IDS Burglar Alarms:
A How-To Guide

GSEC Practical Assignment, Version 1.4b
Option 1 – Research on Topics in Information Security
Mark Embrich
November 28, 2003

Table of Contents

Abstract.

In the context of this paper, a burglar alarm is defined as a cheap, expendable device used as an intrusion detection device. Although the concept of burglar alarms in Information Security has been around for years and the tools to build it have also existed for years, it is not a trivial task to build a burglar alarm.

The goal of this paper is to make the task of building Intrusion Detection burglar alarms less daunting. The method chosen is to put together modular “how-to” guides. The pieces need to be modular because not all burglar alarms need the same functionality and pieces are updated on differing schedules.

1. Introduction.

1.1. SHADOW Architecture.

It was 2001 when I first heard of the concept of intrusion detection devices that were like burglar alarms. Stephen Northcutt was speaking in a SANS GCIA class regarding SHADOW, the intrusion detection system he developed for the Naval Surface Warfare Center/Dahlgren Division. Part of the explanation was regarding the architecture of the SHADOW IDS:

> The SHADOW system consists of two functional pieces: sensors and analyzers. The sensors sit at network boundaries, where a local network is connected to an external one. They are positioned such that they can collect data about packets entering or leaving the local network. The data is saved in files that accumulate on the sensor's disks. Analyzers sit inside the local network, hopefully protected by a firewall, to periodically retrieve and remove the data files from the sensors. The analyzers examine the data to provide views of it from different perspectives, such as potential intrusion events and statistical traffic summaries.
>
> (The SHADOW Team, 2003)

This architecture made a lot of sense to me, especially since the hardware available to me is made up of old workstations. Since these old workstations have less than ideal processing power, we want to make them do as little as possible outside of their primary task. This isn't that big a deal for the analyzers, since they don't have to capture packets.

Another feature of this architecture (also learned from Northcutt) is that it gives less information to the attacker. Since your sensor is more exposed than your analyzer, it is more prone to attack. Should an attacker successfully compromise your sensor, they still won't know your analysis methodology – only that you are capturing packets.

1.2. Redundant and Expendable.

Almost a year later, in another conference, I was in a class taught by Marcus Ranum (who actually appears to be the one who coined the concept of burglar alarms in Information Security). Ranum explained that your top-notch burglar knows all about your top-notch burglar alarms, therefore knows how to circumvent them. So the way you catch a top-notch burglar is through the use of redundant, unexpected alarms. His example was a dummy jewelry box – with an alarm rigged to trigger on opening of the box (it was a honeypot class).

Ranum explains this in an article for ;login:, the Usenix magazine:

> My first "real" job was working for a burglar-alarm company when I was a kid in high school. Now, umpty-whatever years later, I'm basically doing the same thing

> for a living again. My boss at the time used to design great alarm systems; a lot of historic properties and municipal buildings in Maryland (including a nuclear-power plant) had alarm systems that had been designed specifically for those sites by my boss.
>
> One of the distinguishing characteristics of his alarm systems was that he liked to put special traps within the perimeter of the site that was being secured — not just at the boundary of the network, um, uh, building. So the alarms had all of the usual glass-break detectors, window switches, and so on — with the addition of window switches hidden in gun cabinets, jewelry boxes, executive desks, key boxes, and so on. When we wired an alarm system with a bell, we'd put in a low-power circuit that would cause the alarm to go off (silently, of course!) if the bell circuit was cut. If the bell was in a box on the outside of the building, we'd include a contact switch in the bell box to set off the alarm if it was opened or pulled away from the wall.
>
> Never mind infrared and microwave motion detectors (which are pretty obvious LCD-blinking white boxes stuck to a wall) — we used to put pressure-sensitive pads under carpeted floors in hallways. I guess I learned paranoia at an early age! Remember, one person's "paranoia" is another person's "engineering redundancy" — these traps worked extremely well. The special alarms would trigger a different code from the normal ones, so if the system called the police, the cops would know that they were dealing with a professional who had bypassed the first layer of security.
>
> Obviously, you can see where I'm going with this: the same concepts apply to network and even application security.
>
> If you've got a system that you want to keep people from breaking into, ask yourself a couple of leading questions:
>
> - What am I really afraid could go wrong with my system?
> - What would it look like if something were in the process of going wrong?
> - What can I put in place to tell me when it is happening?
>
> (Ranum, 2000)

We want to borrow Ranum's principles of redundancy. Our IDS burglar alarms are not to replace our firewalls, but to run in addition to the firewalls. We want to see what is happening on our networks, particularly things that the firewall may not understand is a problem.

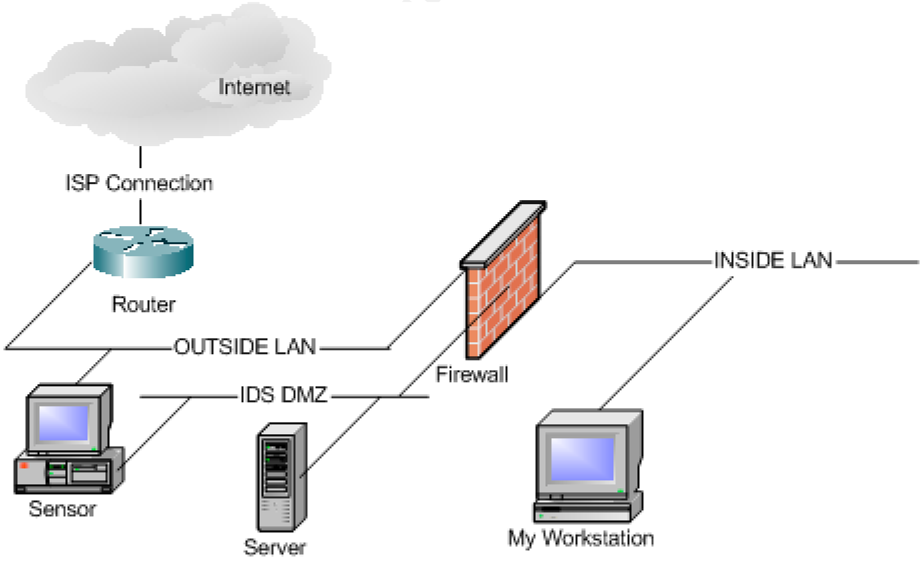
We depart from Ranum's principle of specific targetting, since the network is quite different from the physical world. In the physical world, it is impossible to capture everything, there are too many things to capture: video, audio, temperature, pressure, etc. In our network, there is only one type of activity, electrical impulses travelling down a wire, which form bytes, which in turn form frames, packets, and so on. In our network, it is possible to capture everything. So at the sensor, we do just that, capture everything. Back at the analyzer is where we do our targetting (each snort rule is a target).

Not specifically mentioned, but I read into Ranum's concepts that it's good for the burglar alarms to be cheap enough that we can afford to have many of them. Rather than one big, expensive burglar alarm, we can use multiple, redundant burglar alarms – the same concept as layers of security. In addition to being cheap, they need to be easy to replace. Since the sensors only run a sniffer, they easy to duplicate. The combination of cheap and easy to replace makes the sensors expendable.

1.3. Practical Application.

Through upgrading workstations for our employees, our company ended up with several old computers, for which we had no use. Rather than throw them away, they've gained new life as intrusion detection machines. All I needed to do to the hardware was to replace their hard disks (the old disks were too small) and network interface cards (replaced the 10-base-T NICs with 10/100 NICs).

Following the SHADOW architecture, we want the sensor to be out in a less secured network. In my case, this was our main DMZ, between our external router and firewall. We want the analyzer (I'll call this our server from here on out) to be behind a firewall, so this would usually be on the inside network. I made a change to this, because I wanted the sensor's sniffing interface to have no IP address and I did not want to send the data from the sensor to the server over the sensor's sniffing interface. To get around this, I added a second network interface to the sensor and put the server in another DMZ, such that the sensor to server communication occurs on a different network. Here is an illustration:



2. Server.

We want to install the server first, since the sensor install is a subset of the server install. This means we can use the server install to facilitate the sensor install, but not the other way around.

2.1. Installing Linux.

I selected RedHat 9 as the operating system of the intrusion detection machines for several reasons, cost being the biggest factor:

- Cost of the operating system = $0
- Cost of support (patches) = $0
- Cost for Tripwire = $0 (If I chose Solaris, I would have had to pay for Tripwire)
- Popularity of the operating system. The more people use it, the more likely someone will be able to help me if I run into a problem.

