327]: input_userauth_request: invalid user marine
Apr 26 13:54:30 malak sshd[23326]: pam_unix(sshd:auth): check pass; user unknown
Apr 26 13:54:30 malak sshd[23326]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=202.105.49.16
Apr 26 13:54:30 malak sshd[23326]: pam_succeed_if(sshd:auth): error retrieving information about user marine
Apr 26 13:54:30 malak sshd[23325]: Connection closed by 202.105.49.16
Apr 26 13:54:30 malak sshd[23321]: Failed password for invalid user cady from 202.105.49.16 port 42434 ssh2
Apr 26 13:54:31 malak sshd[23328]: User root from 202.105.49.16 not allowed because not listed in AllowUsers
Apr 26 13:54:31 malak sshd[23329]: input_userauth_request: invalid user root
Apr 26 13:54:31 malak sshd[23328]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=202.105.49.16  user=$
Apr 26 13:54:31 malak sshd[23326]: Failed password for invalid user marine from 202.105.49.16 port 45914 ssh2
Apr 26 13:54:32 malak sshd[23327]: Received disconnect from 202.105.49.16: 11: Bye Bye
Apr 26 13:54:33 malak sshd[23328]: Failed password for invalid user root from 202.105.49.16 port 49276 ssh2
Apr 26 13:54:33 malak sshd[23329]: Received disconnect from 202.105.49.16: 11: Bye Bye
Apr 26 13:54:36 malak sshd[23330]: Invalid user global from 202.105.49.16
Apr 26 13:54:36 malak sshd[23331]: input_userauth_request: invalid user global
Apr 26 13:54:36 malak sshd[23330]: pam_unix(sshd:auth): check pass; user unknown
Apr 26 13:54:36 malak sshd[23330]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=202.105.49.16
Apr 26 13:54:36 malak sshd[23330]: pam_succeed_if(sshd:auth): error retrieving information about user global
Apr 26 13:54:37 malak sshd[23332]: User root from 202.105.49.16 not allowed because not listed in AllowUsers
Apr 26 13:54:37 malak sshd[23333]: input_userauth_request: invalid user root
Apr 26 13:54:37 malak sshd[23332]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=202.105.49.16  user=$
Apr 26 13:54:38 malak sshd[23330]: Failed password for invalid user global from 202.105.49.16 port 49425 ssh2
Apr 26 13:54:38 malak sshd[23334]: Invalid user marine from 202.105.49.16
Apr 26 13:54:38 malak sshd[23335]: input_userauth_request: invalid user marine
Apr 26 13:54:38 malak sshd[23331]: Received disconnect from 202.105.49.16: 11: Bye Bye
Apr 26 13:54:38 malak sshd[23334]: pam_unix(sshd:auth): check pass; user unknown
Apr 26 13:54:38 malak sshd[23334]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=202.105.49.16
Apr 26 13:54:38 malak sshd[23334]: pam_succeed_if(sshd:auth): error retrieving information about user marine
Apr 26 13:54:39 malak sshd[23332]: Failed password for invalid user root from 202.105.49.16 port 53047 ssh2
Apr 26 13:54:39 malak sshd[23333]: Received disconnect from 202.105.49.16: 11: Bye Bye
```

Use A Router

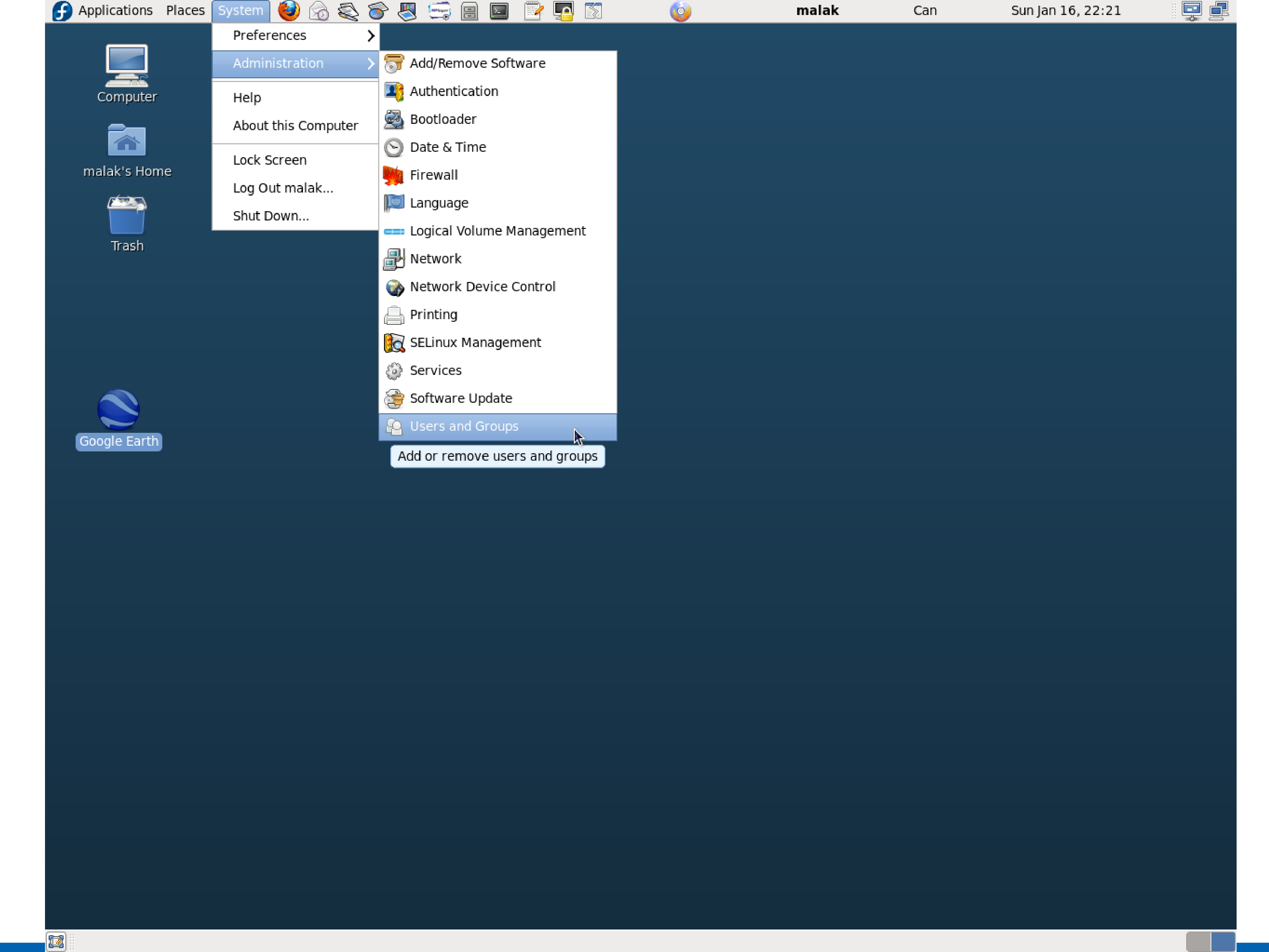
Use A Router

- Connect your computer(s) to a router, and the router to your modem.
- NAT service will block ***unexpected*** packets (scripts, scanning, crackers, login requests to various servers, etc.) from outside sources – but not from within the network it creates!

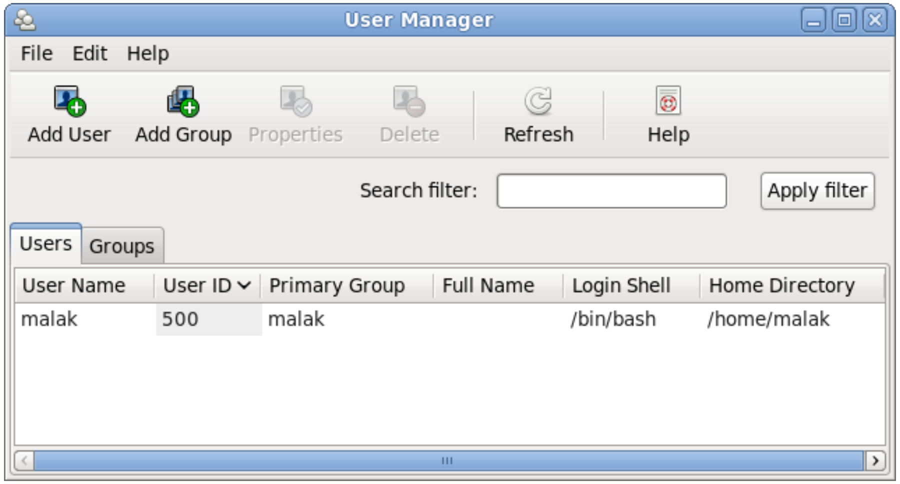
All Users Should Have Their Own Account



f10-preview.fedoraproject.org


Applications
Places
System
malak
Can
Sun Jan 16, 22:21
Preferences
Administration
Help
About this Computer
Lock Screen
Log Out malak...
Shut Down...
Add/Remove Software
Authentication
Bootloader
Date & Time
Firewall
Language
Logical Volume Management
Network
Network Device Control
Printing
SELinux Management
Services
Software Update
Users and Groups
Add or remove users and groups
Computer
malak's Home
Trash
Google Earth

All Users Should Have Their Own Account



User Name	User ID	Primary Group	Full Name	Login Shell	Home Directory
malak	500	malak		/bin/bash	/home/malak

- System | Administration | Users and Groups
- All users have their own unique account(s) with a password, however they log in: ssh, ftp, vnc, and particularly the desktop – each user's data will be safe from other users and intruders

Manage Passwords

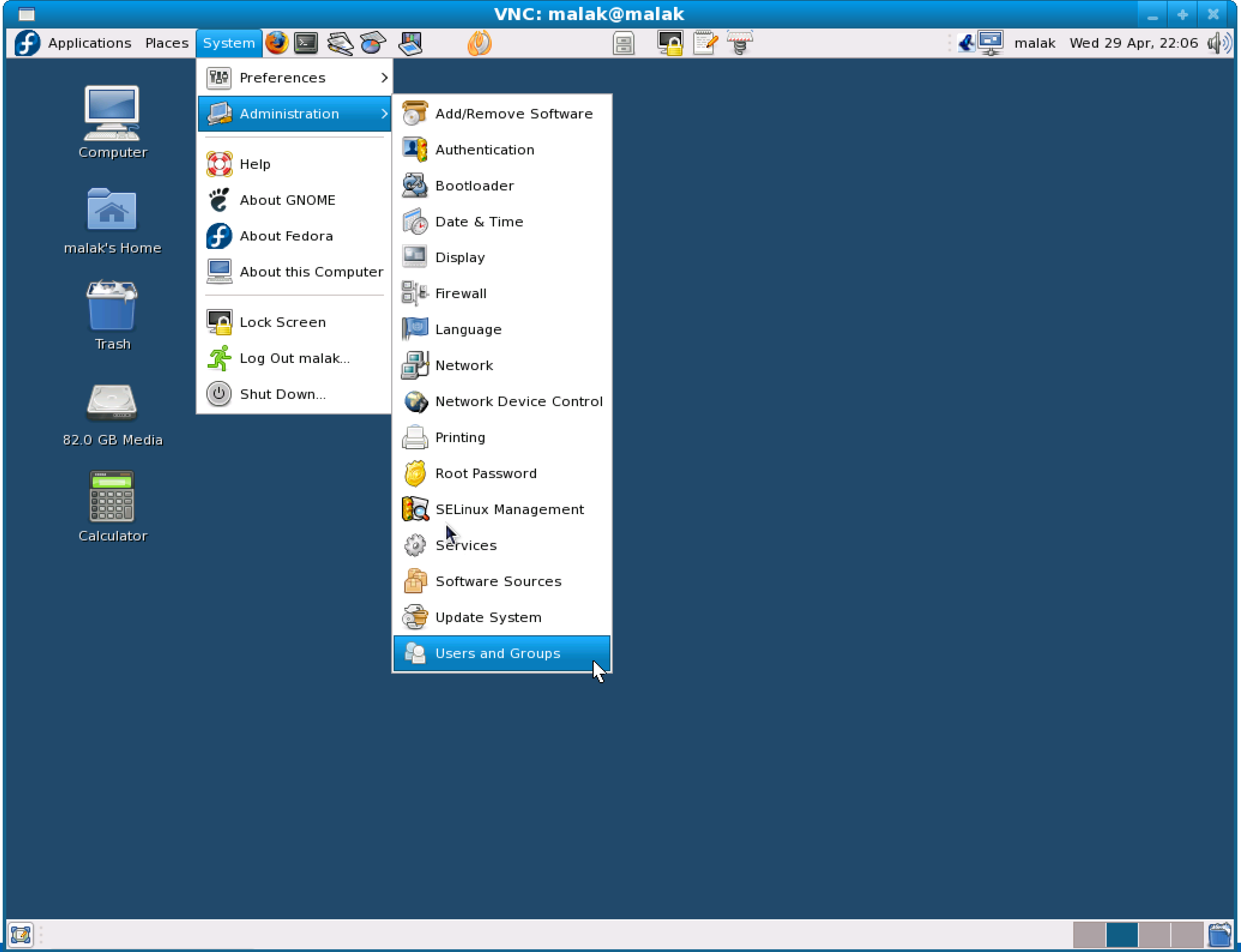
Manage Passwords

- In order to reduce the success of dictionary attacks, enforce passwords that:
  - Are at least 8 characters long
    - 1gp-w+ii instead of pwd
  - Have CAPITAL letters, small letters, digits, and special characters, such as:
    - °!"#$%?&*()_+=<>/^,
    - 1234567890

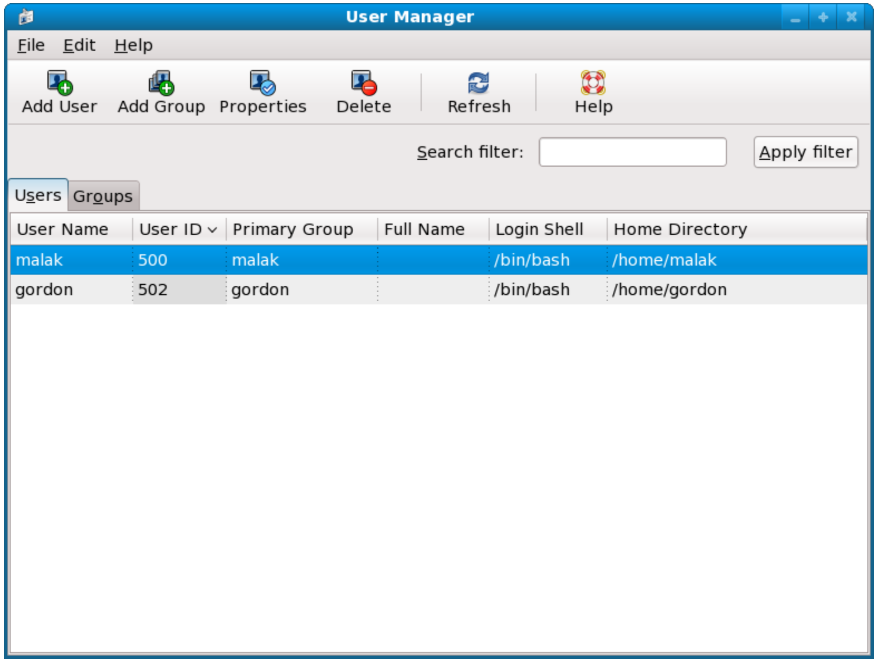
- *1Gp-W+ii* instead of *password*

Managing Passwords

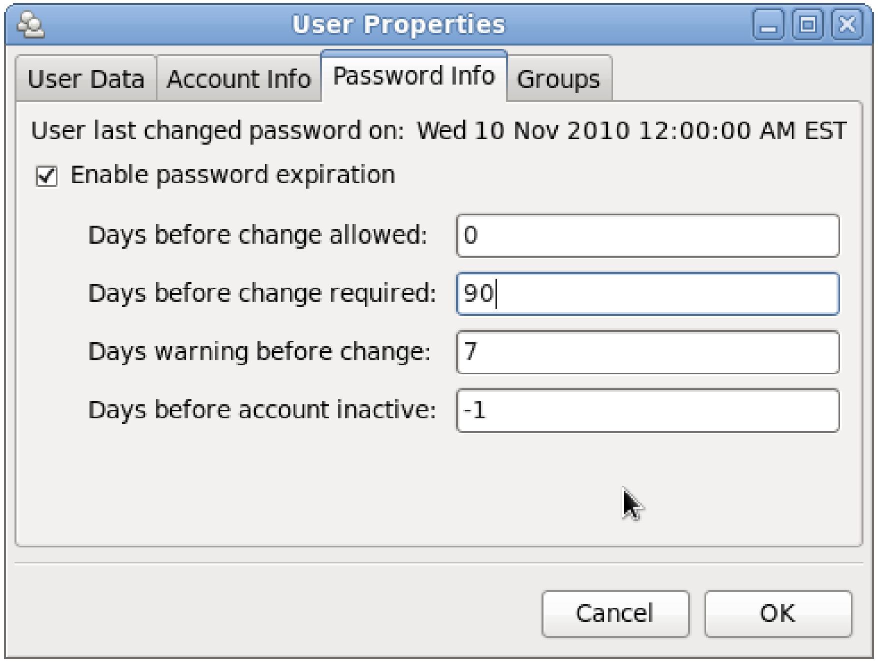
- That are easy to remember but hard to guess, such as the initials to a memorable phrase
    - 1Gp-W+ii --> “(***1*** ***G***ood ***P***ass***W***ord ***I***s ***I***mportant)”
- Give the root an unique password – useful if your account is compromised and the attacker knows your password (see SSH access)


VNC: malak@malak
Applications
Places
System
malak
Wed 29 Apr, 22:06
Computer
malak's Home
Trash
82.0 GB Media
Calculator
Preferences
Administration
Help
About GNOME
About Fedora
About this Computer
Lock Screen
Log Out malak...
Shut Down...
Add/Remove Software
Authentication
Bootloader
Date & Time
Display
Firewall
Language
Network
Network Device Control
Printing
Root Password
SELinux Management
Services
Software Sources
Update System
Users and Groups

Password Expiration



User Name	User ID	Primary Group	Full Name	Login Shell	Home Directory
malak	500	malak		/bin/bash	/home/malak
gordon	502	gordon		/bin/bash	/home/gordon



User last changed password on: Wed 10 Nov 2010 12:00:00 AM EST

☑ Enable password expiration

Days before change allowed: 0

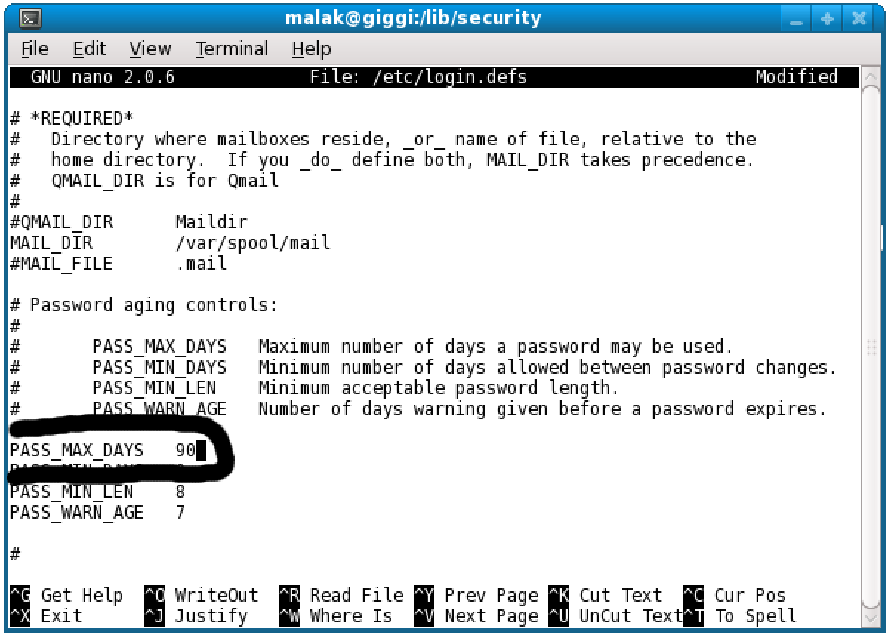
Days before change required: 90

Days warning before change: 7

Days before account inactive: -1

- Sytem Administration Users and Groups, choose user, Password Info tab
- Enforce password expiration, such as every 90 days

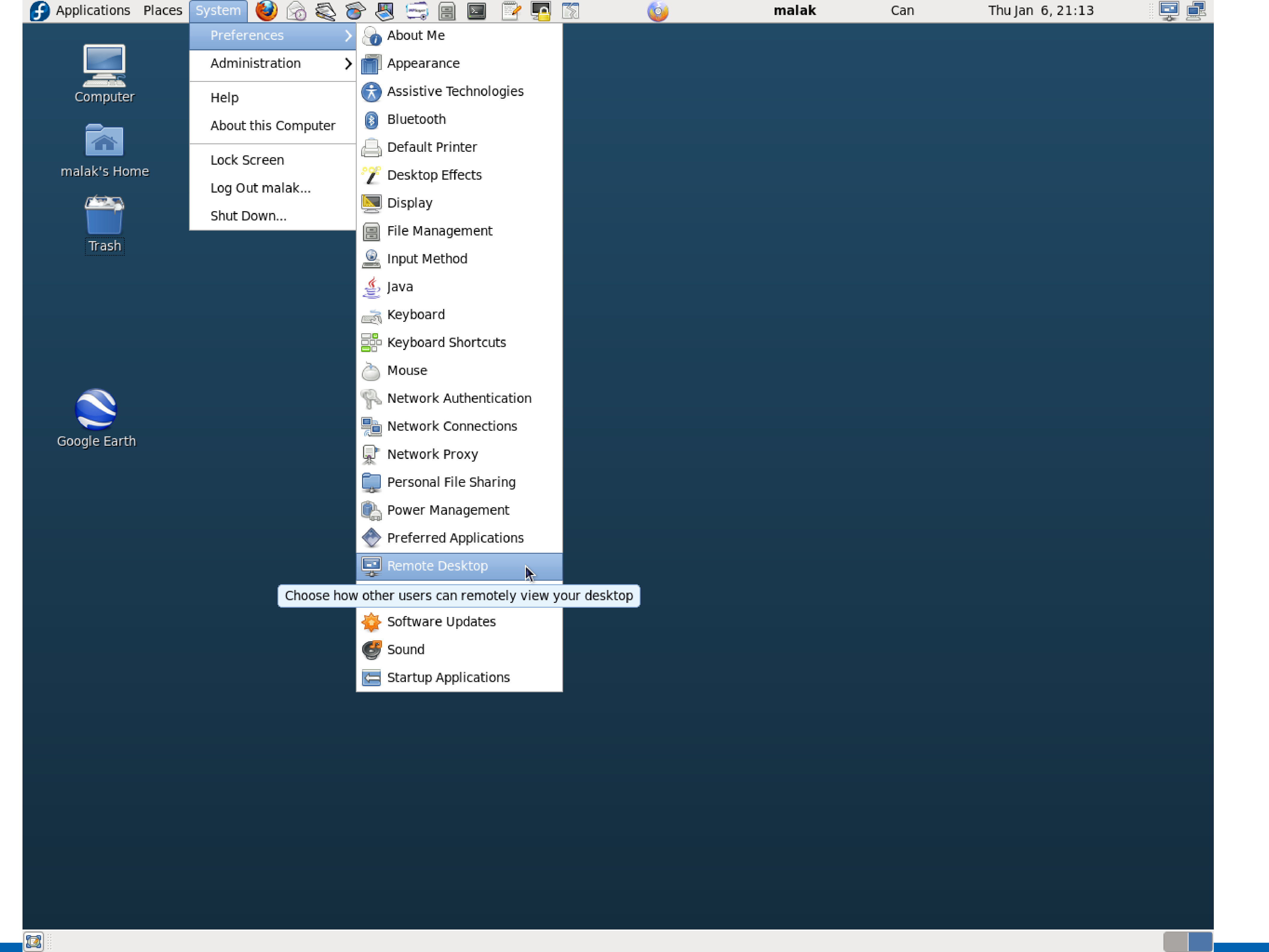
Password Expiration



