Secure Linux Server Techniques for the New Linux Administrator

Curtis Rempel
President
Enigma Logic Inc.

Related Sessions

- 3061:
  - "Secure Your Linux Systems Before Deployment"
  - Today in room N136 at 4:00 PM
- 3921:
  - "Linux and the Six W's of Computer Forensics"
  - Today in room N138 at 4:00 PM
- 3313:
  - "Securing the Linux Environment"
  - Thursday in room N135 at 4:00 PM

Agenda

- Audience
- Purpose
- Focus
- Topics
- Top 10 Linux Security Tips
- Resources
- Summary
- Questions

Audience

- This is a *technical* session - basic Linux familiarity is assumed
- New Linux administrators (Windows background)
- Responsibility for one or more Linux servers
  - Co-existence with Windows servers
  - Migration to Linux
- If you have a few years Linux experience, this session is probably not for you

Purpose

- Provide a good foundation for quickly securing a Linux server
- Provide tips and resources for enhancing Linux security using advanced techniques
- Why?
  - Linux growth rate
  - Security is a hot topic: lawsuits, reputation
  - Lots of resources out there, how to make sense?

Focus

- Red Hat Enterprise Linux
- Predominant corporate Linux server distribution
- Built-in tools
- Add-on packages (free)

Topics

- New Linux administrator pitfalls
- Security philosophy
- Threats
- Current security hot spots
- Windows vs Linux security perceptions
- Linux viruses
- Basic Linux security
- Installation considerations
- Server Hardening Help
- Monitoring and Auditing
- Advanced topics

Non-topics

- Application specific security such as
  - Apache
  - BIND
  - FTP
- Topics related to external hardware
- Network intrusion detection
- Incident response and recovery

The New Linux Administrator Common Pitfalls

- Command line vs. GUI
- Not every tool has a GUI interface
- Not every server has X11 installed
- Open source software can be challenging when you're used to clicking on D:\SETUP.EXE
- Compiling from source
- RPM installation (dependencies?)
- Expect to endure some pain at first!

The New Linux Administrator Common Pitfalls

- Need to learn about Linux
- Make Google your best Linux friend
- Learn to use the Linux documentation resources (www.tldp.org)
- Patience, patience, patience

Security Philosophy

- Two components: Policy + Technical
- Majority is technical
- Without a policy, you're just fire fighting
- Start out with a basic policy
- www.faqs.org/rfcs/rfc2196.html
- Use technical details to augment and refine policy
- This presentation focuses on the technical component

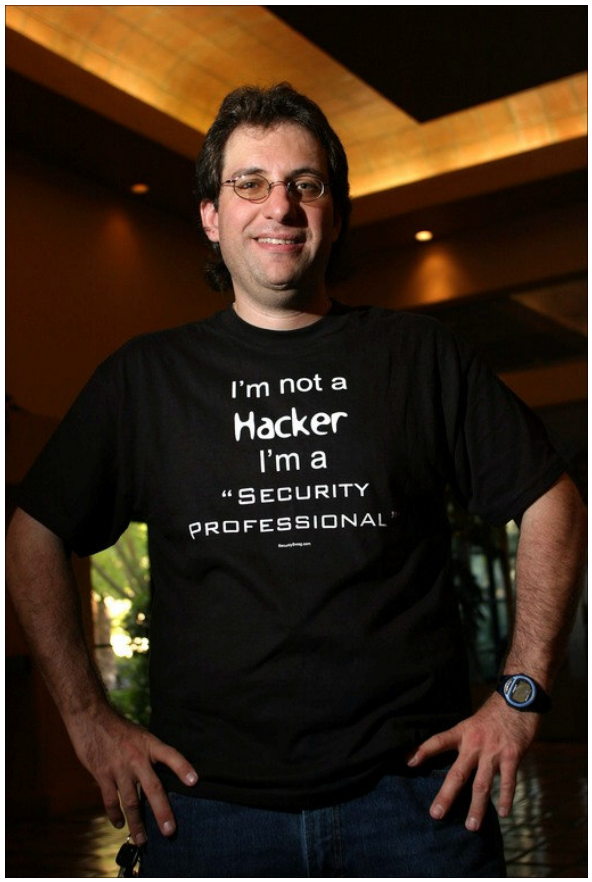
Threats: The Bad Guys

- Internal vs. external threats
- 5 years ago, computer crimes were 75% internal
  - Disgruntled employees
  - Corporate espionage
- 2 years ago, 50% split
- External threats on the rise!

Threats: The Bad Guys

Intrusion Method	Internal	External
Physical access	X	
Permissions	X	X
Sniffing	X	X
Misconfigured software	X	X
Software vulnerabilities	X	X
Social engineering	?	X

Kevin Mitnick Interview



- www.applefritter.com/node/view/3697
- Weakest links in security for most companies
- Social engineering and technical exploits

Current Security Hot Spots

- Wireless
  - Default passwords
  - No encryption and/or authentication
- Desktops
  - Viruses du jour
  - Passwords
  - Physical security
- Laptops and other mobile devices
- Servers
  - Internal
  - External (DMZ)

Server Security

- Windows
  - Monthly patch rollups
  - CERT: Internet Explorer: www.kb.cert.org/vuls/id/713878

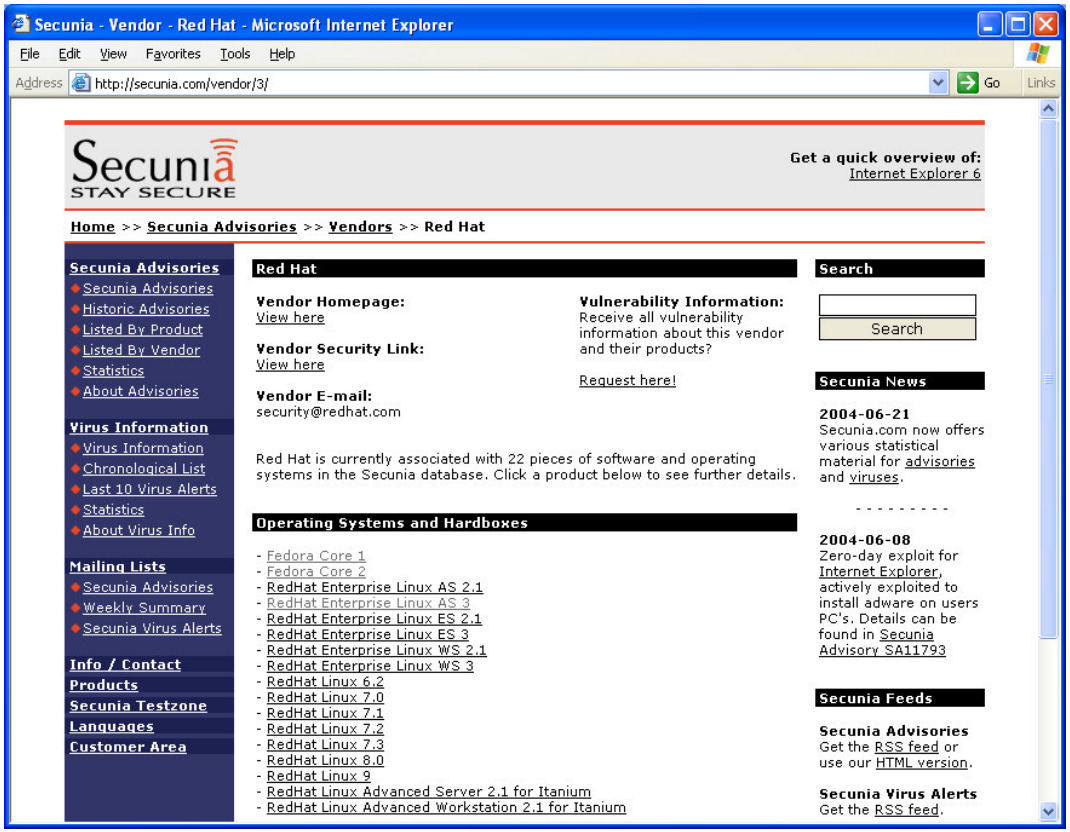
- Linux
  - The Penguin is “a good thing”
  - Source code availability
  - Massive peer review and audit trails
  - Patch development time
  - Major backing from the big guys: HP, IBM
  - Still, open source isn’t always secure
  - Don’t assume you’ve got all the bases covered!

Which is more secure?

- Is Linux more secure than Windows?
- How much time do you have to debate this?
- Linux is a kernel
- A distribution has the common kernel and a whole bunch of other “stuff”
- In order to reach your own conclusions, you need to know what security techniques are available for Linux
- Education is key