Unfortunately, support will no longer be free for RedHat after some time in 2004, so I'll need to look into choosing a different operating system in the future.

2.1.1. Zero Out the Disks.

Assume your burglar alarms will be compromised. To facilitate future forensic investigation, we will want to install our software on hard drives that are a completely blank slate. We can do this using the "dd" utility. The command is:

```
dd if=/dev/zero of=/dev/hdb
```

Where /dev/hdb is the Primary IDE Slave.
In the "dd" command, "if" specifies an input file and "of" specifies an output file.
Change the "of" setting as needed for your case:

Primary Master	=	/dev/hda
Primary Slave	=	/dev/hdb
Secondary Master	=	/dev/hdc
Secondary Slave	=	/dev/hdd

If you want to make sure you and the computer agree on which drives are installed, you can check by doing:

```
ls /proc/ide
```

Example:

```
[membrich@localhost membrich]$ ls /proc/ide
drivers  hda  hdb  hdc  hdd  ide0  ide1  piix
[membrich@localhost membrich]$
```

This means that I have four IDE devices installed. (It's three hard drives and a CD-ROM drive.)

I want to zero out the first hard drive (/dev/hda, the Primary Master). To do this, I can't boot from that drive. My favorite way of solving this dilemma is to use knoppix, which is a Linux distribution that runs off a CD. Knoppix is available at: http://www.knoppix.net/get.php.

After booting to knoppix, here's what I did:

```
root@tty1[/]# dd if=/dev/zero of=/dev/hda bs=256k
dd: writing '/dev/hda': No space left on device
78166+0 records in
78165+0 records out
20490559488 bytes transferred in3075.924042 seconds (6661595 bytes/sec)
```

NOTE: The "bs=256k" option speeds up the process a little by writing bigger chunks at a time.

2.1.2. Installing RedHat 9 from CDs.

Since this is the first machine we're installing, we'll install manually from the CDs.

2.1.2.1. Installation Type.

At the "Installation Type" screen, choose "Custom".

2.1.2.2. Disk Partitioning Setup.

At the "Disk Partitioning Setup" screen, choose "Manual partition with DiskDruid".

I'm installing on a 20 GB hard disk, here's how I did it:

Mount Point	Type	Size	Options
/boot	ext3	150 MB	Fixed size, Force to be a Primary Partition
/	ext3	700 MB	Fixed size, Force to be a Primary Partition
	swap	256 MB	Fixed size, Force to be a Primary Partition
/home	ext3	1000 MB	Fixed size
/usr	ext3	1000 MB	Fixed size
/tmp	ext3	500 MB	Fixed size
/var	ext3		Fill to maximum allowable size

This resulted in:

Device	Mount Point	Type	Size	Start	End
/dev/hda					
/dev/hda1	/boot	ext3	150	1	305

/dev/hda2	/	ext3	700	306	1727
/dev/hda3		swap	256	1728	2247
/dev/hda4		Extended	18435	2248	39703
/dev/hda5	/usr	ext3	1000	2248	4279
/dev/hda6	/home	ext3	1000	4280	6311
/dev/hda7	/tmp	ext3	500	6312	7327
/dev/hda8	/var	ext3	15935	7328	39703

2.1.2.3. Firewall Configuration.

On the "Firewall Configuration" screen, choose "No Firewall".
We can set up iptables later.

2.1.2.4. Package Group Selection.

On the "Package Group Selection" screen, remove all of the check marks on package groups to install:

Desktops

UNCHECK X Windows System

UNCHECK GNOME Desktop Environment

Applications

UNCHECK Graphical Internet

UNCHECK Text-based Internet

UNCHECK Office/Productivity

UNCHECK Sound and Video

UNCHECK Graphics

UNCHECK Printing Support

Then check the "Select Individual Packages" box at the bottom left corner.

2.1.2.4.1. Individual Package Selection.

On the "Individual Package Selection" screen, choose the "Flat View" option.

Checked Items:

acl	
UNCHECK	anacron
UNCHECK	apmd
UNCHECK	aspell
at	
UNCHECK	attr
UNCHECK	autofs
UNCHECK	bc
bind-utils	
CHECK	binutils

CHECK	bison	(needed by snort)
bzip2		
CHECK	bzip2-devel	
CHECK	cpp	
crontabs		
UNCHECK	cyrus-sasl-plain	
UNCHECK	devlabel	
UNCHECK	dhclient	
diffutils		
UNCHECK	dos2unix	
dosfstools		
UNCHECK	dump	
eject		
UNCHECK	elfutils	
UNCHECK	ethtool	
UNCHECK	fbset	
UNCHECK	finger	
CHECK	flex	(needed by snort)
CHECK	freetype	(needed for gd)
CHECK	freetype-devel	(needed for PHP)
UNCHECK	ftp	
CHECK	gcc	(needed to compile 3rd party applications)
CHECK	gd	(needed for ACID)
CHECK	glibc-devel	
CHECK	glibc-kernheaders	
gnupg		
UNCHECK	gpm	
groff		
UNCHECK	hesiod	
iptables		
UNCHECK	irda-utils	
UNCHECK	isdn4k-utils	
UNCHECK	jfsutils	
UNCHECK	jwhois	
UNCHECK	kernel-pcmcia-cs	
CHECK	krb5-devel	(needed for openssl-devel)
UNCHECK	krbafs	
UNCHECK	lftp	
UNCHECK	lha	
CHECK	libjpeg	(needed for gd)
CHECK	libjpeg-devel	(needed for PHP)
CHECK	libpcap	(needed for snort)
CHECK	libpng	(needed for gd)
CHECK	libpng10	(needed for gd)
CHECK	libpng-devel	(needed for PHP)
libstdc++		

UNCHECK	libtool-libs	
UNCHECK	libwvstreams	
UNCHECK	lockdev	
logrotate		
logwatch		
UNCHECK	lokkit	
UNCHECK	lrzsz	
lsof		
CHECK	m4	
UNCHECK	mailcap	
mailx		
make		
man		
man-pages		
UNCHECK	minicom	
mkbootdisk		
UNCHECK	mtools	
UNCHECK	mtr	
UNCHECK	mt-st	
CHECK	mysql	(needed for snort)
CHECK	mysql-devel	(needed for snort)
CHECK	mysql-server	(needed for snort)
netconfig		
UNCHECK	nfs-utils	
UNCHECK	nscd	
UNCHECK	nss-ldap	
ntsysv		
openssh		
openssh-clients		
openssh-server		
CHECK	openssl-devel	
UNCHECK	pam_krb5	
UNCHECK	pam_smb	
parted		
UNCHECK	pax	
pciutils		
perl		
CHECK	perl-CGI	(required for ACID)
CHECK	perl-DBD-MySQL	(required for ACID)
CHECK	perl-DBI	(required for ACID)
perl-filter		
UNCHECK	pinfo	
UNCHECK	portmap	
UNCHECK	ppp	
UNCHECK	procmail	
UNCHECK	pspell	

UNCHECK	pyOpenSSL
UNCHECK	python-optik
UNCHECK	quota
UNCHECK	rdate
UNCHECK	rdist
UNCHECK	redhat-config-network-tui
UNCHECK	reiserfs-utils
UNCHECK	rhnlib
UNCHECK	rmt
UNCHECK	rpm-python
UNCHECK	rp-pppoe
UNCHECK	rsh
UNCHECK	rsync
UNCHECK	sendmail
UNCHECK	setuptool
UNCHECK	slocate
UNCHECK	specspo
UNCHECK	star
UNCHECK	statserial
UNCHECK	stunnel
UNCHECK	sudo
syslinux	
UNCHECK	talk
tcpdump	
tcp_wrappers	
UNCHECK	tcsh
UNCHECK	telnet
time	
timeconfig	
tmpwatch	
traceroute	
CHECK	tripwire
UNCHECK	unix2dos
unzip	
UNCHECK	up2date
utempter	
UNCHECK	vconfig
vixie-cron	
UNCHECK	wget
UNCHECK	wireless-tools
UNCHECK	wvdial
UNCHECK	ypbind
UNCHECK	yp-tools
zip	
CHECK	zlib-devel

Total = 492 MB

2.1.4. Post-Install Cleanup.

2.1.4.1. Add Myself as a User.

```
[root@localhost root]# useradd -c "Mark Embrich" -m -d /home/membrich -u 1101 membrich
[root@localhost root]# passwd membrich
Changing password for user membrich.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

2.1.4.2. Set Up eth0 Interface.

edited /etc/sysconfig/network-scripts/ifcfg-eth0:

```
[membrich@localhost membrich]$ cat /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
BOOTPROTO=static
BROADCAST=172.16.255.255
IPADDR=172.16.1.253
NETMASK=255.255.0.0
NETWORK=172.16.0.0
ONBOOT=yes
```

Restarted eth0 interface by running:

```
[root@localhost root]# /etc/init.d/network restart
```

2.1.4.3. Early Snapshot.