```
  GNU nano 2.0.6              File: /etc/login.defs                    Modified

# *REQUIRED*
#   Directory where mailboxes reside, _or_ name of file, relative to the
#   home directory.  If you _do_ define both, MAIL_DIR takes precedence.
#   QMAIL_DIR is for Qmail
#
#QMAIL_DIR      Maildir
MAIL_DIR        /var/spool/mail
#MAIL_FILE      .mail

# Password aging controls:
#
#       PASS_MAX_DAYS   Maximum number of days a password may be used.
#       PASS_MIN_DAYS   Minimum number of days allowed between password changes.
#       PASS_MIN_LEN    Minimum acceptable password length.
#       PASS_WARN_AGE   Number of days warning given before a password expires.
#
PASS_MAX_DAYS   90
[redacted]
PASS_MIN_LEN    8
PASS_WARN_AGE   7

#

^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

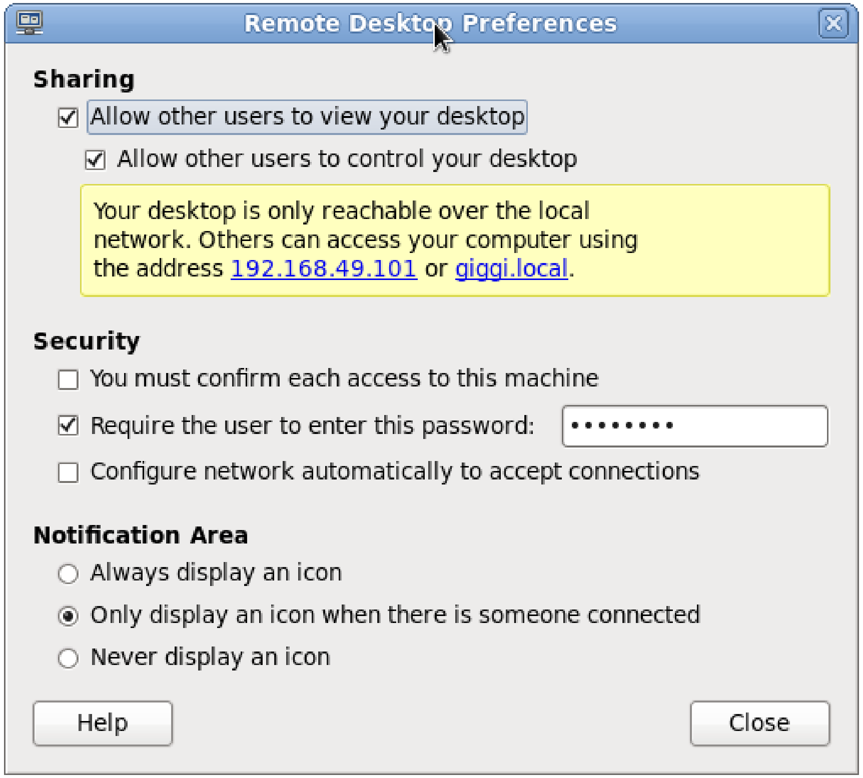
- At the command line and as root, in /etc/login.defs, modify the following line: “PASS_MAX_DAYS ” to a number such as 90 days (3 months)

Control Access To Your Desktop



Choose how other users can remotely view your desktop

Control Remote Access To Your Desktop



Remote Desktop Preferences

Sharing

☑ Allow other users to view your desktop

☑ Allow other users to control your desktop

Your desktop is only reachable over the local network. Others can access your computer using the address 192.168.49.101 or giggi.local.

Security

□ You must confirm each access to this machine

☑ Require the user to enter this password: •••••••••

□ Configure network automatically to accept connections

Notification Area

○ Always display an icon

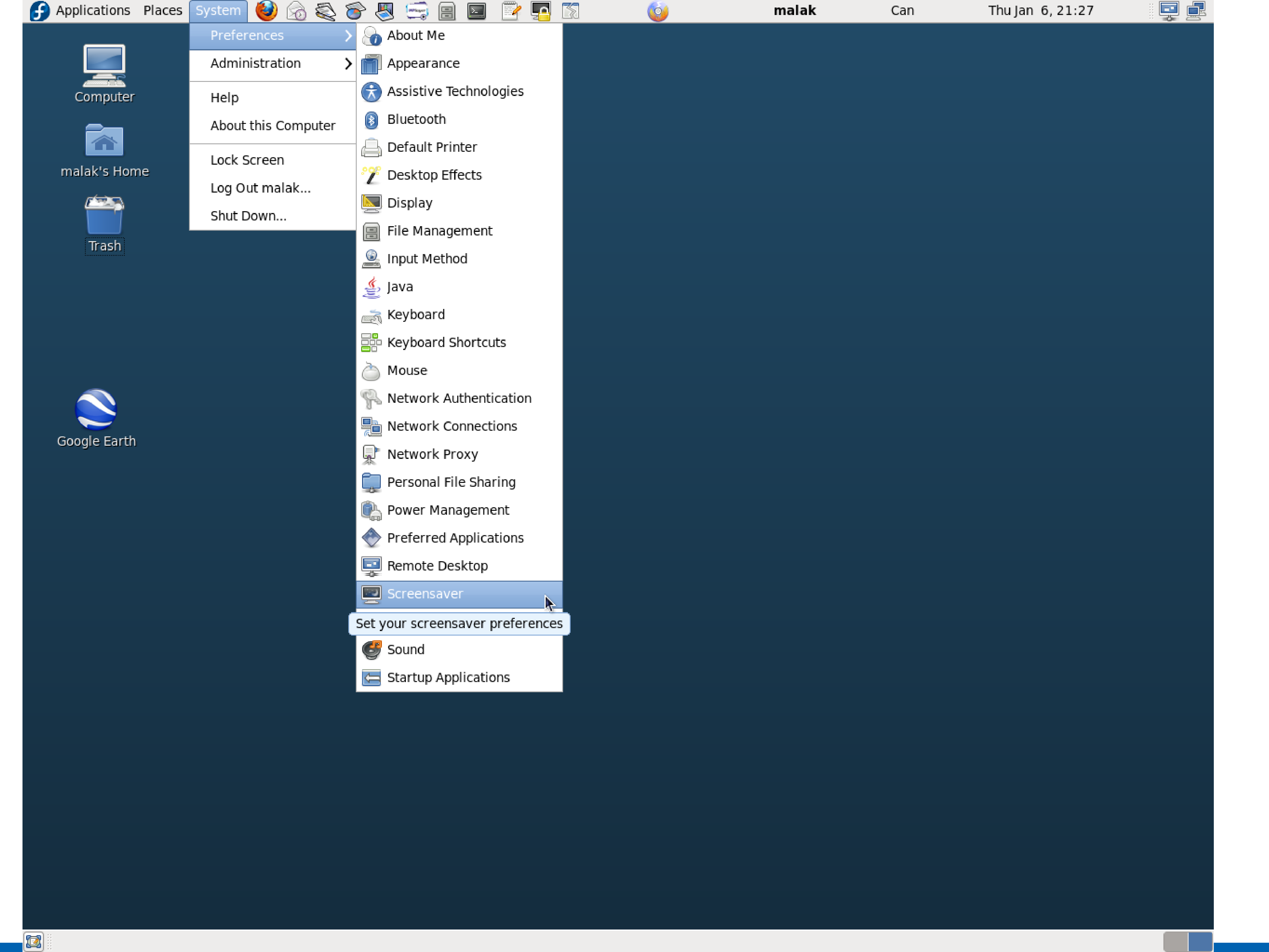
● Only display an icon when there is someone connected

○ Never display an icon

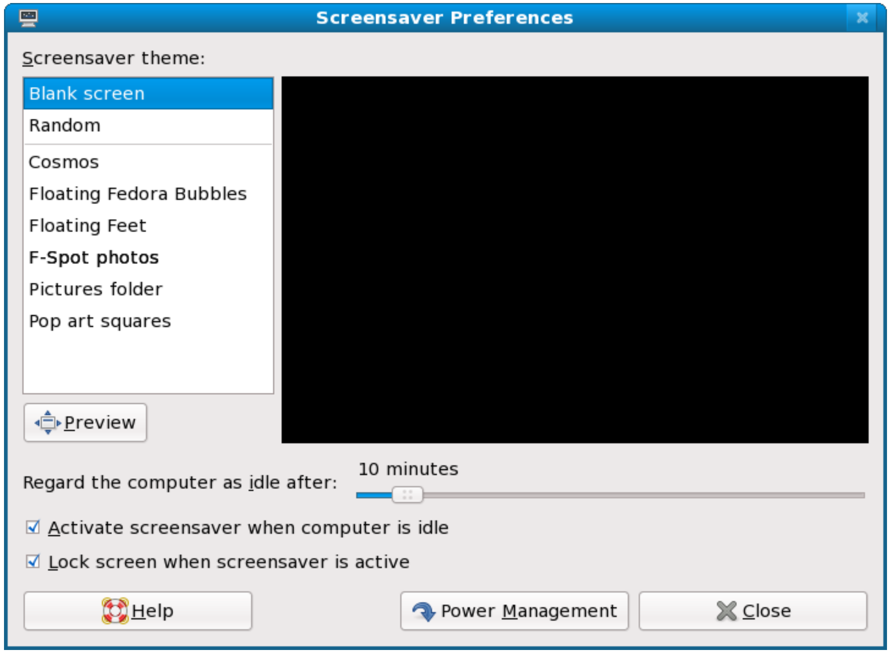
- Remote desktop control: System | Preferences | Remote Desktop
- A system with no logged in desktop users will not allow VNC access
- Note the various options, such as connection confirmation
- In enabling VNC access, you may be broadcasting its availability on Wi-Fi

Control Remote Access To Your Desktop

- The screensaver should require a password in order to unlock the screen
  - System | Preferences | Screensaver
- *This provides a certain amount of protection if you leave your computer for a few minutes (but wait for the end of this presentation!)*


Applications
Places
System
malak
Can
Thu Jan 6, 21:27
Preferences
Administration
Help
About this Computer
Lock Screen
Log Out malak...
Shut Down...
About Me
Appearance
Assistive Technologies
Bluetooth
Default Printer
Desktop Effects
Display
File Management
Input Method
Java
Keyboard
Keyboard Shortcuts
Mouse
Network Authentication
Network Connections
Network Proxy
Personal File Sharing
Power Management
Preferred Applications
Remote Desktop
Screensaver
Set your screensaver preferences
Sound
Startup Applications
Computer
malak's Home
Trash
Google Earth

Automatic Screen Lock



Screensaver Preferences

Screensaver theme:

- Blank screen
- Random
- Cosmos
- Floating Fedora Bubbles
- Floating Feet
- **F-Spot photos**
- Pictures folder
- Pop art squares

