Basic Steps to Running a Secure Fedora Linux Machine

Jarrod Millman
UC Berkeley
Neuroscience Institute

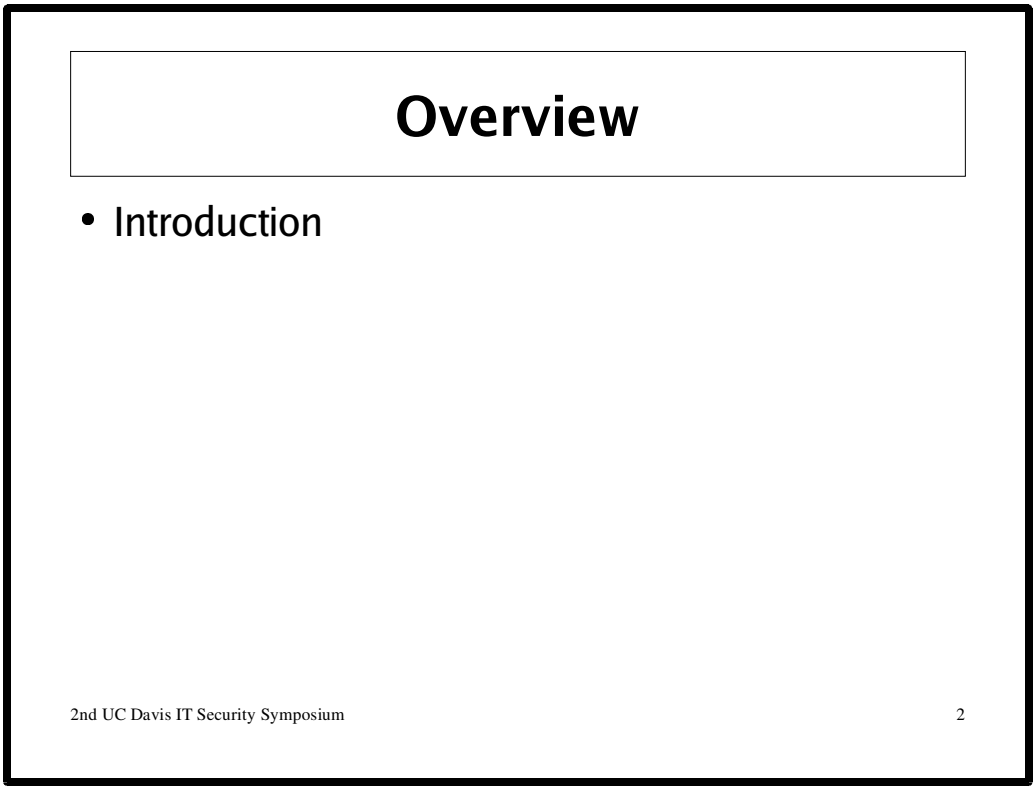
2nd UC Davis IT Security Symposium 1

Session 1
Date: Wednesday, 6/22/2005 1:45 PM to 4:45 PM
Location: 67 Kemper

Session 2 (Repeat)
Date: Friday, 6/24/2005 9:00 AM to 12:00 PM
Location: 67 Kemper

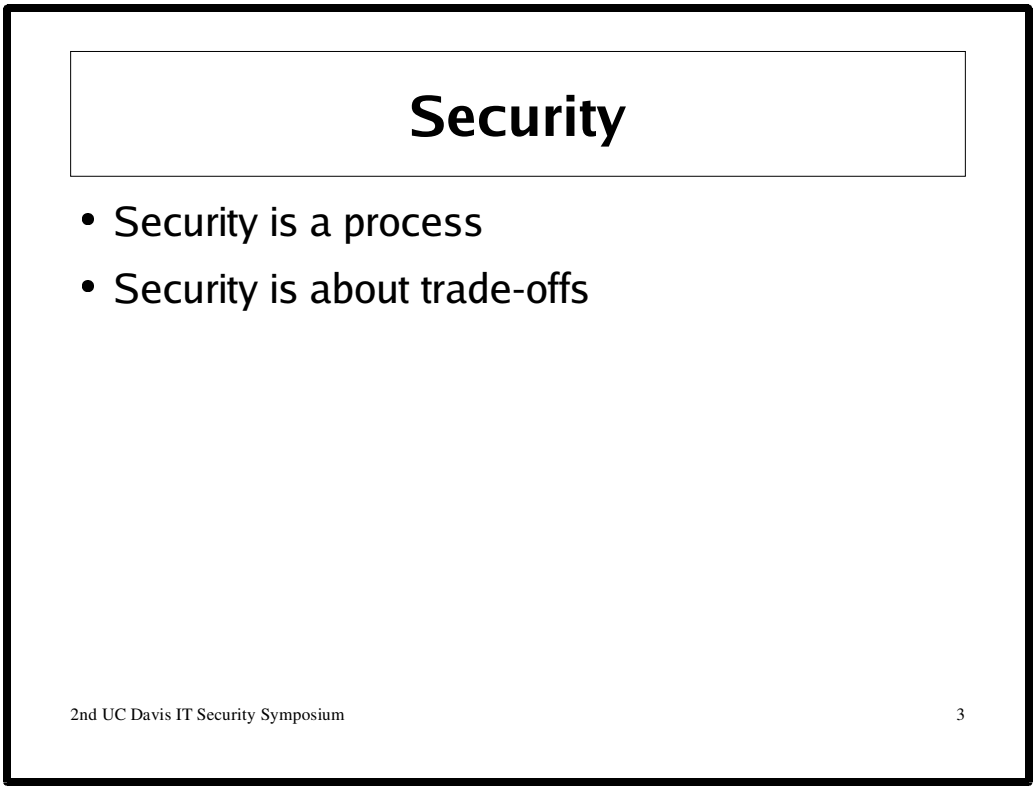
Jarrod Millman
Helen Wills Neuroscience Institute
132 Barker Hall, MC #3190
Berkeley, CA 94720-3190

http://cirl.berkeley.edu/
millman@berkeley.edu



In this 3 hour hands-on lab session, I cover the basic process of securing an individual Linux computer. Specifically, I cover Fedora; although, the material will equally apply to Red Hat Enterprise Linux. Indeed, much of what I cover applies to any UNIX machine. Although I focus on securing an individual machine, the lessons learned provide a foundation for administering a network of machines.

I start with a basic discussion about security. I then cover basic installation issues relating to system security including semi-automated reinstalls. For completeness, I very quickly cover the basic Linux security model: accounts, passwords, and file permissions. The bulk of the lab covers more advanced topics such as: 1) package and service management; 2) system scanning, logging, and monitoring; as well as 3) firewalls and SELinux. Finally, I cover useful security resources and tools as well as showing how a blackhat goes about preparing for and then launching an attack.

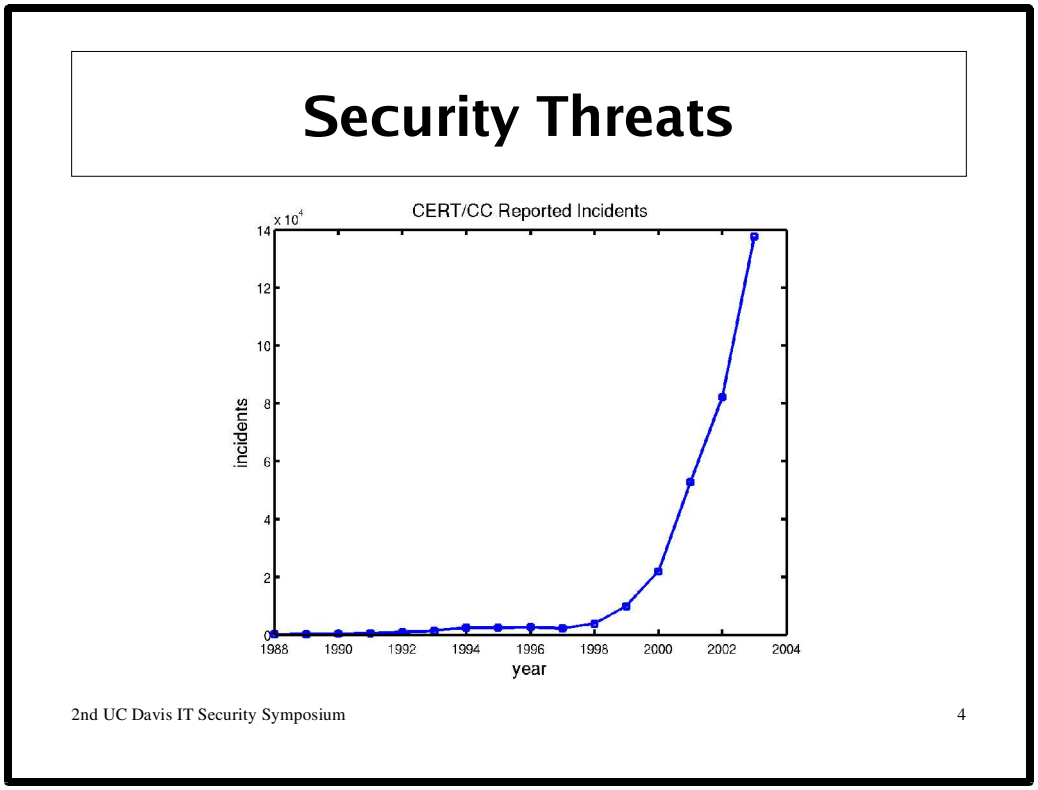


"The superior man, when resting in safety, does not forget that danger may come. When in a state of security he does not forget the possibility of ruin. When all is orderly, he does not forget that disorder may come. Thus his person is not endangered, and his States and all their clans are preserved."
Confucius (551 BC - 479 BC)

General Security
http://www.cve.mitre.org/
http://www.cert.org/
http://www.sans.org/
http://www.securityfocus.com/

Fedora/Redhat Security

http://www.redhat.com/security/



CERN Incidents Reported

"Given the widespread use of automated attack tools, attacks against Internet-connected systems have become so commonplace that counts of the number of incidents reported provide little information with regard to assessing the scope and impact of attacks. Therefore, as of 2004, we will no longer publish the number of incidents reported. Instead, we will be working with others in the community to develop and report on more meaningful metrics, such as the 2004 E-Crime Watch Survey. We welcome ideas and proposals for other collaborations in this area."

http://www.cert.org/stats/cert_stats.html

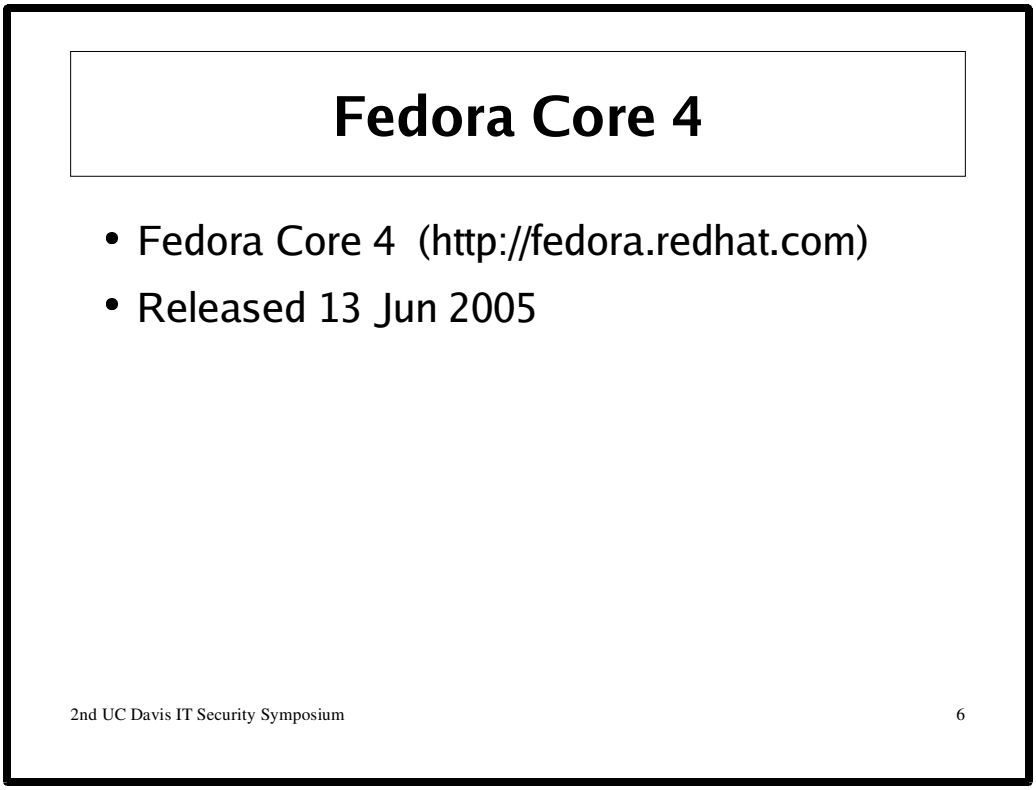
Common Tactics

- Denial of Service (DoS)
- Buffer Overflows
- Trojan Horses
- Physical Access
- Intercepted Communications
- Social Engineering
- Lack of User Cooperation

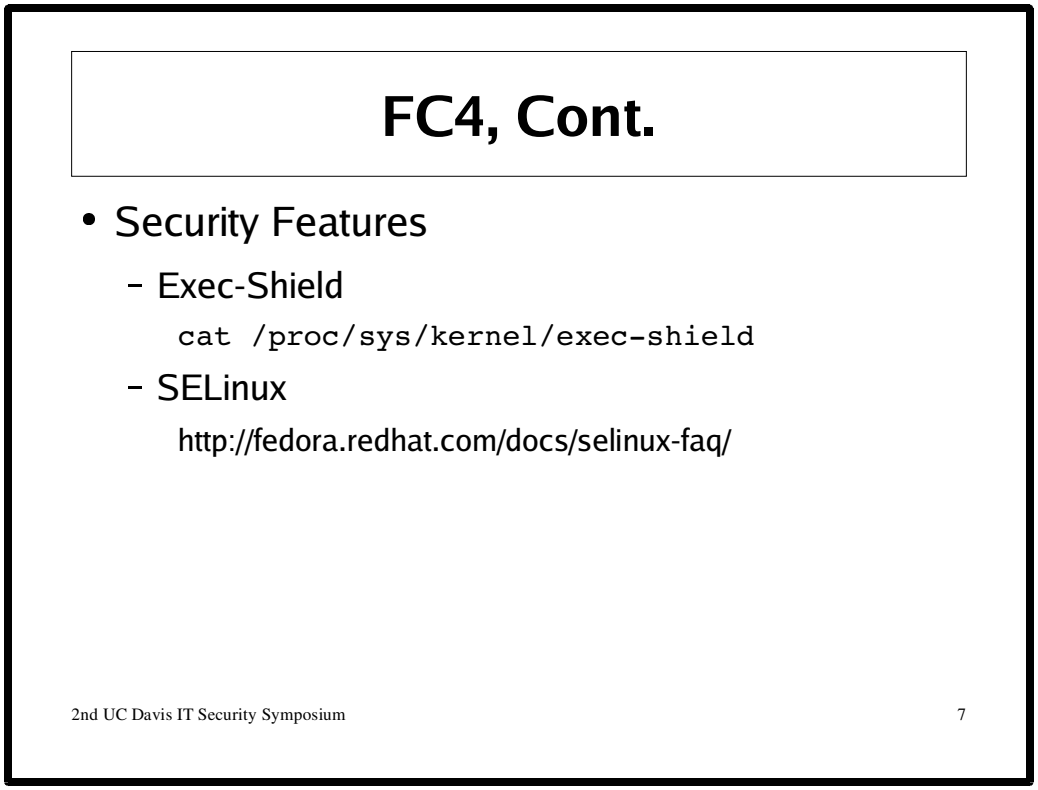
Hackers

- White Hats
- Grey Hats
- Black Hats

NOTE
If its not your network, make sure you ask before running some of the security tools (e.g., scanners, sniffers, etc.) discussed today.