```
[membrich@localhost membrich]$ df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/hda2             689M   72M  583M  11% /
/dev/hda1             146M  8.9M  129M   7% /boot
/dev/hda6             985M   17M  919M   2% /home
none                   31M     0   31M   0% /dev/shm
/dev/hda7             485M  8.1M  452M   2% /tmp
/dev/hda5             985M  316M  620M  34% /usr
/dev/hda8              16G   43M   15G   1% /var
[membrich@localhost membrich]$
```

```
[membrich@localhost membrich]$ netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0     20 172.16.1.253:22         172.16.1.33:1068        ESTABLISHED
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node Path
unix  4      [ ]         DGRAM                    1351   /dev/log
unix  3      [ ]         STREAM     CONNECTED     2821
unix  3      [ ]         STREAM     CONNECTED     2820
unix  2      [ ]         DGRAM                    1501
unix  2      [ ]         DGRAM                    1359
[membrich@localhost membrich]$
```

2.1.4.4. Removing Unnecessary Packages.

```
[root@localhost membrich]# rpm -qa > packages
[root@localhost membrich]# sort packages > sorted_pkg
```

Reviewed the list of packages, here's what we can remove:

```
[root@localhost membrich]# rpm -e ash
[root@localhost membrich]# rpm -e at
[root@localhost membrich]# rpm -e authconfig
[root@localhost membrich]# rpm -e comps
[root@localhost membrich]# rpm -e cpio
[root@localhost membrich]# rpm -e ed
[root@localhost membrich]# rpm -e hdparm
[root@localhost membrich]# rpm -e hotplug
[root@localhost membrich]# rpm -e lilo
```

To remove python, you need to remove (in order):

```
[root@localhost membrich]# rpm -e redhat-config-mouse
[root@localhost membrich]# rpm -e rhpl
[root@localhost membrich]# rpm -e pyxf86config
[root@localhost membrich]# rpm -e python
```

Continue removing unnecessary packages:

```
[root@localhost membrich]# rpm -e raidtools
[root@localhost membrich]# rpm -e redhat-logos
[root@localhost membrich]# rpm -e usbutils

[root@localhost membrich]# rpm -qa > after_pkg
[root@localhost membrich]# sort after_pkg > after_pkg_sorted
[root@localhost membrich]# wc -l sorted_pkg
    163 sorted_pkg
[membrich@localhost membrich]$ wc -l after_pkg_sorted
    147 after_pkg_sorted
[membrich@localhost membrich]$
```

2.1.5. Install Patches.

2.1.5.1. Install RedHat's Public Key.

Import redhat public key (for checking authenticity of patches):
RedHat Public Key can be found on the root directory of CD1.

```
[root@localhost membrich]# mount -t iso9660 /dev/cdrom /mnt/cdrom
mount: block device /dev/cdrom is write-protected, mounting read-only
[root@localhost membrich]# ls /mnt/cdrom
autorun                README.it              RELEASE-NOTES-fr.html
dosutils               README.ja              RELEASE-NOTES.html
EULA                   README.ko              RELEASE-NOTES-it.html
GPL                    README.pt              RELEASE-NOTES-ja.html
images                 README.pt_BR           RELEASE-NOTES-ko.html
isolinux               README.zh_CN           RELEASE-NOTES-pt_BR.html
README                 README.zh_TW           RELEASE-NOTES-pt.html
README-Accessibility   RedHat                 RELEASE-NOTES-zh_CN.html
README.de              RELEASE-NOTES          RELEASE-NOTES-zh_TW.html
README.es              RELEASE-NOTES-de.html  RPM-GPG-KEY
README.fr              RELEASE-NOTES-es.html  TRANS.TBL
[root@localhost membrich]# rpm --import /mnt/cdrom/RPM-GPG-KEY
[root@localhost membrich]#
```

2.1.5.2. Determine Which Patches are Needed.

The RedHat 9 patches are available at: https://rhn.redhat.com/errata/rh9-errata.html.

The easiest way to install the patches is to use RedHat's up2date application, which can automatically download patches from RedHat's web site. However, being somewhat paranoid, I don't use up2date for the following reasons:

1. I don't want to connect an unpatched machine to the Internet.
2. I'm of the opinion that it's only a matter of time until some black hat figures out that compromising these automatic updating servers would be a great way to compromise a huge number of devices very quickly. Just think of your Symantec Antivirus that checks for updates every time you turn on your Windows workstation. What happens if the virus pretends to be an update for your Symantec Antivirus?

This leaves manually determining which patches are needed and manually installing them. Since we've eliminated many of the typically installed patches, we also do not need many of the patches. My method of determining which patches are needed is to look at each patch individually, see which rpm packages are affected, compare this to what packages are installed on the machine.

For example, patch rhsa-2003-091 includes packages:

i386:
krb5-devel-1.2.7-14.i386.rpm
[via FTP] [via HTTP]   49e7783cb50c3694411b7856d098eff5
krb5-libs-1.2.7-14.i386.rpm
[via FTP] [via HTTP]   6cb5040d3a4bd21a801e8c1e5da6388d
krb5-server-1.2.7-14.i386.rpm
[via FTP] [via HTTP]   8eb2a755c2fdf52b779960ec66cc6783
krb5-workstation-1.2.7-14.i386.rpm
[via FTP] [via HTTP]   bbcde88fa4f273c7c45a927dc5b40d58

Compare this to what is installed on our machine:

```
[root@localhost membrich]# rpm -qa | grep krb5
krb5-devel-1.2.7-10
krb5-libs-1.2.7-10
[root@localhost membrich]#
```

We need to download krb5-devel-1.2.7-14.i386.rpm and krb5-libs-1.2.7-14.i386.rpm and install them.

As the time of this writing, November 9, 2003, we need parts of the following patches:

rhsa-2003-091
rhba-2003-136
rhsa-2003-174
rhsa-2003-175
rhba-2003-140
rhsa-2003-199
rhba-2003-263
rhsa-2003-279
rhsa-2003-292
rhsa-2003-256
rhsa-2003-281
rhsa-2003-309

2.1.5.3. Get the Patches to the Server.

I downloaded the necessary rpms to my workstation, then used scp to move them to our machine:

```
D:\download\redhat\patches>dir
 Volume in drive D is New Volume
 Volume Serial Number is 1C0E-19DB

 Directory of D:\download\redhat\patches

11/09/2003  05:04p      <DIR>          .
11/09/2003  05:04p      <DIR>          ..
11/09/2003  04:37p      <DIR>          rhba-2003-136
11/09/2003  04:40p      <DIR>          rhba-2003-140
11/09/2003  04:44p      <DIR>          rhba-2003-263
11/09/2003  04:34p      <DIR>          rhsa-2003-091
11/09/2003  04:38p      <DIR>          rhsa-2003-174
11/09/2003  04:40p      <DIR>          rhsa-2003-175
11/09/2003  04:42p      <DIR>          rhsa-2003-199
11/09/2003  05:01p      <DIR>          rhsa-2003-256
11/09/2003  04:53p      <DIR>          rhsa-2003-279
11/09/2003  05:03p      <DIR>          rhsa-2003-281
11/09/2003  04:57p      <DIR>          rhsa-2003-292
11/09/2003  05:05p      <DIR>          rhsa-2003-309
               0 File(s)              0 bytes
              14 Dir(s)   2,489,262,080 bytes free