Regard the computer as idle after: 10 minutes

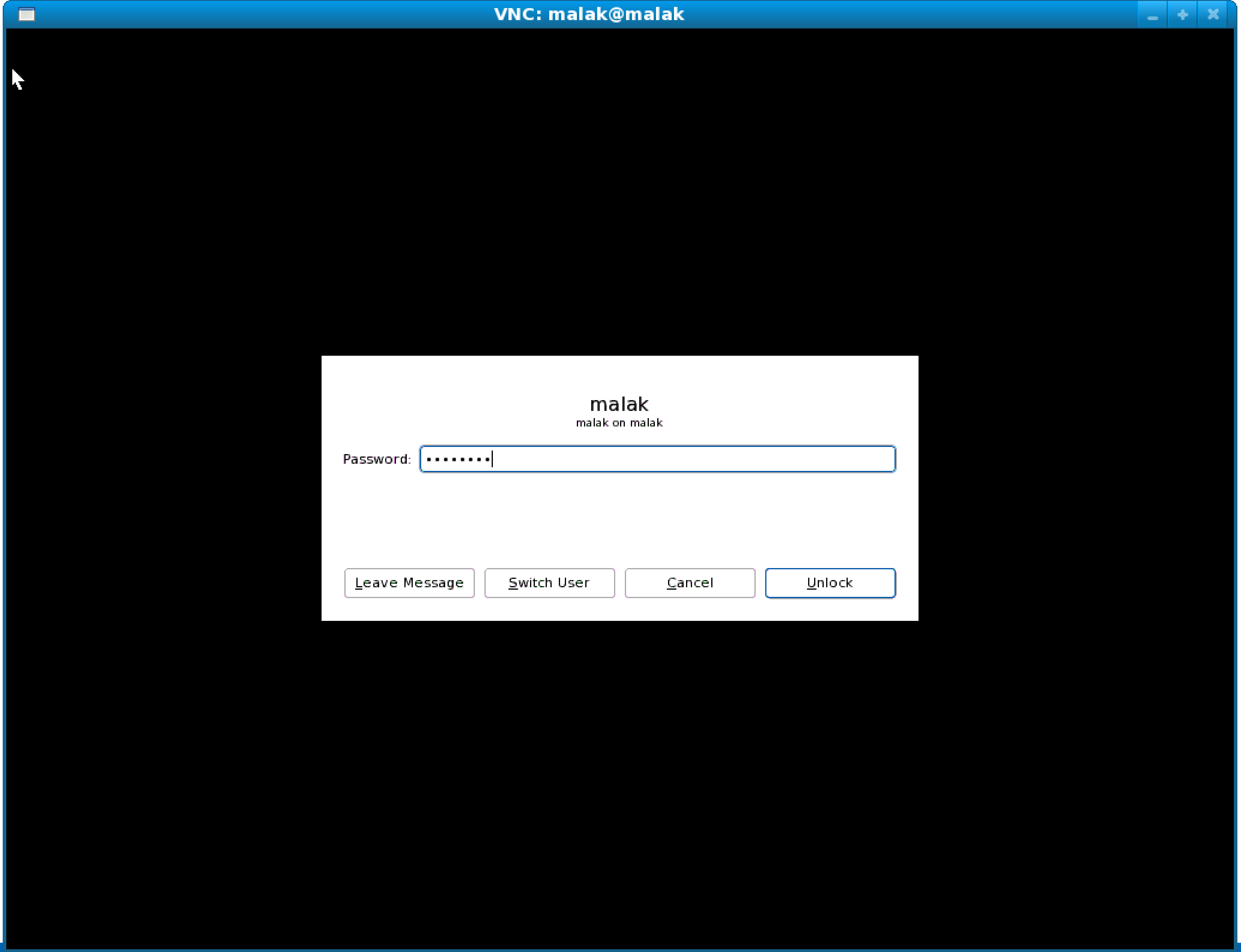
☑ Activate screensaver when computer is idle

☑ Lock screen when screensaver is active

- To automatically lock the screen using the screensaver:

  - System | Screensaver

- Click on “Activate Screen Saver when ...” and “Lock Screen when ...”, and set the delay



VNC: malak@malak

malak

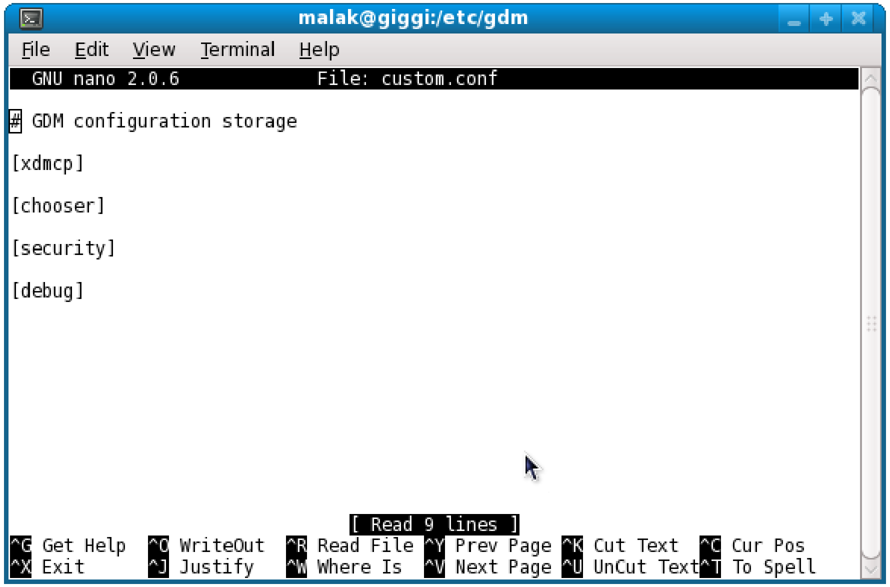
malak on malak

Password: ••••••••

Remove Automatic Login

- *Removing automatic logins provides a small amount amount of protection if you leave your computer for a few minutes (and someone reboots it) or someone steals it (but wait for the end of this presentation!)*

Remove Automatic Login



```
  GNU nano 2.0.6              File: custom.conf

# GDM configuration storage

[xdmcp]

[chooser]

[security]

[debug]

                                [ Read 9 lines ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

- At the command line and as root, modify */etc/gdm/custom.conf* and remove all lines that say “AutomaticLogin” and “AutomaticLoginEnable”

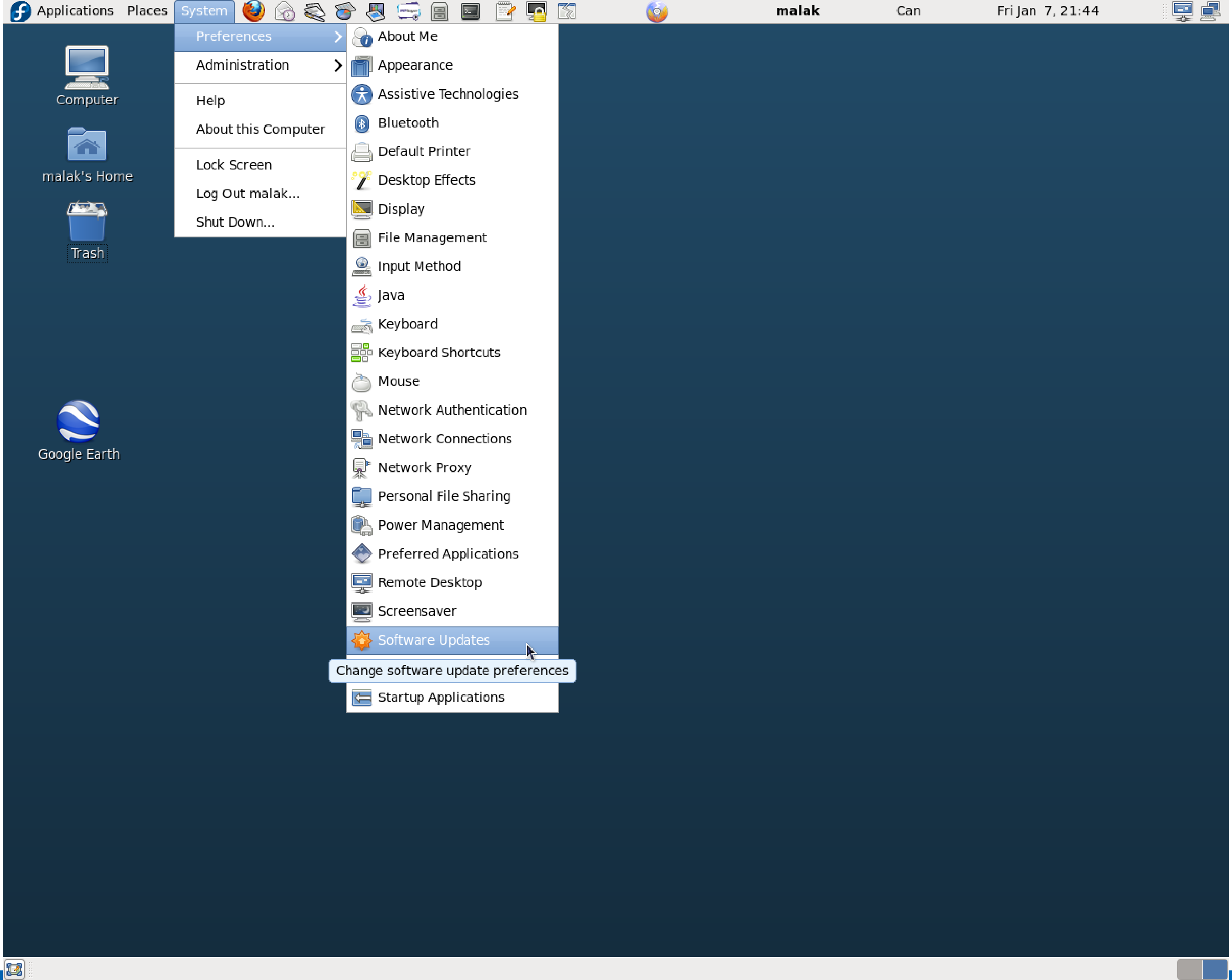
Perform Updates Regularly

Perform Updates Regularly

- Updates normally include:
  - Security patches
  - Software updates with new functions, abilities, improvements, etc.
  - The removal or replacement of packages considered obsolete or inferior to new packages
  - The installation of new software likely to be useful
  - Dependencies

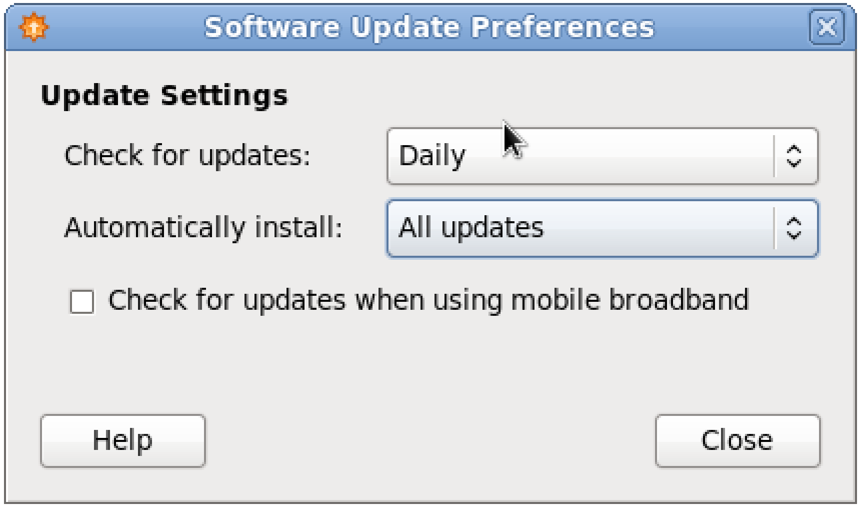
Perform Updates Regularly

- Updates are prepared by either volunteers, paid staff, or both, who work to maintain the distribution up to date, and secure, and make sure that the updates are functional, won't break your system, are complete, and appropriate.
- Updates should normally be done automatically, unless you like to keep close control.



Change software update preferences

Perform Updates Regularly



Update Settings

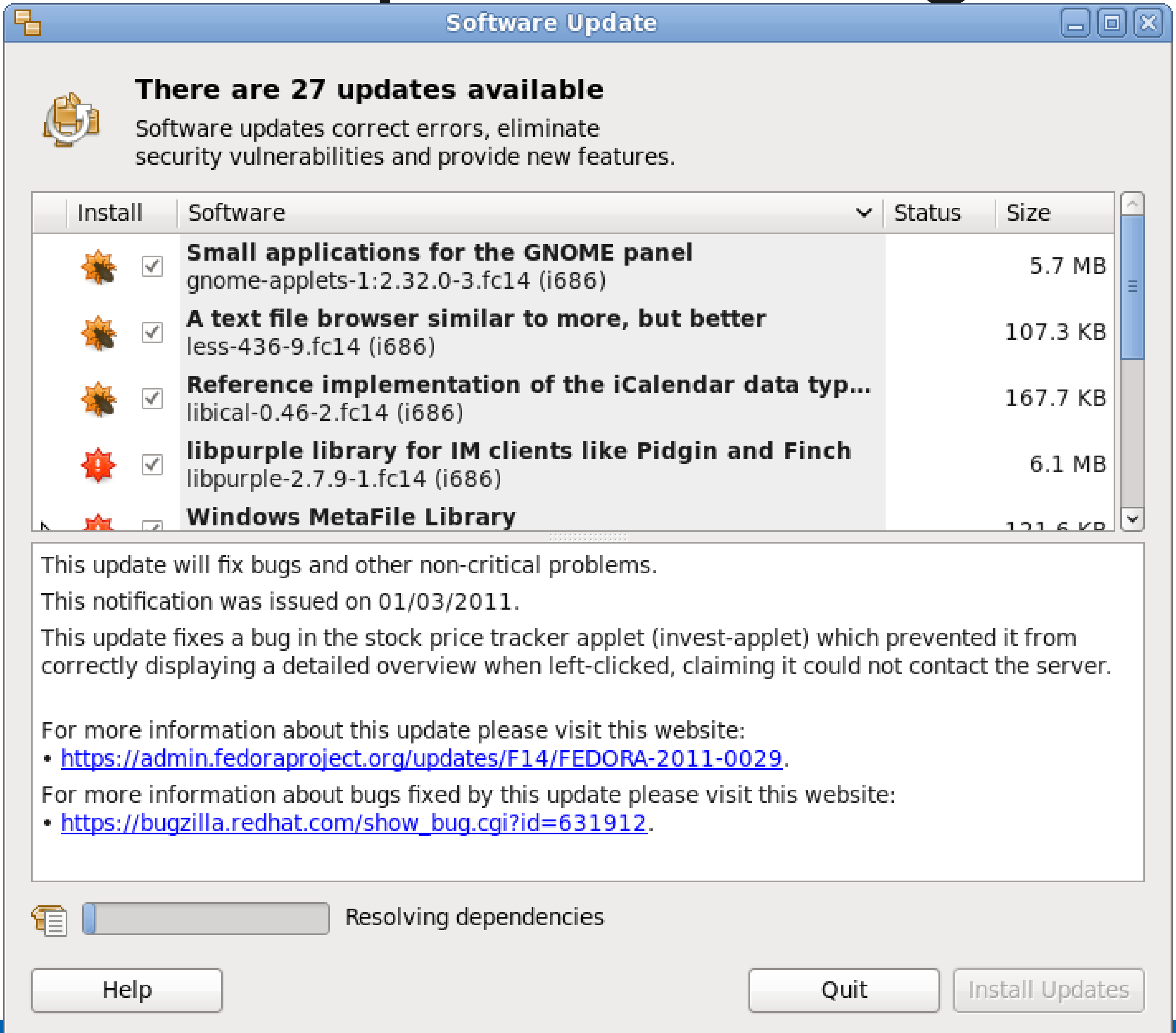
Check for updates: Daily

Automatically install: All updates

□ Check for updates when using mobile broadband

- Unless you like to manually control updates, normally your computer should perform them automatically
- System | Preferences | Software Updates

Perform Updates Regularly



There are 27 updates available

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

Install	Software	Status	Size
☑	**Small applications for the GNOME panel** gnome-applets-1:2.32.0-3.fc14 (i686)		5.7 MB
☑	**A text file browser similar to more, but better** less-436-9.fc14 (i686)		107.3 KB
☑	**Reference implementation of the iCalendar data typ…** libical-0.46-2.fc14 (i686)		167.7 KB
☑	**libpurple library for IM clients like Pidgin and Finch** libpurple-2.7.9-1.fc14 (i686)		6.1 MB
☑	**Windows MetaFile Library**		121.6 KB

This update will fix bugs and other non-critical problems.

This notification was issued on 01/03/2011.

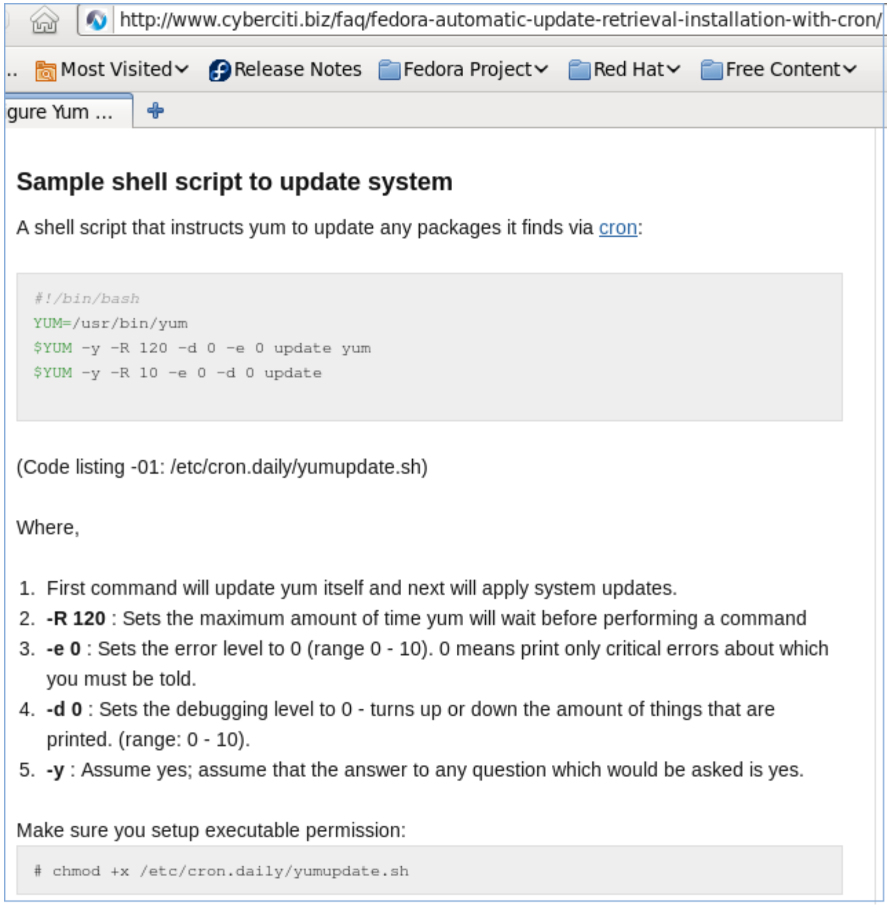
This update fixes a bug in the stock price tracker applet (invest-applet) which prevented it from correctly displaying a detailed overview when left-clicked, claiming it could not contact the server.

For more information about this update please visit this website:
- https://admin.fedoraproject.org/updates/F14/FEDORA-2011-0029.

For more information about bugs fixed by this update please visit this website:
- https://bugzilla.redhat.com/show_bug.cgi?id=631912.

Resolving dependencies

Perform Updates Regularly


http://www.cyberciti.biz/faq/fedora-automatic-update-retrieval-installation-with-cron/
Most Visited
Release Notes
Fedora Project
Red Hat
Free Content
gure Yum ...

Sample shell script to update system

A shell script that instructs yum to update any packages it finds via cron:

```
#!/bin/bash
YUM=/usr/bin/yum
$YUM -y -R 120 -d 0 -e 0 update yum
$YUM -y -R 10 -e 0 -d 0 update
```

(Code listing -01: /etc/cron.daily/yumupdate.sh)

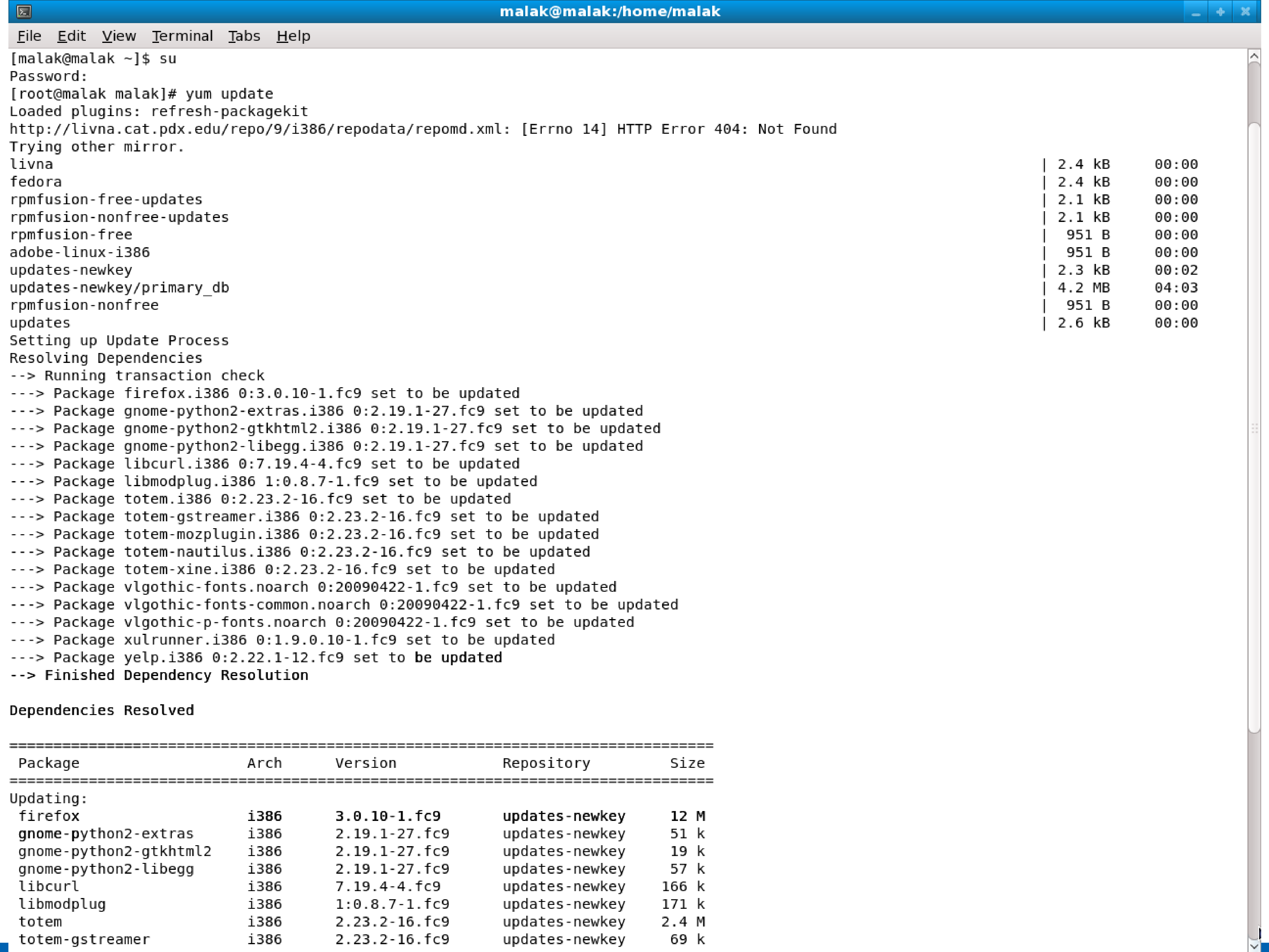
Where,

1. First command will update yum itself and next will apply system updates.
2. **-R 120** : Sets the maximum amount of time yum will wait before performing a command
3. **-e 0** : Sets the error level to 0 (range 0 - 10). 0 means print only critical errors about which you must be told.
4. **-d 0** : Sets the debugging level to 0 - turns up or down the amount of things that are printed. (range: 0 - 10).
5. **-y** : Assume yes; assume that the answer to any question which would be asked is yes.

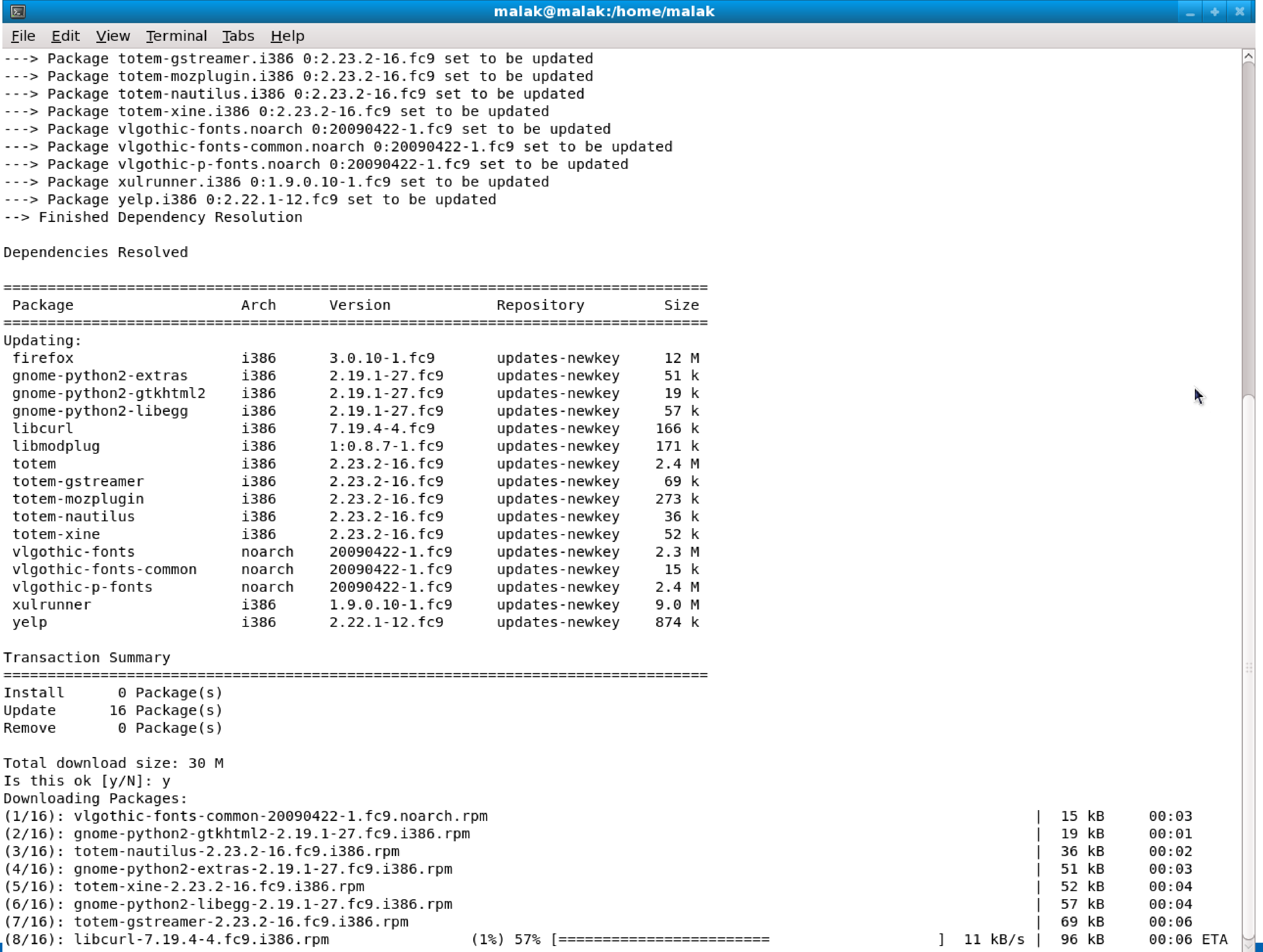
Make sure you setup executable permission:

```
# chmod +x /etc/cron.daily/yumupdate.sh
```

- Automatic updates:
  - as root, set up a cron job (see screenshot)
- Manual updates, at the command line:
  - as root, "*yum update*"
  - *Remember to do so regularly!*



```
[malak@malak ~]$ su
Password:
[root@malak malak]# yum update
Loaded plugins: refresh-packagekit
http://livna.cat.pdx.edu/repo/9/i386/repodata/repomd.xml: [Errno 14] HTTP Error 404: Not Found
Trying other mirror.
livna                                                                                                                | 2.4 kB     00:00
fedora                                                                                                               | 2.4 kB     00:00
rpmfusion-free-updates                                                                                               | 2.1 kB     00:00
rpmfusion-nonfree-updates                                                                                            | 2.1 kB     00:00
rpmfusion-free                                                                                                       |  951 B     00:00
adobe-linux-i386                                                                                                     |  951 B     00:00
updates-newkey                                                                                                       | 2.3 kB     00:02
updates-newkey/primary_db                                                                                            | 4.2 MB     04:03
rpmfusion-nonfree                                                                                                    |  951 B     00:00
updates                                                                                                              | 2.6 kB     00:00
Setting up Update Process
Resolving Dependencies
--> Running transaction check
---> Package firefox.i386 0:3.0.10-1.fc9 set to be updated
---> Package gnome-python2-extras.i386 0:2.19.1-27.fc9 set to be updated
---> Package gnome-python2-gtkhtml2.i386 0:2.19.1-27.fc9 set to be updated
---> Package gnome-python2-libegg.i386 0:2.19.1-27.fc9 set to be updated
---> Package libcurl.i386 0:7.19.4-4.fc9 set to be updated
---> Package libmodplug.i386 1:0.8.7-1.fc9 set to be updated
---> Package totem.i386 0:2.23.2-16.fc9 set to be updated
---> Package totem-gstreamer.i386 0:2.23.2-16.fc9 set to be updated
---> Package totem-mozplugin.i386 0:2.23.2-16.fc9 set to be updated
---> Package totem-nautilus.i386 0:2.23.2-16.fc9 set to be updated
---> Package totem-xine.i386 0:2.23.2-16.fc9 set to be updated
---> Package vlgothic-fonts.noarch 0:20090422-1.fc9 set to be updated
---> Package vlgothic-fonts-common.noarch 0:20090422-1.fc9 set to be updated
---> Package vlgothic-p-fonts.noarch 0:20090422-1.fc9 set to be updated
---> Package xulrunner.i386 0:1.9.0.10-1.fc9 set to be updated
---> Package yelp.i386 0:2.22.1-12.fc9 set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package                   Arch      Version            Repository         Size
================================================================================
Updating:
 firefox                   i386      3.0.10-1.fc9       updates-newkey     12 M
 gnome-python2-extras      i386      2.19.1-27.fc9      updates-newkey     51 k
 gnome-python2-gtkhtml2    i386      2.19.1-27.fc9      updates-newkey     19 k
 gnome-python2-libegg      i386      2.19.1-27.fc9      updates-newkey     57 k
 libcurl                   i386      7.19.4-4.fc9       updates-newkey    166 k
 libmodplug                i386      1:0.8.7-1.fc9      updates-newkey    171 k
 totem                     i386      2.23.2-16.fc9      updates-newkey    2.4 M
 totem-gstreamer           i386      2.23.2-16.fc9      updates-newkey     69 k
```



```
---> Package totem-gstreamer.i386 0:2.23.2-16.fc9 set to be updated
---> Package totem-mozplugin.i386 0:2.23.2-16.fc9 set to be updated
---> Package totem-nautilus.i386 0:2.23.2-16.fc9 set to be updated
---> Package totem-xine.i386 0:2.23.2-16.fc9 set to be updated
---> Package vlgothic-fonts.noarch 0:20090422-1.fc9 set to be updated
---> Package vlgothic-fonts-common.noarch 0:20090422-1.fc9 set to be updated
---> Package vlgothic-p-fonts.noarch 0:20090422-1.fc9 set to be updated
---> Package xulrunner.i386 0:1.9.0.10-1.fc9 set to be updated
---> Package yelp.i386 0:2.22.1-12.fc9 set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package                   Arch      Version            Repository        Size
================================================================================
Updating:
 firefox                   i386      3.0.10-1.fc9       updates-newkey     12 M
 gnome-python2-extras      i386      2.19.1-27.fc9      updates-newkey     51 k
 gnome-python2-gtkhtml2    i386      2.19.1-27.fc9      updates-newkey     19 k
 gnome-python2-libegg      i386      2.19.1-27.fc9      updates-newkey     57 k
 libcurl                   i386      7.19.4-4.fc9       updates-newkey    166 k
 libmodplug                i386      1:0.8.7-1.fc9      updates-newkey    171 k
 totem                     i386      2.23.2-16.fc9      updates-newkey    2.4 M
 totem-gstreamer           i386      2.23.2-16.fc9      updates-newkey     69 k
 totem-mozplugin           i386      2.23.2-16.fc9      updates-newkey    273 k
 totem-nautilus            i386      2.23.2-16.fc9      updates-newkey     36 k
 totem-xine                i386      2.23.2-16.fc9      updates-newkey     52 k
 vlgothic-fonts            noarch    20090422-1.fc9     updates-newkey    2.3 M
 vlgothic-fonts-common     noarch    20090422-1.fc9     updates-newkey     15 k
 vlgothic-p-fonts          noarch    20090422-1.fc9     updates-newkey    2.4 M
 xulrunner                 i386      1.9.0.10-1.fc9     updates-newkey    9.0 M
 yelp                      i386      2.22.1-12.fc9      updates-newkey    874 k

Transaction Summary
================================================================================
Install      0 Package(s)
Update      16 Package(s)
Remove       0 Package(s)