"Fedora Core is a completely free, user friendly, and secure general purpose platform based on Linux. The Fedora Project is an open source project that pioneers leading edge technology and concepts sponsored by Red Hat and supported by the Fedora community."
http://fedora.redhat.com/docs/release-notes/fc4/



FC4 CVE status
"For 20030101-20050607 there are a potential 863 CVE named vulnerabilities that could have affected FC4 packages. 759 (88%) of those are fixed because FC4 includes an upstream version that includes a fix, 10 (1%) are still outstanding, and 94 (11%) are fixed with a backported patch."
Mark Cox
http://people.redhat.com/mjc/20050505-fc4
See Also:
http://people.redhat.com/mjc

FC4 SELinux
http://fedora.redhat.com/projects/selinux/

RHEL 4 Security Guide
http://www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/security-guide/

RHEL 4 SELinux Guide
http://www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/selinux-guide/

Security Enhancements in RHEL (Besides SELinux)
http://people.redhat.com/drepper/nonselsec-slides.pdf
http://people.redhat.com/drepper/nonselsec.pdf

Kickstart

- Automates Fedora installs
  - Reads from text file rather than prompting the user
  - Extremely flexible & customizable
  - Mass deployment & system recovery

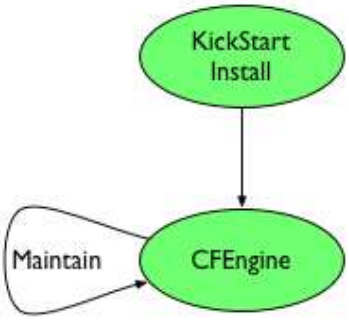
2nd UC Davis IT Security Symposium 8

Kickstart
Please see the RHEL 4 System Admininstrators Guide:
http://www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/sysadmin-guide/

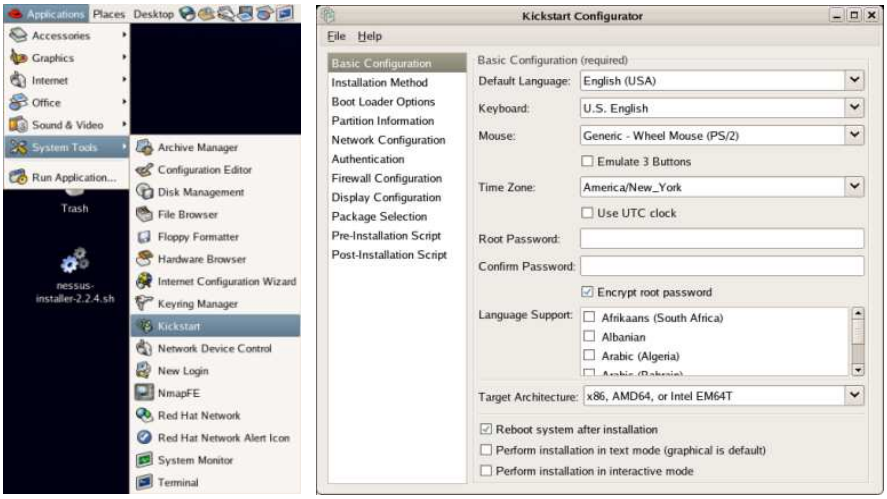
CFEngine
CFEngine is "an autonomous agent and a middle to high level policy language and agent for building expert systems to administrate and configure large computer networks. Cfengine is designed to be a part of a computer immune system." The best starting point is the projects homepage: http://www.cfengine.org/

Install

```
sudo yum install cfengine
```



Kickstart Configurator



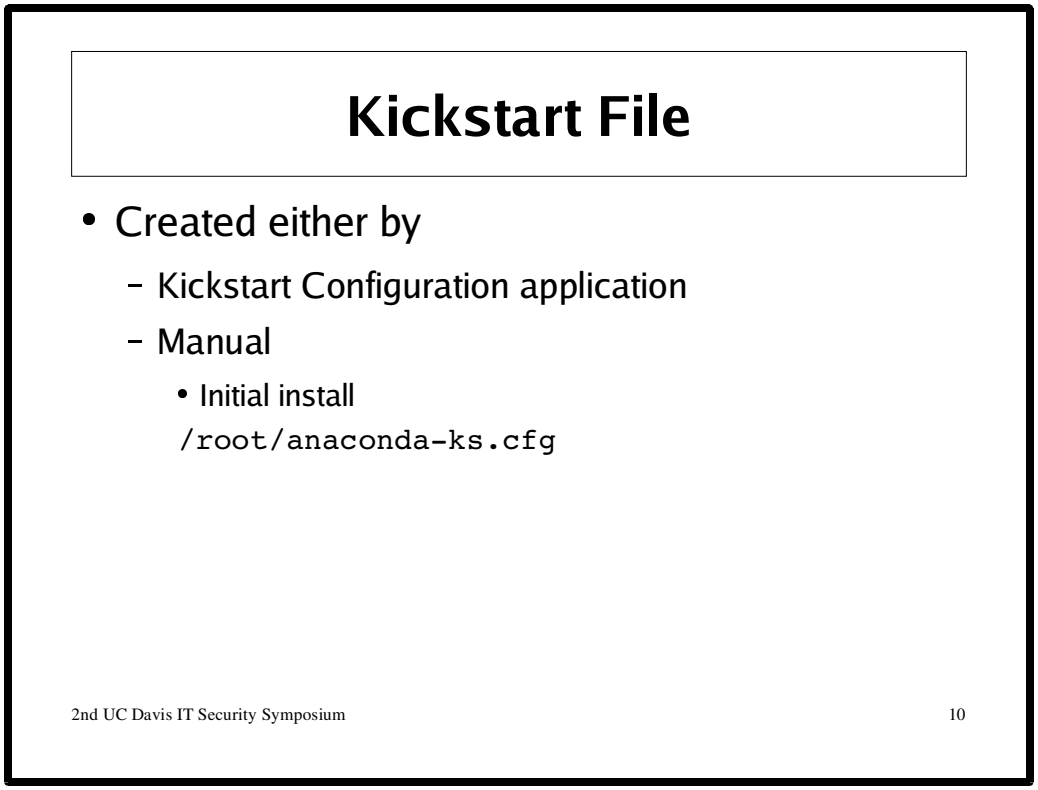
2nd UC Davis IT Security Symposium 9

Install

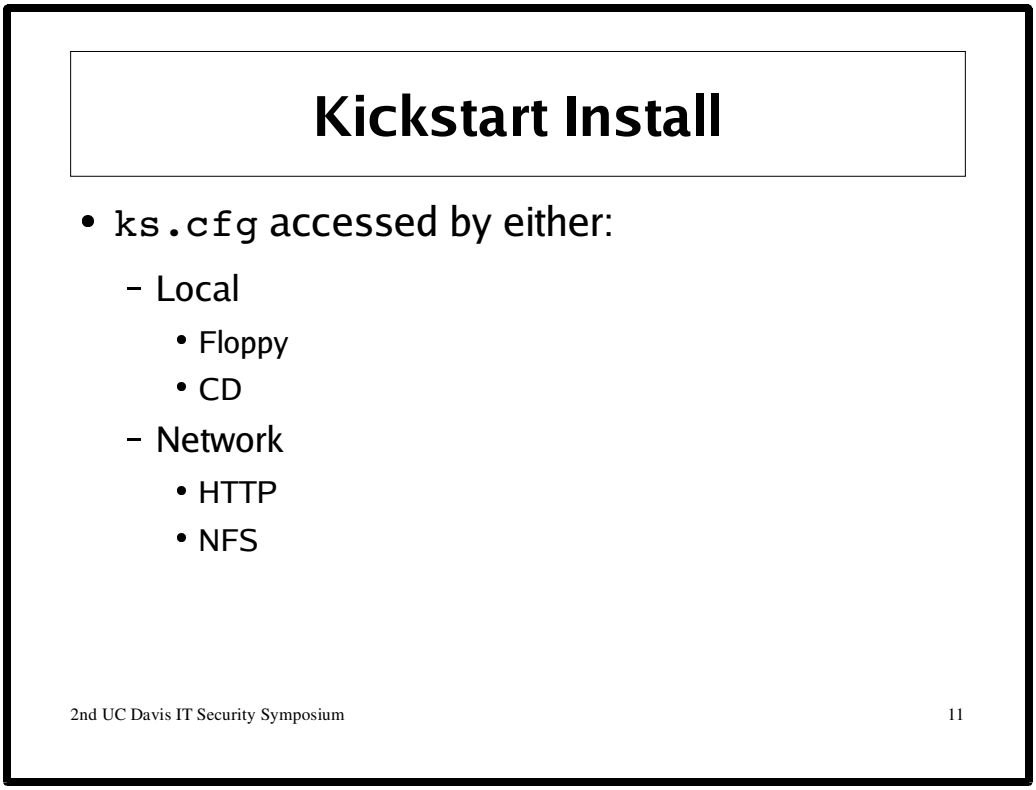
```
sudo yum install system-config-kickstart
```

Run

```
/usr/sbin/system-config-kickstart
```

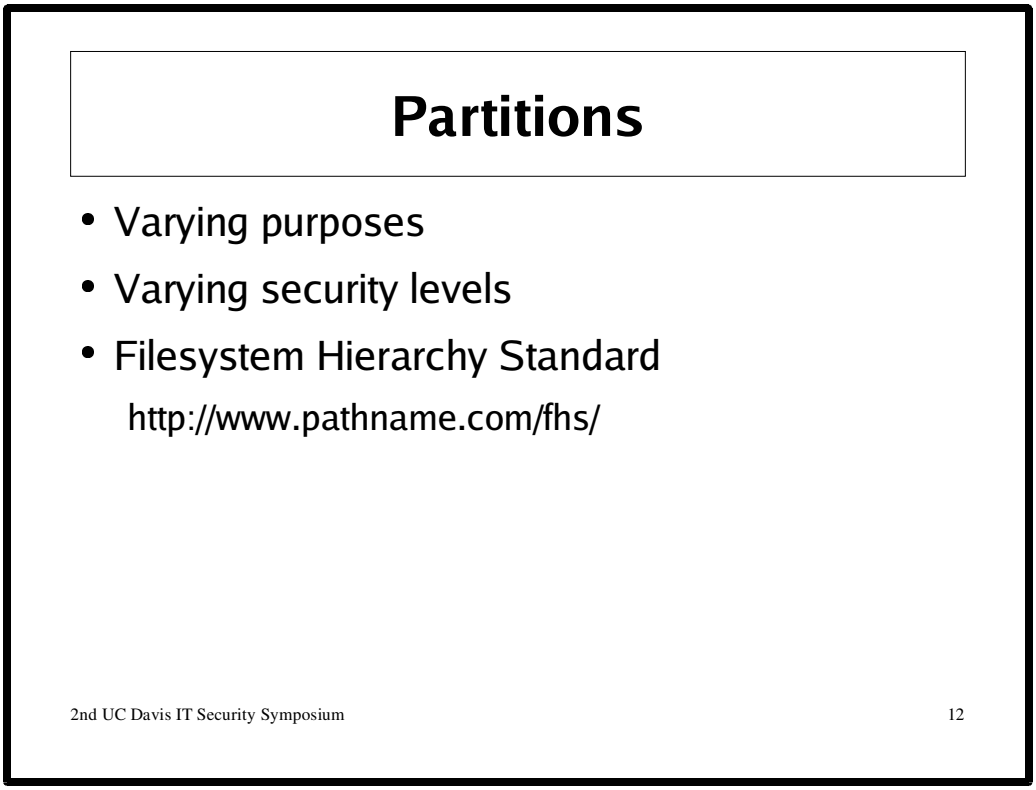




```
# Kickstart file

install
url --url http://192.168.5.5/fc/4/update-iso/original-release
lang en_US.UTF-8
langsupport --default=en_US.UTF-8 en_US.UTF-8 en_US en en_US.UTF-8
   en_US en
keyboard us
network --device eth0 --bootproto dhcp
rootpw --iscrypted $1$JJr9Oivb$yVY//2IxvmcNm3vGFpJ4Q/
firewall --enabled --port=22:tcp
selinux --enforcing
authconfig --enableshadow --enablemd5
timezone --utc America/Los_Angeles

%packages
@ office
@ editors
@ gnome-desktop
@ java
@ base-x
@ graphical-internet

%post
```

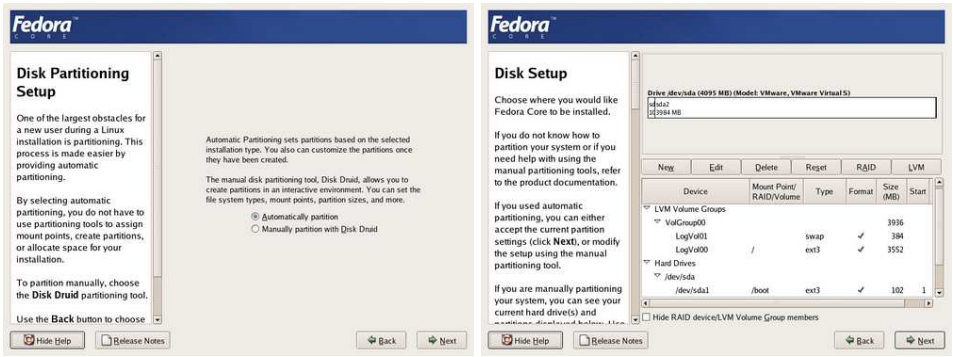
To begin a Kickstart Installation you boot off FC4 Install CD1 and enter a command at the boot prompt. For example,

Floppy
```
linux ks=floppy
```
CD
```
linux ks=cdrom:/ks.cfg
```
HTTP
```
linux ks=http://<server>/<path>
```
NFS
```
linux ks=nfs:<server>:/<path>
```

Consider creating separate partitions for these directories:
`/`, `/boot`, `/usr`, `/var`, `/tmp`, and `/home`

Partitions, Cont.



2nd UC Davis IT Security Symposium 13

General

http://fedora.redhat.com/docs/fedora-install-guide-en/fc4/ch-disk-partitioning.html

Mount Options (`/etc/fstab`)

`acl`
Allow Access Control Lists for files and directories.

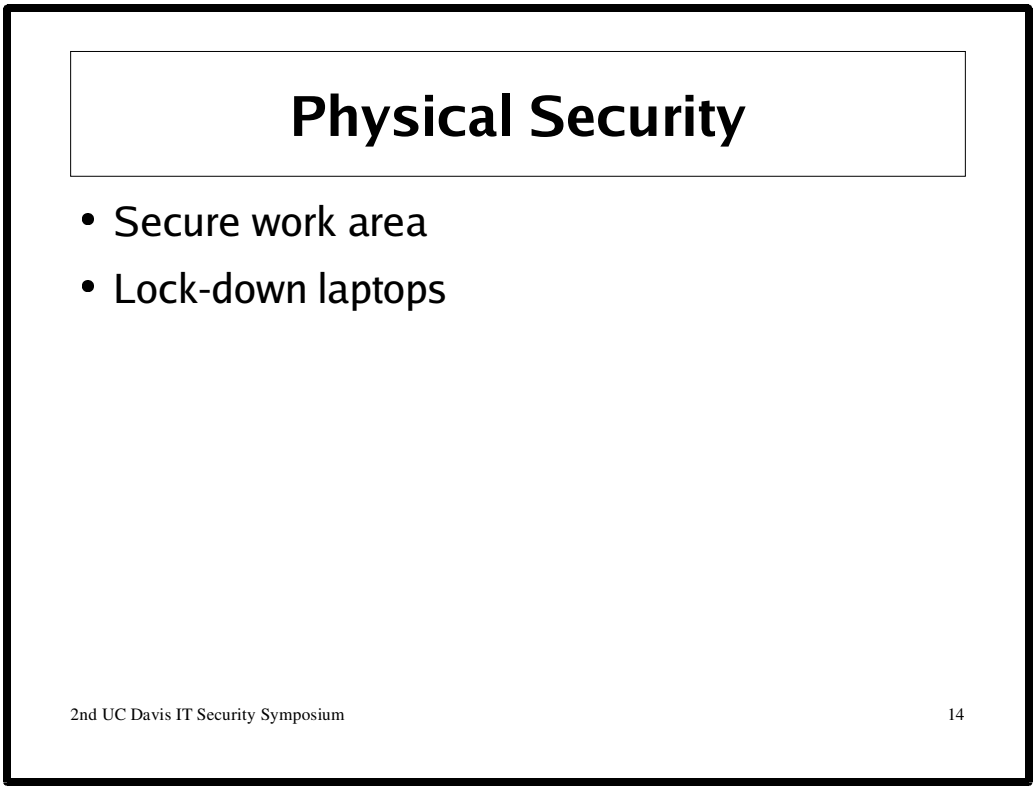
`defaults`
Use default options: `rw`, `suid`, `dev`, `exec`, `auto`, `nouser`, and `async`.