D:\download\redhat\patches>pscp -r * membrich@172.16.1.253:/home/membrich
membrich@172.16.1.253's password:
glibc-2.3.2-27.9.i386.rpm |       3222 kB | 1074.2 kB/s | ETA: 00:00:00 | 100%
glibc-common-2.3.2-27.9.i |      12148 kB | 1104.4 kB/s | ETA: 00:00:00 | 100%
glibc-devel-2.3.2-27.9.i3 |       2285 kB | 1142.9 kB/s | ETA: 00:00:00 | 100%
bash-2.05b-20.1.i386.rpm  |        737 kB | 737.4 kB/s | ETA: 00:00:00 | 100%
kernel-2.4.20-20.9.i586.r |      13468 kB | 1122.4 kB/s | ETA: 00:00:00 | 100%
krb5-devel-1.2.7-14.i386. |        713 kB | 713.7 kB/s | ETA: 00:00:00 | 100%
krb5-libs-1.2.7-14.i386.r |        410 kB | 410.7 kB/s | ETA: 00:00:00 | 100%
tcpdump-3.7.2-1.9.1.i386. |        299 kB | 299.5 kB/s | ETA: 00:00:00 | 100%
gnupg-1.2.1-4.i386.rpm    |       1209 kB | 604.9 kB/s | ETA: 00:00:00 | 100%
unzip-5.50-33.i386.rpm    |        136 kB | 136.8 kB/s | ETA: 00:00:00 | 100%
perl-5.8.0-88.3.i386.rpm  |      14143 kB | 1088.0 kB/s | ETA: 00:00:00 | 100%
perl-CGI-2.81-88.3.i386.r |        183 kB | 183.7 kB/s | ETA: 00:00:00 | 100%
openssh-3.5p1-11.i386.rpm |        177 kB | 177.6 kB/s | ETA: 00:00:00 | 100%
openssh-clients-3.5p1-11. |        300 kB | 300.0 kB/s | ETA: 00:00:00 | 100%
```

```
openssh-server-3.5p1-11.i |        177 kB | 177.1 kB/s | ETA: 00:00:00 | 100%
mysql-3.23.58-1.9.i386.rp |       5831 kB | 1166.2 kB/s | ETA: 00:00:00 | 100%
mysql-devel-3.23.58-1.9.i |        567 kB | 567.4 kB/s | ETA: 00:00:00 | 100%
mysql-server-3.23.58-1.9. |       1097 kB | 1097.1 kB/s | ETA: 00:00:00 | 100%
openssl-0.9.7a-20.i386.rp |       1103 kB | 1104.0 kB/s | ETA: 00:00:00 | 100%
openssl-devel-0.9.7a-20.i |       1611 kB | 805.8 kB/s | ETA: 00:00:00 | 100%
coreutils-4.5.3-19.0.2.i3 |       2357 kB | 1178.6 kB/s | ETA: 00:00:00 | 100%

D:\download\redhat\patches>
```

2.1.5.4. Install the Patches.

The order in which you install the patches is important.

I'll document this section by using two parts for each patch. First, I'll include the important information from the RedHat web site. Then I'll show you what I actually did to install the patch.

2.1.5.4.1. RHSA-2003-091.

https://rhn.redhat.com/errata/RHSA-2003-091.html
Updated kerberos packages fix various vulnerabilities

Advisory: RHSA-2003:091-22
Last updated on: 2003-04-02

i386:
krb5-devel-1.2.7-14.i386.rpm
[via FTP] [via HTTP]   49e7783cb50c3694411b7856d098eff5
krb5-libs-1.2.7-14.i386.rpm
[via FTP] [via HTTP]   6cb5040d3a4bd21a801e8c1e5da6388d

rpm -Fvh [filenames]

(“Updated Kerberos Packages Fix Various Vulnerabilities.” 2003)

```
[root@localhost membrich]# rpm --checksig rhsa-2003-091/*
rhsa-2003-091/krb5-devel-1.2.7-14.i386.rpm: (sha1) dsa sha1 md5 gpg OK
rhsa-2003-091/krb5-libs-1.2.7-14.i386.rpm: (sha1) dsa sha1 md5 gpg OK
[root@localhost membrich]# rpm -Fvh rhsa-2003-091/*.rpm
Preparing...                ########################################### [100%]
   1:krb5-libs              ########################################### [ 50%]
   2:krb5-devel             ########################################### [100%]
[root@localhost membrich]#
```

2.1.5.4.2. RHBA-2003-136.

https://rhn.redhat.com/errata/RHBA-2003-136.html
glibc bugfix errata

Advisory: RHBA-2003:136-07
Last updated on: 2003-04-09

NOTE: Make sure you get the right glibc-2.3.27.9.iX86.rpm file. My server is a Pentium, so I'll use the i386 version.

i686:
glibc-2.3.2-27.9.i686.rpm
[via FTP] [via HTTP]   17698f5ff98d3cee2a72b2f206bc1589
i386:
glibc-2.3.2-27.9.i386.rpm
[via FTP] [via HTTP]   8fe9a661fd031b405d75a0e22a57925b
glibc-common-2.3.2-27.9.i386.rpm
[via FTP] [via HTTP]   dc5b2aa636ff96c2ecfa144d373eac64
glibc-devel-2.3.2-27.9.i386.rpm
[via FTP] [via HTTP]   780dda739f56779fa953df64ddaeaeff

rpm -Fvh [filenames]

(“Glibc Bugfix Errata.” 2003)

```
[root@localhost membrich]# rpm --checksig rhba-2003-136/*
rhba-2003-136/glibc-2.3.2-27.9.i386.rpm: (sha1) dsa sha1 md5 gpg OK
rhba-2003-136/glibc-common-2.3.2-27.9.i386.rpm: (sha1) dsa sha1 md5 gpg OK
rhba-2003-136/glibc-devel-2.3.2-27.9.i386.rpm: (sha1) dsa sha1 md5 gpg OK
[root@localhost membrich]# rpm -Fvh rhba-2003-136/*.rpm
Preparing...                ########################################### [100%]
   1:glibc-common           ########################################### [ 33%]
   2:glibc                  ########################################### [ 67%]
Stopping sshd:[  OK  ]
Starting sshd:[  OK  ]
   3:glibc-devel            ########################################### [100%]
[root@localhost membrich]#
```

2.1.5.4.3. RHSA-2003-174.

https://rhn.redhat.com/errata/RHSA-2003-174.html
Updated tcpdump packages fix privilege dropping error

Advisory: RHSA-2003:174-04
Last updated on: 2003-05-15

i386:
tcpdump-3.7.2-1.9.1.i386.rpm
[via FTP] [via HTTP]   6cff8bf6b2425c361eec70ba3017d82b

(update instructions missing, assuming "rpm -Fvh")

(“Updated Tcpdump Packages Fix Privilege Dropping Error.” 2003)

```
[root@localhost membrich]# rpm --checksig rhsa-2003-174/*
rhsa-2003-174/tcpdump-3.7.2-1.9.1.i386.rpm: (sha1) dsa sha1 md5 gpg OK
[root@localhost membrich]# rpm -Fvh rhsa-2003-174/*.rpm
Preparing...                ########################################### [100%]
   1:tcpdump                ########################################### [100%]
[root@localhost membrich]#
```

2.1.5.4.4. RHSA-2003-175.

https://rhn.redhat.com/errata/RHSA-2003-175.html
Updated gnupg packages fix validation bug

Advisory: RHSA-2003:175-06
Last updated on: 2003-05-20

i386:
gnupg-1.2.1-4.i386.rpm
[via FTP] [via HTTP]   d0a0ad4a6e8708711d4bd5cae6118767

rpm -Fvh [filenames]

(“Updated Gnupg Packages Fix Validation Bug.” 2003)

```
[root@localhost membrich]# rpm --checksig rhsa-2003-175/*
rhsa-2003-175/gnupg-1.2.1-4.i386.rpm: (sha1) dsa sha1 md5 gpg OK
[root@localhost membrich]# rpm -Fvh rhsa-2003-175/*.rpm
Preparing...                ########################################### [100%]
   1:gnupg                  ########################################### [100%]
[root@localhost membrich]#
```

2.1.5.4.5. RHBA-2003-140.

https://rhn.redhat.com/errata/RHBA-2003-140.html
Updated bash packages fix several bugs

Advisory: RHBA-2003:140-05
Last updated on: 2003-06-23

i386:
bash-2.05b-20.1.i386.rpm
[via FTP] [via HTTP]   fa2aa425bd39ba4a9857dba700227dea

rpm -Fvh [filenames]

(“Updated Bash Packages Fix Several Bugs.” 2003)