Total download size: 30 M
Is this ok [y/N]: y
Downloading Packages:
(1/16): vlgothic-fonts-common-20090422-1.fc9.noarch.rpm                                                              |  15 kB     00:03
(2/16): gnome-python2-gtkhtml2-2.19.1-27.fc9.i386.rpm                                                                |  19 kB     00:01
(3/16): totem-nautilus-2.23.2-16.fc9.i386.rpm                                                                        |  36 kB     00:02
(4/16): gnome-python2-extras-2.19.1-27.fc9.i386.rpm                                                                  |  51 kB     00:03
(5/16): totem-xine-2.23.2-16.fc9.i386.rpm                                                                            |  52 kB     00:04
(6/16): gnome-python2-libegg-2.19.1-27.fc9.i386.rpm                                                                  |  57 kB     00:04
(7/16): totem-gstreamer-2.23.2-16.fc9.i386.rpm                                                                       |  69 kB     00:06
(8/16): libcurl-7.19.4-4.fc9.i386.rpm                (1%) 57% [=========================                  ]  11 kB/s |  96 kB     00:06 ETA
```

Install Software From Repositories

Install Software From Repositories

- In Windows, software is downloaded from anywhere and is installed directly; it is a complete package with all the necessary parts.
- In Windows, aside from the "Windows" part, you are responsible for keeping track of all the installed software, the availability of updates and security patches, and to install them. (***Some stand-alone software have automatic update options, however they only apply to that piece of software.***)

Install Software From Repositories

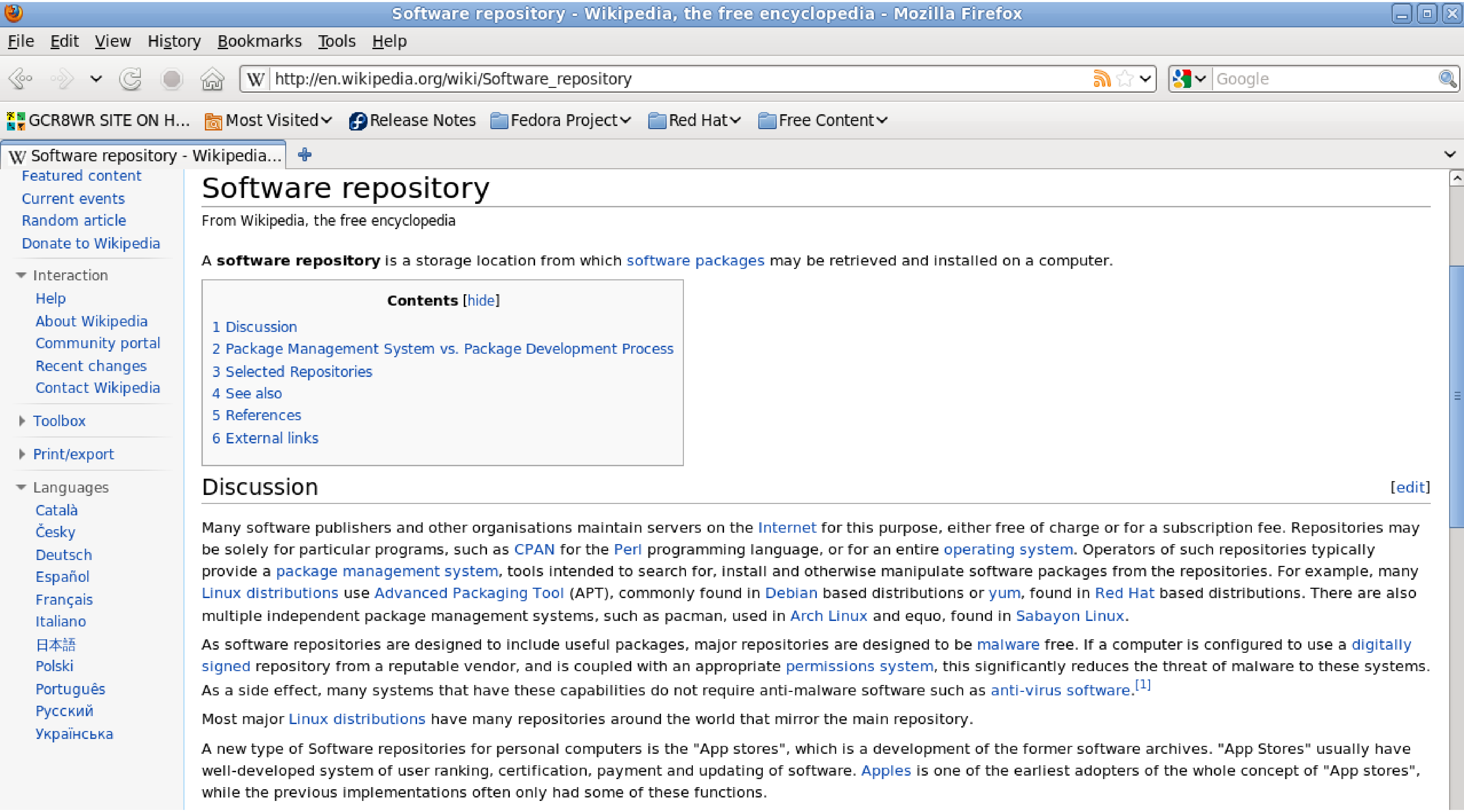
- In Linux, software is normally installed using a **package manager** that coordinates software installation, including dependencies, as well as versions, updates, and security patches.
- Essentially, *ALL* software installed from your package manager – the “Linux part”, fonts, the desktop, or applications – will be updated and have security patches applied through the repositories soon after they're available.

Install Software From Repositories

- *As such, normally when you're installing software and you can install either from a repository or elsewhere, it's preferred to install from the repositories.*

Install Software From Repositories

- *Some software you'll install on your system won't be in the repositories: However, the important part is to choose a system that has the software you need in its repositories, OR to tolerate the occasional piece of software from “off the homestead” sources while keeping unsupported software to a minimum.*



Software repository

From Wikipedia, the free encyclopedia

A **software repository** is a storage location from which software packages may be retrieved and installed on a computer.

Contents [hide]

Discussion

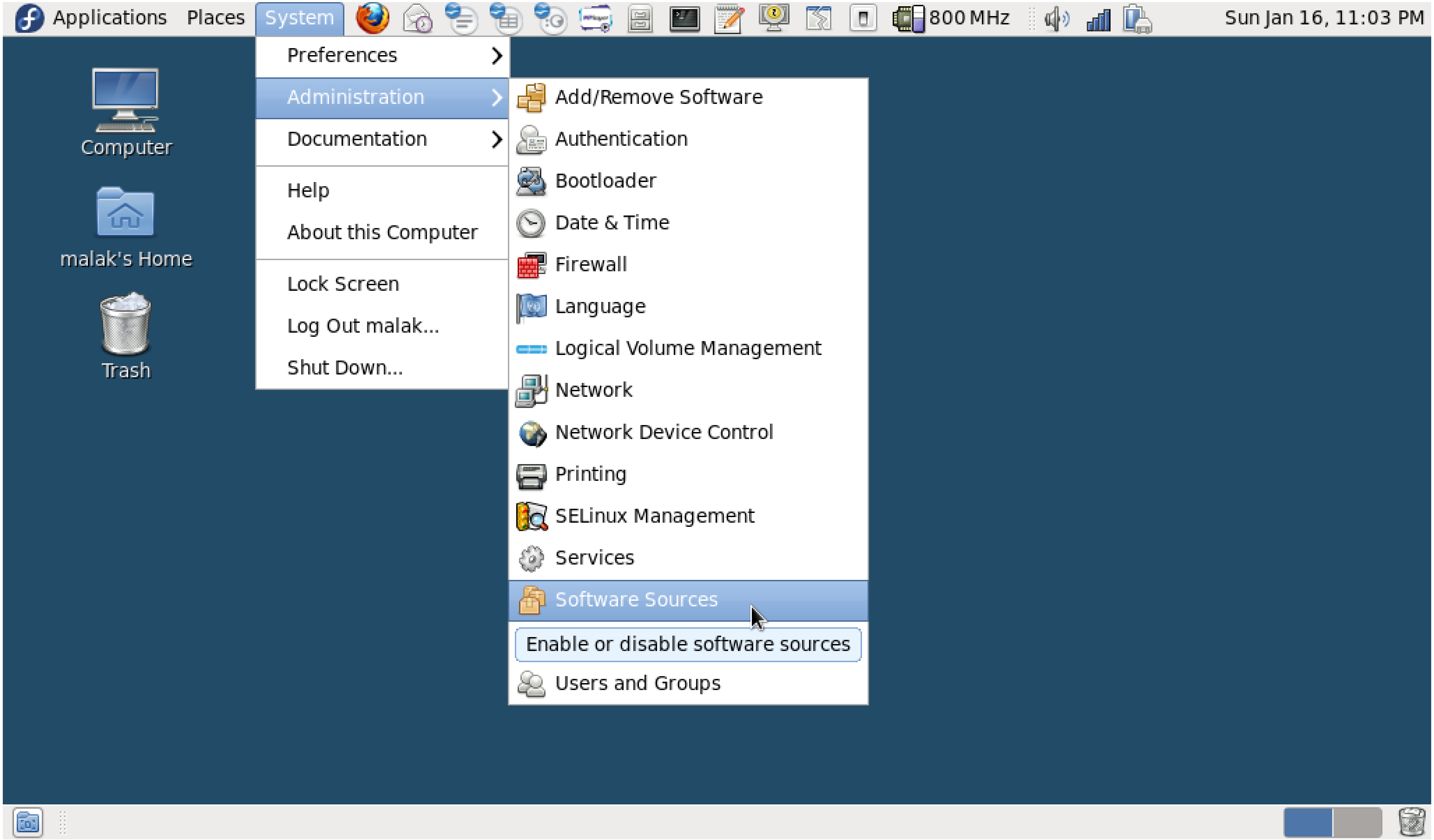
[edit]

Many software publishers and other organisations maintain servers on the Internet for this purpose, either free of charge or for a subscription fee. Repositories may be solely for particular programs, such as CPAN for the Perl programming language, or for an entire operating system. Operators of such repositories typically provide a package management system, tools intended to search for, install and otherwise manipulate software packages from the repositories. For example, many Linux distributions use Advanced Packaging Tool (APT), commonly found in Debian based distributions or yum, found in Red Hat based distributions. There are also multiple independent package management systems, such as pacman, used in Arch Linux and equo, found in Sabayon Linux.

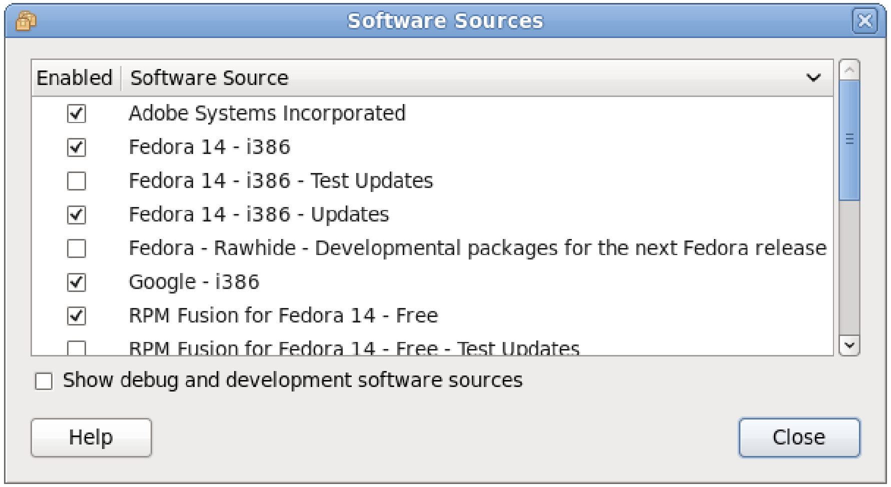
As software repositories are designed to include useful packages, major repositories are designed to be malware free. If a computer is configured to use a digitally signed repository from a reputable vendor, and is coupled with an appropriate permissions system, this significantly reduces the threat of malware to these systems. As a side effect, many systems that have these capabilities do not require anti-malware software such as anti-virus software.[1]

Most major Linux distributions have many repositories around the world that mirror the main repository.

A new type of Software repositories for personal computers is the "App stores", which is a development of the former software archives. "App Stores" usually have well-developed system of user ranking, certification, payment and updating of software. Apples is one of the earliest adopters of the whole concept of "App stores", while the previous implementations often only had some of these functions.


Applications
Places
System
800 MHz
Sun Jan 16, 11:03 PM
Computer
malak's Home
Trash
Preferences
Administration
Documentation
Help
About this Computer
Lock Screen
Log Out malak...
Shut Down...
Add/Remove Software
Authentication
Bootloader
Date & Time
Firewall
Language
Logical Volume Management
Network
Network Device Control
Printing
SELinux Management
Services
Software Sources
Enable or disable software sources
Users and Groups

Install Software From Repositories

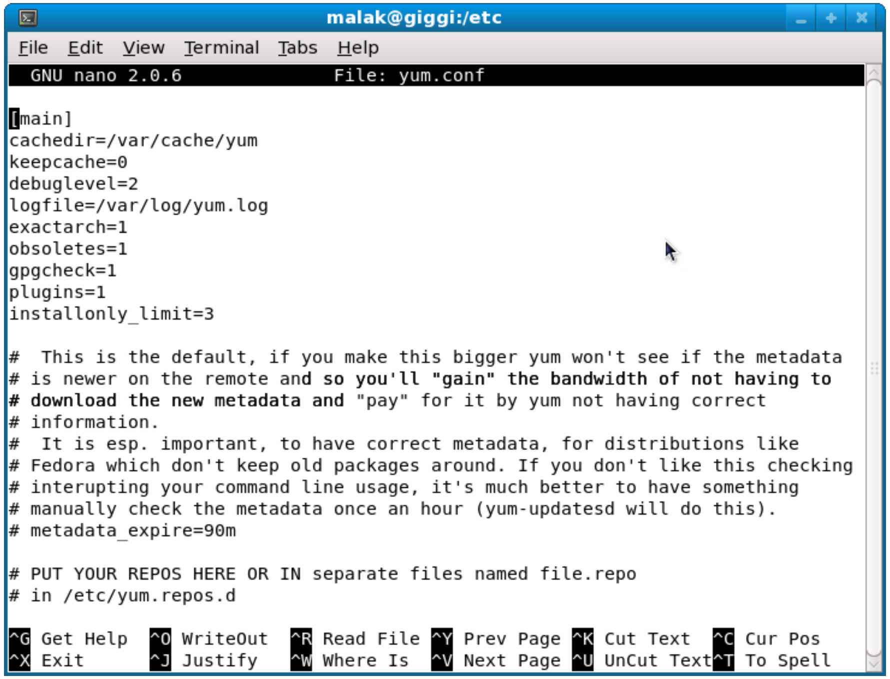


Enabled	Software Source
☑	Adobe Systems Incorporated
☑	Fedora 14 - i386
□	Fedora 14 - i386 - Test Updates
☑	Fedora 14 - i386 - Updates
□	Fedora - Rawhide - Developmental packages for the next Fedora release
☑	Google - i386
☑	RPM Fusion for Fedora 14 - Free
□	RPM Fusion for Fedora 14 - Free - Test Updates

□ Show debug and development software sources

- System | Administration | Software Sources

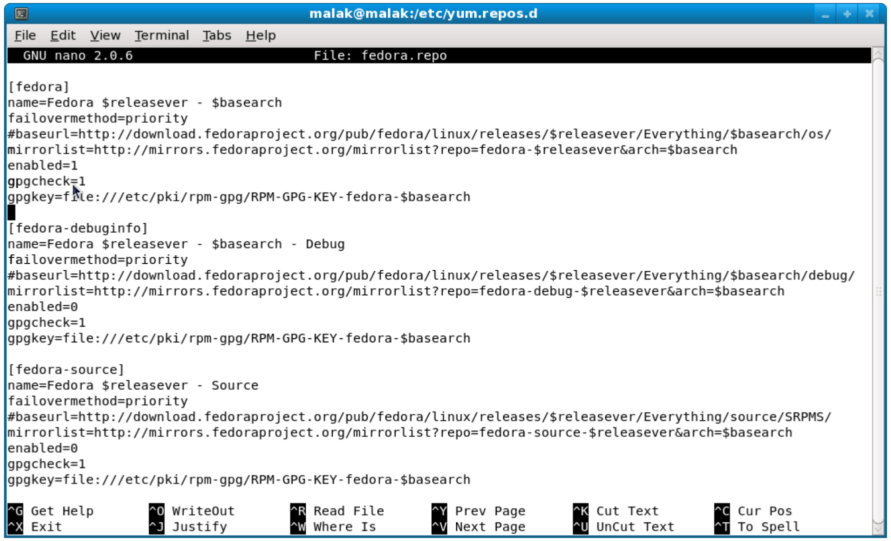
Repository Files



```
  GNU nano 2.0.6              File: yum.conf

[main]
cachedir=/var/cache/yum
keepcache=0
debuglevel=2
logfile=/var/log/yum.log
exactarch=1
obsoletes=1
gpgcheck=1
plugins=1
installonly_limit=3

#  This is the default, if you make this bigger yum won't see if the metadata
# is newer on the remote and so you'll "gain" the bandwidth of not having to
# download the new metadata and "pay" for it by yum not having correct
# information.
#  It is esp. important, to have correct metadata, for distributions like
# Fedora which don't keep old packages around. If you don't like this checking
# interupting your command line usage, it's much better to have something
# manually check the metadata once an hour (yum-updatesd will do this).
# metadata_expire=90m

# PUT YOUR REPOS HERE OR IN separate files named file.repo
# in /etc/yum.repos.d

^G Get Help   ^O WriteOut   ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit       ^J Justify    ^W Where Is   ^V Next Page  ^U UnCut Text^T To Spell
```

- You can add repository information, normally found on the repository's webpage, to */etc/yum.conf*
- Some repositories' web pages have automatic installation links to add the repository to your system, which will add the necessary information to your system

Repository Files



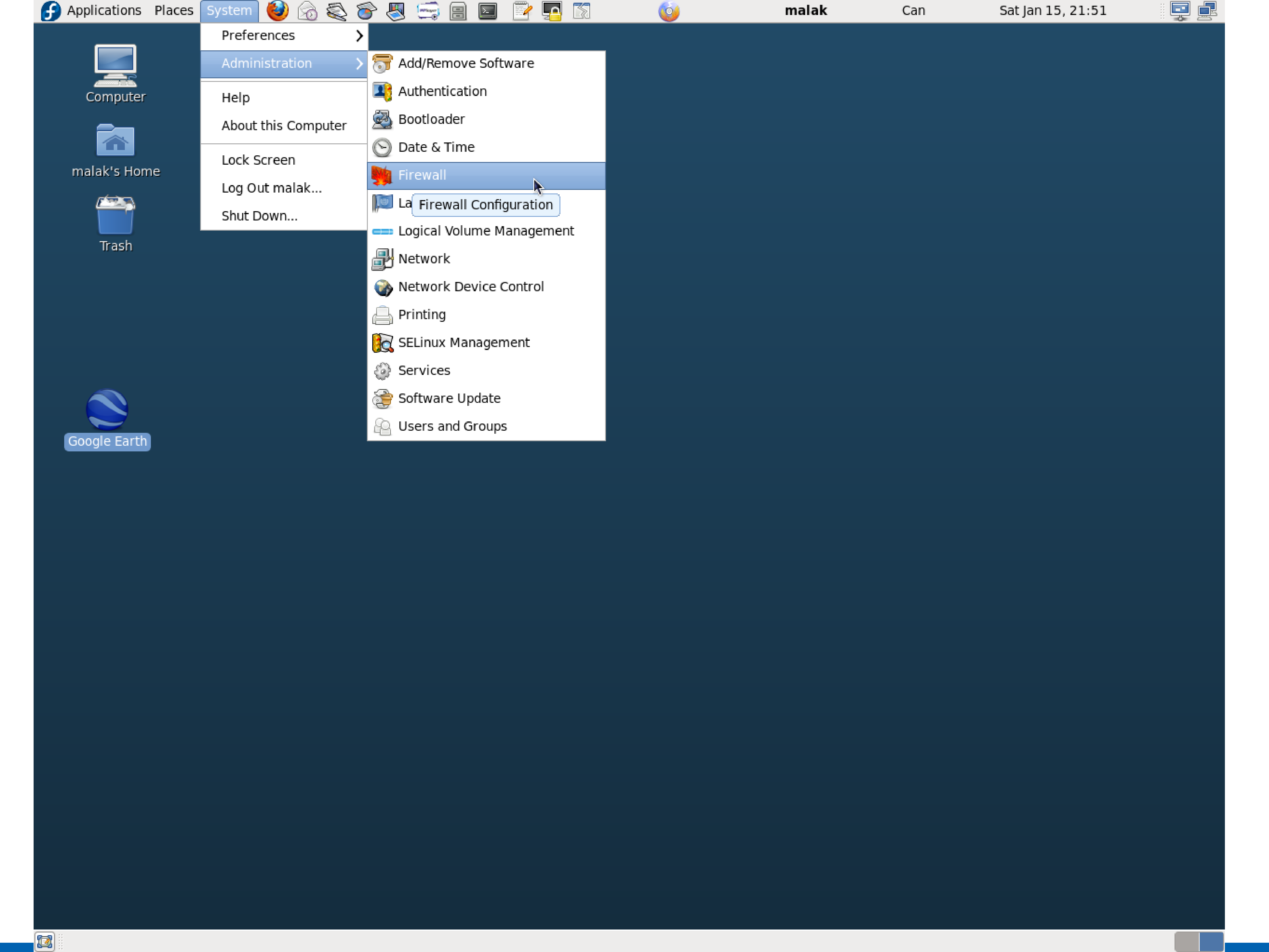
```
  GNU nano 2.0.6                         File: fedora.repo