Secunia

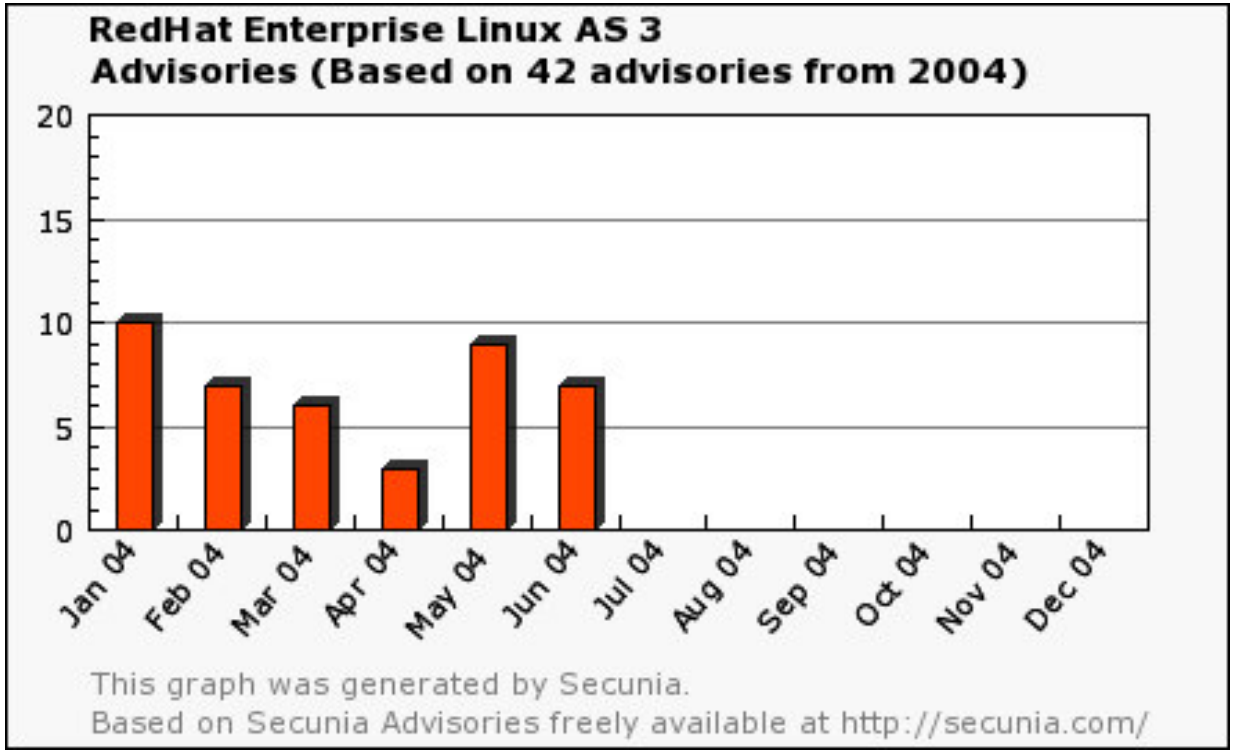
Vulnerabilities by vendor



Source: www.secunia.com

RedHat Enterprise Linux AS 3

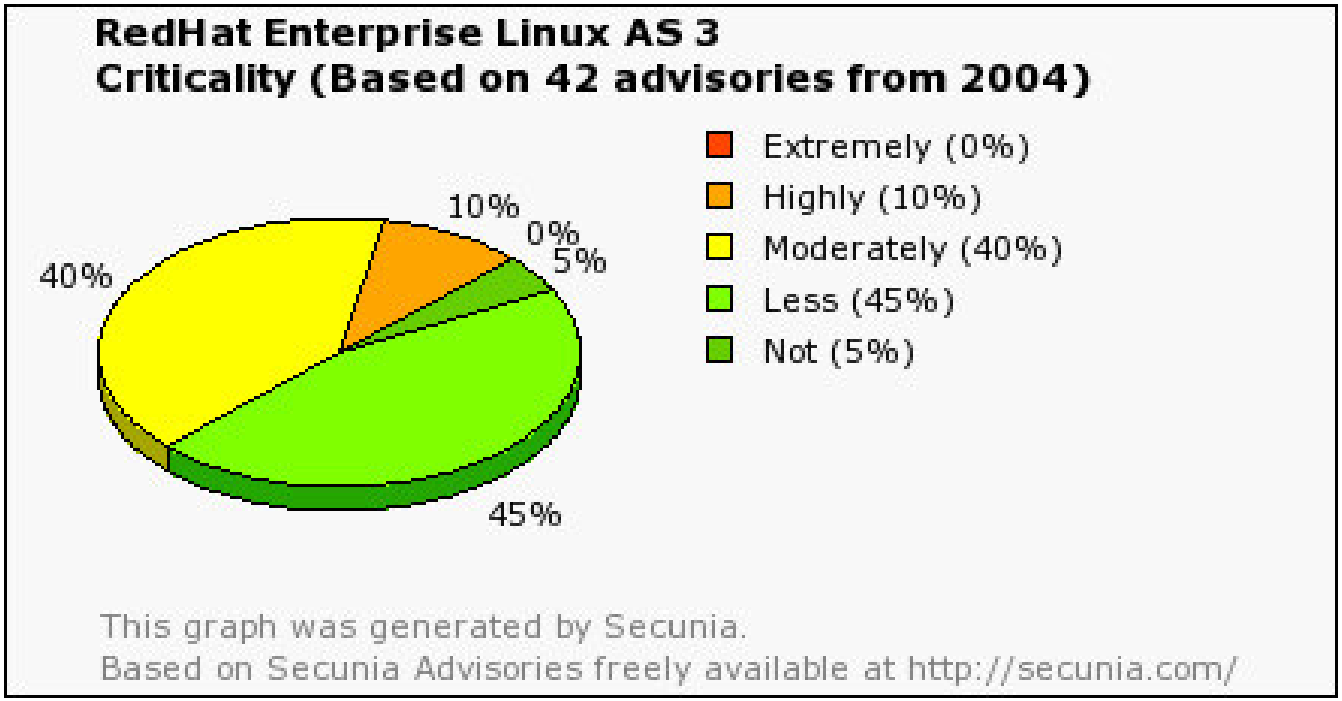
2004 Advisories



Source: www.secunia.com

RedHat Enterprise Linux AS 3

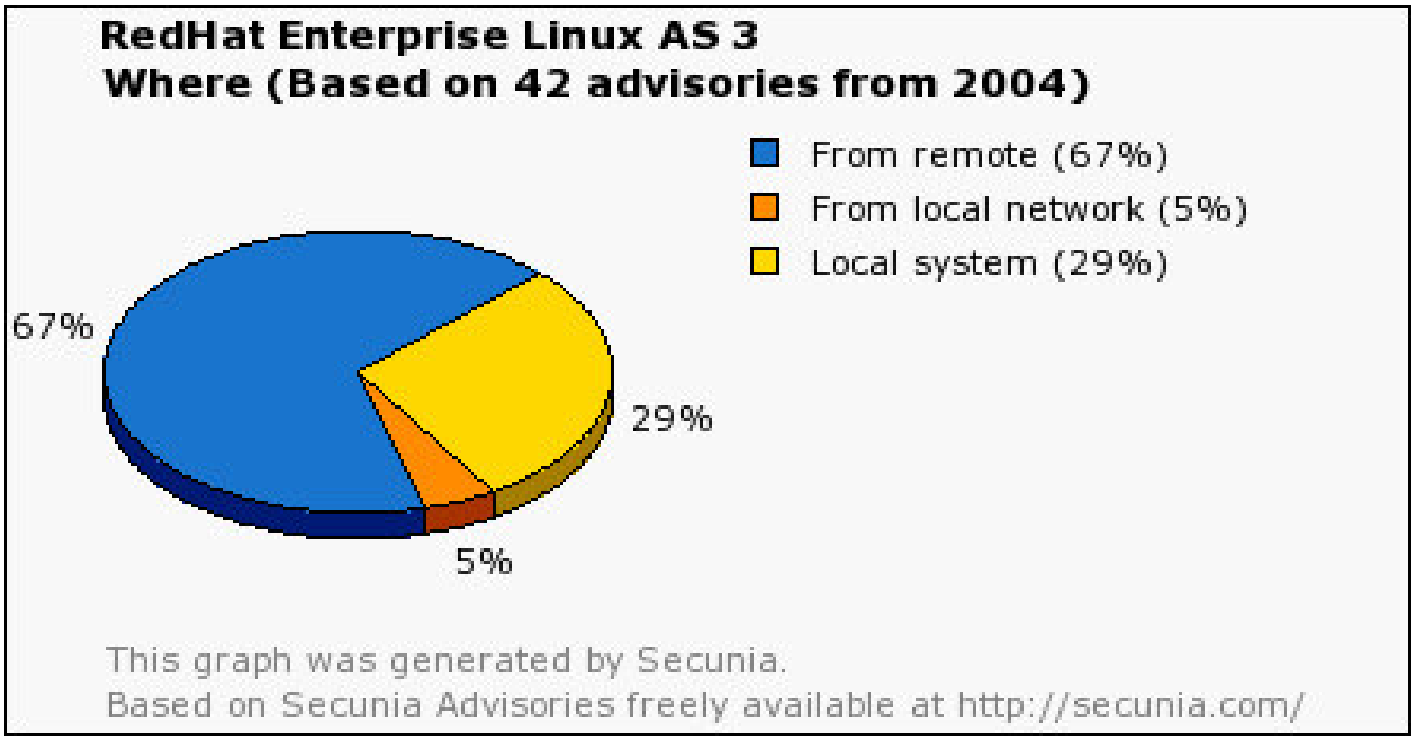
Criticality



Source: www.secunia.com

RedHat Enterprise Linux AS 3

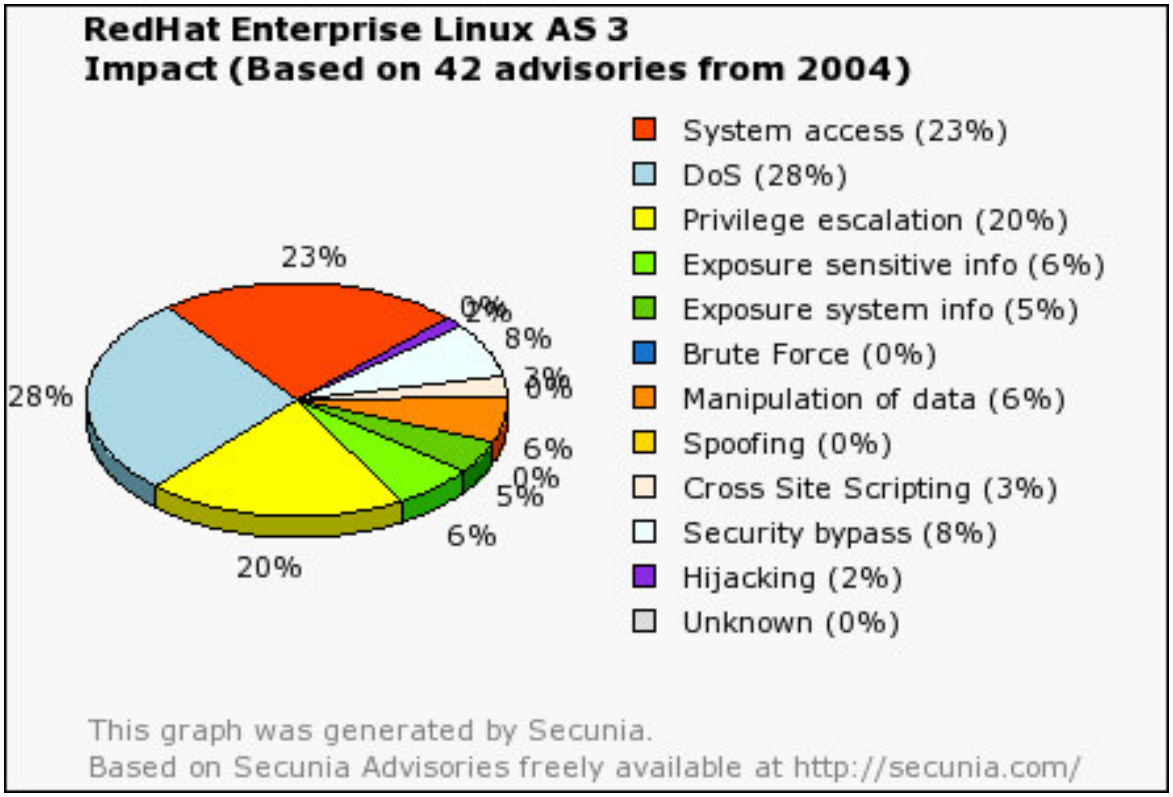
Where



Source: www.secunia.com

RedHat Enterprise Linux AS 3

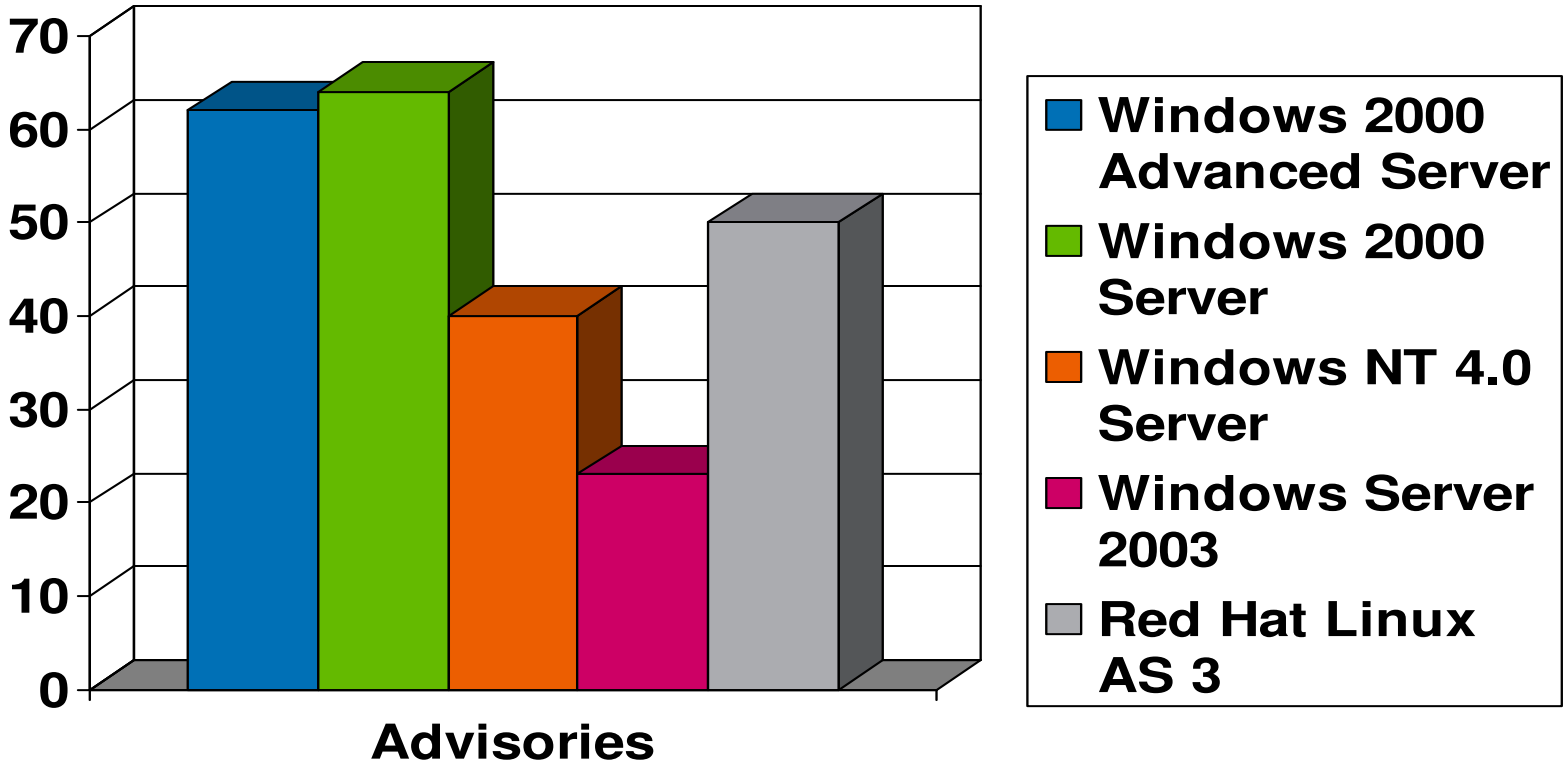
Impact



Source: www.secunia.com

Windows vs. Red Hat Enterprise Linux

2004 Advisories



Source: www.secunia.com

Viruses

- “Do viruses exist on Linux?” Sure!
- ELF Virus Writing HOWTO: virus.enemy.org/virus-writing-HOWTO/_html/index.html
- “Do I need Linux antivirus software?”
- No, but you may want to improve your system administration skills and best practices
- Why? You need root access
- Linux viruses are easy to write but you will only shoot your own foot, not somebody else's

The First Linux “Virus” – BLISS

- First sited January 31, 1997
- Attaches itself to **writable** binaries
- Log left in /tmp/.bliss
- Handy command line switch (that actually works): --bliss-uninfect-files-please
- “harmless” when run as a regular user
- “messy” when run as root!
- **Lesson: use root for system administration and nothing else!**

Linux “Viruses”

- Fundamental operating system architectural differences between Windows and Linux
- Windows has application functionality buried deep within the operating system (remember Microsoft arguing with DOJ about Internet Explorer?)
- Linux has a clear separation between kernel space and user space

Linux “Viruses”

- **If you never run untrusted executables as root, you can only harm whatever you have access to**
- “What if I’m evil and insert some code to be ultimately executed as root?”
- Package signing technology prevents you from doing this (GPG keys)
- But still, it really depends who you ask ...

"Contrary to popular misconception, Microsoft does not have the worst track record when it comes to security vulnerabilities … "

"... Also contrary to public wisdom, Unix and Linux-based systems are just as vulnerable to viruses, Trojans, and worms, ..."

Aberdeen

February, 2003

"The problem with answering this question is that those asking it know *only* OSes where viruses, trojan-horse programs, worms, nasty Javascripts, ActiveX controls with destructive payloads, and ordinary misbehaved"

"applications are a constant threat to their computing. Therefore, they *refuse to believe* Linux could be different, no matter what they hear."

Rick Moen

linuxmafia.com

"… because Linux users' sources for privileged executables enjoy paranoid-grade scrutiny (such that any unauthorised changes would be detected and remedied)."

Rick Moen

linuxmafia.com

Linux “Viruses”

- If this is really a non issue, why are the big antivirus companies selling Linux antivirus products?

"… Because gullible people have money, too, that's why."

Rick Moen

linuxmafia.com

"Linux.Svat is not dangerous and is very unlikely to spread. On most Linux systems the /usr/local/include is only writable by root; …"

"… therefore, an infected file would have to be run as root for the installation routine of the virus to work."

Symantec

http://securityresponse.symantec.com/avcenter/venc/data/linux.svat.html

"One of the problems is that as Linux moves on the corporate and consumer desktops the level of sophistication by the average user will go down significantly and then we will have millions and millions of people who will

install/uninstall Linux applications daily and many under the root account. These people will never look at source code and if they did it would be meaningless to them. They would not know if the code is good, bad or malicious, they will just install it and try it.

This is when Linux antivirus software will become very important, as important as it is today on Microsoft Windows computers.”

Keith Peer, CEO Central Command

www.desktoplinux.com June, 2004

Linux Virus Summary

- Write access to executables required
- Typical user has little to no executables anyway
- Propagation is difficult with no privileges
- Automatic execution does not exist
- Very little code is distributed in binary format only
- Software is typically signed and can be verified

Linux Virus Summary

- Caveat emptor: a simple Google search for “Linux antivirus” will show you dozens of companies willing to accept your money in exchange for software that you *may not need*.
- You can read more of Rick’s “rants” as he calls them at:
  linuxmafia.com/~rick/faq/index.php?page=virus

What about Windows Viruses on Linux?

- You bet!
- Samba file server
- Mail server
- Microsoft Office documents
- Dual boot considerations
- MBR backup:

```
dd if=/dev/hda of=mbr.img bs=512 count=1
```

- MBR restore:

```
dd if=mbr.img of=/dev/hda bs=512 count=1
```

Free Antivirus Scanning on Linux

- Clam Antivirus
- clamav.sourceforge.net
- Command line based
- Integration with mail servers
- Automatic updates

the number of developers who regard Linux as “the most innately secure operating system” leaped 19 percent over the past six months.

Evans Data Corp.

June, 2004

Linux Security Basics

- Users and Groups
- root Security
- Passwords
- Permissions

Linux Security Basics: Users and Groups

Users and Groups: Intro

- Red Hat: User Private Group Scheme

/etc/passwd:

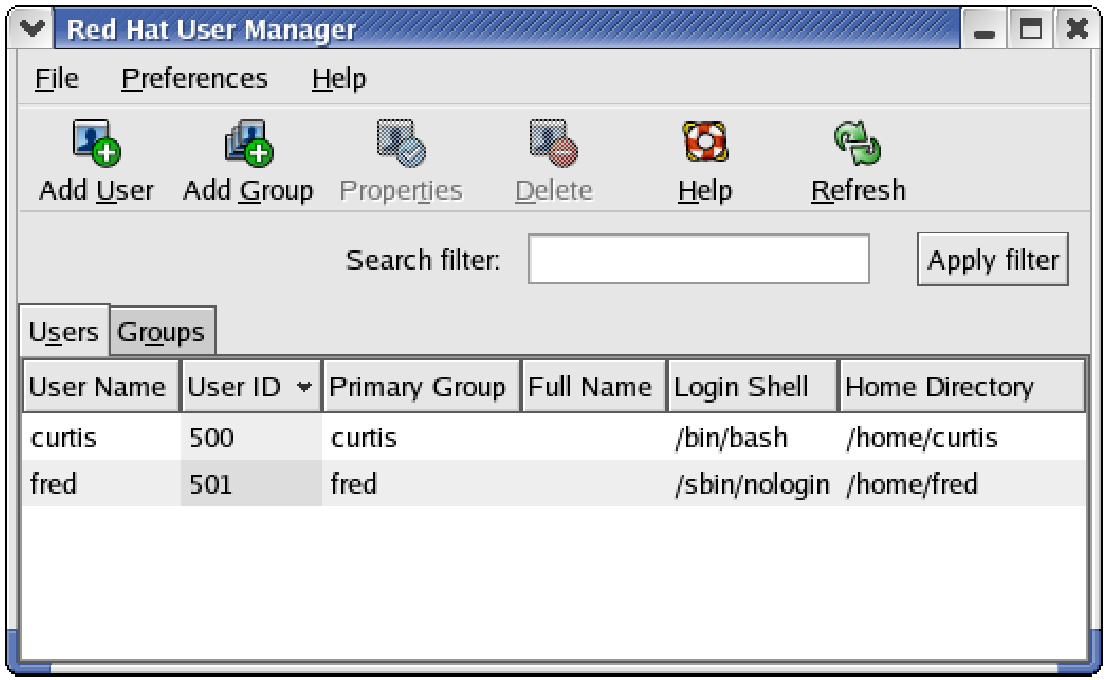
curtis:x:500:500::/home/curtis:/bin/bash

/etc/group

curtis:x:500:

Users and Groups: Tools

- useradd, userdel, usermod
- groupadd, groupdel, groupmod
- `redhat-config-users`



Adding Users

- Template files: /etc/skel
  - .bash_profile
  - .bashrc
  - .bash_logout
- Inadvertent new users from software installation
- Copy /etc/passwd prior to install and do ‘diff’ later

Deleting Users

- `userdel -r`
- Finding orphaned files:
  `find / -user fred -print`
  `find / -uid 500 -print`
- Change shell to /sbin/nologin (nologin.txt)
- “This account is currently not available”
- /bin/false allows network access! (as long as it is listed in /etc/shells)
- Check for cron jobs: `crontab -u fred -l`
- Check for at jobs: `atq`

Deleting Users

- Remove ~*user*/.ssh/authorized_keys*
- Check visudo for any privileges
- Processes: `ps aux | grep ^user`
- public_html
- .forward
- /etc/aliases