```
[root@localhost membrich]# rpm --checksig rhba-2003-140/*
rhba-2003-140/bash-2.05b-20.1.i386.rpm: (sha1) dsa sha1 md5 gpg OK
[root@localhost membrich]# rpm -Fvh rhba-2003-140/*.rpm
Preparing...                ########################################### [100%]
   1:bash                   ########################################### [100%]
[root@localhost membrich]#
```

2.1.5.4.6. RHSA-2003-199.

https://rhn.redhat.com/errata/RHSA-2003-199.html
Updated unzip packages fix trojan vulnerability

Advisory: RHSA-2003:199-14
Last updated on: 2003-08-15

i386:
unzip-5.50-33.i386.rpm
[via FTP] [via HTTP]   e6d52c854a8ebba7dacb678a5edb5cb8

rpm -Fvh [filenames]

(“Updated Unzip Packages Fix Trojan Vulnerability.” 2003)

```
[root@localhost membrich]# rpm --checksig rhsa-2003-199/*
rhsa-2003-199/unzip-5.50-33.i386.rpm: (sha1) dsa sha1 md5 gpg OK
[root@localhost membrich]# rpm -Fvh rhsa-2003-199/*.rpm
Preparing...                ########################################### [100%]
   1:unzip                  ########################################### [100%]
[root@localhost membrich]#
```

2.1.5.4.7. RHBA-2003-263.

https://rhn.redhat.com/errata/RHBA-2003-263.html
Updated 2.4 kernel resolves obscure bugs.

Advisory: RHBA-2003:263-05
Last updated on: 2003-08-20

NOTE: Make sure you get the right kernel-2.4.20-20.9.iX86.rpm file. My server is a Pentium, so I'll use the i586 version. You can check your processor by using "uname -p":

```
[root@localhost membrich]# uname -p
```

```
i586
```

i386:
kernel-2.4.20-20.9.i386.rpm
[via FTP] [via HTTP]   7f855d126d0c66fa68c27b1b699d4d27
i586:
kernel-2.4.20-20.9.i586.rpm
[via FTP] [via HTTP]   0a5456524d186b2bf75325a2f843bd9f
i686:
kernel-2.4.20-20.9.i686.rpm
[via FTP] [via HTTP]   ed8725afb1fdaed2e3038d539043bff0

To install kernel packages manually, use "rpm -ivh <package>" and modify system settings to boot the kernel you have installed. To do this, edit /boot/grub/grub.conf and change the default entry to "default=0" (or, if you have chosen to use LILO as your boot loader, edit /etc/lilo.conf and run lilo)

Do not use "rpm -Uvh" as that will remove your running kernel binaries from your system. You may use "rpm -e" to remove old kernels after determining that the new kernel functions properly on your system.

(“Updated 2.4 Kernel Resolves Obscure Bugs.” 2003)

```
[root@localhost membrich]# rpm --checksig rhba-2003-263/*
rhba-2003-263/kernel-2.4.20-20.9.i586.rpm: (sha1) dsa sha1 md5 gpg OK
[root@localhost membrich]# rpm -ivh rhba-2003-263/*.rpm
Preparing...                ############################################ [100%]
   1:kernel                 ############################################ [100%]
[root@localhost membrich]#
```

Edited /boot/grub/grub.conf, changed default from 1 to 0.

```
[root@localhost membrich]# cp /boot/grub/grub.conf /boot/grub/grub.conf.old
[root@localhost membrich]# vi /boot/grub/grub.conf
```

Changed grub.conf from:

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/hda2
#          initrd /initrd-version.img
#boot=/dev/hda
default=1
timeout=10
splashimage=(hd0,0)/grub/splash.xpm.gz
```

```
title Red Hat Linux (2.4.20-20.9)
        root (hd0,0)
        kernel /vmlinuz-2.4.20-20.9 ro root=LABEL=/
        initrd /initrd-2.4.20-20.9.img
title Red Hat Linux (2.4.20-8)
        root (hd0,0)
        kernel /vmlinuz-2.4.20-8 ro root=LABEL=/
        initrd /initrd-2.4.20-8.img
```

To:

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/hda2
#          initrd /initrd-version.img
#boot=/dev/hda
default=0
timeout=10
splashimage=(hd0,0)/grub/splash.xpm.gz
title Red Hat Linux (2.4.20-20.9)
        root (hd0,0)
        kernel /vmlinuz-2.4.20-20.9 ro root=LABEL=/
        initrd /initrd-2.4.20-20.9.img
title Red Hat Linux (2.4.20-8)
        root (hd0,0)
        kernel /vmlinuz-2.4.20-8 ro root=LABEL=/
        initrd /initrd-2.4.20-8.img
```

Changing the "default" setting from 1 to 0 means it'll boot the first kernel listed rather than the second by default. You can still manually select the second kernel at boot time. We want to boot the first kernel because that's the newer one, the one we just installed.

Reboot the server:

```
[root@localhost membrich]# /sbin/shutdown -r now

Broadcast message from root (pts/0) (Tue Nov 11 00:27:16 2003):

The system is going down for reboot NOW!
```

Got some garbage during grub part of boot, because I removed the "redhat-logos" package. To fix this, remove the "splashimage" line from grub.conf.

Changed /boot/grub/grub.conf from:

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/hda2
#          initrd /initrd-version.img
#boot=/dev/hda
default=0
timeout=10
splashimage=(hd0,0)/grub/splash.xpm.gz
title Red Hat Linux (2.4.20-20.9)
        root (hd0,0)
        kernel /vmlinuz-2.4.20-20.9 ro root=LABEL=/
        initrd /initrd-2.4.20-20.9.img
title Red Hat Linux (2.4.20-8)
        root (hd0,0)
        kernel /vmlinuz-2.4.20-8 ro root=LABEL=/
        initrd /initrd-2.4.20-8.img
```

To:

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/hda2
#          initrd /initrd-version.img
#boot=/dev/hda
default=0
timeout=10
#splashimage=(hd0,0)/grub/splash.xpm.gz
title Red Hat Linux (2.4.20-20.9)
        root (hd0,0)
        kernel /vmlinuz-2.4.20-20.9 ro root=LABEL=/
        initrd /initrd-2.4.20-20.9.img
title Red Hat Linux (2.4.20-8)
        root (hd0,0)
        kernel /vmlinuz-2.4.20-8 ro root=LABEL=/
        initrd /initrd-2.4.20-8.img
```

Rebooted again:

```
[root@localhost membrich]# /sbin/shutdown -r now

Broadcast message from root (pts/0) (Tue Nov 11 00:27:16 2003):

The system is going down for reboot NOW!
```

That fixed it, got the text-based version of Grub this time.

Once we're satisfied that the new kernel works, we can remove the old kernel by simply removing the old kernel's package:

```
[root@localhost membrich]# rpm -qa | grep kernel
kernel-2.4.20-20.9
kernel-2.4.20-8
[root@localhost membrich]# rpm -e kernel-2.4.20-8
```

Removing the package also removes the entry from grub.conf:

```
[root@localhost membrich]# cat /boot/grub/grub.conf
```

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/hda2
#          initrd /initrd-version.img
#boot=/dev/hda
default=0
timeout=10
#splashimage=(hd0,0)/grub/splash.xpm.gz
title Red Hat Linux (2.4.20-20.9)
        root (hd0,0)
        kernel /vmlinuz-2.4.20-20.9 ro root=LABEL=/
        initrd /initrd-2.4.20-20.9.img
[root@localhost membrich]#
```

2.1.5.4.8. RHSA-2003-279.

https://rhn.redhat.com/errata/RHSA-2003-279.html
Updated OpenSSH packages fix potential vulnerabilities

Advisory: RHSA-2003:279-17
Last updated on: 2003-09-17

i386:
openssh-3.5p1-11.i386.rpm
[via FTP] [via HTTP]   8598eddc12b2f06c34464a24d549d9af
openssh-clients-3.5p1-11.i386.rpm
[via FTP] [via HTTP]   922cf88933eeda965d6ad7534051c17e
openssh-server-3.5p1-11.i386.rpm
[via FTP] [via HTTP]   f58b37fc0290039448c450c3eb9630df

rpm -Fvh [filenames]