`nodev`
Do not interpret character or block special devices on the file system.

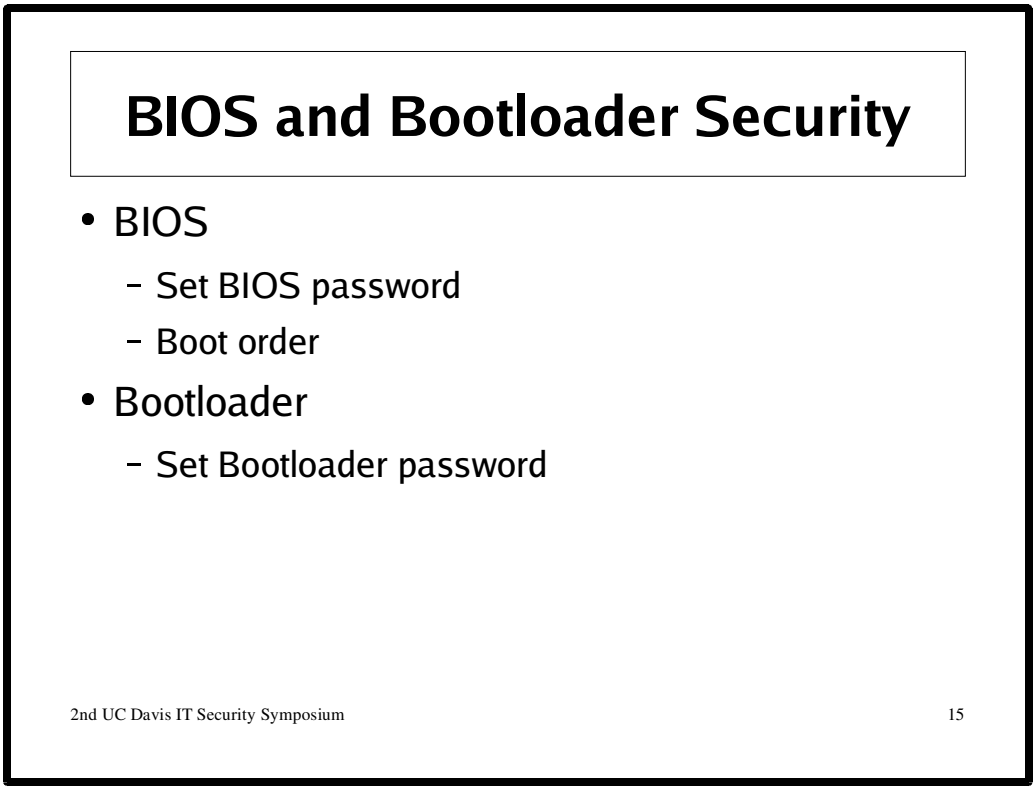
`noexec`
Do not allow direct execution of any binaries on the mounted file system. (Until recently it was possible to run binaries anyway using a command like /lib/ld*.so /mnt/binary. This trick fails since Linux 2.4.25 / 2.6.0.)

`nosuid`
Do not allow set-user-identifier or set-group-identifier bits to take effect. (This seems safe, but is in fact rather unsafe if you have suid-perl(1) installed.)

`nouser`
Forbid an ordinary (i.e., non-root) user to mount the file system. This is the default.



HAAS Business School
http://edition.cnn.com/2005/TECH/03/29/stolen.laptop/



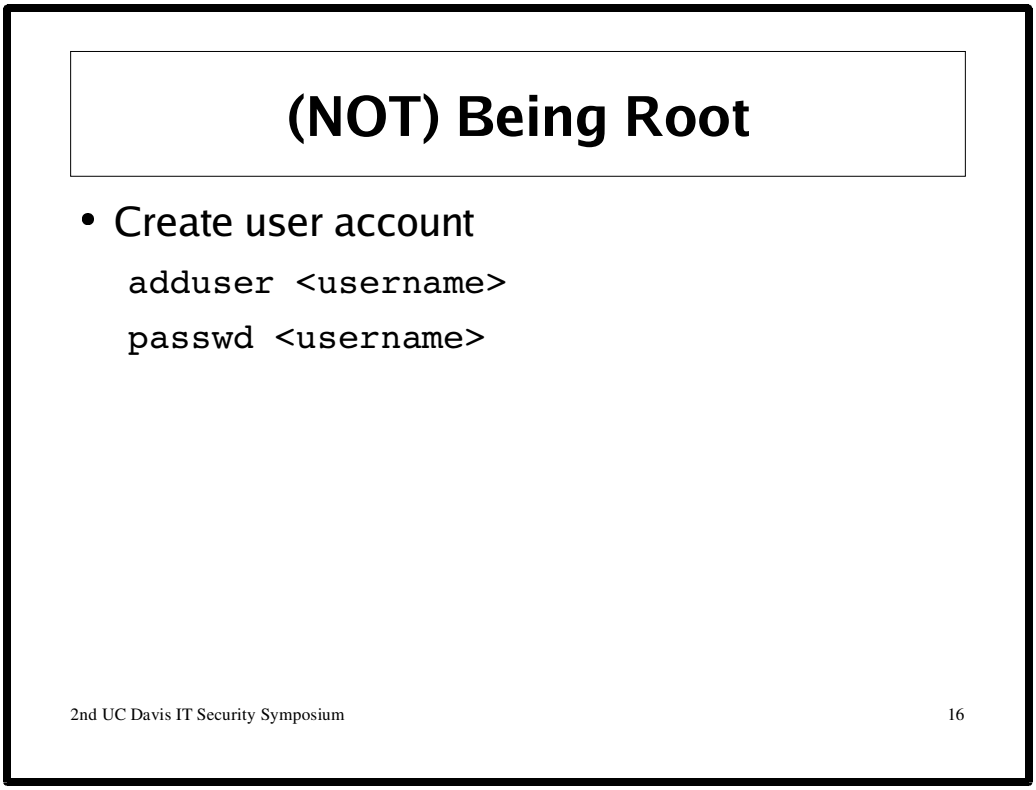
GRUB

GRUB is the GNU GRand Unified Bootloader and is the default FC4 bootloader. To password protect it first create encrpyt your password using GRUB:

```
/sbin/grub

grub> md5crypt

Password: ****
Encrypted: $1$HXkKy0$xpLu8eJffYgM0uosS.ELh1

grub> quit
```

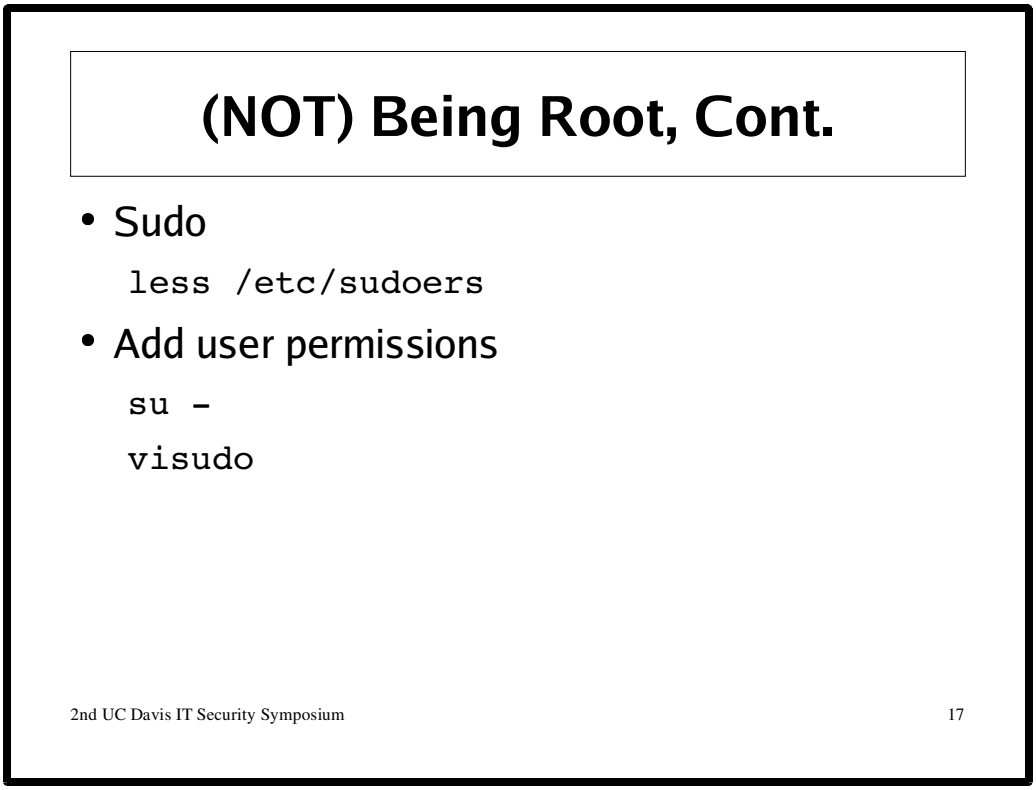
Then add the following line to the `/boot/grub/grub.conf` file (use a different password):

```
password -md5 $1$HXkKy0$xpLu8eJffYgM0uosS.ELh1
```

Restrict Root Logins

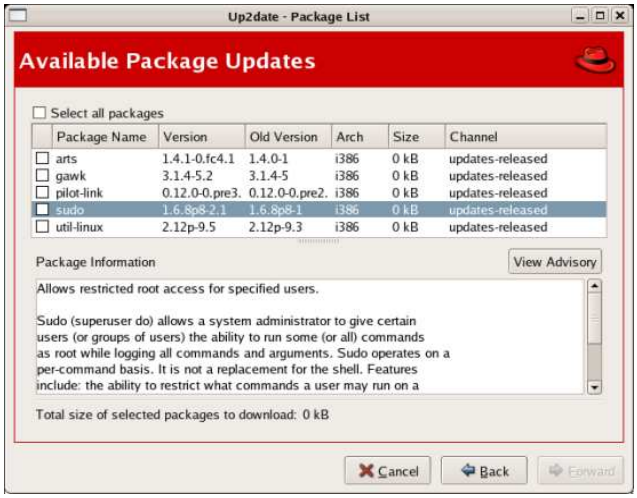
`/etc/securetty`



Sudo Logging

```
/var/log/secure
sudo /usr/sbin/logwatch --print --service sudo --range all
```


Updating Packages



2nd UC Davis IT Security Symposium 18

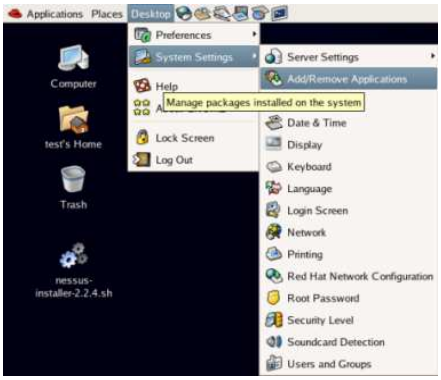
Yum

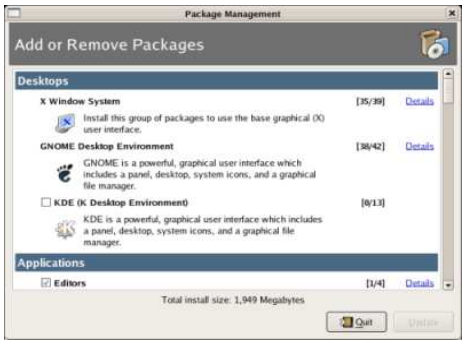
```
sudo yum check-update
sudo yum update
```

up2date

apt

Adding & Deleting Packages





2nd UC Davis IT Security Symposium 19

Run

```
system-config-packages
```

YUM

```
yum search
yum install
```

RPM

```
rpm -Uvh
rpm -ivh
rpm -e
```


Users & Accounts

- Who's logged on?

  `w`

- Who's been logged in recently?

  `last`

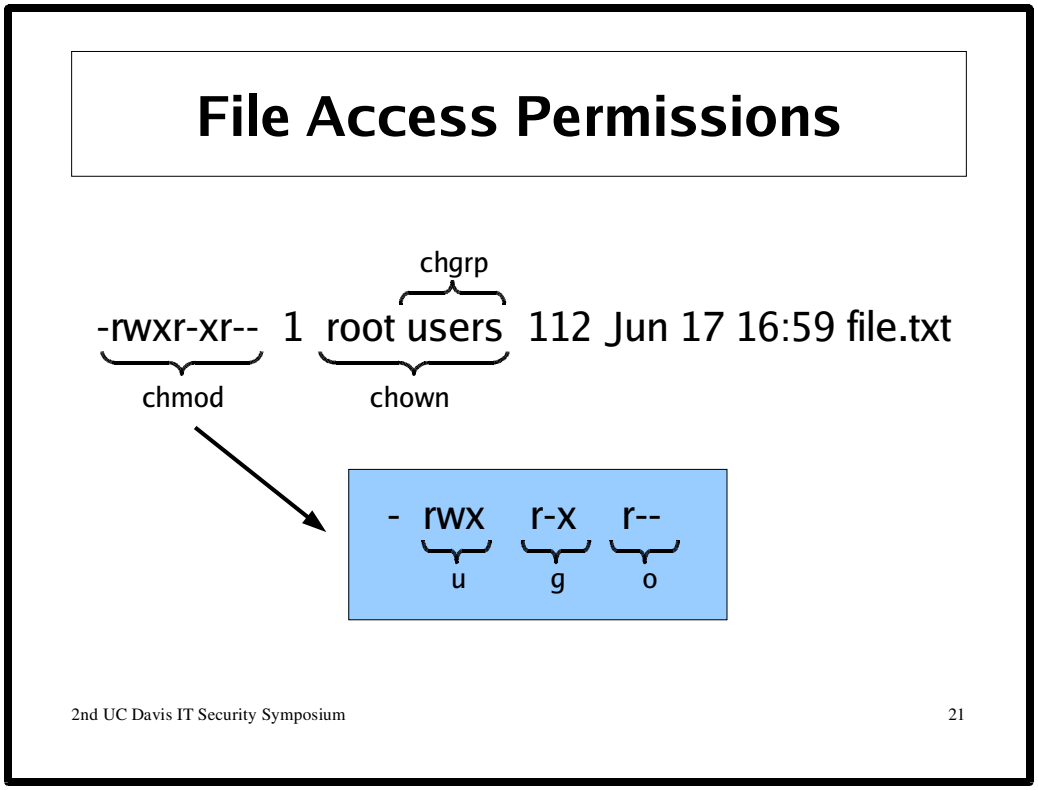
- Who's unsuccessfully tried to log on?