Users: /etc/passwd

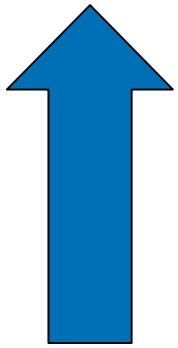
- Field 1: user
- Field 2: password
- Field 3: UID
- Field 4: GID
- Field 5: general info (name, comment)
- Field 6: home directory
- Field 7: login shell

curtis:x:500:500::/home/curtis:/bin/bash

Users: /etc/shadow

- Contains encrypted password plus password aging information

```
curtis:$1$J2rCr12d$KmHTzH0AwL9HE7gUZLGQZ/:125
 96:0:99999:7:::
```



Encrypted password

Groups: /etc/group

- Group membership information
- Unique GID per group
- Field 1: group name
- Field 2: group password
- Field 3: GID
- Field 4: group members

admins:x:650:curtis,mark,tom

Linux Security Basics: root Security

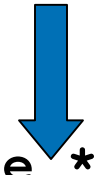
root Level Security

- Caution: be careful with fat finger syndrome
- Use root only as necessary
- Typos: `rm file*` vs `rm file *`
- “Are you sure?” - alias your commands:
  `alias rm=‘rm –i’`

root Level Security

```
[root@sandbox root]# ls
file1  file2  file3  report
[root@sandbox root]# rm file*
[root@sandbox root]# ls
report
```

Now again with fat fingers:



Hit the space bar!

```
[root@sandbox root]# ls
file1  file2  file3  report
[root@sandbox root]# rm file *
rm: cannot lstat `file': No such file or directory
[root@sandbox root]# ls
[root@sandbox root]#
```

Woops!

root Level Security

- /etc/securetty: where root can log in from
- **Do not remove/rename this file to allow root logins via telnet!!**
- No . or empty directory in PATH:
  PATH=.:/bin:/sbin:/usr/bin:/usr/sbin
  PATH=:/bin:/sbin:/usr/bin:/usr/sbin

su Trojan

```
#!/bin/sh
echo -n "Password: "
stty -echo
read password
echo
echo $password  >  /tmp/.rootpw 2>/dev/null
stty echo
echo "su: incorrect password"
rm su
```

root Level Security

- root has UID 0
- **Any user with UID 0 is equivalent to root!**
- Check /etc/passwd for UID 0 accounts:

```
[root@sandbox root]# awk -F: '$3==0 { print }' /etc/passwd
root:x:0:0:root:/root:/bin/bash
r00t:x:0:0:root:/root:/bin/bash
```

root Level Security

```
login: r00t
Password:
Last login: Mon Jun 28 13:49:44 from localhost.localdomain
[root@sandbox r00t]# whoami
root
[root@sandbox r00t]# id
uid=0(root) gid=0(root) groups=0(root)
[root@sandbox r00t]#
```

The root Caveat

- A large number of problems on Linux systems are caused by misuse of the root account by inexperienced system administrators
- **If you're not doing system administration, don't use the root account - period**
- Education + caution + experience = ounce of prevention

sudo

- “How not to give out the root password”
- /etc/sudoers
- Selective access to users and commands
- visudo
- sudo command
- User enters their own password
- Granted a “ticket” for 5 minutes
- Everything is logged

/etc/sudoers

```
# Host alias specification

# User alias specification

User_Alias ADMINS=curtis

# Cmnd alias specification

Cmnd_Alias FDISK=/sbin/fdisk


# User privilege specification

root    ALL=(ALL) ALL

ADMINS ALL=(ALL) FDISK
```

sudo example

```
[curtis@sandbox curtis]$ fdisk /dev/hdb
bash: fdisk: command not found
[curtis@sandbox curtis]$ /sbin/fdisk /dev/hdb

Unable to open /dev/hdb
[curtis@sandbox curtis]$ sudo /sbin/fdisk /dev/hdb
Password:

Command (m for help): p

Disk /dev/hdb: 4311 MB, 4311982080 bytes
255 heads, 63 sectors/track, 524 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot    Start       End    Blocks   Id  System

Command (m for help): q

[curtis@sandbox curtis]$ /sbin/fdisk /dev/hdb

Unable to open /dev/hdb
```

Not in PATH

No privilege

Prompt for user's own password

Success!

No privilege

sudo example

```
[curtis@sandbox curtis]$ sudo /sbin/fdisk /dev/hdb

Command (m for help): q

[curtis@sandbox curtis]$ date
Thu Jul  1 11:04:26 MDT 2004
[curtis@sandbox curtis]$ sudo /sbin/init 6
Sorry, user curtis is not allowed to execute '/sbin/init 6'
  as root on sandbox.lan.
[curtis@sandbox curtis]$ date
Thu Jul  1 11:05:22 MDT 2004
[curtis@sandbox curtis]$ date
Thu Jul  1 11:12:53 MDT 2004
[curtis@sandbox curtis]$ sudo /sbin/fdisk /dev/hdb
Password:
```

Ticket has expired, password required

```
Command (m for help): q

[curtis@sandbox curtis]$
```

sudo example

- Everything is logged:

```
Jul  1 11:03:58 sandbox sudo:   curtis : TTY=pts/1 ;
 PWD=/home/curtis ; USER=root ; COMMAND=/sbin/fdisk /dev/hdb
Jul  1 11:04:19 sandbox sudo:   curtis : TTY=pts/1 ;
 PWD=/home/curtis ; USER=root ; COMMAND=/sbin/fdisk /dev/hdb
Jul  1 11:05:11 sandbox sudo:   curtis : command not allowed ;
 TTY=pts/1 ; PWD=/home/curtis ; USER=root ; COMMAND=/sbin/init 6
Jul  1 11:13:07 sandbox sudo:   curtis : TTY=pts/1 ;
 PWD=/home/curtis ; USER=root ; COMMAND=/sbin/fdisk /dev/hdb
```

sudo

- Don’t be lazy!

joe ALL=(ALL) ALL

Linux Security Basics: Passwords

Passwords

- Aging: `chage`, `redhat-config-users`
- `chage -m 7 -M 90 -W 28 user`
- -m = minimum days before can change password
- -M = maximum days a password can be kept
- -W = number of days warned before expiry
- /etc/login.defs
- Check for blank passwords:
  `awk -F: '$2==""' { print $1 }' /etc/shadow`
- If you're not using crack, you should be (!)

Crack

- ftp.cerias.purdue.edu/pub/tools/unix/pwdutils/crack
- Dictionary attack
- Encrypts words and compares to encrypted passwords
- Generate report
- Email users with weak passwords

Forgot the root password

- No problem (if you have physical access)
- Boot to single user mode:
  - Press ‘e’ to edit the GRUB boot menu item
  - Press down arrow to the “kernel” line
  - Press ‘e’ to append
  - Press spacebar, ‘1’, and Enter.
  - Press ‘b’ to boot
  - At the “#” prompt, type ‘passwd’
  - At the “#” prompt, type ‘init 5’
  - You’re done!
- Boot CD 1 and type `linux rescue` at the boot: prompt.

Physical Access

- All bets are off!
- Root access in a matter of minutes
- Tom's Root Boot floppy: www.toms.net/rb
- GRUB boot loader password
- Disable boot media in BIOS
- BIOS password
- Locked case
- Keystroke catcher:

GRUB Password

```
[root@sandbox root]# grub-md5-crypt
Password:
Retype password:
$1$iTcKR0$B4fQUasB04eRE6GzNaRYD.
```

Add to /etc/grub.conf:

```
password --md5 $1$iTcKR0$B4fQUasB04eRE6GzNaRYD.
```

Linux Security Basics: Permissions

Permissions

- Files have one owner and one group
- Change owner: chown
- Change group: chgrp
- Permission levels:
  - Owner (user)
  - Group
  - Other

Permission Types

- Read (r)
  - See contents of file
  - List directory
- Write (w)
  - Change existing files
  - Create new and remove existing files
- Execute (x)
  - Execute binary/shell script
  - Get into directory

Setting Permissions

- The “mode”
- chmod command
- `chmod g+rw file`
- `chmod o=r file`
- `chmod 755 file`
- World writable files:

```
find / -perm -2 ! -type l -ls
```

umask

- Default file protection
- Display: `umask`
- Set: `umask` *`value`*
- Directories: subtract from 777
- Files: subtract from 666
- **Cannot create new files with execute permission**

umask

```
[curtis@sandbox curtis]$ umask
0002
[curtis@sandbox curtis]$ touch myfile
[curtis@sandbox curtis]$ ls -l myfile
-rw-rw-r--    1 curtis   curtis          0 Jun 28 14:23 myfile
[curtis@sandbox curtis]$ mkdir mydir
[curtis@sandbox curtis]$ ls -ld mydir
drwxrwxr-x    2 curtis   curtis       1024 Jun 28 14:23 mydir
```

With a umask of 0002:

new files will have permission 666-002=664
664 = rw-rw-r--

new directories will have permission 777-002=775
775 = rwxrwxr-x

ACLs

```
[root@sandbox root]# cd /test
[root@sandbox test]# touch myfile
[root@sandbox test]# setfacl -m u:curtis:rwx myfile
setfacl: myfile: Operation not supported
[root@sandbox test]# cd
[root@sandbox root]# umount /test
[root@sandbox root]# mount /dev/hdb1 /test -o acl
[root@sandbox root]# cd /test
[root@sandbox test]# setfacl -m u:curtis:rwx myfile
[root@sandbox test]# getfacl myfile
# file: myfile
# owner: root
# group: root
user::rwx
user:curtis:rwx
group::r--
mask::rwx
other::---

[root@sandbox test]# echo "secret stuff in here" > myfile
[root@sandbox test]# ls -l
total 14
drwx------    2 root     root        12288 Jul  1 12:06 lost+found
-rw-r--r--+   1 root     root           21 Jul  1 12:08 myfile
[root@sandbox test]# chmod 700 myfile
[root@sandbox test]# ls -l
total 14
drwx------    2 root     root        12288 Jul  1 12:06 lost+found
-rwx------+   1 root     root           21 Jul  1 12:08 myfile
```

Filesystem not mounted with ACL support

Grant full access to curtis

ACL indicator

No access for everybody else

ACLs

```
[curtis@sandbox curtis]$ cat /test/myfile
secret stuff in here
[curtis@sandbox curtis]$ ls -l /test
total 14
drwx------    2 root     root        12288 Jul  1 12:06 lost+found
-rwxr-x---+   1 root     root           21 Jul  1 12:08 myfile
[curtis@sandbox curtis]$
```

SUID

- Program executes as the owner for the duration of the program
- Typically the owner is root
- The kernel will not honor SUID shell scripts!
- Changing your password: /usr/bin/passwd

```
[curtis@sandbox curtis]$ ls -l /usr/bin/passwd
-r-s--x--x    1 root     root        16336 Feb 13  2003 /usr/bin/passwd

[curtis@sandbox curtis]$ ls -l /etc/passwd
-rw-r--r--    1 root     root         2204 Jun 28 13:48 /etc/passwd

[curtis@sandbox curtis]$ ls -l /etc/shadow
-rw-------    1 root     root         1487 Jun 28 13:49 /etc/shadow
```

SUID

```
[root@sandbox root]# find / -perm -4000 -exec ls -ld {} \;
-rws--x--x    1 root     root      1948123 Oct  3  2003 /usr/X11R6/bin/XFree86
-rwsr-xr-x    1 root     root        13190 Sep 25  2003 /usr/sbin/usernetctl
-rws--x--x    1 root     root        26744 Sep 25  2003 /usr/sbin/userhelper
-rwsr-xr-x    1 root     root         7796 Aug 11  2003 /usr/sbin/userisdnctl
-r-sr-sr-x    1 uucp     uucp      2313614 Jan 25  2003 /usr/sbin/uucico
-r-sr-sr-x    1 uucp     uucp      1395163 Jan 25  2003 /usr/sbin/uuxqt
-r-s--x---    1 root     apache      20393 Sep 25  2003 /usr/sbin/suexec
-rwsr-x---    1 root     disk        63679 Jul 17  2003 /usr/sbin/amcheck
-rwsr-xr-x    1 root     root        35340 Jun  4  2003 /usr/bin/chage
-rwsr-xr-x    1 root     root        36156 Jun  4  2003 /usr/bin/gpasswd
-rws--x--x    1 root     root        14140 Sep 25  2003 /usr/bin/chfn
-rws--x--x    1 root     root        11676 Sep 25  2003 /usr/bin/chsh
-rws--x--x    1 root     root         4800 Sep 25  2003 /usr/bin/newgrp
-r-s--x--x    1 root     root        16336 Feb 13  2003 /usr/bin/passwd
-rwsr-xr-x    1 root     root        15388 Jun 27  2003 /usr/bin/rcp
-rwsr-xr-x    1 root     root        11136 Jun 27  2003 /usr/bin/rlogin
-rwsr-xr-x    1 root     root         7836 Jun 27  2003 /usr/bin/rsh
-rwsr-xr-x    1 root     root        36904 Sep 12  2003 /usr/bin/at
---s--x--x    1 root     root        85432 May 19  2003 /usr/bin/sudo
-rwsr-xr-x    1 root     root       110114 Feb 19  2003 /usr/bin/crontab
```

[...]

SGID

- Files created in a directory with SGID retain group ownership from directory itself

```
[root@sandbox root]# groupadd sales
[root@sandbox root]# useradd -G sales joe
[root@sandbox root]# useradd -G sales dave
[root@sandbox root]# mkdir /sales
[root@sandbox root]# ls -ld /sales
drwxrwxr-x    2 root     sales        1024 Jun 28 14:16
 /sales
[root@sandbox root]# chmod g+s /sales
[root@sandbox root]# ls -ld /sales
drwxrwsr-x    2 root     sales        1024 Jun 28 14:16
 /sales
```

Sticky Bit

- Only the owner can delete files in the directory
- /tmp

```
[root@sandbox root]# ls -ld /tmp
drwxrwxrwt   11 root     root          4096 Jun 28 14:10 /tmp
```

Installation Considerations

Installation Considerations

- Boxed set or downloaded ISOs (md5sum)
- Pull the network cable
- Partitioning
- Install minimal set of packages
- Apply patches
- Remove unnecessary packages
- Disable unnecessary services
- Secure required services

Installation Considerations

- Secure filesystems
- Logging
- Banners
- Establish baselines
- Reboot
- Plug in network cable

Partitioning

- Minimal: / and swap (sometimes /boot as well)
- Divide key directories across partitions
- Prevent:
  - Accidental/malicious writes
  - Unauthorized execution
  - Free space denial of service
- Filesystem Hierarchy Standard (FHS): www.pathname.com/fhs
- Typical server partitions: /, /usr, /var, /tmp, /home
- Further subdivision: /var/spool/mail, /var/www, /var/ftp

Partitioning

Mount point	Size	Purpose
/	300 MB	Root files
/usr	6000 MB	Binaries
/var	Depends 500 MB	Logs, mail, printing, web, ftp
/tmp	Depends 500 MB	Scratch
/home	Remainder or separate disk	User files

Apply Patches

- Keeping up to date foils the “script kiddies”
- Red Hat Network : up2date
- www.redhat.com/security
- www.redhat.com/mailing-lists
- Auto update: two schools of thought
  - Yes: from vendor
  - No: elsewhere
- Cautious production environment: don’t apply all patches, just the security related patches
- www.autorpm.org

Remove Unnecessary Packages

- Add/Remove: `redhat-config-packages`
- List all packages: `rpm -qa | sort`
- Query a package description: `rpm -qi` *`package`*
- Query a file for package: `rpm -qf` *`file`*
- Query a package files: `rpm -ql` *`package`*
- Most recently installed: `rpm -qa --last | less`
- Remove a package: `rpm -e` *`package`*

Disable Unnecessary Services

- Standalone services
- xinetd services
- NFS: portmap, rpc.mountd, rpc.nfsd
- Samba: smbd, nmbd
- Printing: cupsd, lpd
- DNS: named
- finger

Disable Unnecessary Services

- Enumerate:
  - Process listing: `ps ax`
  - Live network services: `netstat -nlp --inet`
  - Service startup: `chkconfig --list`
- Disable service startup:
  `chkconfig service off`
- Disable service immediately:
  `service service stop`
- Use port scanner to verify
- Rinse (reboot) and repeat