[fedora]
name=Fedora $releasever - $basearch
failovermethod=priority
#baseurl=http://download.fedoraproject.org/pub/fedora/linux/releases/$releasever/Everything/$basearch/os/
mirrorlist=http://mirrors.fedoraproject.org/mirrorlist?repo=fedora-$releasever&arch=$basearch
enabled=1
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-fedora-$basearch

[fedora-debuginfo]
name=Fedora $releasever - $basearch - Debug
failovermethod=priority
#baseurl=http://download.fedoraproject.org/pub/fedora/linux/releases/$releasever/Everything/$basearch/debug/
mirrorlist=http://mirrors.fedoraproject.org/mirrorlist?repo=fedora-debug-$releasever&arch=$basearch
enabled=0
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-fedora-$basearch

[fedora-source]
name=Fedora $releasever - Source
failovermethod=priority
#baseurl=http://download.fedoraproject.org/pub/fedora/linux/releases/$releasever/Everything/source/SRPMS/
mirrorlist=http://mirrors.fedoraproject.org/mirrorlist?repo=fedora-source-$releasever&arch=$basearch
enabled=0
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-fedora-$basearch

^G Get Help      ^O WriteOut      ^R Read File     ^Y Prev Page     ^K Cut Text      ^C Cur Pos
^X Exit          ^J Justify       ^W Where Is      ^V Next Page     ^U UnCut Text    ^T To Spell
```

- You can also have separate repository files in */etc/yum/repo.d* which are named *file.repo*, where *file* normally represents the repository's name
  - ***Normally the text to cut & paste can be found on the repository's web page***

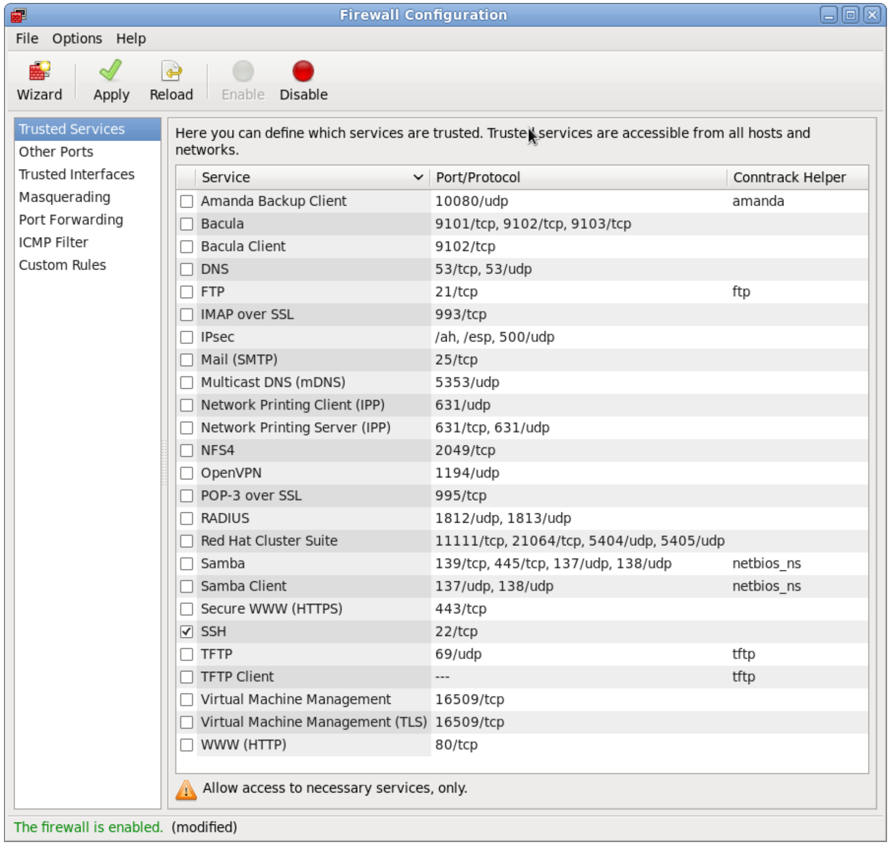
Activate Your Firewall and Tune Appropriately

Activate Your Firewall and Tune Appropriately

- Firewalls basically act as a traffic cops, and enforce rules for what type of network traffic is allowed into and out of your computer


Applications
Places
System
malak
Can
Sat Jan 15, 21:51
Preferences
Administration
Help
About this Computer
Lock Screen
Log Out malak...
Shut Down...
Add/Remove Software
Authentication
Bootloader
Date & Time
Firewall
La
Firewall Configuration
Logical Volume Management
Network
Network Device Control
Printing
SELinux Management
Services
Software Update
Users and Groups
Computer
malak's Home
Trash
Google Earth

Activate Your Firewall and Tune Appropriately



Here you can define which services are trusted. Trusted services are accessible from all hosts and networks.

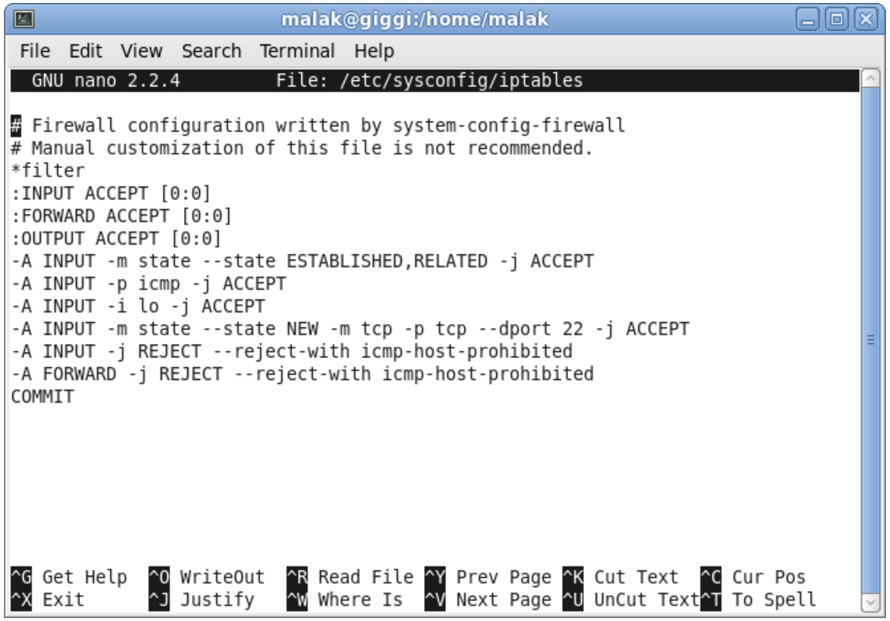
	Service	Port/Protocol	Conntrack Helper
☐	Amanda Backup Client	10080/udp	amanda
☐	Bacula	9101/tcp, 9102/tcp, 9103/tcp	
☐	Bacula Client	9102/tcp	
☐	DNS	53/tcp, 53/udp	
☐	FTP	21/tcp	ftp
☐	IMAP over SSL	993/tcp	
☐	IPsec	/ah, /esp, 500/udp	
☐	Mail (SMTP)	25/tcp	
☐	Multicast DNS (mDNS)	5353/udp	
☐	Network Printing Client (IPP)	631/udp	
☐	Network Printing Server (IPP)	631/tcp, 631/udp	
☐	NFS4	2049/tcp	
☐	OpenVPN	1194/udp	
☐	POP-3 over SSL	995/tcp	
☐	RADIUS	1812/udp, 1813/udp	
☐	Red Hat Cluster Suite	11111/tcp, 21064/tcp, 5404/udp, 5405/udp	
☐	Samba	139/tcp, 445/tcp, 137/udp, 138/udp	netbios_ns
☐	Samba Client	137/udp, 138/udp	netbios_ns
☐	Secure WWW (HTTPS)	443/tcp	
☑	SSH	22/tcp	
☐	TFTP	69/udp	tftp
☐	TFTP Client	---	tftp
☐	Virtual Machine Management	16509/tcp	
☐	Virtual Machine Management (TLS)	16509/tcp	
☐	WWW (HTTP)	80/tcp	

⚠ Allow access to necessary services, only.

The firewall is enabled. (modified)

- System | Administration | Firewall
- Check the services for which you'll allow network traffic, leave those you won't allow unchecked
- Other configurations can be set

Activate Your Firewall and Tune Appropriately


malak@giggi:/home/malak
File Edit View Search Terminal Help
GNU nano 2.2.4 File: /etc/sysconfig/iptables
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell

```
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

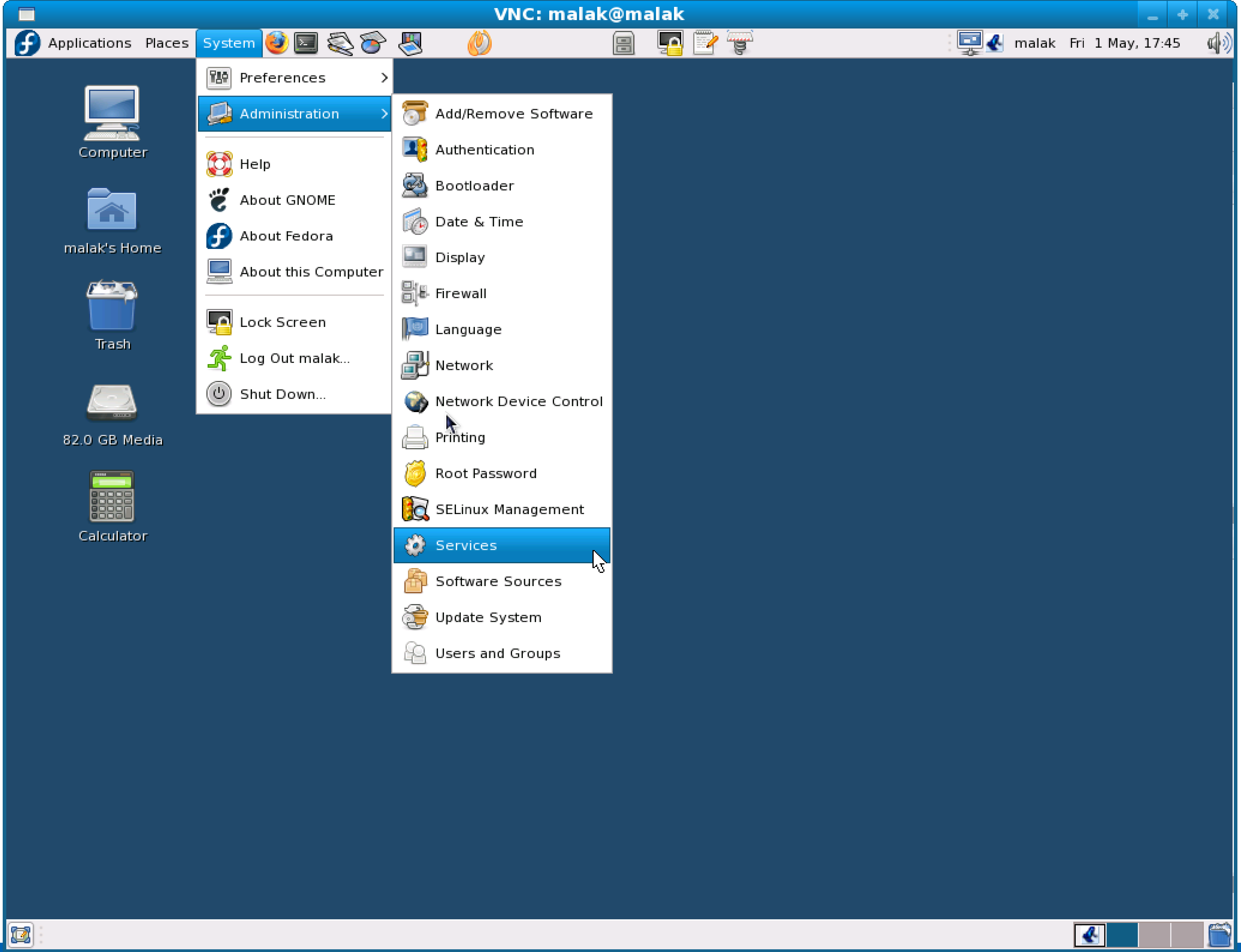
- At the command line and as root, edit the */etc/sysconfig/iptables* file
- ***Manual customization of the file is not recommended***

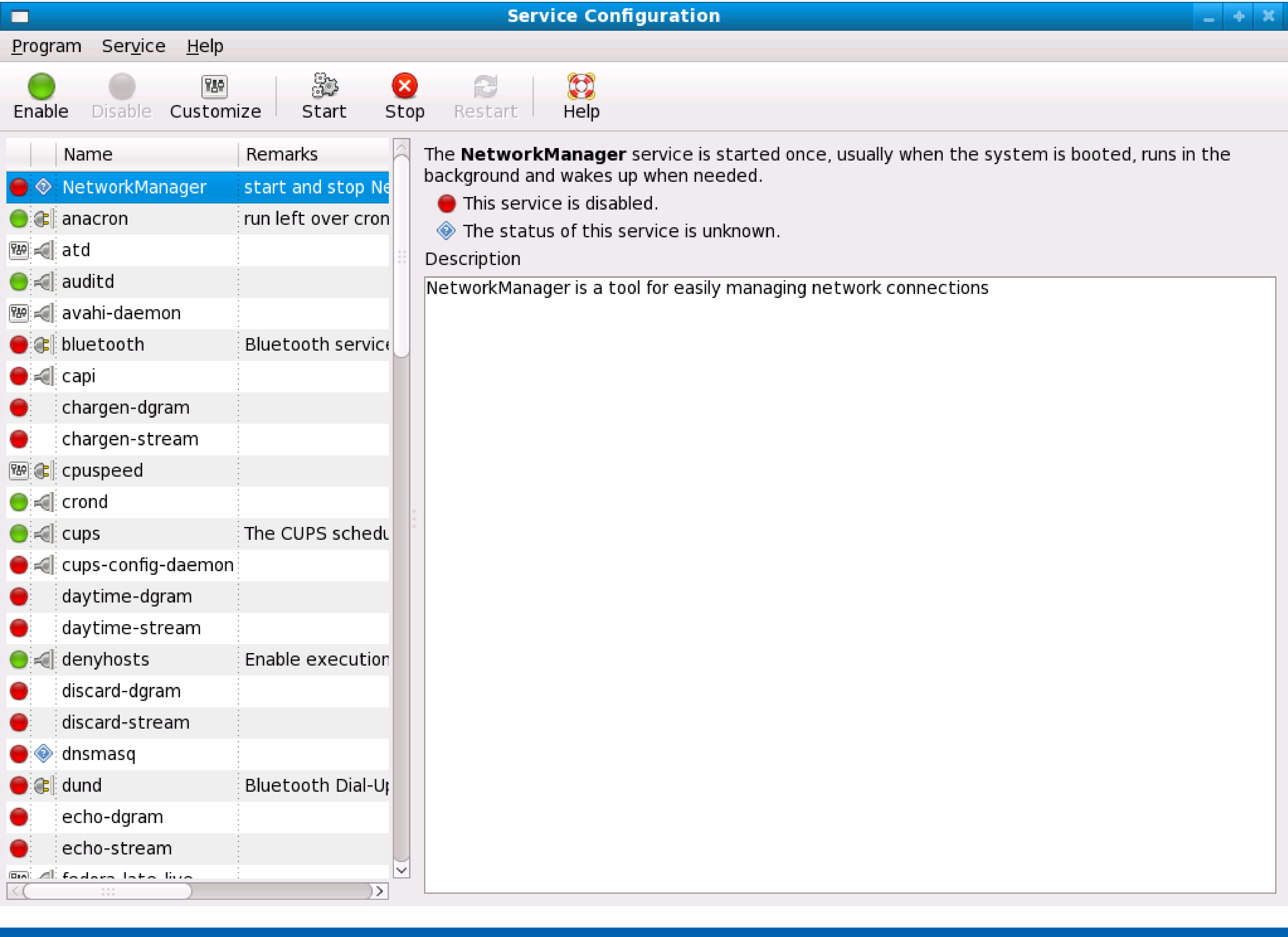
Turn Off Unneeded System Services

Turn Off Unneeded System Services

- If you don't access your computer remotely by certain services, the ones you don't need should be turned off so as to limit them as intrusion vectors by crackers
- System | Administration | Services

- ftp
- sshd
- vnc
- httpd
- sendmail
- netconsole


VNC: malak@malak
Applications
Places
System
malak
Fri 1 May, 17:45
Computer
malak's Home
Trash
82.0 GB Media
Calculator
Preferences
Administration
Help
About GNOME
About Fedora
About this Computer
Lock Screen
Log Out malak...
Shut Down...
Add/Remove Software
Authentication
Bootloader
Date & Time
Display
Firewall
Language
Network
Network Device Control
Printing
Root Password
SELinux Management
Services
Software Sources
Update System
Users and Groups



	Name	Remarks
🔴 ◈	NetworkManager	start and stop Ne
🟢	anacron	run left over cron
	atd	
🟢	auditd	
	avahi-daemon	
🔴	bluetooth	Bluetooth service
🔴	capi	
🔴	chargen-dgram	
🔴	chargen-stream	
	cpuspeed	
🟢	crond	
🟢	cups	The CUPS schedu
🔴	cups-config-daemon	
🔴	daytime-dgram	
🔴	daytime-stream	
🟢	denyhosts	Enable execution
🔴	discard-dgram	
🔴	discard-stream	
🔴 ◈	dnsmasq	
🔴	dund	Bluetooth Dial-U
🔴	echo-dgram	
🔴	echo-stream	
	fedora-late-live	

The **NetworkManager** service is started once, usually when the system is booted, runs in the background and wakes up when needed.