  `lastb`

2nd UC Davis IT Security Symposium 20

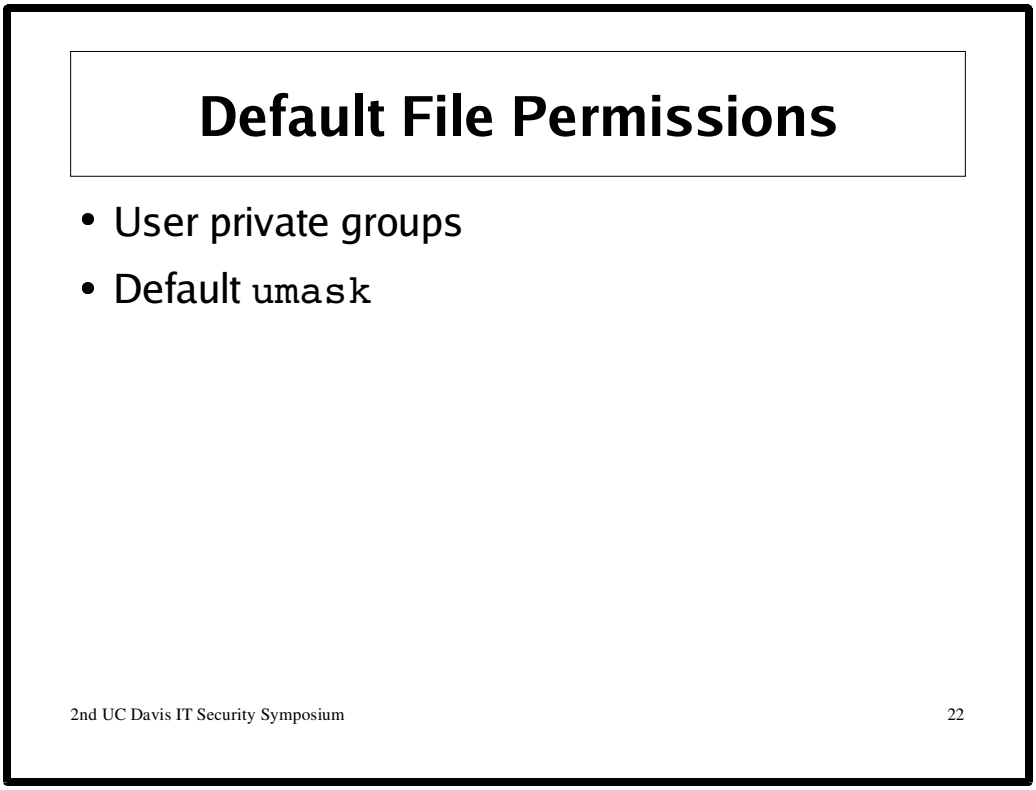
Any suspect account should be immediately locked:
passwd -l <username>

Periodically checking who is logged in to your machine is a good start. Furthermore, it is useful to keep any eye on `/etc/passwd`. Look for duplicate accounts with the same UID.

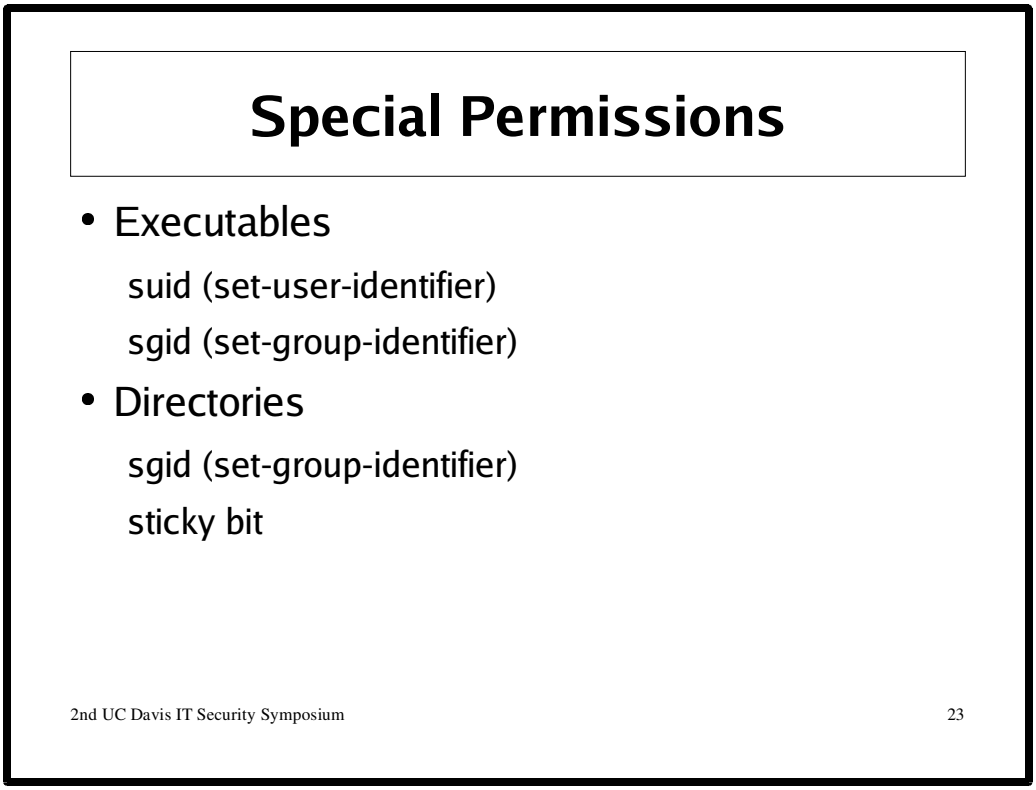


Understanding File Permissions
To see the file permission of a file use the `ls -l` command.

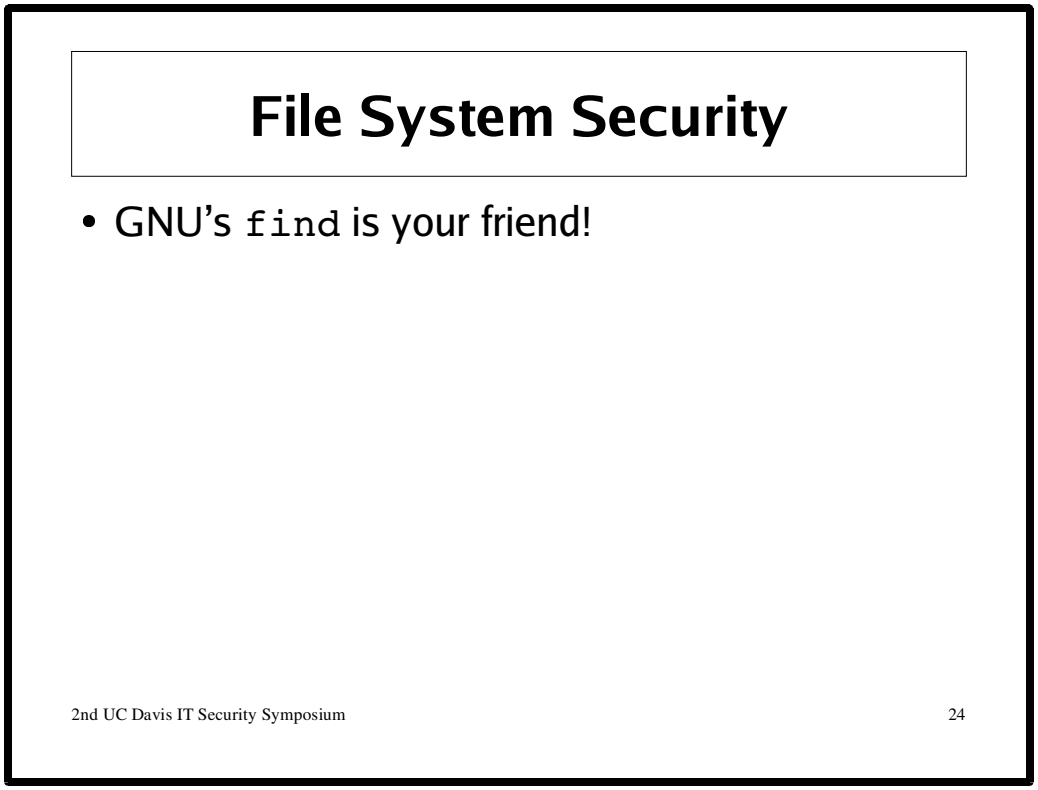
Changing File Permissions



Default File Permissions (umask)
dfd



setUID and setGUD
dfd



SUID/SGID

```
sudo find / -xdev -type f -perm +ug=s
```

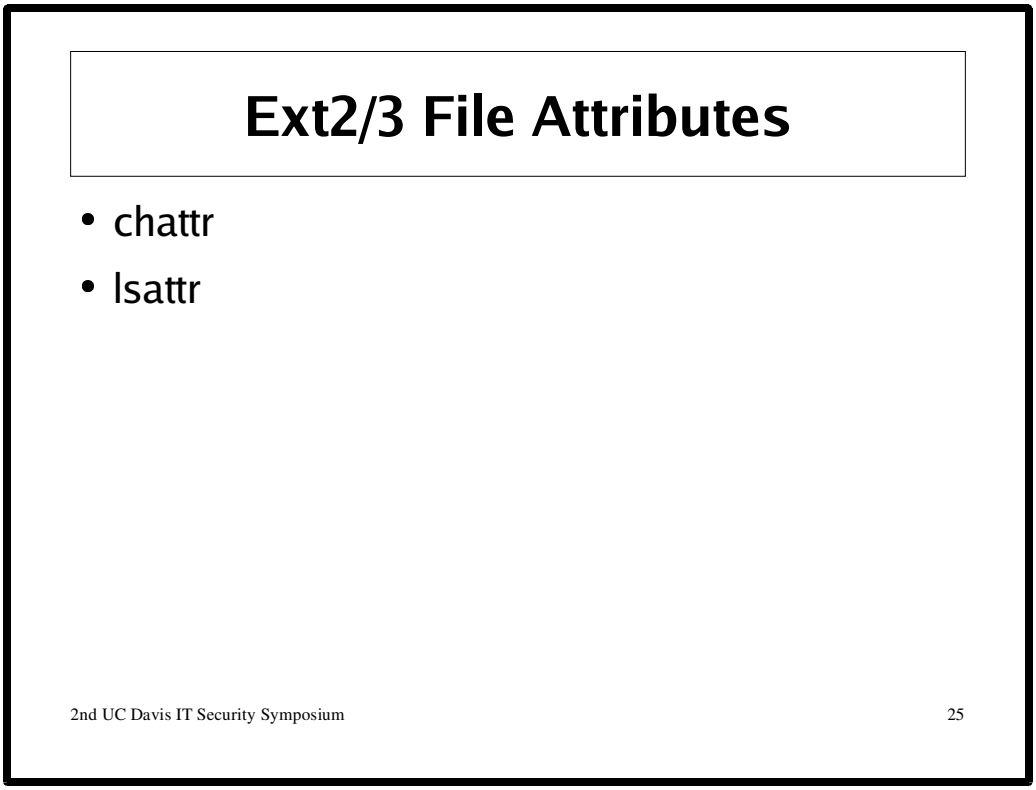
Device Special Files

```
sudo find /  \( -type b -o -type c \) -ls
sudo find /dev -type f ! -name MAKEDEV
```

World Writable Files

```
sudo find / -path /proc -prune -o \
    -perm +o=w ! \( -type d -perm +o=t \) ! -type l
```

For more information see:
O'Reilly's Linux Security Cookbook

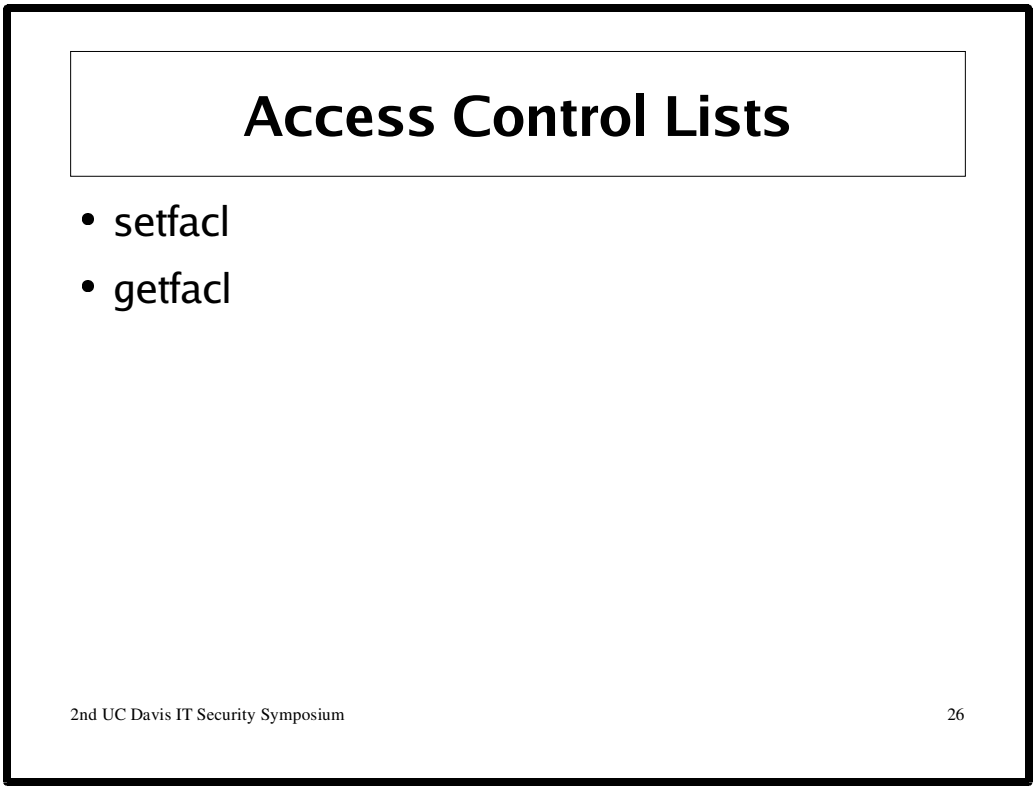


These are worth a look; in particular these attributes are worth consideration:

a
File can only be opened in the append mode.

i
File is immutable. I.e., it cannot be deleted, renamed, linked to, or changed.