Processes

```
[root@sandbox root]# ps ax
PID TTY      STAT   TIME COMMAND
    1 ?        S      0:04 init
    2 ?        SW     0:00 [keventd]
    3 ?        SW     0:00 [kapmd]
    4 ?        SWN    0:00 [ksoftirqd/0]
    7 ?        SW     0:00 [bdflush]
    5 ?        SW     0:00 [kswapd]
    6 ?        SW     0:00 [kscand]
    8 ?        SW     0:00 [kupdated]
    9 ?        SW     0:00 [mdrecoveryd]
   13 ?        SW     0:00 [kjournald]
   69 ?        SW     0:00 [khubd]
  177 ?        SW     0:00 [kjournald]
  178 ?        SW     0:00 [kjournald]
  179 ?        SW     0:00 [kjournald]
  180 ?        SW     0:00 [kjournald]
  181 ?        SW     0:00 [kjournald]
  524 ?        S      0:00 /sbin/dhclient -1 -q -lf /var/lib/dhcp/dhclient-
 eth0.
  563 ?        S      0:00 syslogd -m 0
  567 ?        S      0:00 klogd -x
  593 ?        S      0:00 portmap
  612 ?        S      0:00 rpc.statd
  680 ?        S      0:00 /usr/sbin/apmd -p 10 -w 5 -W -P /etc/sysconfig/apm-
 sc
```

Processes

```
 719 ?        S      0:00 cupsd
 773 ?        S      0:00 /usr/sbin/sshd
 787 ?        S      0:00 xinetd -stayalive -pidfile
/var/run/xinetd.pid
 813 ?        S      0:00 sendmail: accepting connections
 822 ?        S      0:00 sendmail: Queue runner@01:00:00 for
/var/spool/client
 832 ?        S      0:00 gpm -t imps2 -m /dev/mouse
 842 ?        S      0:00 /usr/sbin/cannaserver -syslog -u bin
 853 ?        S      0:00 crond
 864 ?        S      0:00 /usr/bin/jserver
1055 ?        S      0:00 xfs -droppriv -daemon
1064 ?        S      0:00 /usr/sbin/atd
1089 tty1     S      0:00 /sbin/mingetty tty1
1090 tty2     S      0:00 /sbin/mingetty tty2
1091 tty3     S      0:00 /sbin/mingetty tty3
1092 tty4     S      0:00 /sbin/mingetty tty4
1093 tty5     S      0:00 /sbin/mingetty tty5
1094 tty6     S      0:00 /sbin/mingetty tty6
1095 ?        S      0:00 /usr/bin/gdm-binary -nodaemon
1148 ?        S      0:00 /usr/bin/gdm-binary -nodaemon
1149 ?        S      0:07 /usr/X11R6/bin/X :0 -auth
/var/gdm/:0.Xauth vt7
```

Processes

```
13302 ?        S      0:18 /usr/bin/gnome-session
13357 ?        S      0:00 /usr/bin/ssh-agent /etc/X11/xinit/Xclients
13361 ?        S      0:01 /usr/libexec/gconfd-2 5
13364 ?        S      0:00 /usr/libexec/bonobo-activation-server --ac-activate
  -
13366 ?        S      0:01 gnome-settings-daemon --oaf-activate-
  iid=OAFIID:GNOME
13371 ?        S      0:00 fam
13376 ?        S      0:00 xscreensaver -nosplash
13379 ?        S      0:02 /usr/bin/metacity --sm-client-id=default1
13383 ?        S      0:02 gnome-panel --sm-client-id default2
13385 ?        S      0:03 nautilus --no-default-window --sm-client-id
  default3
13387 ?        S      0:00 magicdev --sm-client-id default4
13389 ?        S      0:00 eggcups --sm-client-id default6
13391 ?        S      0:00 pam-panel-icon --sm-client-id default0
13393 ?        SN     0:01 /usr/bin/python /usr/bin/rhn-applet-gui --sm-
  client-i
13394 ?        S      0:00 /sbin/pam_timestamp_check -d root
13399 ?        S      0:00 /usr/libexec/notification-area-applet --oaf-
  activate-
13442 ?        S      0:03 /usr/bin/gnome-terminal
13443 ?        S      0:00 gnome-pty-helper
13444 pts/0    S      0:00 bash
13478 pts/0    S      0:00 su -
13481 pts/0    S      0:00 -bash
13542 pts/0    R      0:00 ps ax
```

netstat -nlp --inet

```
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:704             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:2049            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:32770           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:32771         0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:32772           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:901             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:722             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:3551            0.0.0.0:*               LISTEN
```

netstat -nlp --inet

```
udp        0      0 0.0.0.0:32768           0.0.0.0:*
udp        0      0 0.0.0.0:2049            0.0.0.0:*
udp        0      0 0.0.0.0:32770           0.0.0.0:*
udp        0      0 192.168.0.101:137       0.0.0.0:*
udp        0      0 0.0.0.0:137             0.0.0.0:*
udp        0      0 192.168.0.101:138       0.0.0.0:*
udp        0      0 0.0.0.0:138             0.0.0.0:*
udp        0      0 0.0.0.0:909             0.0.0.0:*
udp        0      0 127.0.0.1:33425         0.0.0.0:*
udp        0      0 0.0.0.0:701             0.0.0.0:*
udp        0      0 0.0.0.0:719             0.0.0.0:*
udp        0      0 0.0.0.0:111             0.0.0.0:*
udp        0      0 0.0.0.0:631             0.0.0.0:*
udp        0      0 192.168.0.101:123       0.0.0.0:*
udp        0      0 127.0.0.1:123           0.0.0.0:*
udp        0      0 0.0.0.0:123             0.0.0.0:*
```

netstat -luntp

```
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:32768           0.0.0.0:*               LISTEN      612/rpc.statd
tcp        0      0 127.0.0.1:32769         0.0.0.0:*               LISTEN      787/xinetd
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      593/portmap
tcp        0      0 0.0.0.0:6000            0.0.0.0:*               LISTEN      1149/X
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      773/sshd
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      719/cupsd
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      813/sendmail: accep
udp        0      0 0.0.0.0:32768           0.0.0.0:*                           612/rpc.statd
udp        0      0 0.0.0.0:788             0.0.0.0:*                           612/rpc.statd
udp        0      0 0.0.0.0:68              0.0.0.0:*                           524/dhclient
udp        0      0 0.0.0.0:111             0.0.0.0:*                           593/portmap
udp        0      0 0.0.0.0:631             0.0.0.0:*                           719/cupsd
```

netstat -lutp

```
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 *:32768                 *:*                     LISTEN      612/rpc.statd
tcp        0      0 localhost.localdo:32769 *:*                     LISTEN      787/xinetd
tcp        0      0 *:sunrpc                *:*                     LISTEN      593/portmap
tcp        0      0 *:x11                   *:*                     LISTEN      1149/X
tcp        0      0 *:ssh                   *:*                     LISTEN      773/sshd
tcp        0      0 localhost.localdoma:ipp *:*                     LISTEN      719/cupsd
tcp        0      0 localhost.localdom:smtp *:*                     LISTEN      813/sendmail: accep
udp        0      0 *:32768                 *:*                                 612/rpc.statd
udp        0      0 *:788                   *:*                                 612/rpc.statd
udp        0      0 *:bootpc                *:*                                 524/dhclient
udp        0      0 *:sunrpc                *:*                                 593/portmap
udp        0      0 *:ipp                   *:*                                 719/cupsd
```

Service Startup

```
[root@sandbox root]# chkconfig --list
microcode_ctl     0:off   1:off   2:on    3:on    4:on    5:on    6:off
gpm               0:off   1:off   2:on    3:on    4:on    5:on    6:off
kudzu             0:off   1:off   2:off   3:on    4:on    5:on    6:off
syslog            0:off   1:off   2:on    3:on    4:on    5:on    6:off
netfs             0:off   1:off   2:off   3:on    4:on    5:on    6:off
network           0:off   1:off   2:on    3:on    4:on    5:on    6:off
random            0:off   1:off   2:on    3:on    4:on    5:on    6:off
rawdevices        0:off   1:off   2:off   3:on    4:on    5:on    6:off
saslauthd         0:off   1:off   2:off   3:off   4:off   5:off   6:off

[…]

xinetd based services:
  krb5-telnet:    off
  rsync: off
  eklogin:        off
  gssftp:         off

[…]
```

Service Startup

- Check default run level:
  `awk -F: '/^id:/ { print $2 }' /etc/inittab`
- Check previous/current run level:
  `runlevel`
- List services activated for default run level:

```
chkconfig --list | \
awk 'NR==1,/^xinetd based/ {
        if ($1 != "xinetd" && $7 == "5:on")
            print $1}' | \
sort | nl
```

Service Startup

```
[root@sandbox root]# chkconfig --list | awk 'NR==1,/^xinetd based/ {if ($1 != "xinetd" &&
  $7 == "5:on") print $1}' | sort | nl
     1  apmd
     2  arptables_jf
     3  atd
     4  autofs
     5  canna
     6  crond
     7  cups
     8  firstboot
     9  FreeWnn
    10  gpm
    11  hpoj
    12  ip6tables
    13  iptables
    14  irqbalance
    15  isdn
    16  keytable
    17  kudzu
    18  mdmonitor
    19  microcode_ctl
    20  netfs
    21  network
    22  nfslock
    23  pcmcia
    24  portmap
    25  random
    26  rawdevices
    27  rhnsd
    28  sendmail
    29  sshd
    30  syslog
    31  xfs
[root@sandbox root]#
```

Secure Required Services

telnet

- Clear text!
- telnet and telnet-server packages
- Previously integrated, now separate
- Use client only for testing purposes (i.e. printers, web servers, mail servers, etc.

telnet with SMTP

```
[curtis@sandbox curtis]$ telnet mail.bogus-isp.net 25
Trying 64.1.2.3...
Connected to mail.bogus-isp.net (64.1.2.3).
Escape character is '^]'.
220 mail.bogus-isp.net ESMTP server (InterMail
 vM.6.01.03.02 201-2130
HELO microsoft.com
250 mail.bogus-isp.net
MAIL FROM:<bill@microsoft.com>
250 Sender <bill@microsoft.com> Ok
RCPT TO:<president@whitehouse.gov>
250 Recipient <president@whitehouse.gov> Ok
```

telnet with SMTP (cont'd)

```
DATA
354 Ok Send data ending with <CRLF>.<CRLF>
Subject: lunch
Hi George,

When would you like to do lunch?

Sincerely,

Bill
.
QUIT
250 Message received:
 20040629205027.TTKZ29210.mail.bogus-isp.net@mim
221 mail.bogus-isp.net ESMTP server closing connection
Connection closed by foreign host.
```

ssh

- www.openssh.org
- /etc/ssh/sshd_config
- Encrypted
- Replaces rsh, rcp, rlogin, telnet, etc.
- Remote session/command: ssh
- Remote copy: scp
- Login can be automated using public key cryptography

Automated ssh authentication

```
[curtis@sandbox curtis]$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/curtis/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/curtis/.ssh/id_rsa.
Your public key has been saved in /home/curtis/.ssh/id_rsa.pub.
The key fingerprint is:
d0:52:6e:f8:c4:9f:72:04:54:7b:b4:60:d2:e5:dd:60 curtis@sandbox.lan
[curtis@sandbox curtis]$ ssh snoopy "mkdir .ssh; chmod 0700 .ssh"
The authenticity of host 'snoopy (192.168.0.101)' can't be
  established.
RSA key fingerprint is
  c6:5e:79:9c:3c:b8:ff:fd:41:7d:7a:07:ab:df:ae:3b.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'snoopy,192.168.0.101' (RSA) to the list
  of known hosts.
curtis@snoopy's password:
[curtis@sandbox curtis]$ scp .ssh/id_rsa.pub
  snoopy:.ssh/authorized_keys2
curtis@snoopy's password:
```

Automated ssh authentication

```
[curtis@sandbox curtis]$ ssh snoopy who
curtis   :0           Jul  1 15:44
curtis   pts/1        Jul  2 11:57 (:0.0)
curtis   pts/4        Jul  1 15:46 (:0.0)
curtis   pts/5        Jul  1 15:47 (:0.0)
curtis   pts/6        Jul  1 15:48 (:0.0)
[curtis@sandbox curtis]$ ssh snoopy hostname
snoopy.lan
[curtis@sandbox curtis]$ ssh snoopy
[curtis@snoopy curtis]$ exit
logout

Connection to snoopy closed.
[curtis@sandbox curtis]$
```

/etc/ssh/sshd_config

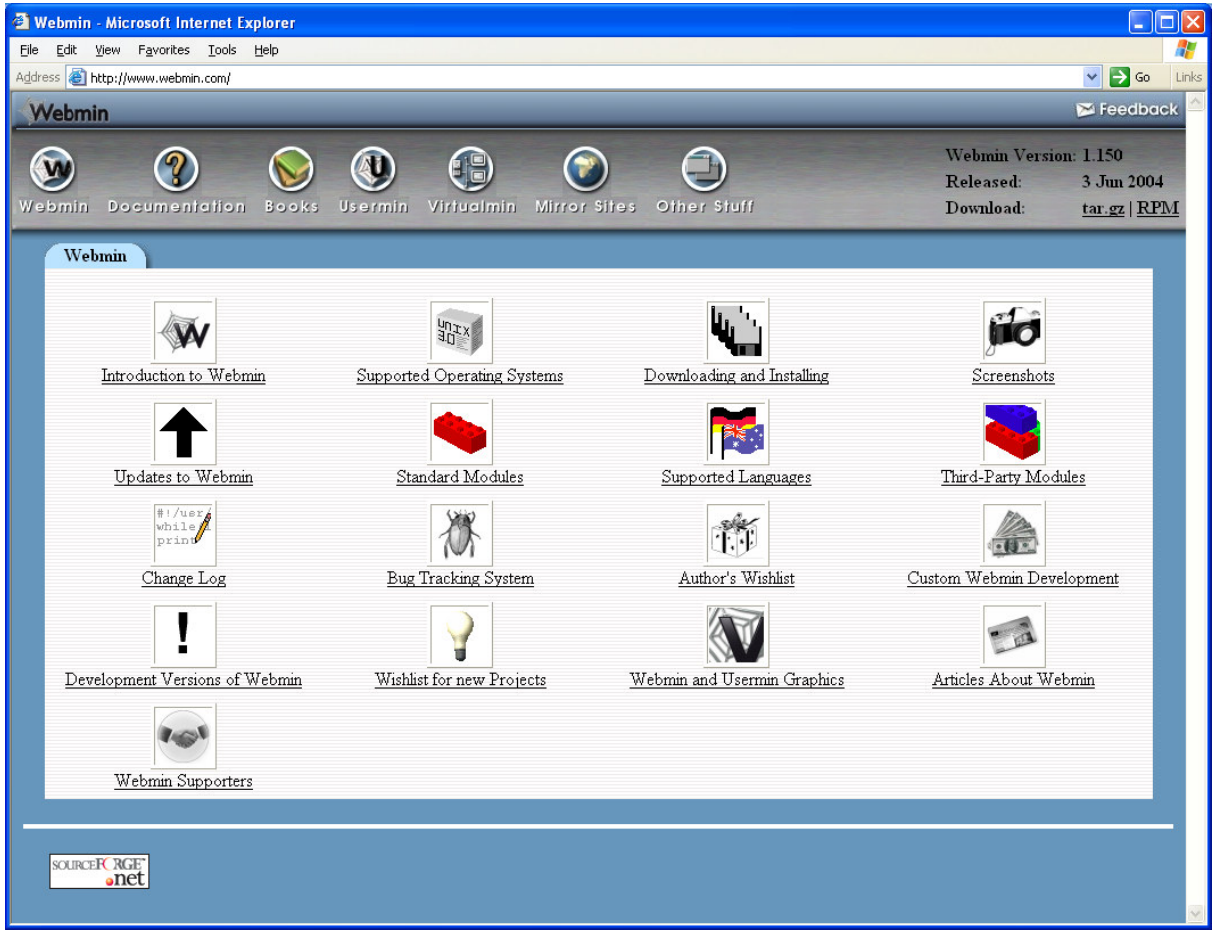
- Default: PermitRootLogin yes
- Default: X11Forwarding yes

Port forwarding with SSH

- ssh -f -N -L 10001:server1:10000 somehost.com
- local port 10001 mapped to port 10000 on remote host “server1” at somehost.com
- local port must not be currently bound