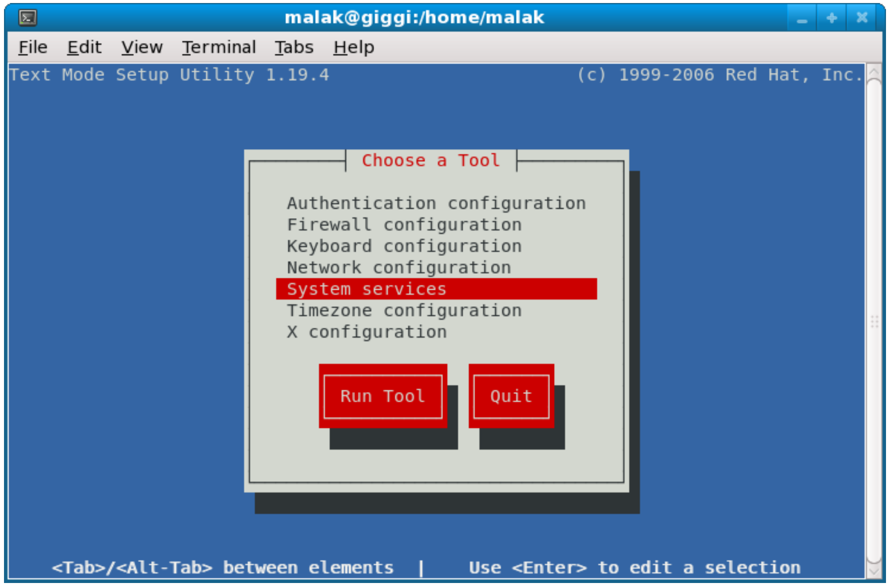
🔴 This service is disabled.

◈ The status of this service is unknown.

Description

NetworkManager is a tool for easily managing network connections

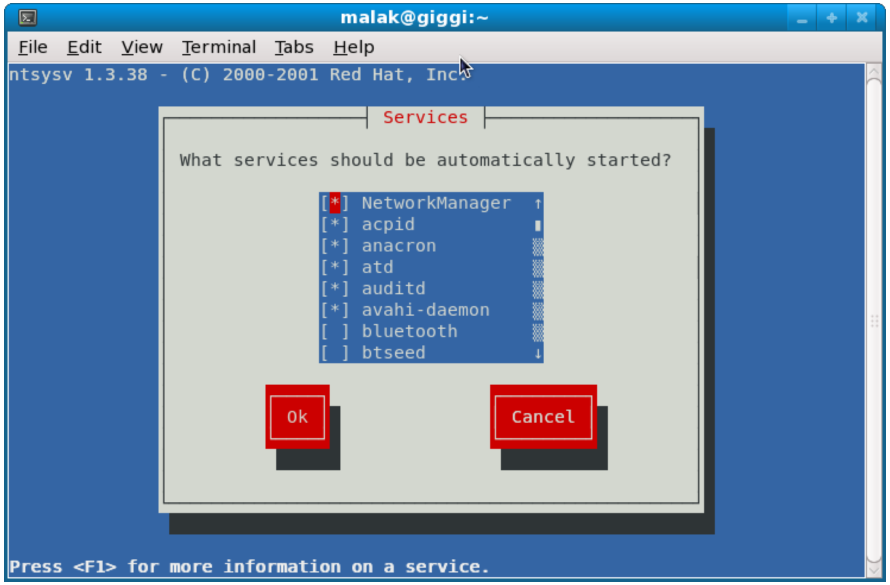
Turn Off Unneeded System Services



```
malak@giggi:/home/malak
File  Edit  View  Terminal  Tabs  Help
Text Mode Setup Utility 1.19.4                          (c) 1999-2006 Red Hat, Inc.

                    ┤ Choose a Tool ├

                 Authentication configuration
                 Firewall configuration
                 Keyboard configuration
                 Network configuration
                 System services
                 Timezone configuration
                 X configuration

                   Run Tool        Quit

    <Tab>/<Alt-Tab> between elements   |     Use <Enter> to edit a selection
```

- At the command line and as root, enter the *setup* command, and you'll see this menu; choose "System services"

Turn Off Unneeded System Services



```
ntsysv 1.3.38 - (C) 2000-2001 Red Hat, Inc.

                    Services

  What services should be automatically started?

              [*] NetworkManager
              [*] acpid
              [*] anacron
              [*] atd
              [*] auditd
              [*] avahi-daemon
              [ ] bluetooth
              [ ] btseed

           Ok                    Cancel

Press <F1> for more information on a service.
```

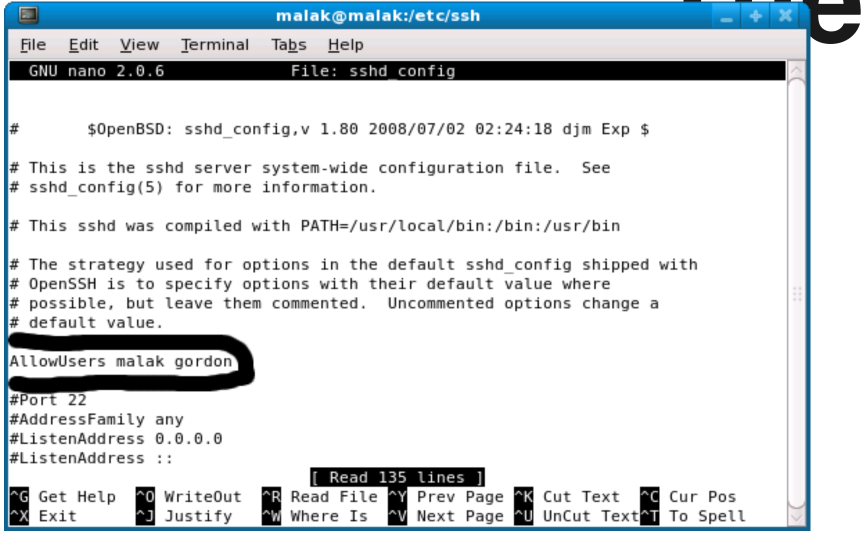
- In the service list, select the targeted services (up/down keys) and activate/deactivate (space key)
- Changes take effect at next boot-up

Limit SSH Access To Only The Users You Allow, And Exclude The root User

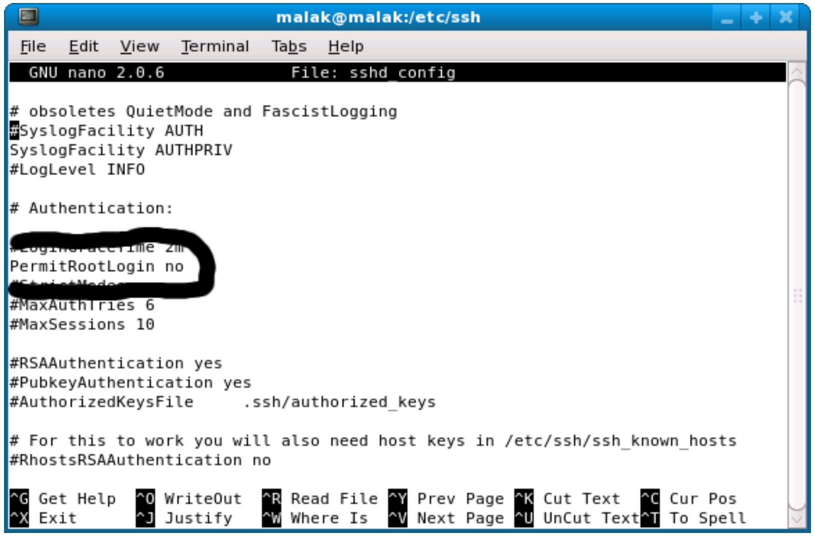
Limit SSH Access To Only The Users You Trust, And Exclude The root User

- SSH access should only be for those users you trust with a command line, and who have reason to have it
- Given the power of root, it should not be allowed direct SSH access; further, if root has an unique password, a cracker would have to figure out:
  - A valid SSH account;
  - Its password;
  - Then the root account password.

Limit SSH Access To Only The Users You Trust, And Exclude The root User



```
  GNU nano 2.0.6              File: sshd_config

#       $OpenBSD: sshd_config,v 1.80 2008/07/02 02:24:18 djm Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/bin:/usr/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options change a
# default value.

AllowUsers malak gordon

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
                                  [ Read 135 lines ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

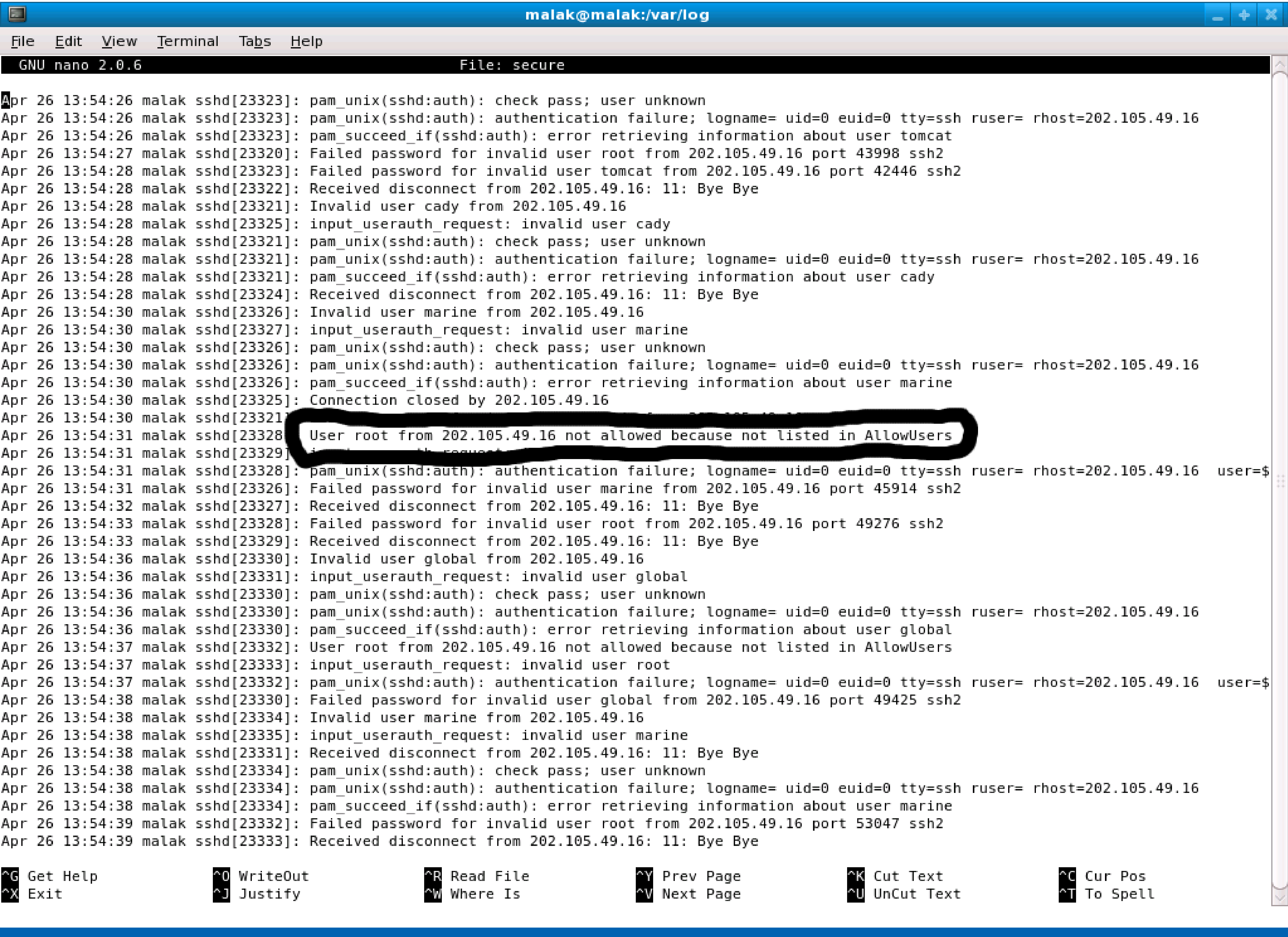


```
  GNU nano 2.0.6              File: sshd_config

# obsoletes QuietMode and FascistLogging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

[redacted]
PermitRootLogin no
[redacted]
#MaxAuthTries 6
#MaxSessions 10

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

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#RhostsRSAAuthentication no

^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

- At the command line and as root, open ***/etc/ssh/sshd_config*** , and add a line with ***AllowUsers*** followed by the users you allow, separated by spaces

- Edit the line ***PermitRootLogin*** so that "***no***" is entered, and delete the "#" at the beginning of the line; ***particularly useful if the root password is unique***

- Be sure that there isn't a "#" at the beginning of the lines, or the condition will be ignored

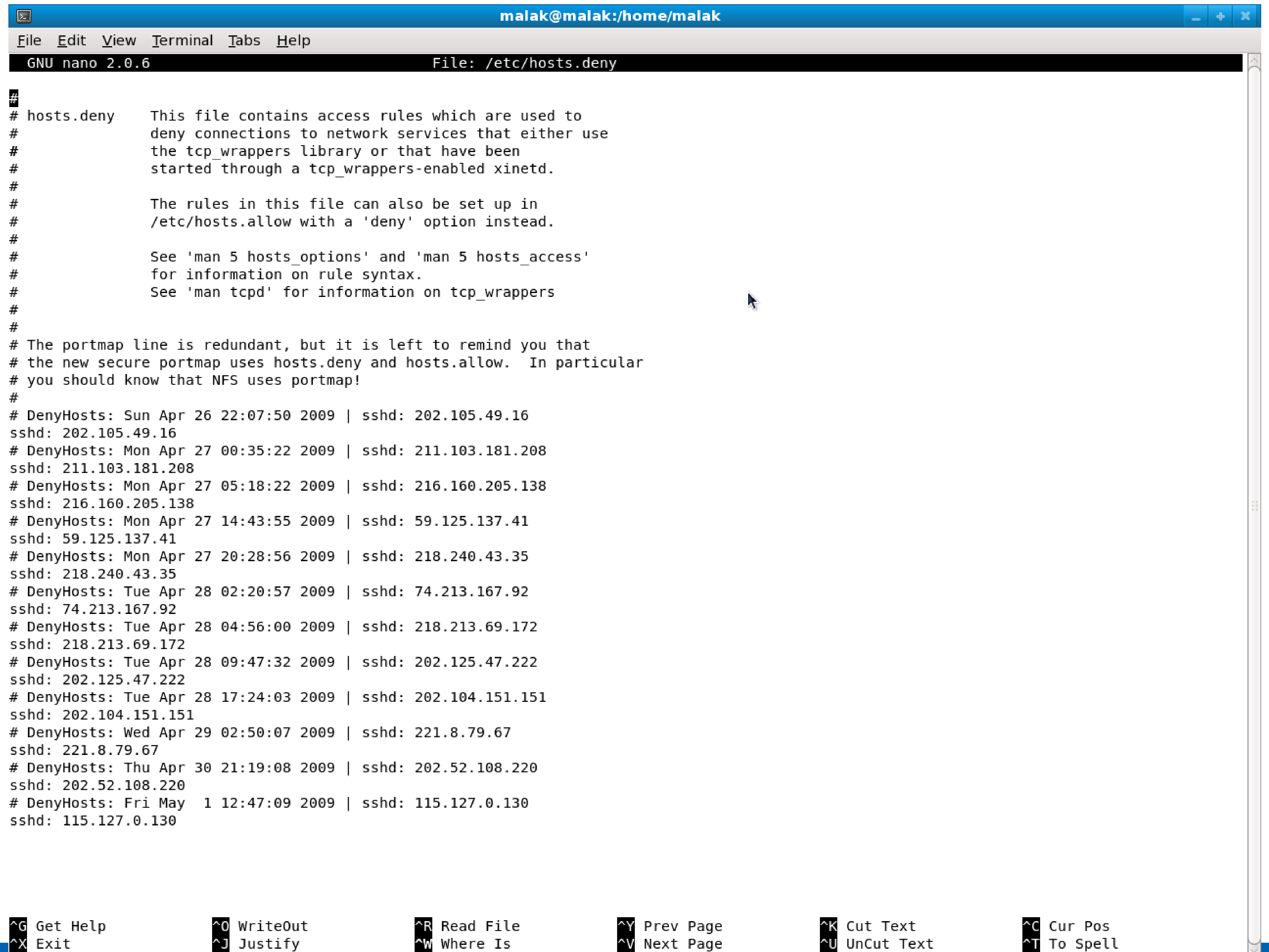


```
  GNU nano 2.0.6                     File: secure

Apr 26 13:54:26 malak sshd[23323]: pam_unix(sshd:auth): check pass; user unknown
Apr 26 13:54:26 malak sshd[23323]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=202.105.49.16
Apr 26 13:54:26 malak sshd[23323]: pam_succeed_if(sshd:auth): error retrieving information about user tomcat
Apr 26 13:54:27 malak sshd[23320]: Failed password for invalid user root from 202.105.49.16 port 43998 ssh2
Apr 26 13:54:28 malak sshd[23323]: Failed password for invalid user tomcat from 202.105.49.16 port 42446 ssh2
Apr 26 13:54:28 malak sshd[23322]: Received disconnect from 202.105.49.16: 11: Bye Bye
Apr 26 13:54:28 malak sshd[23321]: Invalid user cady from 202.105.49.16
Apr 26 13:54:28 malak sshd[23325]: input_userauth_request: invalid user cady
Apr 26 13:54:28 malak sshd[23321]: pam_unix(sshd:auth): check pass; user unknown
Apr 26 13:54:28 malak sshd[23321]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=202.105.49.16
Apr 26 13:54:28 malak sshd[23321]: pam_succeed_if(sshd:auth): error retrieving information about user cady
Apr 26 13:54:28 malak sshd[23324]: Received disconnect from 202.105.49.16: 11: Bye Bye
Apr 26 13:54:30 malak sshd[23326]: Invalid user marine from 202.105.49.16
Apr 26 13:54:30 malak sshd[23327]: input_userauth_request: invalid user marine
Apr 26 13:54:30 malak sshd[23326]: pam_unix(sshd:auth): check pass; user unknown
Apr 26 13:54:30 malak sshd[23326]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=202.105.49.16
Apr 26 13:54:30 malak sshd[23326]: pam_succeed_if(sshd:auth): error retrieving information about user marine
Apr 26 13:54:30 malak sshd[23325]: Connection closed by 202.105.49.16
Apr 26 13:54:30 malak sshd[23321 [illegible]
Apr 26 13:54:31 malak sshd[23328  User root from 202.105.49.16 not allowed because not listed in AllowUsers
Apr 26 13:54:31 malak sshd[23329] [illegible]
Apr 26 13:54:31 malak sshd[23328]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=202.105.49.16  user=$
Apr 26 13:54:31 malak sshd[23326]: Failed password for invalid user marine from 202.105.49.16 port 45914 ssh2
Apr 26 13:54:32 malak sshd[23327]: Received disconnect from 202.105.49.16: 11: Bye Bye
Apr 26 13:54:33 malak sshd[23328]: Failed password for invalid user root from 202.105.49.16 port 49276 ssh2
Apr 26 13:54:33 malak sshd[23329]: Received disconnect from 202.105.49.16: 11: Bye Bye
Apr 26 13:54:36 malak sshd[23330]: Invalid user global from 202.105.49.16
Apr 26 13:54:36 malak sshd[23331]: input_userauth_request: invalid user global
Apr 26 13:54:36 malak sshd[23330]: pam_unix(sshd:auth): check pass; user unknown
Apr 26 13:54:36 malak sshd[23330]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=202.105.49.16
Apr 26 13:54:36 malak sshd[23330]: pam_succeed_if(sshd:auth): error retrieving information about user global
Apr 26 13:54:37 malak sshd[23332]: User root from 202.105.49.16 not allowed because not listed in AllowUsers
Apr 26 13:54:37 malak sshd[23333]: input_userauth_request: invalid user root
Apr 26 13:54:37 malak sshd[23332]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=202.105.49.16  user=$
Apr 26 13:54:38 malak sshd[23330]: Failed password for invalid user global from 202.105.49.16 port 49425 ssh2
Apr 26 13:54:38 malak sshd[23334]: Invalid user marine from 202.105.49.16
Apr 26 13:54:38 malak sshd[23335]: input_userauth_request: invalid user marine
Apr 26 13:54:38 malak sshd[23331]: Received disconnect from 202.105.49.16: 11: Bye Bye
Apr 26 13:54:38 malak sshd[23334]: pam_unix(sshd:auth): check pass; user unknown
Apr 26 13:54:38 malak sshd[23334]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=202.105.49.16
Apr 26 13:54:38 malak sshd[23334]: pam_succeed_if(sshd:auth): error retrieving information about user marine
Apr 26 13:54:39 malak sshd[23332]: Failed password for invalid user root from 202.105.49.16 port 53047 ssh2
Apr 26 13:54:39 malak sshd[23333]: Received disconnect from 202.105.49.16: 11: Bye Bye

^G Get Help      ^O WriteOut      ^R Read File     ^Y Prev Page     ^K Cut Text      ^C Cur Pos
^X Exit          ^J Justify       ^W Where Is      ^V Next Page     ^U UnCut Text    ^T To Spell
```