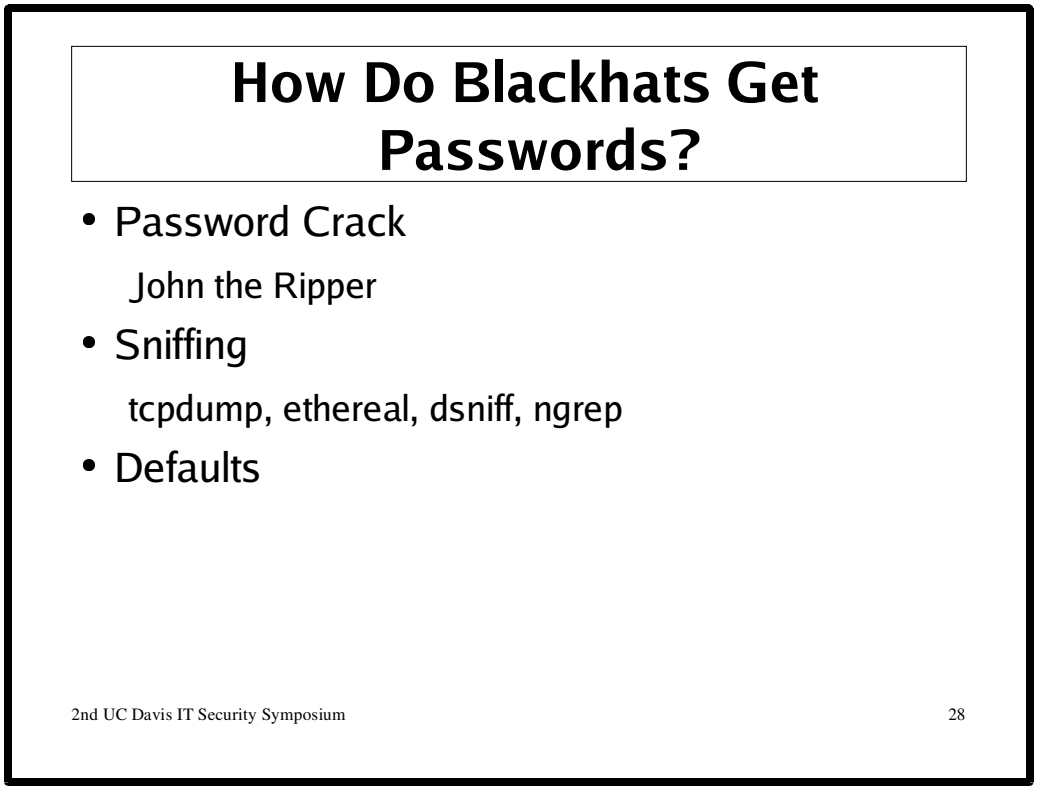
s
When the file is deleted, it's blocks are overwritten with zeroes.



See **Chapter 14: Access Control Lists** in **RHEL 4 System Administration Guide**:
http://www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/sysadmin-guide/

Ideas for creating memorable passwords

* Use the first letters of the words of a unique phrase or sentence. Then substitute in some digits and symbols. For example, the sentence
  I find Jarrod to be easy-going and straightforward
  might yield
  1fJ2be-g&sf
  Of course, this password should still conform to the above rules.
* Try combining two or more words together or taking the first (or second or last) letter of each word in an easily remembered phrase. Then mangle the result by adding capitals, digits and punctuation characters. For example,
  gOt%L0st! - got lost!
  heLP4me$ - help for me (money)
* Use misspelled words (WhutdooUmeenIkan'tSpel?).
* Something that no one but you would ever think of. The best password is one that is totally random to anyone else except you. It is difficult to tell you how to come up with these, but people are able to do it. Use your imagination!

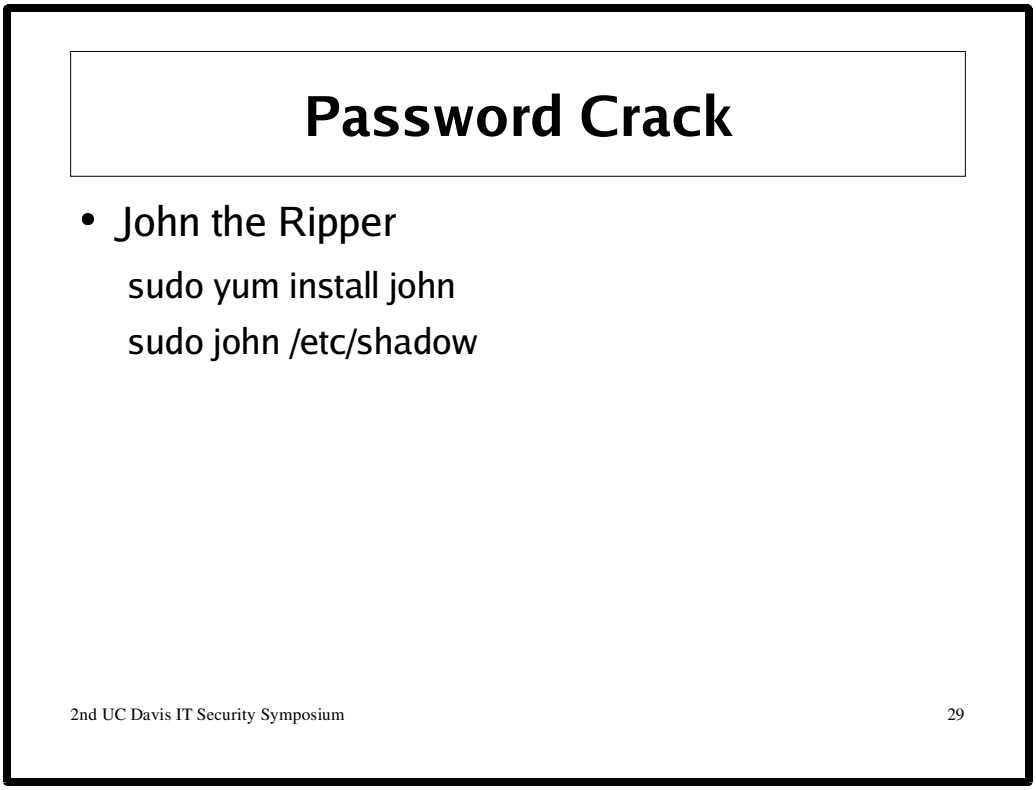


Do

* Use a password with mixed-case alphabetics.
* Use a password with nonalphabetic characters, e.g., digits or punctuation.
* Use a password that is easy to remember, so you don't have to write it down.
* Use a password that you can type quickly, without having to look at the keyboard.
* Use different passwords for account, e.g., your email account, bank account.

Don't

* Use any words contained in (English or foreign language) dictionaries, spelling lists, or other lists of words in any form (as-is, reversed, capitalized, doubled, etc.)
* Use information easily obtained about you. E.g., your name, login name, spouse's or child's name, license plate numbers, telephone numbers, social security numbers, the brand of your automobile, the name of the street you live on, etc. use a password of all digits, or all the same letter. This significantly decreases the search time for an intruder.
* Use a password shorter than 8 characters.
* Use a keyboard pattern such as qwertyui or oeuidhtn (look at a Dvorak keyboard).
* Give or share your password, in particular to someone claiming to be from computer support or a vendor.
* Store or send your password in plain text.
* Email your password to yourself or someone else.



"John the Ripper is a fast password cracker, currently available for many flavors of Unix (11 are officially supported, not counting different architectures), DOS, Win32, BeOS, and OpenVMS. Its primary purpose is to detect weak Unix passwords. Besides several crypt(3) password hash types most commonly found on various Unix flavors, supported out of the box are Kerberos AFS and Windows NT/2000/XP/2003 LM hashes, plus several more with contributed patches."
http://www.openwall.com/john/

Wordlists:
http://www.openwall.com/wordlists/
ftp://ftp.ox.ac.uk/pub/wordlists/

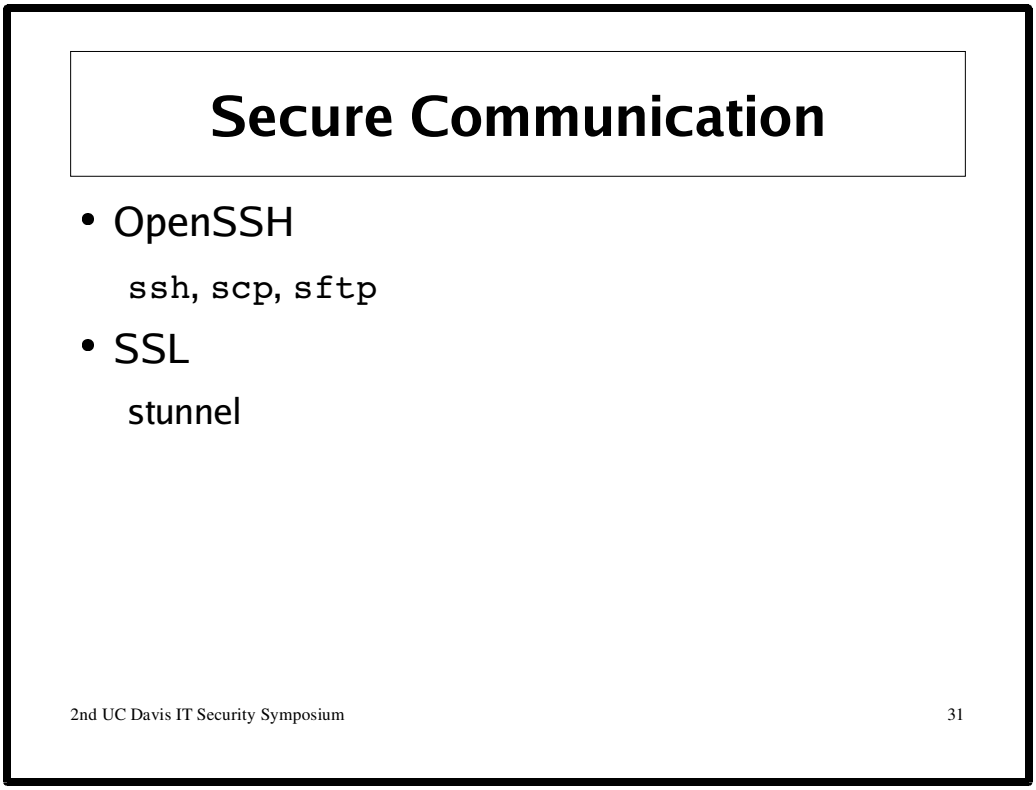
Network Sniffing

- TCPDump

```
sudo /usr/sbin/tcpdump
```

- Ethereal

```
sudo yum install ethereal-gnome
ethereal
```

Stricter Controls in openssh

"The version of OpenSSH in Fedora Core 4 is based on OpenSSH 3.9 and includes strict permission and ownership checks for the user configuration file ~/.ssh/config. If this file does not have appropriate ownership and permissions, ssh will exit.

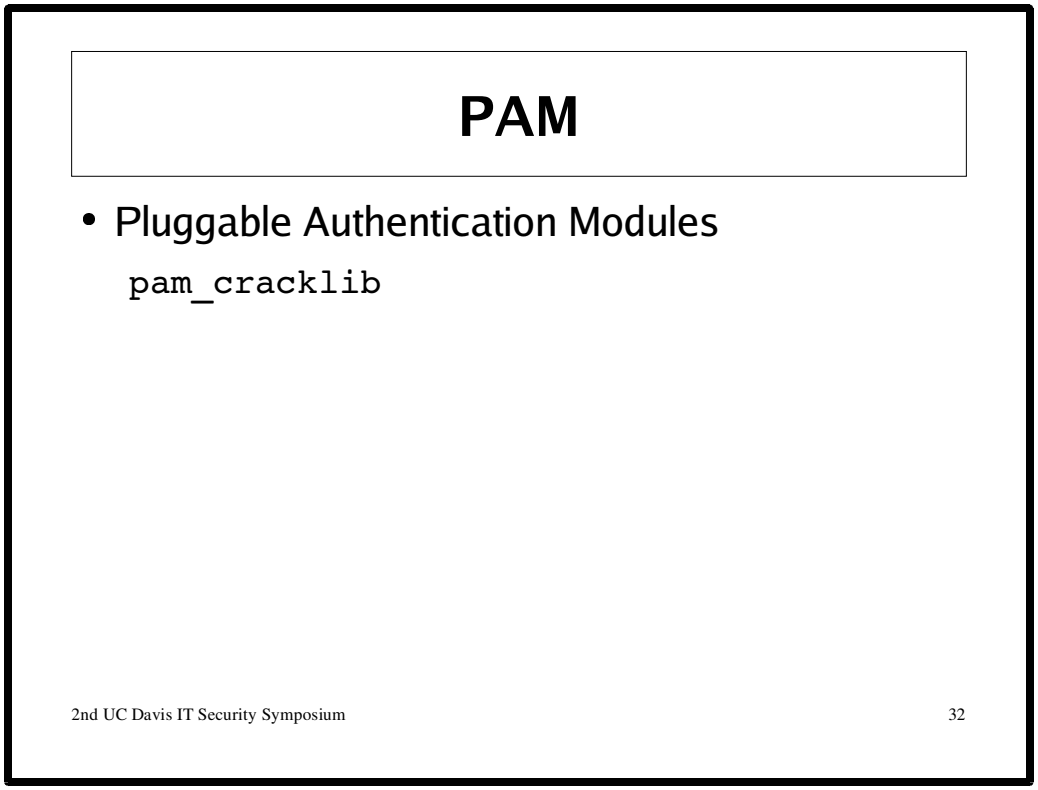
Check that ~/.ssh/config is owned by the owner of ~/, and that its permissions are set to mode 600.

```
ls -l ~/.ssh/config
-rw-------  1 user user 400 May  5 18:44 ~/.ssh/config
```

The directory ~/ is command-line shorthand for the logged in user's home directory, usually /home/username/.

In addition, OpenSSH is no longer configured to request X11 forwarding by default when connecting to servers. To enable X11 forwarding, the -X or -Y option must be specified, or the ForwardX11 option must be enabled in the ~/.ssh/config file.

The behavior of ssh clients that are invoked with the -X option has changed. In OpenSSH 3.8 and later, X11 forwarding is performed in a way that applications run as untrusted clients by default. Previously, X11 forwarding was performed so that applications always ran as trusted clients. Some applications may not function properly when run as untrusted clients. To forward X11 so that applications are run as trusted clients, invoke ssh with the -Y option instead of the -X option, or set ForwardX11Trusted in the ~/.ssh/config file."



"Q0: What exactly is PAM?
PAM = Pluggable Authentication Modules

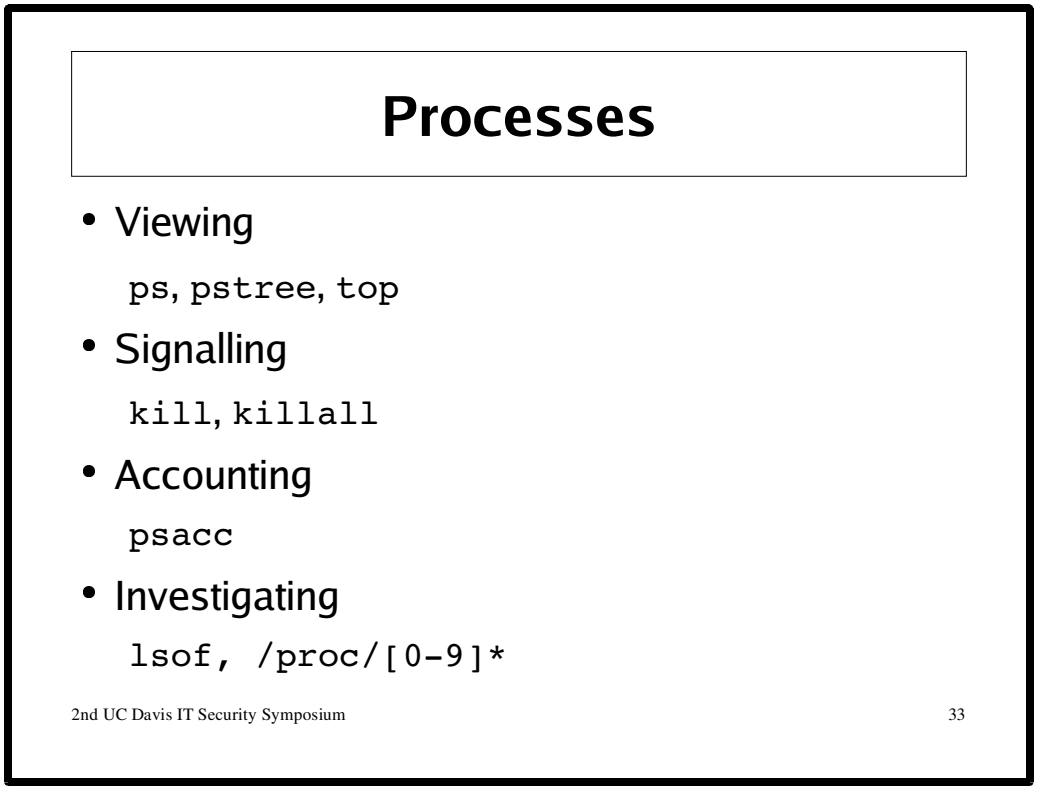
Basically, it is a flexible mechanism for authenticating users.