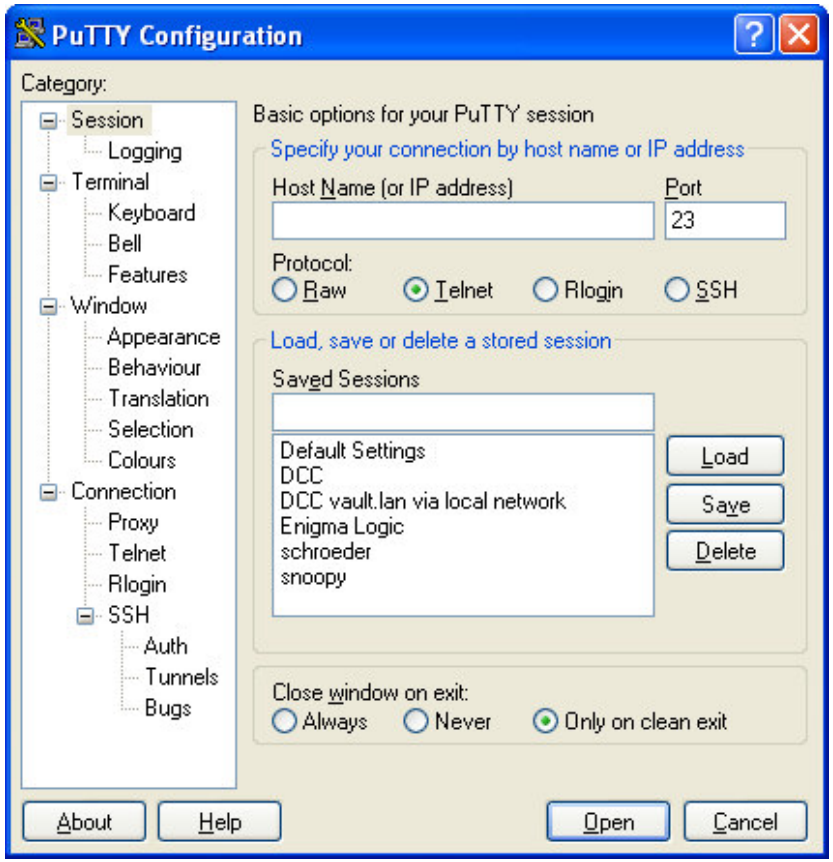
webmin via ssh forwarding

- www.webmin.com



ssh client

- PuTTy
- www.chiark.greenend.org.uk/~sgtatham/putty/



Remote Access: OpenVPN

- openvpn.sourceforge.net
- Cross platform tunnels between Linux, Windows 2000/XP, Mac OS X, Solaris, etc.
- Security model similar to IPSec but lighter footprint
- Easy setup: no kernel recompile, native Windows installer
- Supports both bridging and routing

Network File System (NFS)

- Access controlled via /etc/exports
- Mapping of UID/GID pairs across systems
- root is mapped to nobody by default (root_squash)
- Be very careful with no_root_squash
- Export read only unless otherwise necessary
- Limit use of wildcards

/etc/exports

```
/dir1 *.myhost.com(ro)
/dir2 * .myhost.com(ro)
/dir3 *.myhost.com (ro)
```

- dir1 is shared ro to any host in myhost.com
- dir2 is shared ro to anybody and any host in myhost.com
- dir3 is shared ro to any host in myhost.com and ro to anybody

/etc/exports

```
/dir1 *.myhost.com(rw)
/dir2 *  .myhost.com(rw)
/dir3 *.myhost.com (rw)
```

- dir1 is shared rw to any host in myhost.com
- dir2 is shared ro to anybody and rw to any host in myhost.com
- dir3 is shared ro to any host in myhost.com and rw to anybody

xinetd

- Superserver
- Replaces older inetd
- Adds access control by IP, network, time, etc.
- Configuration: /etc/xinetd.conf
- Individual services: /etc/xinetd.d

xinetd directives

- only_from = 127.0.0.1 192.168.1.0/24
- no_access = 192.168.1.5
- cps = 25 30
- per_source = 5
- access_times = 8:00-17:00

/etc/xinetd.d/telnet

```
# default: on
# description: The telnet server serves telnet sessions; it uses \
#       unencrypted username/password pairs for authentication.
service telnet
{
        disable = no
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/sbin/in.telnetd
        log_on_failure  += USERID
}
```

Disable:

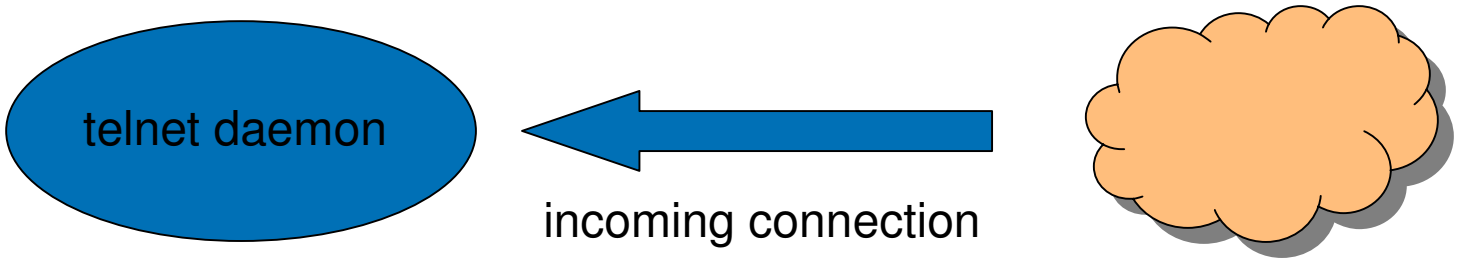
- Set “disable=yes” using editor
- Restart xinetd: `service xinetd restart`

or simply: `chkconfig telnet off`

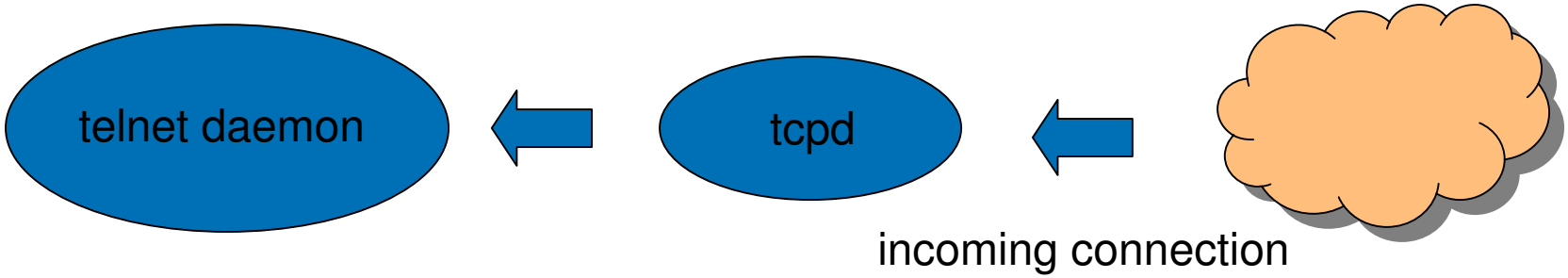
does both commands

tcp wrappers

Without tcp wrappers:



With tcp wrappers:



tcp wrappers

- /usr/sbin/tcpd
- /etc/hosts.allow
- /etc/hosts.deny
- If incoming address is in hosts.allow, accept and skip hosts.deny
- If incoming address is not in hosts.allow, but it is in hosts.deny, deny the connection
- If incoming address is not in either file, accept it
- Default: deny everything

tcp wrappers

Locating programs that are tcp wrapper aware:

```
[root@sandbox root]# find /usr/sbin -exec grep hosts_access
 {} \;
Binary file /usr/sbin/tcpd matches
Binary file /usr/sbin/stunnel matches
Binary file /usr/sbin/sshd matches
Binary file /usr/sbin/xinetd matches
Binary file /usr/sbin/vsftpd matches
Binary file /usr/sbin/in.tftpd matches
```

tcp wrappers

- /etc/hosts.deny

```
in.telnetd:  ALL:  spawn (/bin/mail -s "`hostname` telnet
 refused" root@myhost.com) &
ALL:  ALL
```

- Deny all telnet access and send email when attempted
- Default deny all services to everybody

tcp wrappers

- /etc/hosts.allow

```
ipop3d: .mycorp.com EXCEPT finance.mycorp.com
vsftpd: finance.mycorp.com, it.mycorp.com
```

- Allow POP3 email to everybody except finance
- Allow FTP to finance and IT departments

iptables

- www.netfilter.org
- `redhat-config-security-level`
- Default: deny everything
- Accept only what you need (and then rethink those services!)
- /etc/sysconfig/iptables

iptables

- Save rules: `service iptables save`
- List rules: `iptables -L --line-numbers`
- Flush rules (in memory): `iptables -F`
- www.linux-firewall-tools.com

iptables

- Policies:

```
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
```

- Examples:
  - Block all traffic from 192.168.1.2:

```
iptables -A INPUT -s 192.168.1.2 -j DROP
```

  - Limit ping to 1 request per second:

```
iptables -A INPUT -p icmp --icmp-type echo-
request -m limit --limit 1/s -i eth0 -j
ACCEPT
```

  - Block all outbound web browsing:

```
iptables -A OUTPUT --dport 80 -j DROP
```

PAM

- Pluggable Authentication Modules
- No need to recompile binaries, change on the fly
- /etc/pam.d/rlogin, rsh, etc.:
  auth required pam_rhosts_auth.so no_rhosts
- The Linux-PAM System Administrator's Guide:
  www.kernel.org/pub/linux/libs/pam/Linux-PAM-html/pam.html
- User Authentication HOW-TO:
  www.tldp.org/HOWTO/User-Authentication-HOWTO/x115.html

cron and at access

- /etc/cron.allow
- /etc/cron.deny
- /etc/at.allow
- /etc/at.deny

Secure Filesystems

/etc/fstab

- Filesystem mount options
- `man mount`
- nodev - do not interpret character or block special devices on the file system
- nosuid - do not allow SUID/SGID bits to take effect
- noexec - do not allow execution of any binaries
- ro - read only

/etc/fstab

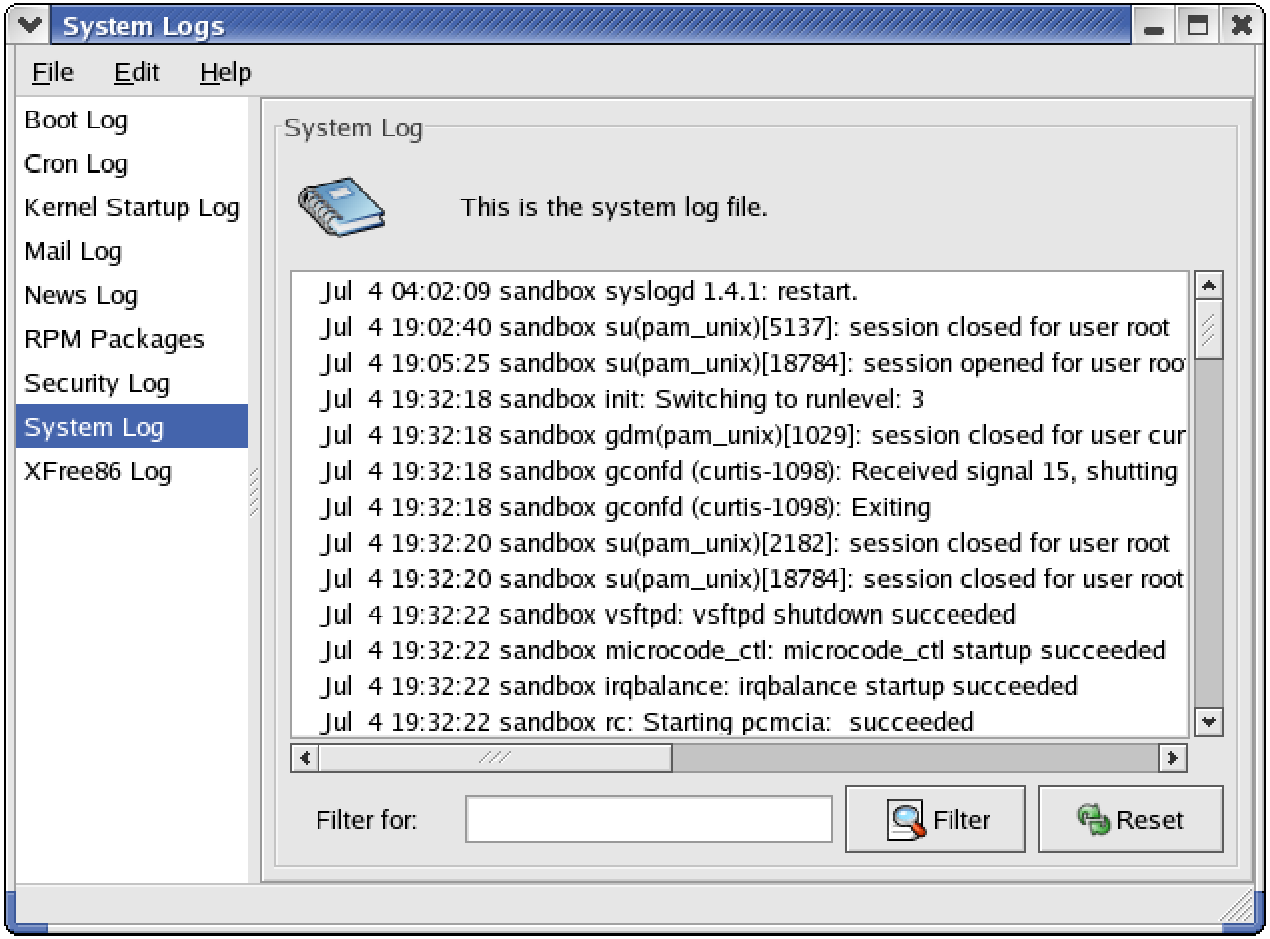
Mount point	Option
/	ro
/usr	ro
/boot	ro
/home	nodev, nosuid, noexec (?)
/tmp /var	nodev, nosuid, noexec
/mnt/cdrom /mnt/floppy	nodev, nosuid

Disk Quotas

- Prevention of denial of service attack
- Add usrquota to options field:
```
/dev/hdb1  /users  ext3  defaults,usrquota 1 1
```
- Remount filesystem:
```
mount -o remount /users
```
- Build quota files:
```
quotacheck -avu
```
- Enable quotas:
```
quotaon /users
```
- Add user quotas:
```
edquota
```

Logging

redhat-logviewer



/var/log

- /var/log/messages: general messages (“catch all”)
- /var/log/boot.log: startup/shutdown
- /var/log/dmesg: kernel messages from boot
- /var/log/vsftpd.log: ftp
- /var/log/maillog: inbound/outbound email
- /var/log/secure: login attempts
- Useful command: `tail -f /var/log/messages`

ntp

- www.ntp.org
- Clock synchronization helps when examining logs
- /etc/ntp.conf
- `redhat-config-date`

syslogd

- /etc/syslog.conf
- `man syslog.conf`
- Facilities: auth, authpriv, kern, mail, local0-7, etc.
- Priorities: info, warning, err, crit, emerg, etc.
- /var/log/*
- ntsyslog.sourceforge.net

syslogd

- Centralized logging - major security benefit
- /etc/sysconfig/syslog:
  SYSLOGD_OPTIONS="-m 0 -r"
- syslog.conf: *.* @*ip_of_central_logging_machine*
- `service syslog restart`
- `iptables -A INPUT -t filter -p udp --dport 514 -s 192.168.1.0/24 -j ACCEPT`

syslogd

- Test with logger:

On sandbox:

```
[root@sandbox root]# logger -p local0.info "This space
 intentionally left blank."
```

On snoopy:

```
[root@snoopy root]# tail -1 /var/log/messages
Jul  7 10:49:41 sandbox curtis: This space
 intentionally left blank.
```

chattr - append only

```
[root@sandbox root]# echo "This is a test" > my.log
[root@sandbox root]# cat my.log
This is a test
[root@sandbox root]# echo > my.log
[root@sandbox root]# cat my.log

[root@sandbox root]# chattr +a my.log
[root@sandbox root]# echo > my.log
-bash: my.log: Operation not permitted
[root@sandbox root]# echo "This is a test" > my.log
-bash: my.log: Operation not permitted
[root@sandbox root]# echo "This is a test" >> my.log
[root@sandbox root]# cat my.log

This is a test
[root@sandbox root]# rm my.log
rm: remove regular file `my.log'? y
rm: cannot remove `my.log': Operation not permitted
[root@sandbox root]# chattr -a my.log
[root@sandbox root]# rm my.log
rm: remove regular file `my.log'? y
[root@sandbox root]#
```

Banners

Login/Service Banners

- /etc/motd
- /etc/issue – get rid of OS version etc.
- /etc/issue.net - network
- Caution: rc.local possibly overwrites!
- xinetd
- X11
- tcp wrappers

Login Banners: /etc/issue

Before:

```
Red Hat Enterprise Linux AS release 3 (Taroon)
Kernel 2.4.21-4.EL on an i686
login: curtis
Password:
Last login: Mon Jun 28 10:31:48 on :0
[curtis@sandbox curtis]$
```