(“Updated OpenSSH Packages Fix Potential Vulnerabilities.” 2003)

```
[root@localhost membrich]# rpm --checksig rhsa-2003-279/*
rhsa-2003-279/openssh-3.5p1-11.i386.rpm: (sha1) dsa sha1 md5 gpg OK
rhsa-2003-279/openssh-clients-3.5p1-11.i386.rpm: (sha1) dsa sha1 md5 gpg OK
rhsa-2003-279/openssh-server-3.5p1-11.i386.rpm: (sha1) dsa sha1 md5 gpg OK
[root@localhost membrich]# rpm -Fvh rhsa-2003-279/*.rpm
Preparing...                ########################################### [100%]
   1:openssh                ########################################### [ 33%]
   2:openssh-clients        ########################################### [ 67%]
   3:openssh-server         ########################################### [100%]
[root@localhost membrich]#
```

2.1.5.4.9. RHSA-2003-292.

https://rhn.redhat.com/errata/RHSA-2003-292.html

Updated OpenSSL packages fix vulnerabilities

Advisory: RHSA-2003:292-12
Last updated on: 2003-09-30

i386:
openssl-0.9.7a-20.i386.rpm
[via FTP] [via HTTP]   91269d6393def01e0a796e40b74a970d
openssl-devel-0.9.7a-20.i386.rpm
[via FTP] [via HTTP]   957ff6ab058b3041a9995a93698a0cca
i686:
openssl-0.9.7a-20.i686.rpm
[via FTP] [via HTTP]   4fc16039f6893f039cd36b83c37a4fa6

To update all RPMs for your particular architecture, run:

rpm -Fvh [filenames]

("Updated OpenSSL Packages Fix Vulnerabilities." 2003)

```
[root@localhost membrich]# rpm --checksig rhsa-2003-292/*
rhsa-2003-292/openssl-0.9.7a-20.i386.rpm: (sha1) dsa sha1 md5 gpg OK
rhsa-2003-292/openssl-devel-0.9.7a-20.i386.rpm: (sha1) dsa sha1 md5 gpg OK
 [root@localhost membrich]# rpm -Fvh rhsa-2003-292/*.rpm
Preparing...                ########################################### [100%]
   1:openssl                ########################################### [ 50%]
   2:openssl-devel          ########################################### [100%]
[root@localhost membrich]#
```

2.1.5.4.10. RHSA-2003-256.

https://rhn.redhat.com/errata/RHSA-2003-256.html
Updated Perl packages fix security issues.

Advisory: RHSA-2003:256-15
Last updated on: 2003-10-03

i386:
perl-5.8.0-88.3.i386.rpm
[via FTP] [via HTTP]   0ac800e33acab6522169d72dac29721b
perl-CGI-2.81-88.3.i386.rpm
[via FTP] [via HTTP]   cc53faea268b17b68d1494e9cd4d442b

To update all RPMs for your particular architecture, run:

rpm -Fvh [filenames]

(“Updated Perl Packages Fix Security Issues.” 2003)

```
[root@localhost membrich]# rpm --checksig rhsa-2003-256/*.rpm
rhsa-2003-256/perl-5.8.0-88.3.i386.rpm: (sha1) dsa sha1 md5 gpg OK
rhsa-2003-256/perl-CGI-2.81-88.3.i386.rpm: (sha1) dsa sha1 md5 gpg OK
[root@localhost membrich]# rpm -Fvh rhsa-2003-256/*.rpm
Preparing...                ########################################### [100%]
   1:perl                   ########################################### [ 50%]
   2:perl-CGI               ########################################### [100%]
[root@localhost membrich]#
```

2.1.5.4.11. RHSA-2003-281.

https://rhn.redhat.com/errata/RHSA-2003-281.html
Updated MySQL packages fix vulnerability

Advisory: RHSA-2003:281-08
Last updated on: 2003-10-09

i386:
mysql-3.23.58-1.9.i386.rpm
[via FTP] [via HTTP]   aa674d9d284788f8c354f3f20b6aec57
mysql-devel-3.23.58-1.9.i386.rpm
[via FTP] [via HTTP]   8eac37417227bf2c0c7d13a2eafcb80f
mysql-server-3.23.58-1.9.i386.rpm
[via FTP] [via HTTP]   78b516147ff717a2db347260e85e6688

(“Updated MySQL Packages Fix Vulnerability.” 2003)

no instructions, assuming "rpm -Fvh"

```
[root@localhost membrich]# rpm --checksig rhsa-2003-281/*.rpm
rhsa-2003-281/mysql-3.23.58-1.9.i386.rpm: (sha1) dsa sha1 md5 gpg OK
rhsa-2003-281/mysql-devel-3.23.58-1.9.i386.rpm: (sha1) dsa sha1 md5 gpg OK
rhsa-2003-281/mysql-server-3.23.58-1.9.i386.rpm: (sha1) dsa sha1 md5 gpg OK
[root@localhost membrich]# rpm -Fvh rhsa-2003-281/*.rpm
Preparing...                ########################################### [100%]
   1:mysql                  ########################################### [ 33%]
   2:mysql-devel            ########################################### [ 67%]
   3:mysql-server           ########################################### [100%]
[root@localhost membrich]#
```

2.1.5.4.12. RHSA-2003-309.

https://rhn.redhat.com/errata/RHSA-2003-309.html
Updated fileutils/coreutils package fix ls vulnerabilities

Advisory: RHSA-2003:309-08
Last updated on: 2003-11-03

i386:
coreutils-4.5.3-19.0.2.i386.rpm
[via FTP] [via HTTP]   da3fc5f54917452a4fa704330e193e24

To update all RPMs for your particular architecture, run:

rpm -Fvh [filenames]

(“Updated Fileutils/Coreutils Package Fix ls Vulnerabilities.” 2003)

```
[root@localhost membrich]# rpm --checksig rhsa-2003-309/*.rpm
rhsa-2003-309/coreutils-4.5.3-19.0.2.i386.rpm: (sha1) dsa sha1 md5 gpg OK
[root@localhost membrich]# rpm -Fvh rhsa-2003-309/*.rpm
Preparing...                ########################################### [100%]
   1:coreutils              ########################################### [100%]
[root@localhost membrich]#
```

2.2. Install 3rd Party Applications.

2.2.1. Mysql.

Already installed by RPMs, but does not have the script to cause it to start automatically. Need to link an /etc/rcX.d/S??????????? to /etc/init.d/mysqld

```
[root@localhost membrich]# ln -s /etc/init.d/mysqld /etc/rc3.d/S98mysqld
lrwxrwxrwx    1 root     root           18 Nov 14 00:41 /etc/rc3.d/S98mysqld ->
/etc/init.d/mysqld
[root@localhost membrich]#
```

Reboot to make sure it works:

```
[root@localhost membrich]# ps -eaf | grep sql
root       564     1  0 00:44 ?        00:00:00 /bin/sh /usr/bin/safe_mysqld --
defaults-file=/etc/my.cnf
mysql      598   564  0 00:44 ?        00:00:00 /usr/libexec/mysqld --defaults-
file=/etc/my.cnf --basedir=/usr --datadir=/var/lib/mysql --user=mysql --pid-
file=/var/run/mysqld/mysqld.pid --skip-locking
root       666   639  0 00:45 pts/0    00:00:00 grep sql
[root@localhost membrich]#
```

Need to change the password for mysql (it starts out blank):

```
[root@localhost membrich]# mysqladmin -u root password <your password>
```

Test your password.

```
[root@localhost membrich]# mysql -u root -p
```

```
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2 to server version: 3.23.58

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> quit
Bye
[root@localhost membrich]#
```

2.2.2. Snort.

Got latest version from http://www.snort.org/dl/
At the time of this writing, the latest version is 2.0.4.
Get the MD5 file too, so you can check the signature.

2.2.2.1. Check the MD5 Signature.

```
[membrich@localhost membrich]$ md5sum snort-2.0.4.tar.gz
8cff1ab5b6ab0ff507fb7264a05be05b  snort-2.0.4.tar.gz
[membrich@localhost membrich]$ cat snort-2.0.4.tar.gz.gz
md5  : 8cff1ab5b6ab0ff507fb7264a05be05b  snort-2.0.4.tar.gz
sha1 : 9ae95612d05c8bd605c689353f38d919a0d753ba  snort-2.0.4.tar.gz
```

Looks good.