Since the beginnings of UNIX, authenticating a user has been accomplished via the user entering a password and the system checking if the entered password corresponds to the encrypted official password that is stored in `/etc/passwd`. The idea being that the user *is* really that user if and only if they can correctly enter their secret password.

That was in the beginning. Since then, a number of new ways of authenticating users have become popular. Including more complicated replacements for the `/etc/passwd` file, and hardware devices Smart cards etc..

The problem is that each time a new authentication scheme is developed, it requires all the necessary programs (login, ftpd etc...) to be rewritten to support it.

PAM provides a way to develop programs that are independent of authentication scheme. These programs need "authentication modules" to be attatched to them at run-time in order to work. Which authentication module is to be attatched is dependent upon the local system setup and is at the discretion of the local system administrator."
http://www.kernel.org/pub/linux/libs/pam/FAQ



Crackers will often try to remove all evidence of their presence. One way they do this is by installing some files and then starting up some process using it. Once the process is started, the cracker can then delete the files. The process will still have access to these files since it will have its own file descriptors.

For an excellent discussion of this issue and how to deal with it, please read the following articles by Brian Hatch:

07-May-2002: Recovering files from /Proc
The ability to use files seemingly deleted from the /proc directory helps savvy attackers avoid detection and remove incriminating files.
14-May-2002: Investigating Processes, Part 1
This week, Brian shares some more /proc tricks for investigating programs running on your machine.
21-May-2002: Our Continuing /proc and lsof Investigation
Following up on last week's useful /proc and lsof investigative tools, Brian goes back and addresses the tidbits he didn't have time for last week.

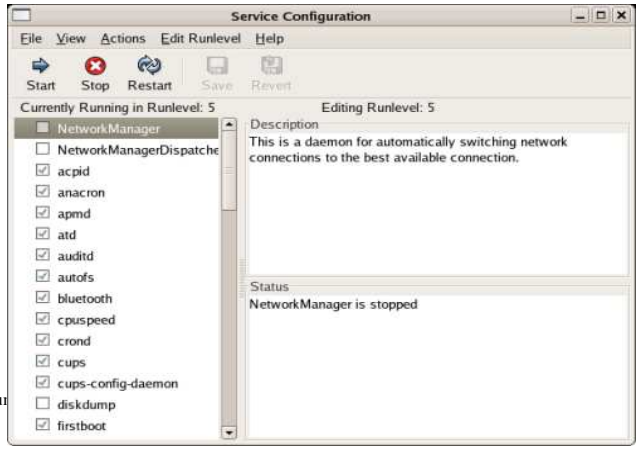
These and other articles by Brian can be found here:
http://www.hackinglinuxexposed.com/articles/

Services

- Configuring

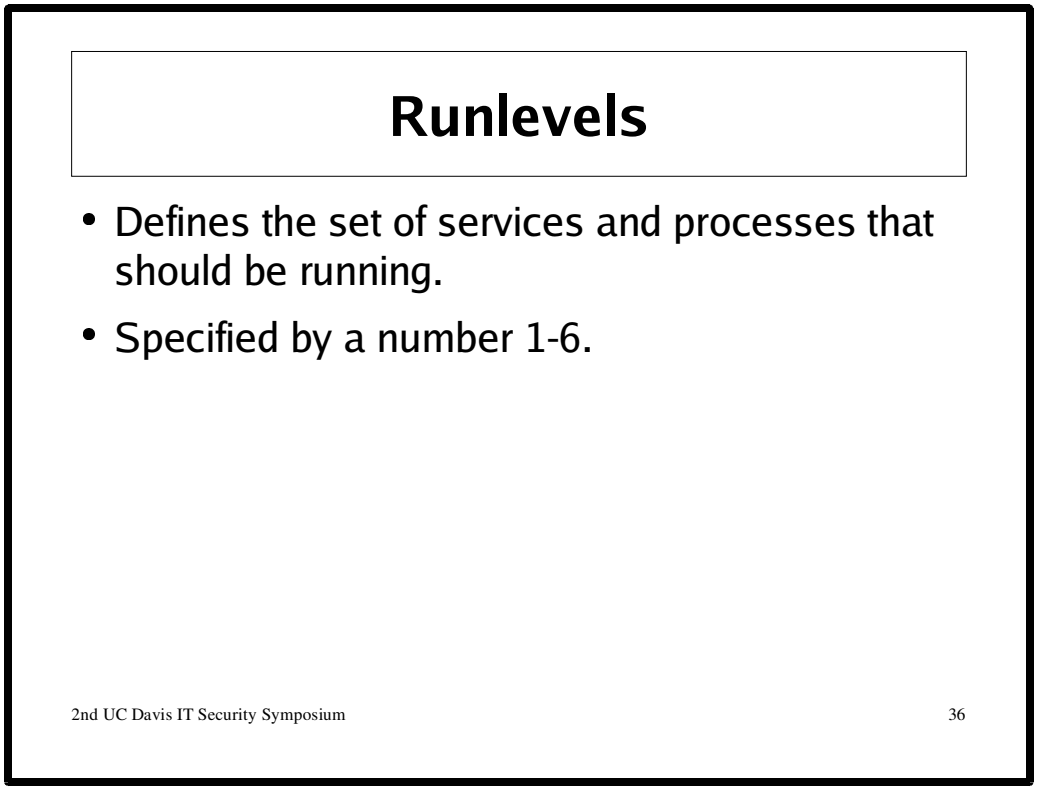
  `chkconfig`, `service`

Services Configuration Tool



2nd UC Davis IT Security Symposiu

`system-config-services`

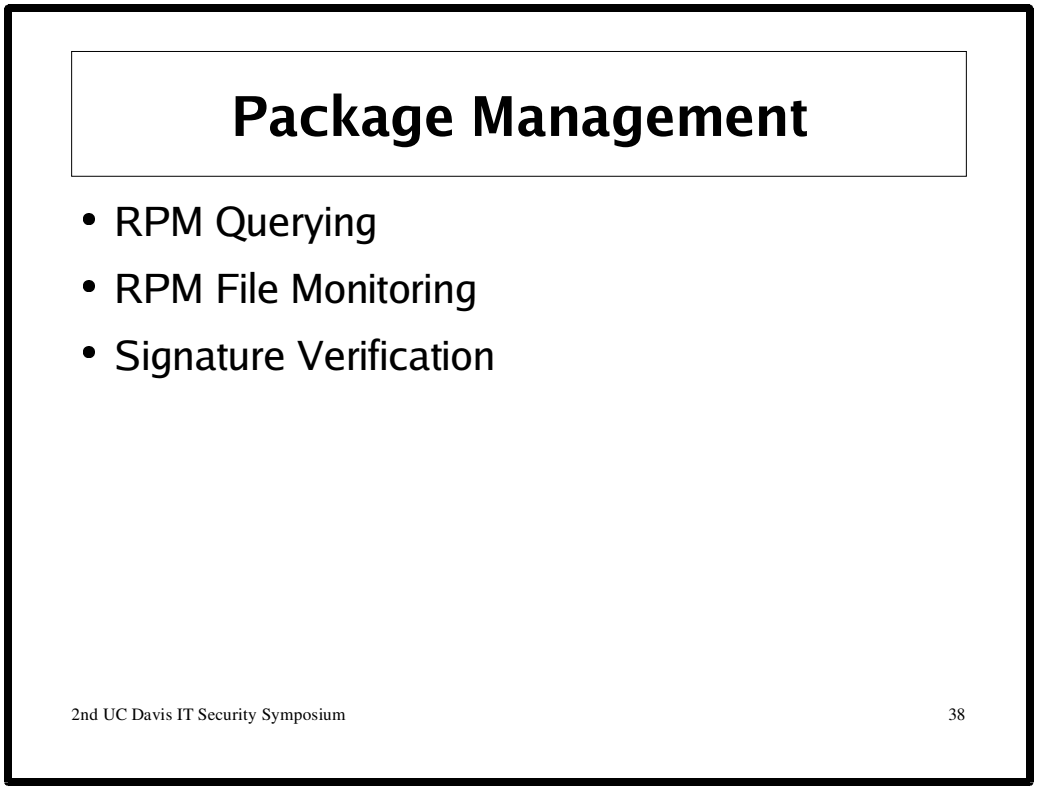


Runlevels
0: Halt
1: Single User Mode
2: Basic Multi-user Mode
3: Full Multi-user without X
4: Not Used
5: Mutli-user with X
6: Reboot

Default runlevel is specified in `/etc/inittab`. You can force a system into a specific runlevel with the `init` command. The specific services that are to be started or killed when going from one runlevel to another are found in `/etc/rc.d`.

TCP_wrappers

- `/etc/hosts.allow`
- `/etc/hosts.deny`



Set up

```
# Grab some packages from Dag Wieers
DAG=http://dag.wieers.com/packages
sudo wget ${DAG}/perl-Tk/perl-Tk-804.027-1.2.fc4.rf.i386.rpm
sudo wget ${DAG}/perl-Curses/perl-Curses-1.12-1.2.fc4.rf.i386.rpm
```

Querying

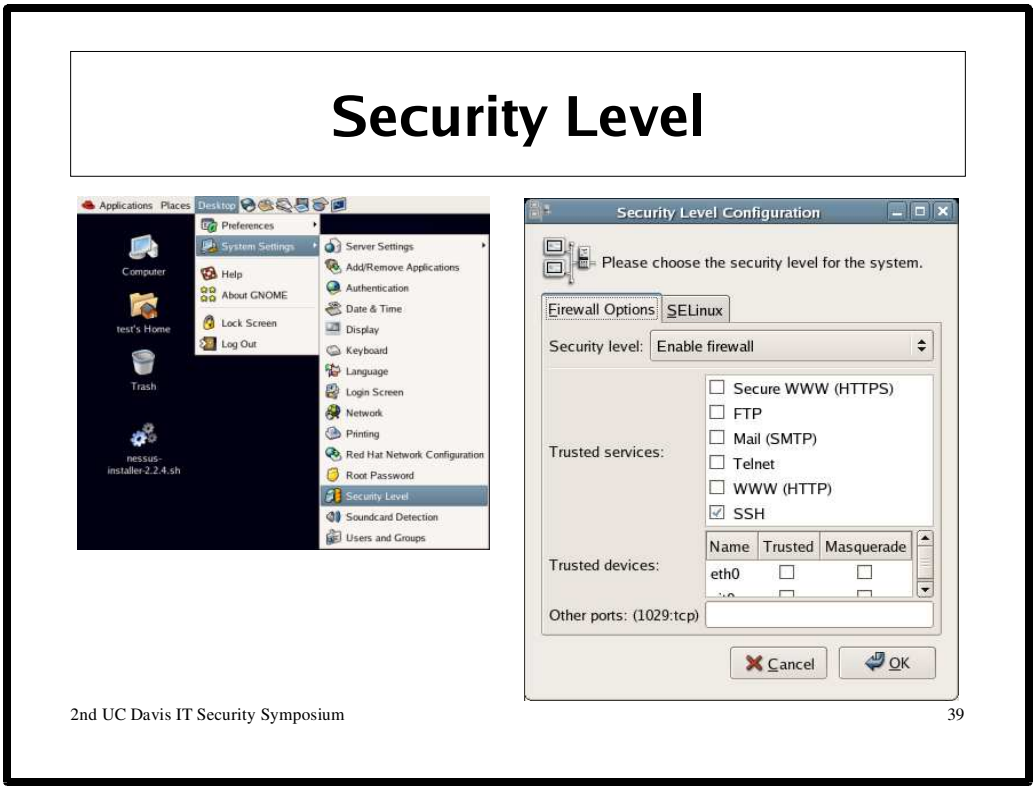
```
rpm -qf /usr/lib/libwrap.a
rpm -qif /usr/lib/libwrap.a
rpm -qp perl-Tk-804.027-1.2.fc4.rf.i386.rpm
```

File Monitoring

```
rpm -V tcp_wrappers
rpm -Va
rpm -Vp perl-Tk-804.027-1.2.fc4.rf.i386.rpm
```

Signature Verification

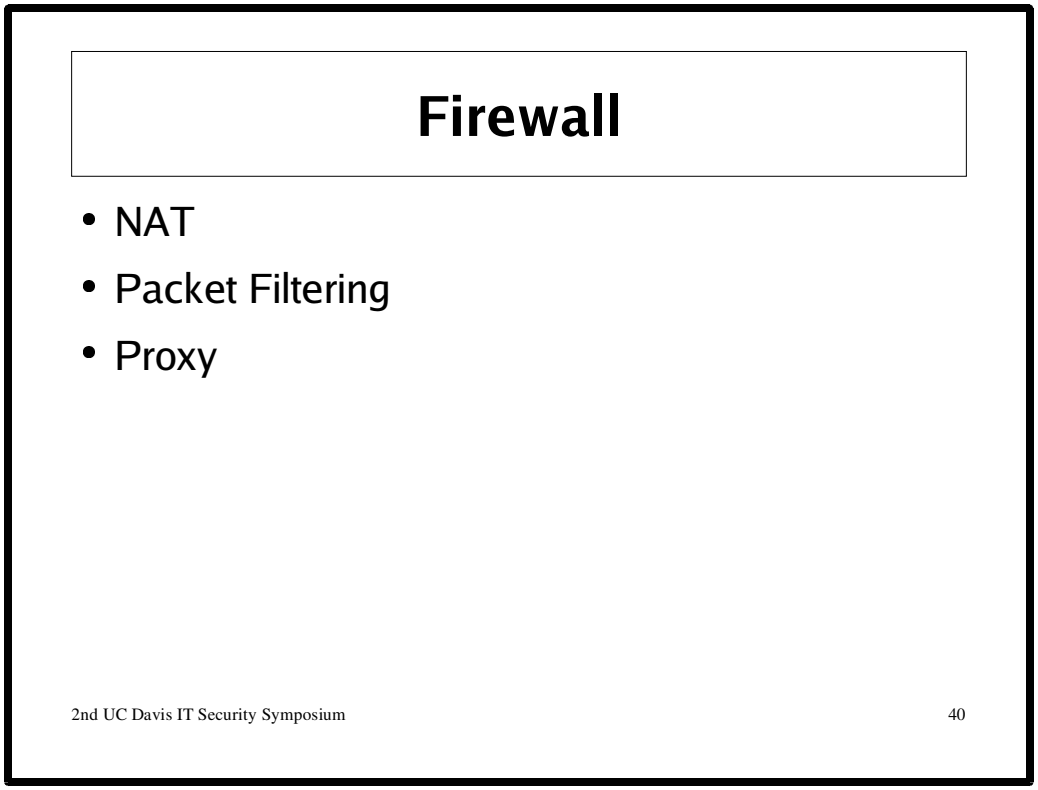
```
# Install Dag's GPG key
rpm -q gpg-pubkey --qf "%{summary} -> %{version}-%{release}\n"
sudo rpm --import ${DAG}/RPM-GPG-KEY.dag.txt
rpm -q gpg-pubkey --qf "%{summary} -> %{version}-%{release}\n"
rpm --checksig perl*
# Install the packages
sudo rpm -Uvh perl-Curses-1.12-1.2.fc4.rf.i386.rpm
sudo rpm -Uvh perl-Tk-804.027-1.2.fc4.rf.i386.rpm
```