After:

```
*** UNAUTHORIZED ACCESS STRICTLY PROHIBITED ***

login:
```

Service Banners: xinetd

- Add to service configuration file and reload xinetd
- /etc/xinetd.d/telnet:
  banner = /etc/banners/in.telnetd
- `service xinetd reload`

Login Banners: X11

- /etc/X11/gdm/gdm.conf
- Welcome=*string*
- Or use `gdmsetup`

Service Banners: tcp wrappers

```
[root@sandbox root]# cat /etc/hosts.deny
in.telnetd : ALL : banners /etc/banners

[root@sandbox root]# cat /etc/banners/in.telnetd
Authorized use only.  All activity may be monitored and reported.
[root@sandbox root]#
```

Meanwhile on snoopy:

```
[root@snoopy root]# telnet sandbox
Trying 192.168.0.250...
Connected to sandbox.lan (192.168.0.250).
Escape character is '^]'.
Authorized use only.  All activity may be monitored and reported.
Connection closed by foreign host.
[root@snoopy root]#
```

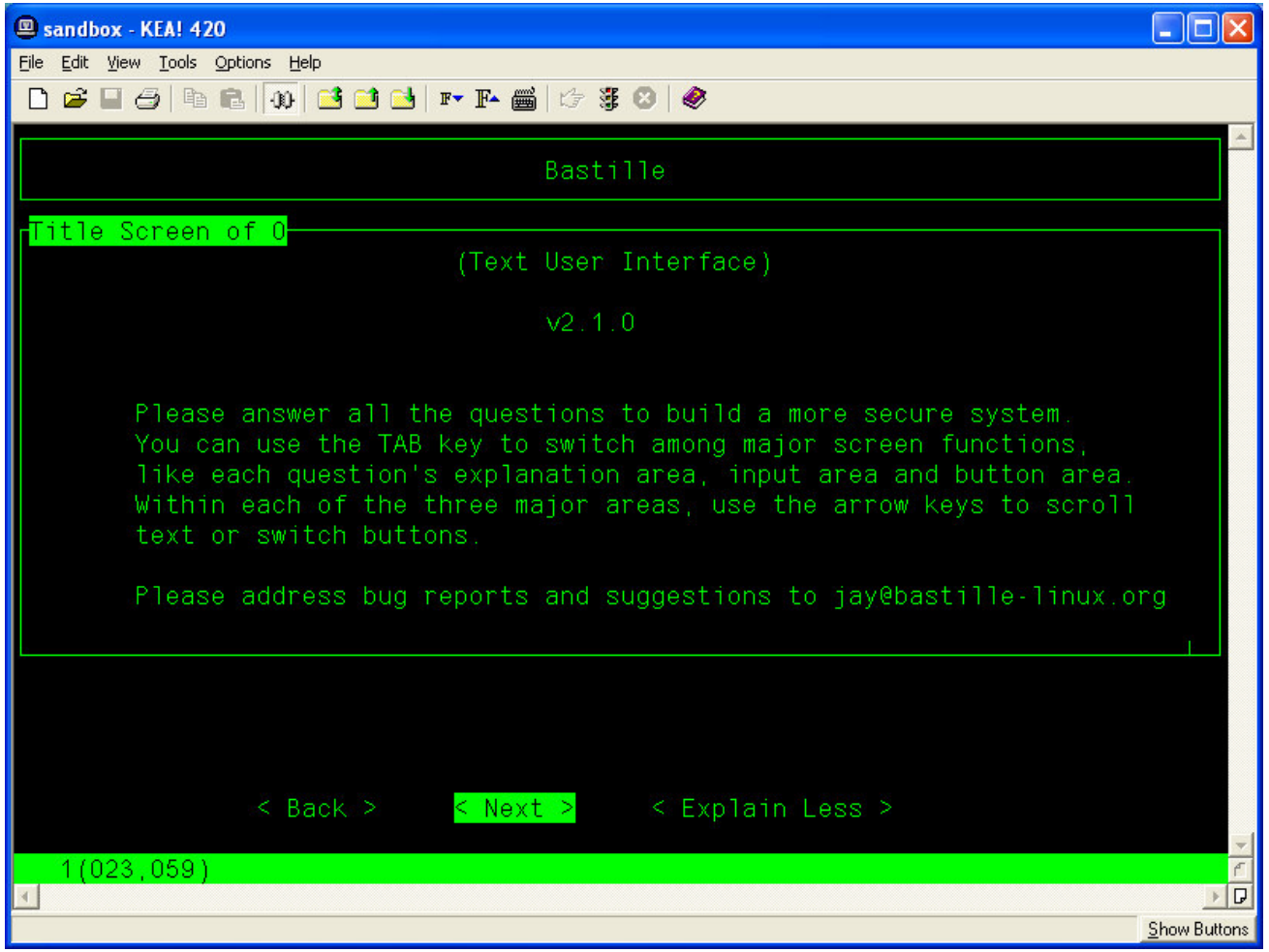
/var/log/messages:

```
Jul  4 22:04:11 sandbox xinetd[2520]: libwrap refused connection to
  telnet (libwrap=in.telnetd) from 192.168.0.249
```

Server Hardening Help: Bastille

- www.bastille-linux.org
- Hardening script for Red Hat and other Linux distributions as well as HP-UX and Mac OS X

Bastille


sandbox - KEA! 420
File Edit View Tools Options Help
Bastille
Title Screen of 0
(Text User Interface)
v2.1.0
Please answer all the questions to build a more secure system.
You can use the TAB key to switch among major screen functions,
like each question's explanation area, input area and button area.
Within each of the three major areas, use the arrow keys to scroll
text or switch buttons.
Please address bug reports and suggestions to jay@bastille-linux.org
< Back >
< Next >
< Explain Less >
1(023,059)
Show Buttons

Bastille

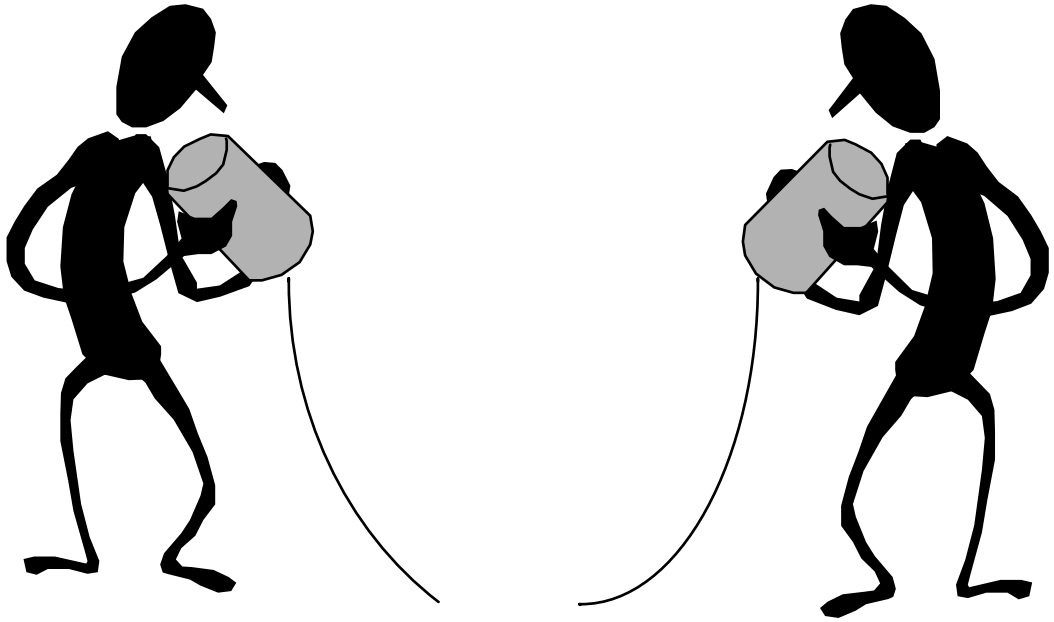
- Would you like to
  - set more restrictive permissions on the administration utilities?
  - disable SUID status for mount/umount, ping, at, traceroute?
  - disable the r-tools?
  - enforce password aging?
  - restrict the use of cron to administrative accounts?
  - set the default umask?
  - disallow root login on tty's 1-6?
  - password-protect the GRUB prompt?
  - disable CTRL-ALT-DELETE rebooting?

Bastille

- Would you like to
  - password protect single-user mode?
  - set a default-deny on TCP Wrappers and xinetd?
  - ensure the telnet service does not run on this system?
  - ensure inetd's FTP service does not run on this system?
  - display "Authorized Use" messages at log-in time?
  - disable the gcc compiler?
  - put limits on system resource usage?
  - restrict console access to a small group of user accounts?
  - add additional logging?
  - set up process accounting?
  - make a bunch of changes to Apache?

Monitoring and Audit Tools

- How do I know if any of this stuff is working?



logwatch

- www.logwatch.org
- Examines log files and reports “interesting” activity
- Runs daily via cron
- Perl script
- /etc/log.d/scripts/logwatch.pl
- /etc/log.d/conf/logwatch.conf

logwatch: example

```
 ################### LogWatch 4.3.2 (02/18/03) ####################
       Processing Initiated: Sun Apr 18 04:02:03 2004
       Date Range Processed: yesterday
     Detail Level of Output: 0
          Logfiles for Host: vault.lan
 ##################################################################

 -------------------- Kernel Begin ----------------------


WARNING:  Kernel Errors Present
    I/O error: dev 08:00, sect...:  6Time(s)
    sda: I/O error: dev 08:00, sect...:  4Time(s)
   st0: Error with sense data:...:  1Time(s)

 --------------------- Kernel End -----------------------
```

logwatch: example

```
--------------------- pam_unix Begin ------------------------

vsftpd:
   Unknown Entries:
      authentication failure; logname= uid=0 euid=0 tty= ruser=
  rhost=217.229.226.32 : 16 Time(s)

su:
   Authentication Failures:
      curtis(500) -> root: 2 Time(s)
   Sessions Opened:
      curtis(uid=500) -> root: 11 Time(s)


 ---------------------- pam_unix End -------------------------
```

nmap

- www.insecure.org
- The “defacto standard” port scanner
- Runs on: Linux, variety of UNIX flavors, and Windows
- Single IP or range
- Variety of techniques for scanning
- Use it to see what “the bad guys” see from your IP
- **Before you go port scanning somebody else, get their permission!**

nmap RHEL3.0 with default iptables

```
[root@snoopy root]# nmap sandbox

Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2004-06-30 13:26 MDT
All 1657 scanned ports on sandbox.lan (192.168.0.250) are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 72.025 seconds
[root@snoopy root]#
```

nmap RHEL3.0 without iptables

```
[root@snoopy root]# nmap sandbox

Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2004-06-30 13:31 MDT
Interesting ports on sandbox.lan (192.168.0.250):
(The 1654 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
22/tcp   open  ssh
111/tcp  open  rpcbind
6000/tcp open  X11

Nmap run completed -- 1 IP address (1 host up) scanned in 0.446 seconds
[root@snoopy root]#
```

nmap-diff.sh

```
#!/bin/bash

# This script runs periodically via cron to check for differences
# with a baseline nmap scan.

NMAPTARGET="sandbox"

YYMMDD=`date +'%Y%m%d'`

BASENMAP=/root/nmap.baseline
CURRNMAP=/tmp/nmap.$YYMMDD

if [ ! -f $BASENMAP ]
then
   echo "No baseline nmap data - generating baseline now."
   nmap $NMAPTARGET | egrep -v '^(Nmap|Starting)' > $BASENMAP
else
   nmap $NMAPTARGET | egrep -v '^(Nmap|Starting)' > $CURRNMAP
   diff $BASENMAP $CURRNMAP > /dev/null 2>&1
   if [ $? -ne 0 ]
   then
        echo "*** WARNING ***"
        echo
        echo "Current nmap output has changed from baseline."
        echo
        echo "Baseline:"
        echo
        cat $BASENMAP
        echo
        echo "Current:"
        echo
        cat $CURRNMAP
   fi
   rm -f $CURRNMAP
fi
```

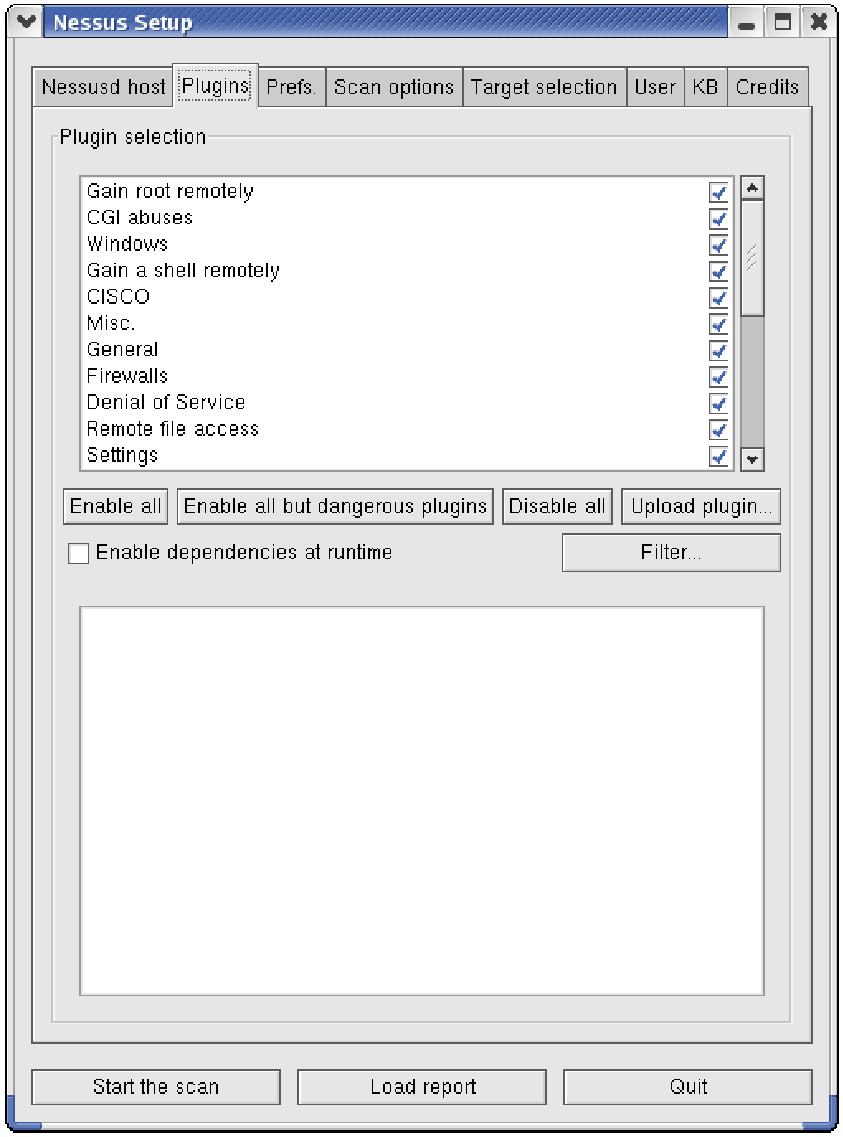
```
[root@sandbox root]# ./nmap-diff.sh
No baseline nmap data - generating baseline now.
[root@sandbox root]# cat nmap.baseline

Interesting ports on sandbox.lan (192.168.0.250):
(The 1598 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh
111/tcp    open        sunrpc
6000/tcp   open        X11

[root@sandbox root]# ./nmap-diff.sh
[root@sandbox root]# chkconfig telnet on
```

```
[root@sandbox root]# ./nmap-diff.sh
*** WARNING ***

Current nmap output has changed from baseline.

Baseline:


Interesting ports on sandbox.lan (192.168.0.250):
(The 1598 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh
111/tcp    open        sunrpc
6000/tcp   open        X11


Current:


Interesting ports on sandbox.lan (192.168.0.250):
(The 1597 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh
23/tcp     open        telnet
111/tcp    open        sunrpc
6000/tcp   open        X11

[root@sandbox root]#
```