2.2.2.2. Install Snort.

```
[membrich@localhost membrich]$ gunzip snort-2.0.4.tar.gz
[membrich@localhost membrich]$ tar -xvf snort-2.0.4.tar
[membrich@localhost membrich]$ cd snort-2.0.4
[membrich@localhost snort-2.0.4]$ ./configure --with-mysql
[membrich@localhost snort-2.0.4]$ make
[membrich@localhost snort-2.0.4]$ su
Password:
[root@localhost snort-2.0.4]# make install
```

2.2.2.3. Set Up Snort Config and Rules Files.

Copy the config files and rules over:

```
[root@localhost snort-2.0.4]# mkdir /usr/local/snort
[root@localhost snort-2.0.4]# cp etc/*.conf /usr/local/snort
[root@localhost snort-2.0.4]# cp etc/*.config /usr/local/snort
[root@localhost snort-2.0.4]# cp -r rules /usr/local/snort
```

Here's how it'll look:

```
[root@localhost snort-2.0.4]# ls /usr/local/snort
classification.config  reference.config  rules  snort.conf
[root@localhost snort-2.0.4]# ls /usr/local/snort/rules
attack-responses.rules  icmp.rules        other-ids.rules  telnet.rules
backdoor.rules          imap.rules        p2p.rules        tftp.rules
bad-traffic.rules       info.rules        policy.rules     virus.rules
chat.rules              local.rules       pop2.rules       web-attacks.rules
```

```
ddos.rules              Makefile          pop3.rules       web-cgi.rules
deleted.rules           Makefile.am       porn.rules       web-client.rules
dns.rules               Makefile.in       rpc.rules        web-coldfusion.rules
dos.rules               misc.rules        rservices.rules  web-frontpage.rules
experimental.rules      multimedia.rules  scan.rules       web-iis.rules
exploit.rules           mysql.rules       shellcode.rules  web-misc.rules
finger.rules            netbios.rules     smtp.rules       web-php.rules
ftp.rules               nntp.rules        snmp.rules       x11.rules
icmp-info.rules         oracle.rules      sql.rules
[root@localhost snort-2.0.4]#
```

Set up the config file:

```
[root@localhost snort-2.0.4]# vi /usr/local/snort/snort.conf
```

Set the HOME_NET variable:

```
#var HOME_NET any
var HOME_NET [172.16.0.0/16]
```

Set the RULE_PATH variable:

```
# Path to your rules files (this can be a relative path)
#var RULE_PATH ../rules
var RULE_PATH /usr/local/snort/rules
```

(Optional: I find this preprocessor useful.) Turn on portscan preprocessor:

```
preprocessor portscan: $HOME_NET 4 3 portscan.log
```

Set up database output:

```
# database: log to a variety of databases
# ---------------------------------------
# See the README.database file for more information about configuring
# and using this plugin.
#
# output database: log, mysql, user=root password=test dbname=db host=localhost
output database: log, mysql, user=snort password=<your password> dbname=snort
host=localhost
```

Turn on all rulesets except ICMP_INFO:

```
include $RULE_PATH/other-ids.rules
include $RULE_PATH/web-attacks.rules
include $RULE_PATH/backdoor.rules
include $RULE_PATH/shellcode.rules
include $RULE_PATH/policy.rules
include $RULE_PATH/porn.rules
include $RULE_PATH/info.rules
# include $RULE_PATH/icmp-info.rules
include $RULE_PATH/virus.rules
include $RULE_PATH/chat.rules
include $RULE_PATH/multimedia.rules
include $RULE_PATH/p2p.rules
```

2.2.3. Nmap (Optional, if you want to install Nessus, you need Nmap.)

Got latest version from http://www.insecure.org/nmap/nmap_download.html

2.2.3.1. Check MD5 Signature.

Got md5 signatures from:
http://seclists.org/lists/nmap-hackers/2003/Oct-Dec/0000.html

> For the more paranoid (smart) members of the list, here are the md5 hashes:
>
> ```
> 6235bed7670833e971ece3d560ab4bf6 nmap-3.48-1.i386.rpm
> a1eb700d736ce475db9dd8259b90c42c nmap-3.48-1.src.rpm
> 8c38559a863efd476c5b042123f1ee3a nmap-3.48.tar.bz2
> e8be0d30326ba0af5e07d3593609143c nmap-3.48.tgz
> 99d04fd44c34ab1eabb1a15c80f232e7 nmap-3.48-win32.zip
> 125b65a40b2bcb8c7acc399e8fa206fd nmap-frontend-3.48-1.i386.rpm
> ```
>
> (Fyoder 2003)

Had difficulty installing from source code, so switched to using the rpm:

```
[membrich@localhost membrich]$ md5sum nmap-3.48-1.i386.rpm
6235bed7670833e971ece3d560ab4bf6  nmap-3.48-1.i386.rpm
```

MD5 signature looks good. Time to install:

2.2.3.2. Install Nmap.

```
[membrich@localhost membrich]$ rpm -ivh nmap-3.48-1.i386.rpm
error: Failed dependencies:
        libstdc++-libc6.2-2.so.3 is needed by nmap-3.48-1
```

Had to install another package that nmap requires:

```
[root@localhost membrich]# mount -t iso9660 /dev/cdrom /mnt/cdrom
mount: block device /dev/cdrom is write-protected, mounting read-only
[root@localhost membrich]# ls /mnt/cdrom/RedHat/RPMS | grep libstdc
compat-libstdc++-7.3-2.96.118.i386.rpm
compat-libstdc++-devel-7.3-2.96.118.i386.rpm
libstdc++-3.2.2-5.i386.rpm
[root@localhost membrich]# rpm -ivh /mnt/cdrom/RedHat/RPMS/compat-libstdc++-7.3-
2.96.118.i386.rpm
Preparing...                ########################################### [100%]
   1:compat-libstdc++       ########################################### [100%]
[root@localhost membrich]#
```

Install nmap:

```
[root@localhost membrich]# rpm -ivh nmap-3.48-1.i386.rpm
Preparing...                ########################################### [100%]
   1:nmap                   ########################################### [100%]
[root@localhost membrich]#
```

Test it:

```
[root@localhost membrich]# nmap -sT localhost

Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2003-11-15 15:14 PST
Interesting ports on localhost.localdomain (127.0.0.1):
(The 1655 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
22/tcp   open  ssh
3306/tcp open  mysql

Nmap run completed -- 1 IP address (1 host up) scanned in 0.777 seconds
[root@localhost membrich]#
```

Looks good.

2.2.4. Nessus (Optional).

Got latest version from http://www.nessus.org/download.html

2.2.4.1. Check the MD5 Signatures.

```
[membrich@localhost membrich]$ cat MD5
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

MD5 (libnasl-2.0.9.tar.gz) = 7626cc58afaa44a3f44f2fb1a31c5ea4
MD5 (nessus-core-2.0.9.tar.gz) = 7bdbdb663d87a894cf8f99b33a5eb8b5
MD5 (nessus-libraries-2.0.9.tar.gz) = 6bca1afa20e48886cde4fe98308efdf3
MD5 (nessus-plugins-2.0.9.tar.gz) = afc233b099a0b36f828d72f891f94721
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.2.3 (Darwin)

iD8DBQE/qXlW8JEETRRZWhoRAiVZAJ0YG3JNkdnqKx4SeeCmapXA9dK9oQCePl0O
C4DePRaWoCvQmo4cf8VWbyA=
=CQQB
-----END PGP SIGNATURE-----
[membrich@localhost membrich]$ md5sum libnasl-2.0.9.tar.gz nessus*
7626cc58afaa44a3f44f2fb1a31c5ea4  libnasl-2.0.9.tar.gz
7bdbdb663d87a894cf8f99b33a5eb8b5  nessus-core-2.0.9.tar.gz
6bca1afa20e48886cde4fe98308efdf3  nessus-libraries-2.0.9.tar.gz
afc233b099a0b36f828d72f891f94721  nessus-plugins-2.0.9.tar.gz
```

There are four parts to install, the order is important.