Security Levels

FC4's security levels are an easy way to increase the security of your system. Basically, they are meant to prevent unauthorized access to your computer. Use the following command to launch the security levels configuration tool:

```
system-config-security
```

netfilter/iptables

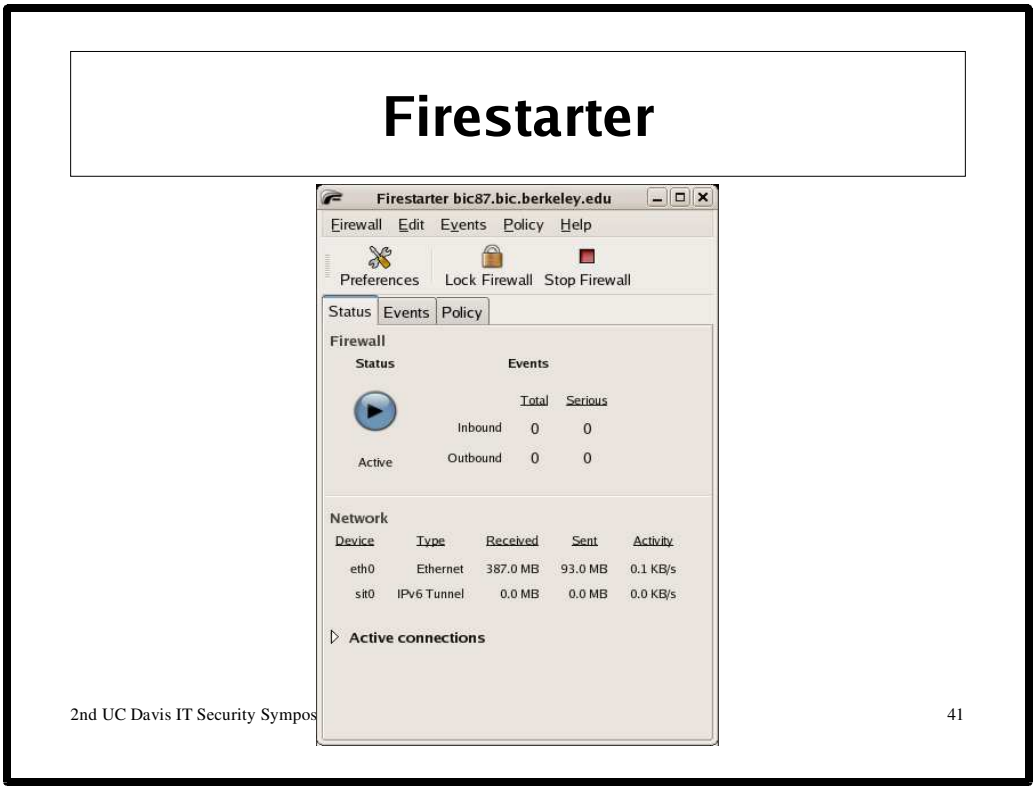
"netfilter and iptables are building blocks of a framework inside the Linux 2.4.x and 2.6.x kernel. This framework enables packet filtering, network address [and port] translation (NA[P]T) and other packet mangling. It is the re-designed and heavily improved successor of the previous Linux 2.2.x ipchains and Linux 2.0.x ipfwadm systems.

netfilter is a set of hooks inside the Linux kernel that allows kernel modules to register callback functions with the network stack. A registered callback function is then called back for every packet that traverses the respective hook within the network stack.

iptables is a generic table structure for the definition of rulesets. Each rule within an IP table consists of a number of classifiers (iptables matches) and one connected action (iptables target).

netfilter, iptables and the connection tracking as well as the NAT subsystem together build the whole framework."

http://www.netfilter.org/



"Firestarter is an Open Source visual firewall program. The software aims to combine ease of use with powerful features, therefore serving both Linux desktop users and system administrators.

We strongly believe that your job is to make the high level security policy decisions and ours is to take care of the underlying details. This is a departure from your typical Linux firewall, which has traditionally required arcane implementation specific knowledge."
http://www.fs-security.com/

Install

```
sudo yum install firestarter
```

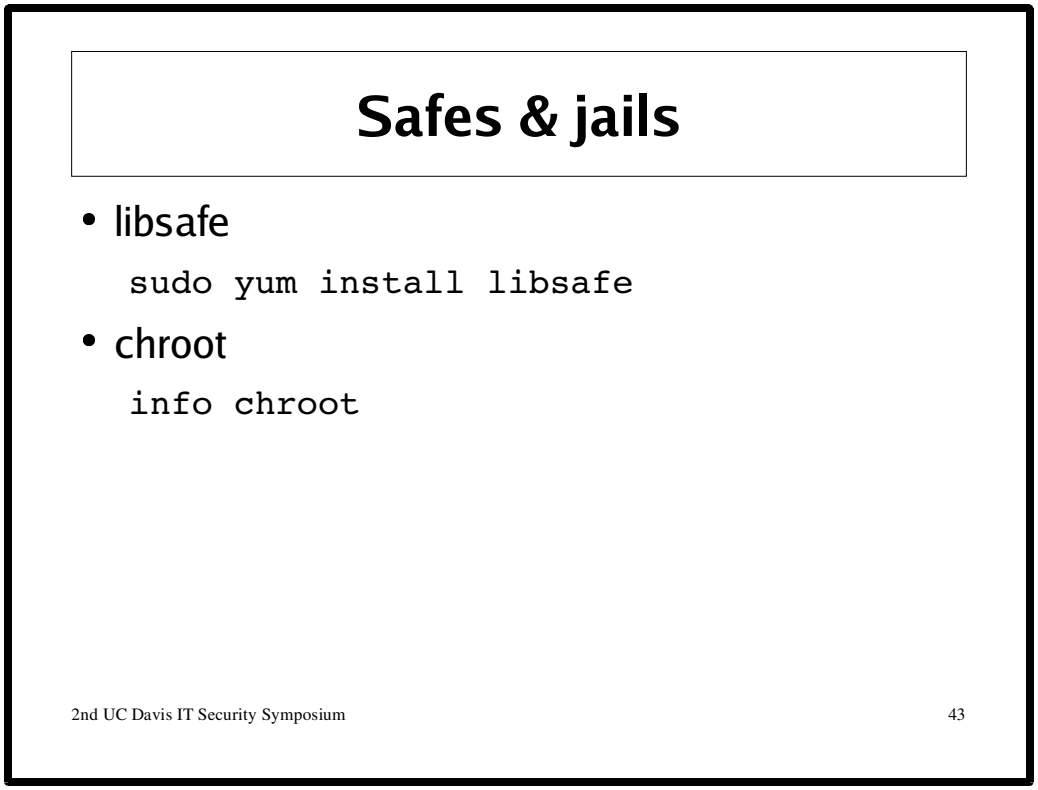

SELinux

`system-config-securitylevel`

2nd UC Davis IT Security Symposium 42

"Security-enhanced Linux (SELinux)is a patch of the Linux® kernel and a number of utilities with enhanced security functionality designed to add mandatory access controls to Linux. The SELinux kernel contains new architectural components originally developed to improve the security of the Flask operating system. These architectural components provide general support for the enforcement of many kinds of mandatory access control policies, including those based on the concepts of Type Enforcement®, Role-based Access Control, and Multi-level Security."
http://fedora.redhat.com/projects/selinux/

See:
http://fedora.redhat.com/docs/selinux-faq/
http://www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/selinux-guide/



libsafe

"The libsafe library protects a process against the exploitation of buffer overflow vulnerabilities in process stacks. Libsafe works with any existing pre-compiled executable (but is incompatible with libc5-linked processes) and can be used transparently, even on a system-wide basis. The method intercepts all calls to library functions that are known to be vulnerable. A substitute version of the corresponding function implements the original functionality, but in a manner that ensures that any buffer overflows are contained within the current stack frame. Libsafe has been shown to detect several known attacks and can potentially prevent yet unknown attacks. Experiments indicate that the performance overhead of libsafe is negligible."

file:///usr/share/doc/libsafe-2.0/doc/libsafe.8.html

For more information see:

http://www.research.avayalabs.com/project/libsafe/

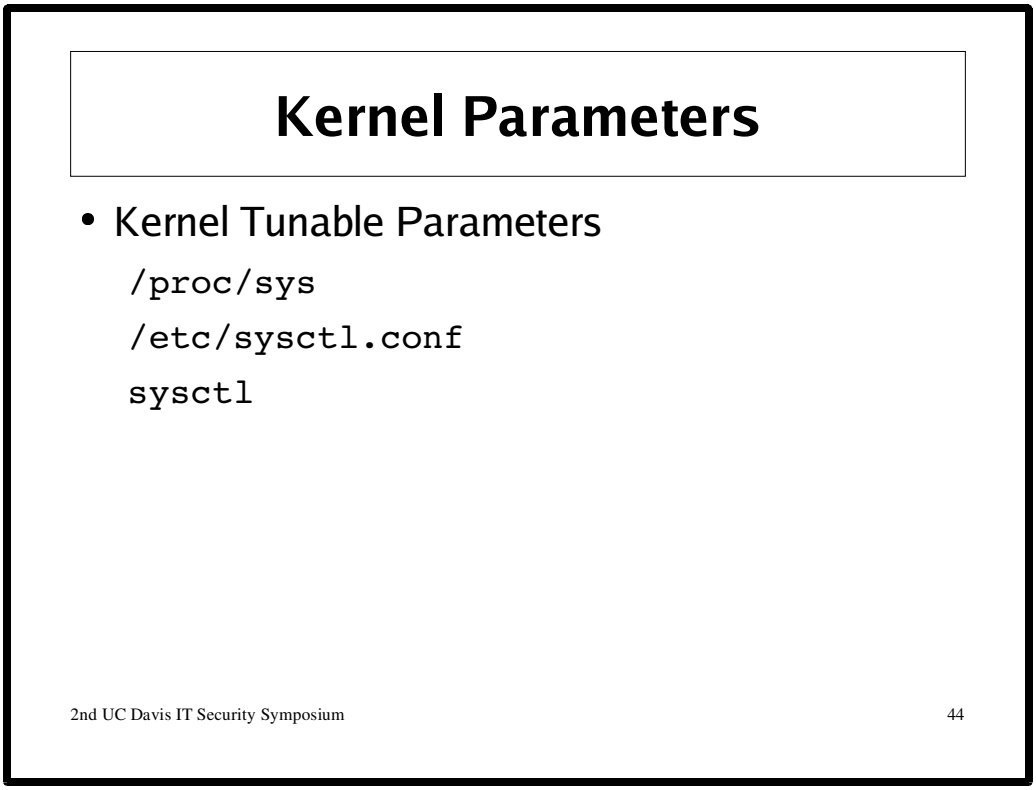
`chroot`

`chroot` is part of the GNU `coreutils` package:

http://www.gnu.org/software/coreutils/

`chroot` is preferred over libsafe in most cases; however, `chroot` is notorious for proving a difficult and time-consumming process. RPMs configured to create a `chroot` environment can occasionally be found (e.g., `bind-chroot`). There is also a project that attempts to make creating `chroot` environments easier called `jail`. Very little work is being done on this project, but it might be worth a look:

http://www.jmcresearch.com/projects/jail/



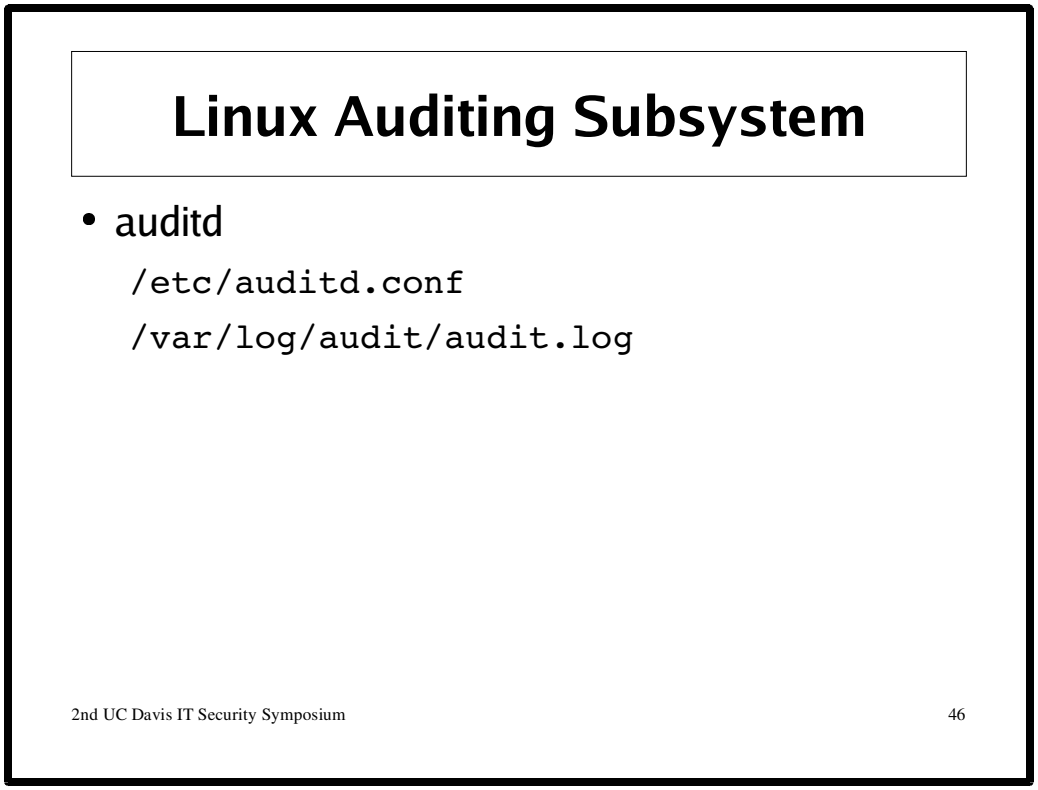
A sample `/etc/sysctl.conf` file:

```
# Disable IP packet forwarding
net.ipv4.ip_forward = 0
# Enable source route verification (IP spoofing protection)
net.ipv4.conf.default.rp_filter = 1
# Ignore ping requests
net.ipv4.icmp_echo_ignore_all = 1
# Do not accept source routing
net.ipv4.conf.default.accept_source_route = 0
# Disable ICMP redirects
net.ipv4.conf.all.accept_redirects = 0
# Ignore broadcast requests
net.ipv4.icmp_echo_ignore_broadcasts = 1
# Disable System Request debugging functionality
kernel.sysrq = 0
# Enable TCP syncookies protection
net.ipv4.tcp_syncookies = 1
# Log bad error message
net.ipv4.icmp_ignore_bogus_error_responses = 1
# Log spoofed, source routed, and redirected packets
net.ipv4.conf.all.log_martians = 1
```

For more information see: http://www.linuxsecurity.com/content/view/111337/65/

System Logs

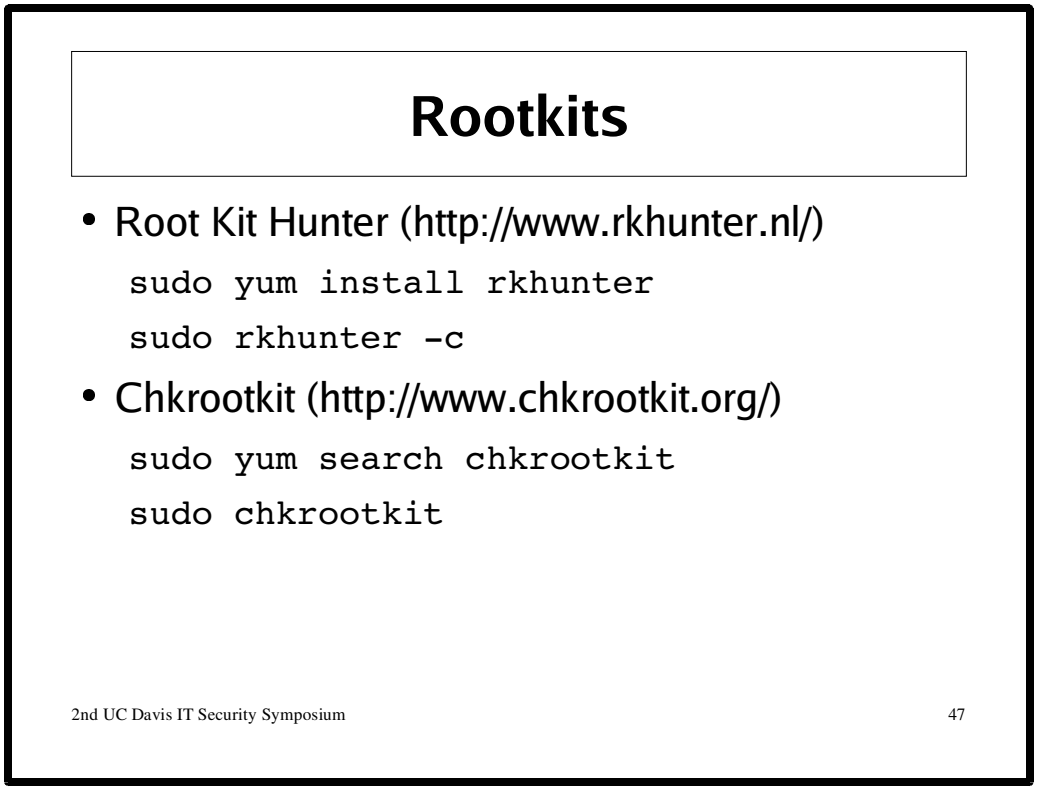
- Syslog
- Remote Log Server



To enable auditing during run-time, execute this command:

```
sudo auditctl -e 1
```

See:
http://people.redhat.com/sgrubb/audit/



Rootkits
df. To see if you are `0wn3d` you can run a rootkit checking utility like `rkhunter` or `chkrootkit`..