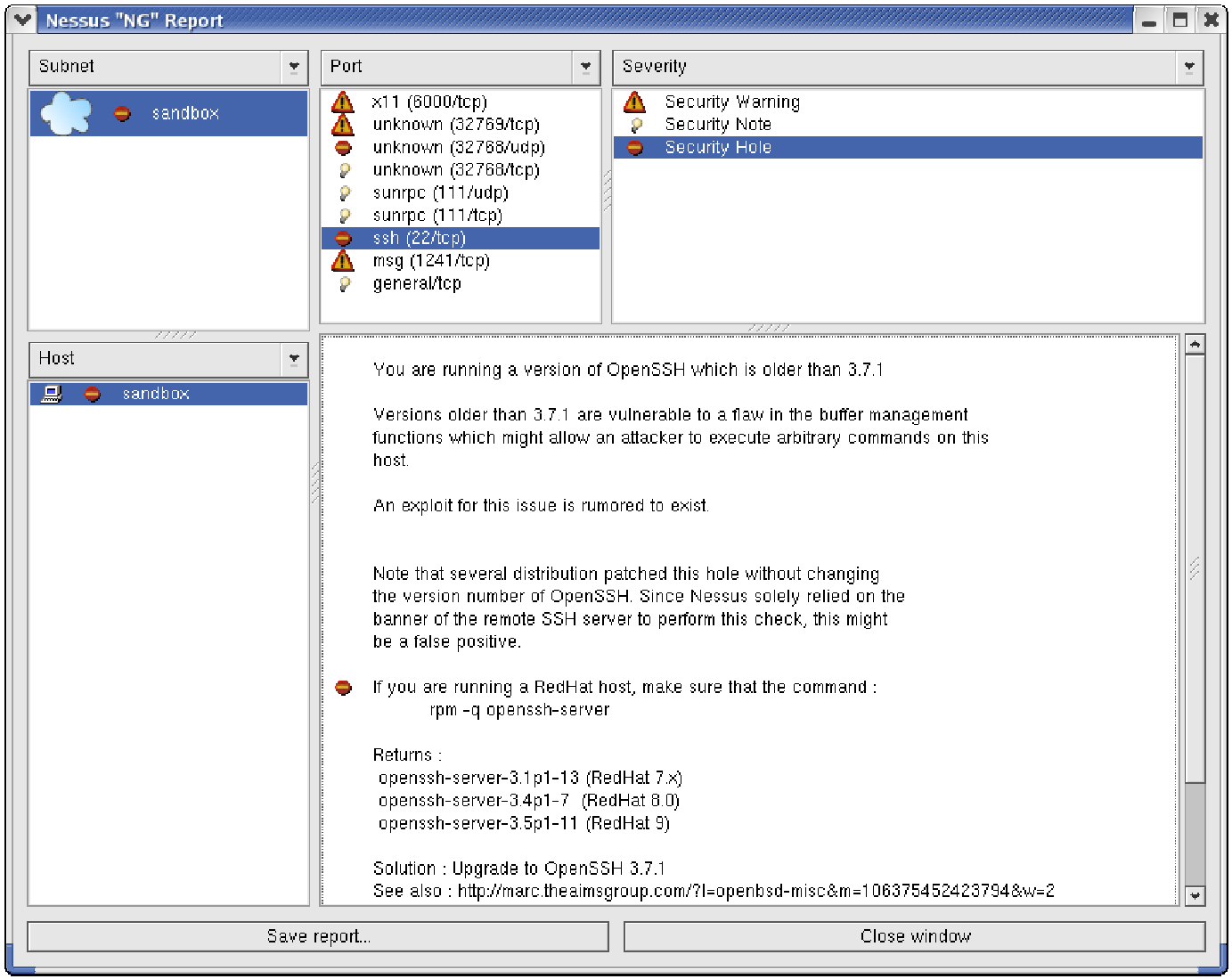
nessus

- www.nessus.org
- Vulnerability scanner
- Client / server architecture
- Updates - get them
- Plugins
- Caution: could crash target!

nessus: plugins



nessus: sample report

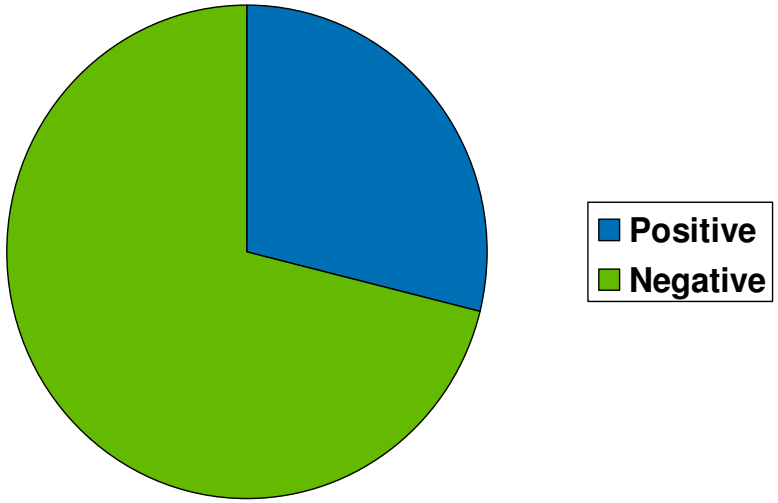


CIS

- www.cisecurity.org
- "The **Center for Internet Security (CIS)** is a non-profit enterprise whose mission is to help organizations reduce the risk of business and e-commerce disruptions resulting from inadequate technical security controls"
- Non-invasive, read-only
- Red Hat and Mandrake Linux
- Not yet available for RHEL 3.0 But ...

How did RHEL 3.0 do?

- Final rating = 5.38 / 10.00
- Positive: 35
- Negative: 142
- Need to interpret results, depends on your particular requirements, level of paranoia, etc.



How did RHEL 3.0 do?

```
Positive: 1.1 System appears to have been patched
 within the last month.
Positive: 1.2 System is running sshd and it's
 configured well.
Positive: 2.2 telnet is deactivated.
Positive: 2.3 ftp is deactivated.
Positive: 2.4 rsh, rcp and rlogin are deactivated.
Positive: 2.5 tftp is deactivated.
Positive: 2.6 imap is deactivated.
Positive: 2.7 POP server is deactivated.
Positive: 3.1 Found a good daemon umask of 022 in
 /etc/rc.d/init.d/functions.
Positive: 3.7 Windows compatibility servers (samba)
 have been deactivated.
```

How did RHEL 3.0 do?

```
[…]
Positive: 5.1 syslog captures authpriv messages.
Positive: 5.3 All logfile permissions and owners match
 benchmark recommendations.
Positive: 6.4 password and group files have right
 permissions and owners.
Positive: 7.2 /etc/hosts.equiv and root's
 .rhosts/.shosts files either don't exist, are zero
 size or are links to /dev/null.
Positive: 8.2 All users have passwords
Positive: 8.5 Only one UID 0 account AND it is named
 root.
```

How did RHEL 3.0 do?

```
Positive: 8.6 root's PATH is clean of group/world
  writable directories or the current-directory link.
Positive: 8.7 No user's home directory is world or
  group writable.
Positive: 6.7 No non-standard SUID/SGID programs found.
```

How did RHEL 3.0 do?

```
Negative: 3.2 xinetd is still active.

Negative: 3.3 Mail daemon is still listening on TCP 25.

Negative: 3.14 cups (printing daemon) not deactivated.

[…]

Negative: 4.1 /proc/sys/net/ipv4/tcp_max_syn_backlog
 should be at least 4096 to handle SYN floods.

[…]

Negative: 6.1 /usr is not mounted nodev.

Negative: 6.1 /var is not mounted nodev.

Negative: 6.1 /tmp is not mounted nodev.

Negative: 6.1 /home is not mounted nodev.

Negative: 6.1 /boot is not mounted nodev.
```

How did RHEL 3.0 do?

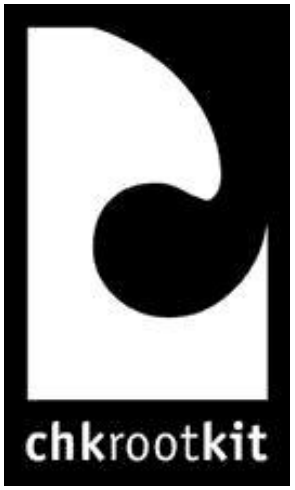
```
Negative: 6.2 Removable filesystem /mnt/cdrom is not
 mounted nosuid.

[…]

Negative: 6.3 PAM allows users to mount removable
 media: <floppy>.  (/etc/security/console.perms)

[…]

Negative: 7.1 rhosts authentication not deactivated in
 /etc/pam.d/rlogin.

Negative: 7.1 rhosts authentication not deactivated in
 /etc/pam.d/rsh.
```

How did RHEL 3.0 do?

```
Negative: 7.7 No Authorized Only message in /etc/motd.

[…]

Negative: 7.7 No Authorized Only banner for telnet in
  file /etc/xinetd.d/telnet.

[…]

Negative: 7.10 GRUB isn't password-protected.

Negative: 7.11 /etc/inittab needs a /sbin/sulogin line
  for single user mode.

Negative: 8.10 Current umask setting in file
  /etc/profile is 000 -- it should be stronger to block
  world-read/write/execute.

[…]
```

chkrootkit

- www.chkrootkit.org
- Shell script
- 55 kits fingerprinted



chkrootkit

```
[root@sandbox chkrootkit-0.43]# ./chkrootkit
ROOTDIR is `/'
Checking `amd'... not infected
Checking `basename'... not infected
Checking `biff'... not found
Checking `chfn'... not infected

[...]

Searching for sniffer's logs, it may take a while... nothing found
Searching for HiDrootkit's default dir... nothing found
Searching for t0rn's default files and dirs... nothing found
Searching for t0rn's v8 defaults... nothing found
Searching for Lion Worm default files and dirs... nothing found
Searching for RSHA's default files and dir... nothing found
Searching for RH-Sharpe's default files... nothing found
Searching for Ambient's rootkit (ark) default files and dirs...
  nothing found
Searching for suspicious files and dirs, it may take a while...

[...]

Checking `scalper'... not infected
Checking `slapper'... not infected
Checking `z2'... nothing deleted
[root@sandbox chkrootkit-0.43]#
```

Package/File Baseline Checking

- rpm –V
  - RPM package files only
  - Baseline: package installation time
- Tripwire & friends
  - All files, including RPM package files
  - Baseline: user definable

rpm -V

- Individual package or all packages (rpm -Va)
- S: file size differs
- M: mode (permissions) differs
- 5: MD5 sum differs
- U: user ownership differs
- G: group ownership differs
- T: modification time differs

rpm -V

```
[root@sandbox root]# rpm -qf /bin/ls
coreutils-4.5.3-26
[root@sandbox root]# rpm -V coreutils
[root@sandbox root]# chown curtis /bin/ls
[root@sandbox root]# ls -l /bin/ls
-rwxr-xr-x    1 curtis   root        68660 Aug 12  2003 /bin/ls
[root@sandbox root]# rpm -V coreutils
.....U..   /bin/ls
[root@sandbox root]# chown root /bin/ls
[root@sandbox root]# rpm -V coreutils
```

Verifying RPM Authenticity

- Import the public key from the vendor (once)
- Check the RPM package you downloaded using
  `rpm --checksig some_package.rpm`

Red Hat GPG key import

```
[root@sandbox tmp]# cat RPM-GPG-KEY
The following public key can be used to verify RPM packages built
  and
signed by Red Hat, Inc. using `rpm -K' using the GNU GPG package.
Questions about this key should be sent to security@redhat.com.

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.0.0 (GNU/Linux)
Comment: For info see http://www.gnupg.org

mQGiBDfqVDgRBADBKr3Bl6PO8BQ0H8sJoD6p9U7Yyl7pjtZqioviPwXP+DCWd4u8
HQzcxAZ57m8ssA1LK1Fx93coJhDzM130+p5BG9mYSWShLabR3N1KXdXQYYcowTOM

[...]

-----END PGP PUBLIC KEY BLOCK-----
[root@sandbox tmp]# rpm --import RPM-GPG-KEY
[root@sandbox tmp]# rpm -qa | grep ^gpg
gpg-pubkey-db42a60e-37ea5438
```

Red Hat GPG key import

```
[root@sandbox tmp]# rpm -qi gpg-pubkey-db42a60e-37ea5438
Name        : gpg-pubkey                   Relocations: (not relocateable)
Version     : db42a60e                         Vendor: (none)
Release     : 37ea5438                     Build Date: Sun 04 Jul 2004
  07:11:42 PM MDT
Install Date: Sun 04 Jul 2004 07:11:42 PM MDT      Build Host: localhost
Group       : Public Keys                  Source RPM: (none)
Size        : 0                               License: pubkey
Signature   : (none)
Summary     : gpg(Red Hat, Inc <security@redhat.com>)
Description :
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: rpm-4.2.1 (beecrypt-3.0.0)

mQGiBDfqVDgRBADBKr3Bl6PO8BQ0H8sJoD6p9U7Yyl7pjtZqioviPwXP+DCWd4u8HQzcxAZ5
7m8ssA1LK1Fx93coJhDzM130+p5BG9mYSWShLabR3N1KXdXQYYcowTOMGxdwYRGr1Spw8Qyd

[...]

-----END PGP PUBLIC KEY BLOCK-----

[root@sandbox tmp]#
```

Keep track of installed software

- All packages:

```
rpm -qa | sort > /tmp/package-
list.`date +'%Y-%m-%d'`
```

- Most recent:

```
rpm -qa --last | head
```

- Non-RPM software:

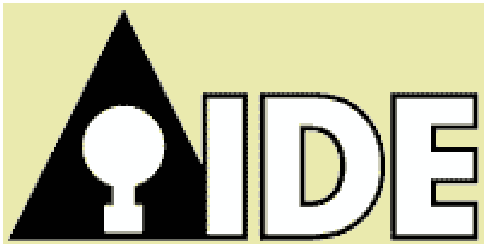
```
ls -alR /usr/local
```

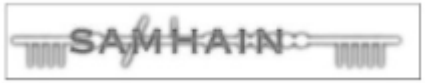
- Audit all RPM packages:

```
rpm -Va
```

Other Integrity Checkers

- www.tripwire.org
- aide.sourceforge.net
- osiris.shmoo.com
- samhain.sourceforge.net





md5 checksums

- Build an initial baseline and periodically check for differences

```
#!/bin/bash

for DIR in sbin bin
do
  for FILE in `ls /$DIR`
  do
    echo $FILE
    md5sum /$DIR/$FILE >> md5sum.rpt
  done
done
```

Build a test box

- **Don't play in production!**
- RHEL 3.0 – full install (~ 4 GB)
- Learn how to use the kickstart utility
- `redhat-config-kickstart`
- www.redhat.com/docs/manuals/enterprise/RHEL-3-Manual/sysadmin-guide/ch-kickstart2.html

Sample kickstart configuration

```
install
reboot
nfs --server=snoopy --dir=/mnt/tmp/rhe3
lang en_US.UTF-8
langsupport --default en_US.UTF-8 en_US.UTF-8
keyboard us
mouse genericwheelps/2 --device psaux
xconfig --card "RIVA TNT" --videoram 16384 --hsync 30-107 --vsync
  50-160 --resoe
network --device eth0 --bootproto dhcp
rootpw --iscrypted $1$9F2QUoad$ctvkO51rmjzYwOJrBi8Hr0
firewall --enabled
authconfig --enableshadow --enablemd5
timezone America/Edmonton
bootloader --location=mbr --append hdd=ide-scsi
clearpart --all --drives=hda,hdb
part /boot --fstype ext3 --size=150 --ondisk=hda
part /var --fstype ext3 --size=1000 --ondisk=hda
part swap --size=384 --ondisk=hda
part / --fstype ext3 --size=300 --ondisk=hda
part /home --fstype ext3 --size=500 --ondisk=hda
part /usr --fstype ext3 --size=6000 --ondisk=hda
part /tmp --fstype ext3 --size=1000 --ondisk=hda
```

Sample kickstart configuration (cont'd)

```
%packages
@ everything
kernel
grub

%post

useradd curtis
echo topsecret | passwd --stdin curtis
```

Sessions

- who
- last
- ps –ef
- top
- lastcomm
- lsof

Process Accounting

```
[root@sandbox root]# chkconfig psacct on
[root@sandbox root]# service psacct start
Starting process accounting:                               [  OK  ]
[root@sandbox root]# ac
        total       86.27
[root@sandbox root]# ac -p
        curtis                             86.28
        total       86.28
```