Install denyhosts

Install denyhosts

- denyhosts is a Python script that analyses sshd logs to determine which IP addresses have repeated login failures.
- After (or even during) a repeated attack against an sshd server, it will add the IP address in question to the /etc/hosts.deny file, causing the system to refuse future connection requests from that IP address.
- denyhosts only modifies /etc/hosts.deny for sshd, but entries in the file can work for other services as well



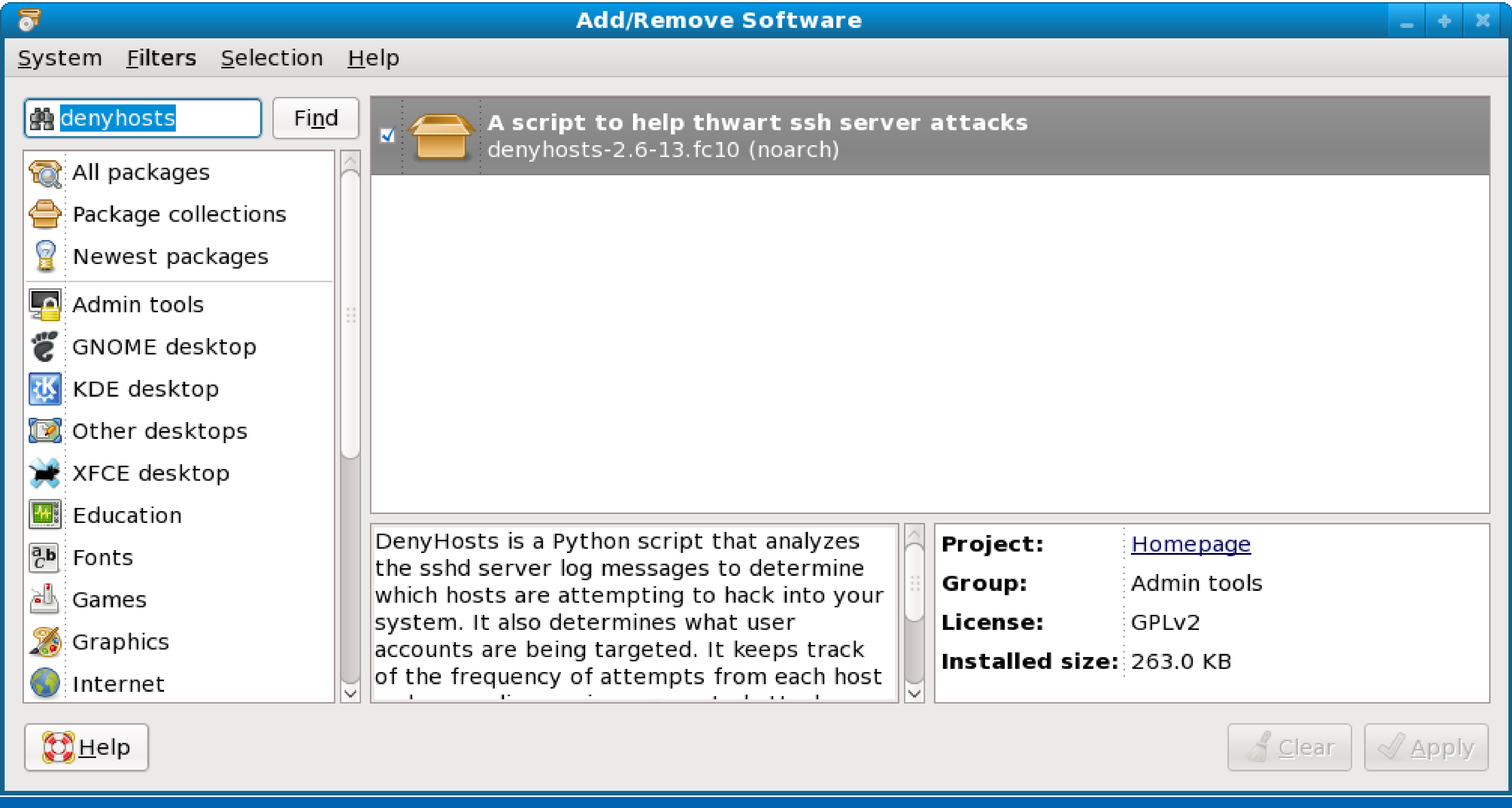
```
  GNU nano 2.0.6                     File: /etc/hosts.deny

#
# hosts.deny    This file contains access rules which are used to
#               deny connections to network services that either use
#               the tcp_wrappers library or that have been
#               started through a tcp_wrappers-enabled xinetd.
#
#               The rules in this file can also be set up in
#               /etc/hosts.allow with a 'deny' option instead.
#
#               See 'man 5 hosts_options' and 'man 5 hosts_access'
#               for information on rule syntax.
#               See 'man tcpd' for information on tcp_wrappers
#
#
# The portmap line is redundant, but it is left to remind you that
# the new secure portmap uses hosts.deny and hosts.allow.  In particular
# you should know that NFS uses portmap!
#
# DenyHosts: Sun Apr 26 22:07:50 2009 | sshd: 202.105.49.16
sshd: 202.105.49.16
# DenyHosts: Mon Apr 27 00:35:22 2009 | sshd: 211.103.181.208
sshd: 211.103.181.208
# DenyHosts: Mon Apr 27 05:18:22 2009 | sshd: 216.160.205.138
sshd: 216.160.205.138
# DenyHosts: Mon Apr 27 14:43:55 2009 | sshd: 59.125.137.41
sshd: 59.125.137.41
# DenyHosts: Mon Apr 27 20:28:56 2009 | sshd: 218.240.43.35
sshd: 218.240.43.35
# DenyHosts: Tue Apr 28 02:20:57 2009 | sshd: 74.213.167.92
sshd: 74.213.167.92
# DenyHosts: Tue Apr 28 04:56:00 2009 | sshd: 218.213.69.172
sshd: 218.213.69.172
# DenyHosts: Tue Apr 28 09:47:32 2009 | sshd: 202.125.47.222
sshd: 202.125.47.222
# DenyHosts: Tue Apr 28 17:24:03 2009 | sshd: 202.104.151.151
sshd: 202.104.151.151
# DenyHosts: Wed Apr 29 02:50:07 2009 | sshd: 221.8.79.67
sshd: 221.8.79.67
# DenyHosts: Thu Apr 30 21:19:08 2009 | sshd: 202.52.108.220
sshd: 202.52.108.220
# DenyHosts: Fri May  1 12:47:09 2009 | sshd: 115.127.0.130
sshd: 115.127.0.130
```

Install denyhosts

- System | Administration | Add / Remove Software
- Enter denyhosts into the search line
- Select the software & click on “apply”

- At the command line and as root, “yum install denyhosts”

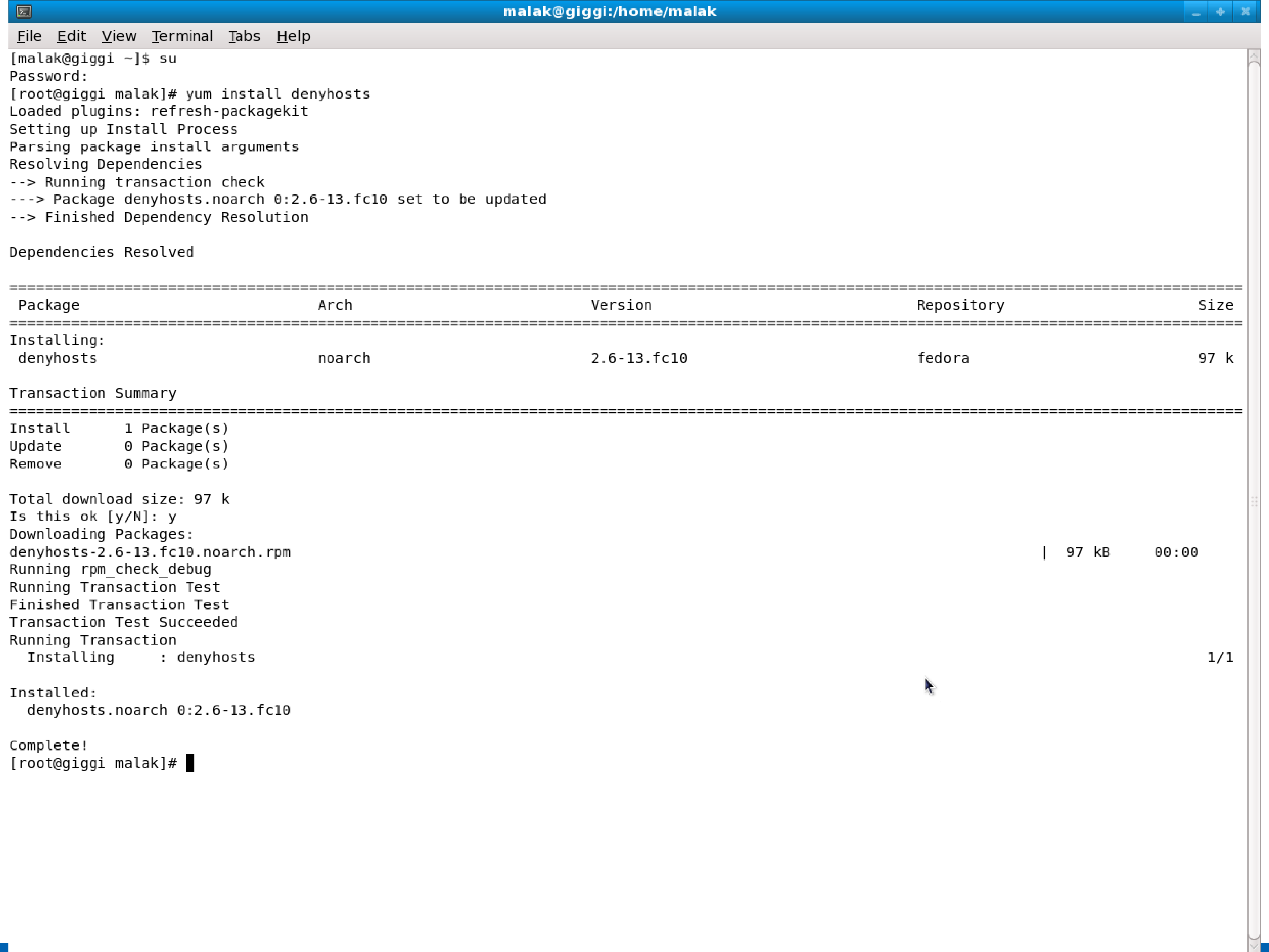
Install denyhosts



☑ **A script to help thwart ssh server attacks**
denyhosts-2.6-13.fc10 (noarch)

DenyHosts is a Python script that analyzes the sshd server log messages to determine which hosts are attempting to hack into your system. It also determines what user accounts are being targeted. It keeps track of the frequency of attempts from each host

Project:	Homepage
Group:	Admin tools
License:	GPLv2
Installed size:	263.0 KB



```
[malak@giggi ~]$ su
Password:
[root@giggi malak]# yum install denyhosts
Loaded plugins: refresh-packagekit
Setting up Install Process
Parsing package install arguments
Resolving Dependencies
--> Running transaction check
---> Package denyhosts.noarch 0:2.6-13.fc10 set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

============================================================================================================================================
 Package                           Arch                           Version                              Repository                      Size
============================================================================================================================================
Installing:
 denyhosts                         noarch                         2.6-13.fc10                          fedora                          97 k

Transaction Summary
============================================================================================================================================
Install      1 Package(s)
Update       0 Package(s)
Remove       0 Package(s)

Total download size: 97 k
Is this ok [y/N]: y
Downloading Packages:
denyhosts-2.6-13.fc10.noarch.rpm                                                                                     |  97 kB     00:00
Running rpm_check_debug
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing     : denyhosts                                                                                                          1/1

Installed:
  denyhosts.noarch 0:2.6-13.fc10

Complete!
[root@giggi malak]# 
```

Other Strategies

Other Strategies

- Install *SELinux* and Operate it in enforcing mode
- Use *NoScript* -- firefox plugin which manages javascript, java, flash and other plugins
- Encrypt your filesystem (such as with *TrueCrypt*);
- Remove junk that accumulates over time (*BleachBit* has a wide variety of "cleaners" for all sorts of junk that accumulates)
- Don't automount devices (important for last strategy)
- Close root terminals when you're finished (important for last strategy)

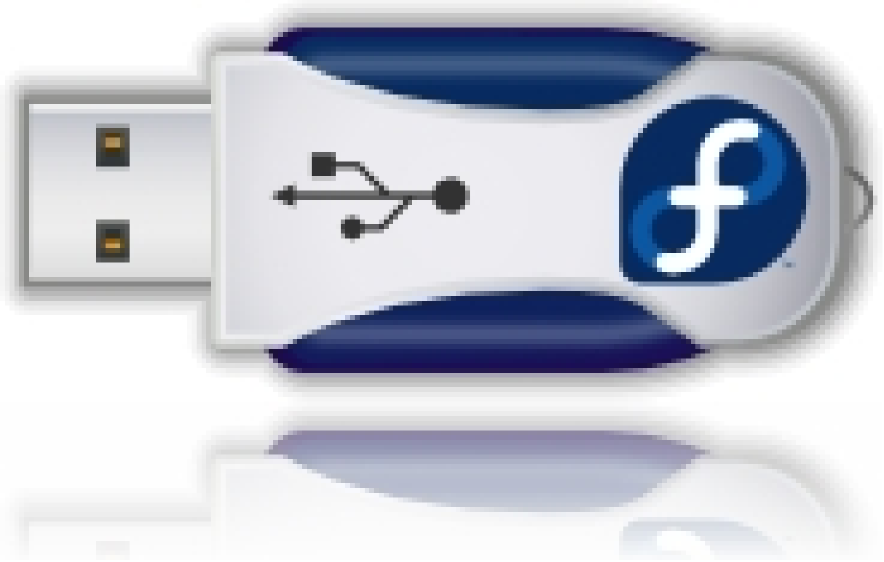
Protect Your Computer's Physical Integrity

Protect Your Computer's Physical Integrity

- Whether you're a beginner or an expert, there's always someone out there who knows more than you on a given subject ... give them physical access to your computer, and they could do all sorts of harm, and/or steal personal information, and/or erase your data, and/or install malware, etc. ...
- ***Sounds too simple to be useful?***

They could insert one of these into your computer ...

Or one of these ...



Or since we're on the subject, why not a hard drive, either a portable USB unit or a traditional hard drive ...

Protect Your Computer!

- It's pretty easy to turn off or unplug a computer and insert a LiveCD or LiveUSB key, or a USB hard drive, or, if you have time, a traditional hard drive; then it's easy to access your personal files or install malware ...

... and it's GAME OVER!

Summary

Summary

- Use a router
- All users should have their own account
- Manage Passwords
- Control Access to Your Desktop
- Perform Updates Regularly
- Install Software From Repositories
- Activate Your Firewall and Tune Appropriately
- Turn Off Unneeded Services
- Limit SSH Access to only the users you allow, and exclude the root user
- Install DenyHosts
- Other Strategies
    - Install SELinux and Operate it in enforcing mode
    - Use NoScript
    - Encrypt your filesystem
    - Remove accumulated junk
    - Don't automount devices
    - Close root sessions at the command line

-Protect your system's physical integrity

Please note:

- This presentation was composed on Fedora 9, 10, 11, 12 and 14 systems.
- If you really wanna know, I'm an environmental field techie who happens to like Linux.

Thank You!

Questions and Comments