Note:
The chkrootkit-0.45-3 RPM for FC 4 seems to have a buglet, which prevents chkrootkit from process its commandline arguments. To fix this simply run this command:

```
sudo perl -pi -e 's:\./chkrootkit:\./chkrootkit \$*:g' \
     /usr/sbin/chkrootkit
```


Network Scanning

- hping

```
sudo yum install hping2
```

- nmap

```
sudo yum install nmap
sudo nmap -A -O -p0-65535 127.0.0.1
sudo yum install nmap-frontend
sudo nmapfe
```

2nd UC Davis IT Security Symposium 48

See:
http://www.hping.org/
http://wiki.hping.org/
http://www.insecure.org/nmap/

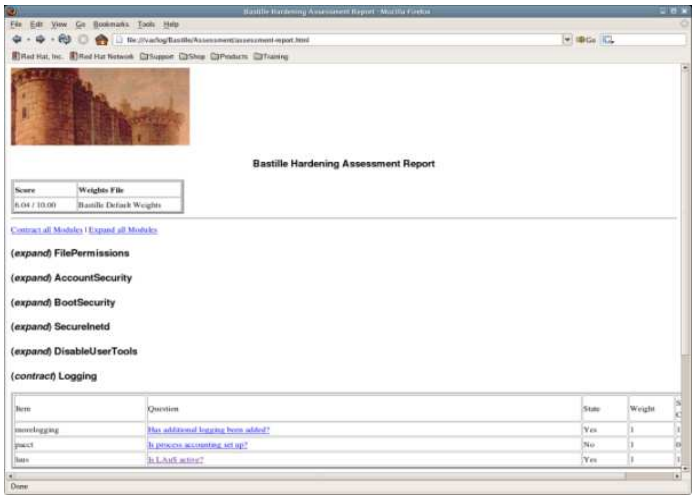
Nessus

- Installation

```
sudo yum install gtk+-devel \
                 sharutils flex bison
sudo sh nessus-installer-2.2.4.sh
```


See:
http://www.nessus.org

Bastille Assessment



2nd UC Davis IT Security Symposium 50

Install Bastille

There are no official FC4 RPMs for Bastille. Instead, the Bastille project provides RPMs for Fedora and RHEL, which depend on Dag Wieers' Apt/Yum RPM repository:

```
BASTILLE=http://unc.dl.sf.net/sourceforge/bastille-linux
sudo wget ${BASTILLE}/Bastille-3.0.4-1.0.noarch.rpm
sudo rpm -Uvh Bastille-3.0.4-1.0.noarch.rpm
```

Bad Idea! (Fudge to run Bastille for demonstration purpose only.)

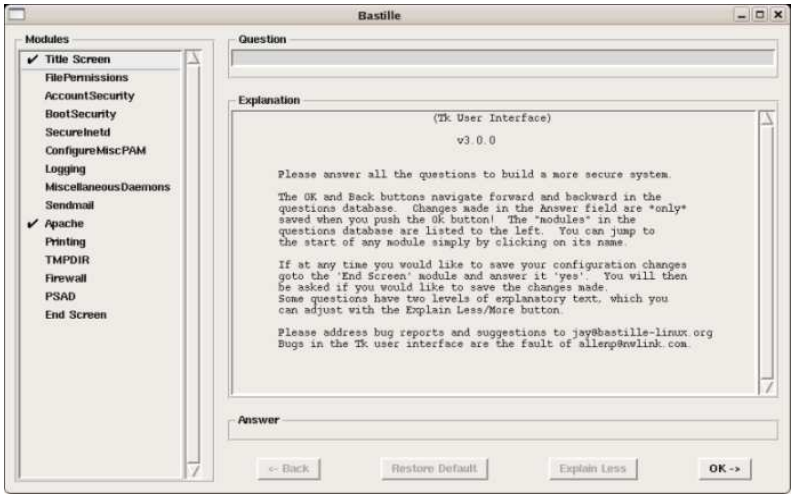
Since the Bastille version 3.0.4 has not been validated to work on FC4. A new version will be released that supports FC4, but until then we can 'fool' bastille into running by executing the following commands:

```
sudo perl -pi -e 's:,"RHFC3",:,"RHFC3","RHFC4",:g' \
            /usr/lib/Bastille/API.pm
sudo perl -pi -e 's:RHFC2 RHFC3:RHFC2 RHFC3 RHFC4:g' \
            /usr/lib/Bastille/IOLoader.pm
```

Generate Bastille Assessment Report

```
sudo bastille -a
```


Bastille Hardening



Run Bastille

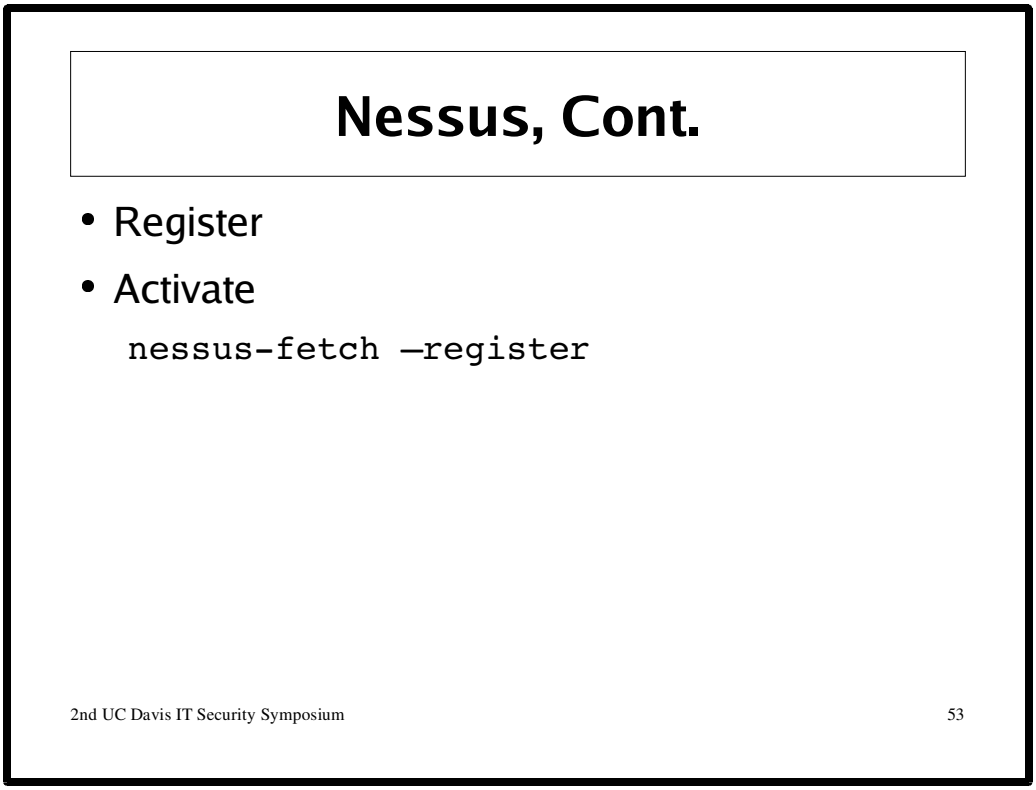
```
sudo /usr/sbin/bastille -x
```


Nessus, Cont.

- Configuration

```
sudo  /usr/local/sbin/nessus-mkcert
sudo /usr/local/sbin/nessus-adduser
```


http://www.nessus.org/demo/



The first time you start the Nessus daemon you should get a message like this:

"You are running a version of Nessus which is not configured to receive a full plugin feed. As a result, your security audits might produce incomplete results. To obtain a full plugin feed, you need to register your Nessus scanner at the following URL : http://www.nessus.org/register/"

Nessus, Cont.

- Updating Plugins

```
sudo nessus-update-plugins -v
```


Nessus, cont.

- Start nessus daemon

  sudo /usr/local/sbin/nessusd -D

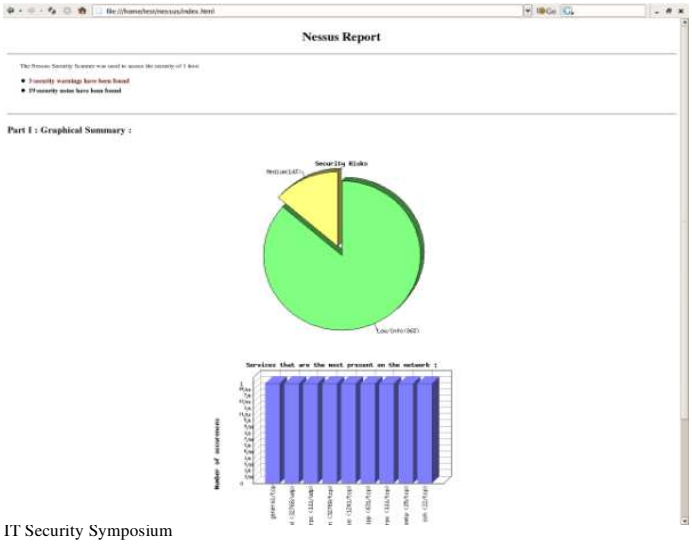
Nessus, Cont.

- Launch

```
sudo  /usr/local/sbin/nessus
```

- Login
- Set target
- Scan

Nessus Report



Intrusion Detection

- Tripwire

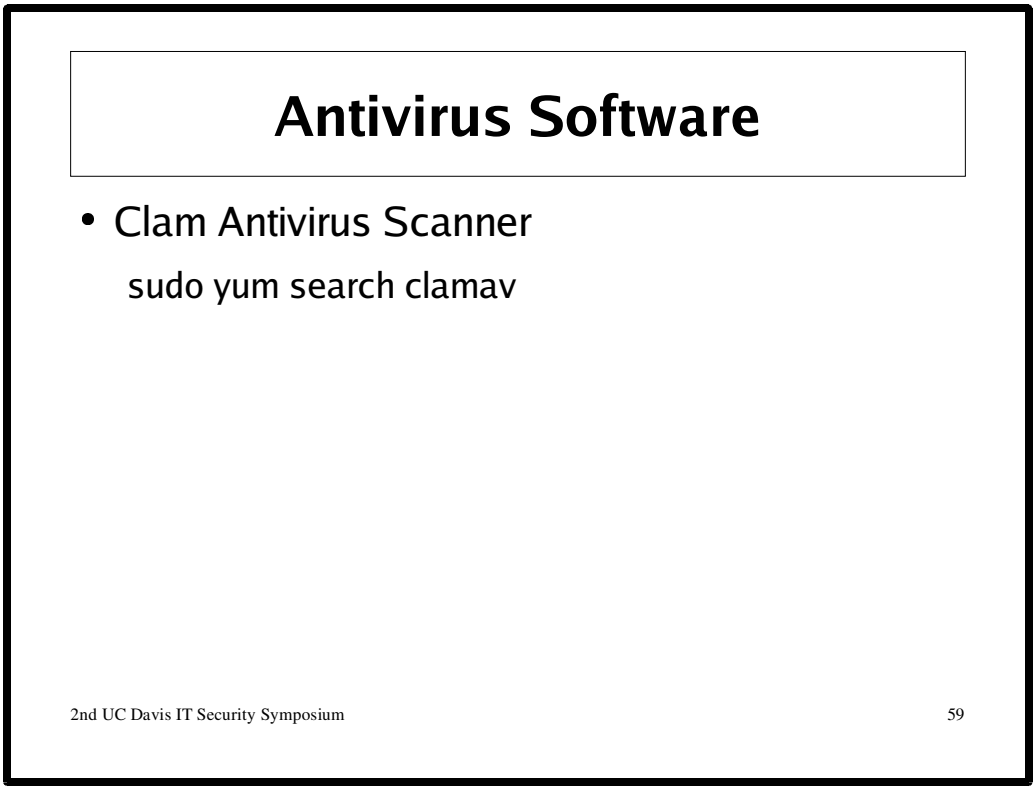
  sudo yum install tripwire

- Snort

  sudo /usr/sbin/snort -v

2nd UC Davis IT Security Symposium 58

http://www.snort.org/



"Clam AntiVirus is an anti-virus toolkit for UNIX. The main purpose of this software is the integration with mail servers (attachment scanning). The package provides a flexible and scalable multi-threaded daemon, a command line scanner, and a tool for automatic updating via Internet. The programs are based on a shared library distributed with the Clam AntiVirus package, which you can use with your own software. The virus database is based on the virus database from OpenAntiVirus, but contains additional signatures (including signatures for popular polymorphic viruses, too) and is KEPT UP TO DATE."
http://www.clamav.net/

Encrypted Filesystems

- cryptoloop
- cryptsetup

  sudo yum install cryptsetup-luks
- CFS

  sudo yum install cfs

For more information see:

http://www.linuxjournal.com/article/6381
http://www.crypto.com/software/
http://fedoranews.org/alex/tutorial/crypto/
http://luks.endorphin.org/
http://www.saout.de/misc/dm-crypt/

Virtualization

- Xen

  XenSE

See:
http://fedora.redhat.com/projects/virtualization/

Virtual Private Networks

- Vpnc

```
sudo yum install vpnc
```

- Openswan

```
sudo yum install openswan
```

62

vpnc
"IPSec VPN client compatible with Cisco equipment. A VPN client compatible with Cisco's EasyVPN equipment.

Supports IPSec (ESP) with Mode Configuration and Xauth. Supports only shared-secret IPSec authentication, 3DES, MD5, and IP tunneling."
http://www.unix-ag.uni-kl.de/~massar/vpnc/

Openswan
"Openswan is a free implementation of IPSEC & IKE for Linux. IPSEC is the Internet Protocol Security and uses strong cryptography to provide both authentication and encryption services. These services allow you to build secure tunnels through untrusted networks. Everything passing through the untrusted net is encrypted by the ipsec gateway machine and decrypted by the gateway at the other end of the tunnel. The resulting tunnel is a virtual private network or VPN."
http://www.openswan.org/

FC5 Future

- Better firewall configuration tool
- More Exec Shield features
- Encrypted Filesystems

See:
http://www.fedoraproject.org/wiki/FC5Future