Process Accounting

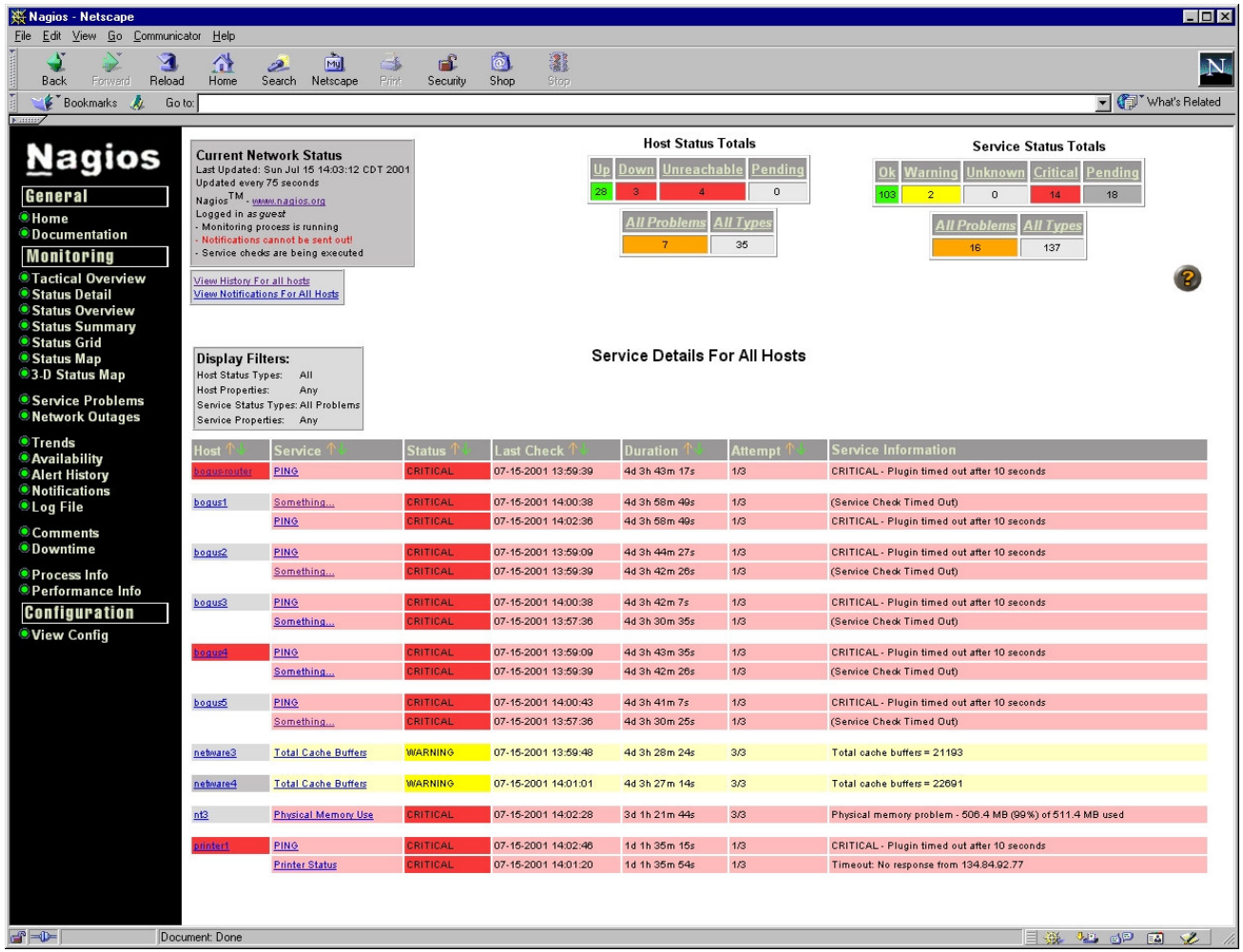
```
[curtis@sandbox curtis]$ date
Fri Jul  2 13:58:42 MDT 2004
[curtis@sandbox curtis]$ who
curtis   :0           Jul  1 11:01
curtis   pts/0        Jul  1 11:02 (:0.0)
curtis   pts/1        Jul  1 11:03 (:0.0)
```

Process Accounting

```
[root@sandbox root]# lastcomm curtis
who                    curtis   ??         0.02 secs Fri Jul  2 13:58
date                   curtis   ??         0.00 secs Fri Jul  2 13:58
su                 S   curtis   ??         0.02 secs Fri Jul  2 13:05
[root@sandbox root]# lastcomm who
who                    curtis   ??         0.02 secs Fri Jul  2 13:58
```

nagios

- www.nagios.org



Advanced Topics

- Kernel 2.6
- Beyond Bastille
- Advanced Auditing

Linux Kernel 2.6 – it's a "Good Thing"

- Modular security architecture
- Finer granularity than "root" or "not root"
- Linux Security Modules (LSM) prevent having to patch kernel (SELinux)
- SELinux will heavily affect RHEL 4.0
- Cryptographic API allows security abstraction at the protocol level

Linux Kernel 2.6 – it's a "Good Thing"

- Buffer overflows: exec-shield patch, no recompile necessary
- User Mode Linux (UML):
  - Kernel patch
  - Allows compilation/execution of binary on host Linux machine
  - Processes within host machine are not allowed access to outside machine
  - Similar to a scaled down version of VMware

Hardening beyond Bastille

- Hardened kernels:
  - Linux Intrusion Defence System
    www.lids.org
  - Rule Set Based Access Control
    www.rsbac.org

- Hardened distributions:
  - SELinux
    www.nsa.gov/selinux
  - OpenWall “Owl”
    www.openwall.com

Secure Auditing for Linux

- secureaudit.sourceforge.net
- Funded by the Defense Advanced Research Projects Agency (DARPA)
- Kernel level auditing package for Red Hat Linux
- C2 level security

Conclusion (yes, it's finally over!)

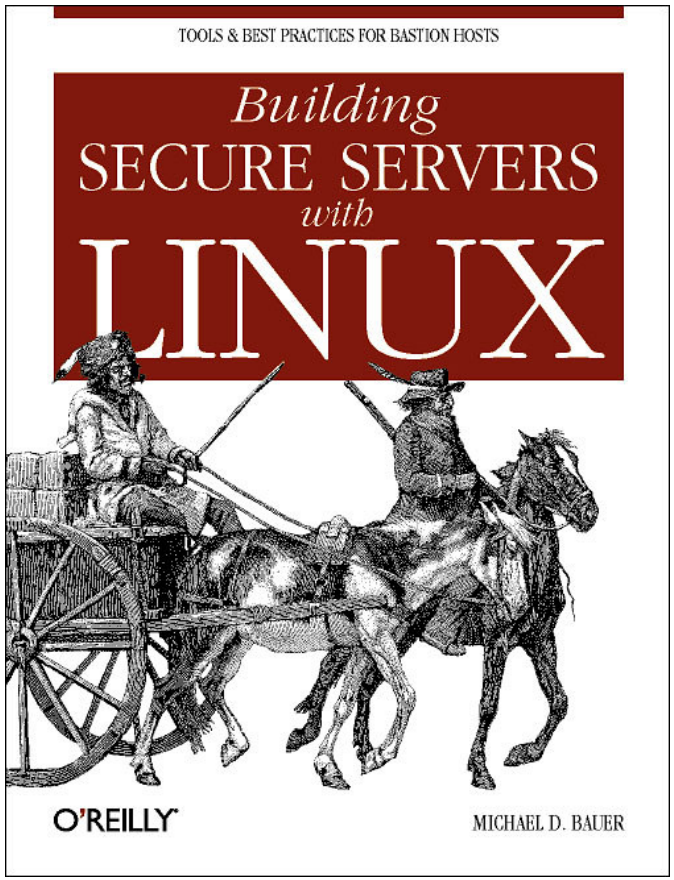
Top 10 Linux Security Tips

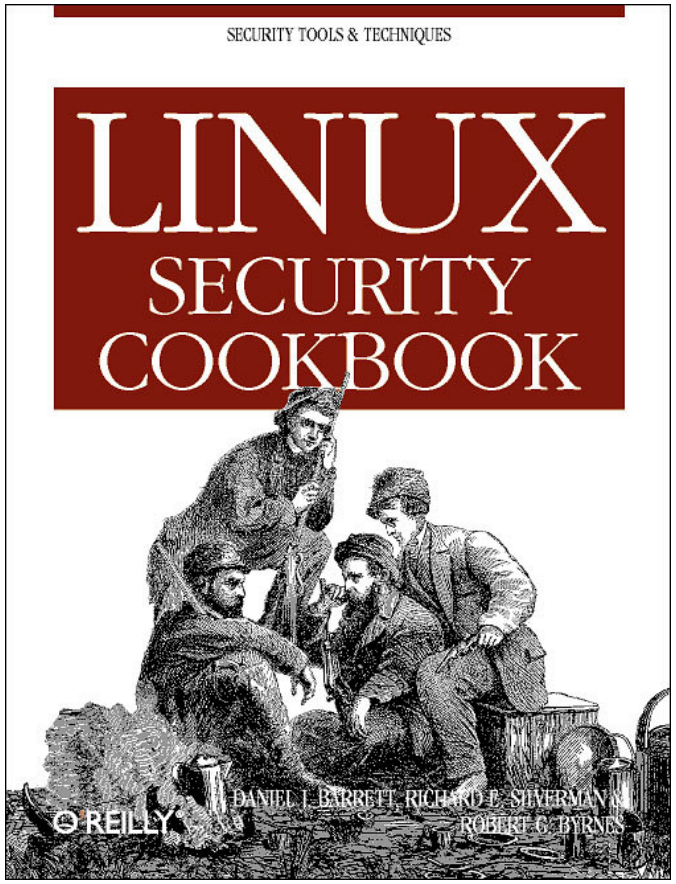
1. Physical security
2. Use root for administration tasks - nothing else!
3. Patches
4. Turn off services you don't need
5. Configure ssh to avoid cleartext protocols

Top 10 Linux Security Tips

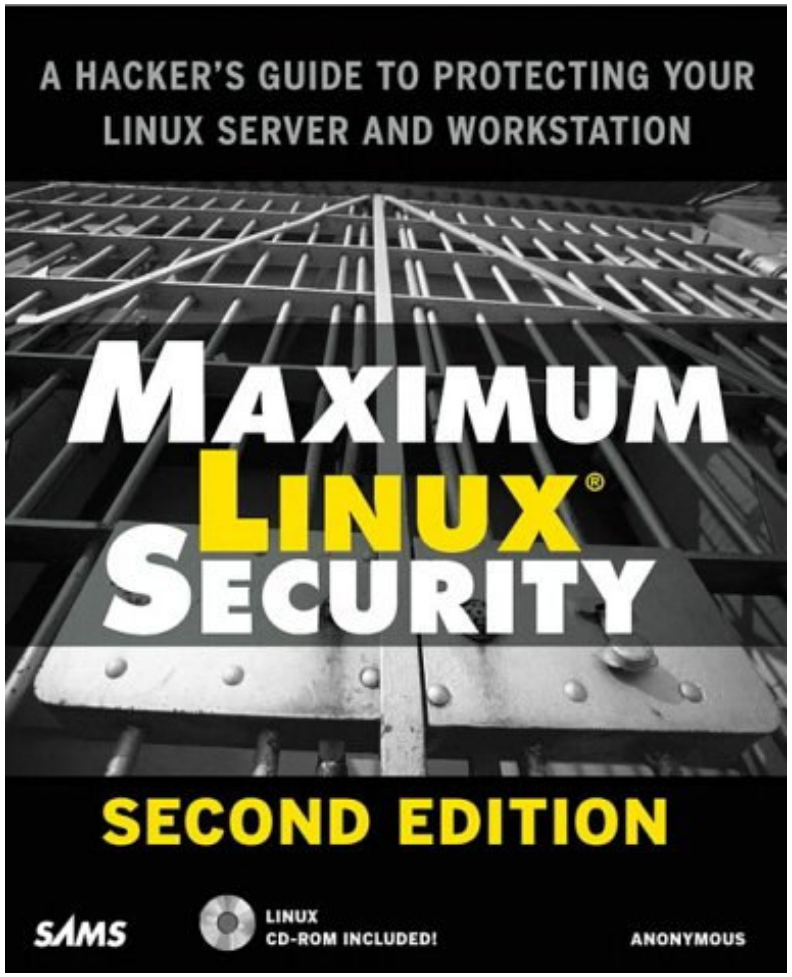
6. Set up a basic firewall
7. Limit access to resources
8. Monitor and automate
9. Backups, backups, backups!
10. Keep your knowledge up to date

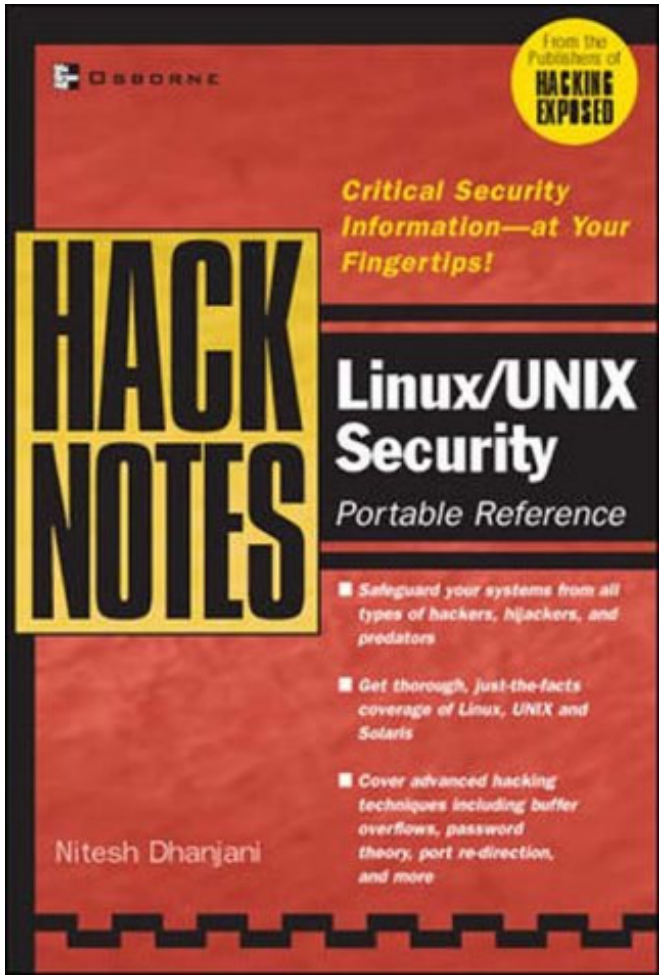
Resources


TOOLS & BEST PRACTICES FOR BASTION HOSTS
Building
SECURE SERVERS
with
LINUX
O'REILLY
MICHAEL D. BAUER


SECURITY TOOLS & TECHNIQUES
LINUX
SECURITY
COOKBOOK
O'REILLY
DANIEL J. BARRETT, RICHARD E. SILVERMAN &
ROBERT G. BYRNES

Resources


A HACKER'S GUIDE TO PROTECTING YOUR LINUX SERVER AND WORKSTATION
MAXIMUM LINUX® SECURITY
SECOND EDITION
SAMS
LINUX CD-ROM INCLUDED!
ANONYMOUS


OSBORNE
From the Publishers of HACKING EXPOSED
Critical Security Information—at Your Fingertips!
HACK NOTES
Linux/UNIX Security
Portable Reference
Safeguard your systems from all types of hackers, hijackers, and predators
Get thorough, just-the-facts coverage of Linux, UNIX and Solaris
Cover advanced hacking techniques including buffer overflows, password theory, port re-direction, and more
Nitesh Dhanjani

Resources

- Red Hat Security Guide: www.redhat.com/docs/manuals/enterprise/RHEL-3-Manual/security-guide/
- www.linuxsecurity.com
- www.cert.org
- cve.mitre.org
- www.sans.org/top20
- www.securityfocus.com
- www.seclists.org

Resources

- Linux Administrators Security Guide: www.seifried.org/lasg/
- www.antionline.com - downloads

Summary

- Know your systems
  - Typical load
  - Processes
  - Applications
  - Logs
  - Usage monitoring
- Know your users
  - What time they work
  - What they typically do
  - Where they typically log in from

Summary

- Start with the basics of securing your system
- The two “biggies”:
  - Choose good passwords
  - Keep up to date with patches
- Monitor advisories
- Use root for the right reasons
- Build a “sandbox” environment and test
- Ongoing education
- Don’t be too confident in your skills, check and double check, even the pros can make preventable mistakes!

A Message From Our Lawyers

- Copyright 2004 Enigma Logic Inc.
- Linux is a registered trademark of Linus Torvalds.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- Other company, product, and service names may be trademarks or service marks of others.
- Presentation may contain useful content.
- Presentation may also contains errors, we're human ya know.
- Caution: more than 150 slides per hour can cause dizziness. Digest content with care. Consult your security guru if headaches persist.
- Your mileage may vary.
- Batteries not included.
- #include <std/disclaimer.h>

HP WORLD 2004

Solutions and Technology Conference & Expo

Co-produced by:

interex

shared knowledge • shared power

encompass

AN HP USER GROUP