2.2.4.2. Nessus Libraries.

```
[membrich@localhost membrich]$ gunzip nessus-libraries-2.0.9.tar.gz
[membrich@localhost membrich]$ tar -xvf nessus-libraries-2.0.9.tar
[membrich@localhost membrich]$ cd nessus-libraries
[membrich@localhost nessus-libraries]$ ./configure
[membrich@localhost nessus-libraries]$ make
[membrich@localhost nessus-libraries]$ su
Password:
[root@localhost nessus-libraries]# make install
```

```
--------------------------------------------------------------
 nessus-libraries has been sucessfully installed.
 Make sure that /usr/local/bin is in your PATH before you
 continue
 Be sure to add /usr/local/lib in /etc/ld.so.conf and type 'ldconfig'
 --------------------------------------------------------------
```

Added /usr/local/lib to /etc/ld.so.conf:

```
[root@rocket nessus-libraries]# cat /etc/ld.so.conf
/usr/kerberos/lib
/usr/lib/mysql
/usr/local/lib
[root@rocket nessus-libraries]# /sbin/ldconfig
```

Path has /usr/local/bin:

```
[root@localhost nessus-libraries]# echo $PATH
/usr/local/bin:/bin:/usr/bin:/usr/X11R6/bin:/home/membrich/bin
```

2.2.4.3. Libnasl.

```
[membrich@localhost membrich]$ gunzip libnasl-2.0.9.tar.gz
[membrich@localhost membrich]$ tar -xvf libnasl-2.0.9.tar
[membrich@localhost membrich]$ cd libnasl
[membrich@localhost libnasl]$ ./configure
[membrich@localhost libnasl]$ make
[membrich@localhost libnasl]$ su
Password:
[root@localhost libnasl]# make install
```

2.2.4.4. Nessus Core.

```
[membrich@localhost membrich]$ gunzip nessus-core-2.0.9.tar.gz
[membrich@localhost membrich]$ tar -xvf nessus-core-2.0.9.tar
[membrich@localhost membrich]$ cd nessus-core
[membrich@localhost nessus-core]$ ./configure --disable-gtk
[membrich@localhost nessus-core]$ make
[membrich@localhost nessus-core]$ su
Password:
[root@localhost nessus-core]# make install

--------------------------------------------------------------
 nessus-core has been sucessfully installed.
 Make sure that /usr/local/bin and /usr/local/sbin are in your PATH before
 you continue.
 nessusd has been installed into /usr/local/sbin
 --------------------------------------------------------------
```

Edited my .bash_profile, added /usr/local/sbin to the PATH statement. Changed .bash_profile from:

```
# .bash_profile

# Get the aliases and functions
if [ -f ~/.bashrc ]; then
        . ~/.bashrc
```

```
fi

# User specific environment and startup programs

PATH=$PATH:$HOME/bin

export PATH
unset USERNAME
```

To:

```
# .bash_profile

# Get the aliases and functions
if [ -f ~/.bashrc ]; then
        . ~/.bashrc
fi

# User specific environment and startup programs

PATH=$PATH:$HOME/bin:/usr/local/sbin

export PATH
unset USERNAME
```

Log out, log back in to make sure /usr/local/sbin has been added to the path:

```
[membrich@localhost membrich]$ echo $PATH
/usr/local/bin:/bin:/usr/bin:/usr/X11R6/bin:/home/membrich/bin:/usr/local/sbin
[membrich@localhost membrich]$
```

2.2.4.4. Nessus Plugins.

```
[membrich@localhost membrich]$ gunzip nessus-plugins-2.0.9.tar.gz
[membrich@localhost membrich]$ tar -xvf nessus-plugins-2.0.9.tar
[membrich@localhost membrich]$ cd nessus-plugins
[membrich@localhost nessus-plugins]$ ./configure
[membrich@localhost nessus-plugins]$ make
[membrich@localhost nessus-plugins]$ su
Password:
[root@localhost nessus-plugins]# make install
```

2.2.4.5. Setup Nessus.

2.2.4.5.1. Create a Nessus User Account.

```
[membrich@localhost membrich]$ su
Password:
[root@localhost membrich]# nessus-adduser
nessusd: error while loading shared libraries: libnasl.so.2: cannot open shared object
file: No such file or directory
Executing nessusd failed. Make sure your library loader is configured properly and
that nessusd is in your $PATH
[root@localhost membrich]# cat /etc/ld.so.conf
/usr/kerberos/lib
/usr/lib/mysql
/usr/local/lib
[root@localhost membrich]# /sbin/ldconfig
```

```
[root@localhost membrich]# nessus-adduser
Using /var/tmp as a temporary file holder

Add a new nessusd user
----------------------


Login : nessus
Authentication (pass/cert) [pass] :
Login password : <your password>

User rules
----------
nessusd has a rules system which allows you to restrict the hosts
that nessus has the right to test. For instance, you may want
him to be able to scan his own host only.

Please see the nessus-adduser(8) man page for the rules syntax

Enter the rules for this user, and hit ctrl-D once you are done :
(the user can have an empty rules set)


Login             : nessus
Password          : nessus
DN                :
Rules             :


Is that ok ? (y/n) [y]
user added.
[root@localhost membrich]#
```

2.2.4.5.2. Create Nessus Certificate.

```
[root@localhost membrich]# nessus-mkcert

--------------------------------------------------------------------------------
                        Creation of the Nessus SSL Certificate
--------------------------------------------------------------------------------

This script will now ask you the relevant information to create the SSL
certificate of Nessus. Note that this information will *NOT* be sent to
anybody (everything stays local), but anyone with the ability to connect to your
Nessus daemon will be able to retrieve this information.


CA certificate life time in days [1460]:
Server certificate life time in days [365]:
Your country (two letter code) [FR]: US
Your state or province name [none]: CA
Your location (e.g. town) [Paris]: Hayward
Your organization [Nessus Users United]: My Company

--------------------------------------------------------------------------------
                        Creation of the Nessus SSL Certificate
--------------------------------------------------------------------------------

Congratulations. Your server certificate was properly created.

/usr/local/etc/nessus/nessusd.conf updated
```

```
The following files were created :

. Certification authority :
   Certificate = /usr/local/com/nessus/CA/cacert.pem
   Private key = /usr/local/var/nessus/CA/cakey.pem

. Nessus Server :
    Certificate = /usr/local/com/nessus/CA/servercert.pem
    Private key = /usr/local/var/nessus/CA/serverkey.pem

Press [ENTER] to exit
```

2.2.4.5.3. Start the Nessus Daemon.

```
[root@localhost membrich]# nessusd -D
[root@localhost membrich]# ps -eaf | grep nessus
root     30099     1  0 16:48 ?        00:00:00 nessusd: waiting for incoming
connections
root     30101 29966  2 16:48 pts/0    00:00:00 grep nessus
```

2.2.4.5.4. Test it.

```
[root@localhost membrich]# echo 172.16.1.253 > hosts
[root@localhost membrich]# cat hosts
172.16.1.253
[root@localhost membrich]# nessus -q localhost 1241 nessus <password> hosts test
Please choose your level of SSL paranoia (Hint: if you want to manage many
servers from your client, choose 2. Otherwise, choose 1, or 3, if you are
paranoid.
2
*** The plugins that have the ability to crash remote services or hosts
have been disabled. You should activate them if you want your security
audit to be complete
[root@localhost membrich]#
```

2.2.4.5.5. Results.

```
[root@localhost membrich]# cat test
172.16.1.253|ssh (22/tcp)|11712|INFO|;You are running OpenSSH-portable 3.6.1 or
older.;;There is a flaw in this version which may allow an attacker to;bypass the
access controls set by the administrator of this server.;;OpenSSH features a mechanism
which can restrict the list of;hosts a given user can log from by specifying a
pattern;in the user key file (ie: *.mynetwork.com would let a user;connect only from
the local network).;;However there is a flaw in the way OpenSSH does reverse DNS
lookups.;If an attacker configures his DNS server to send a numeric IP address;when a
reverse lookup is performed, he may be able to circumvent;this mechanism.;;Solution :
Upgrade to OpenSSH 3.6.2 when it comes out;Risk Factor : Low;CVE : CAN-2003-0386;BID :
7831;
172.16.1.253|ssh (22/tcp)|10882|INFO|;The remote SSH daemon supports connections
made;using the version 1.33 and/or 1.5 of the SSH protocol.;;These protocols are not
completely cryptographically;safe so they should not be used.;;Solution : ; If you use
OpenSSH, set the option 'Protocol' to '2'; If you use SSH.com's set the option
'Ssh1Compatibility' to 'no';  ;Risk factor : Low;
172.16.1.253|ssh (22/tcp)|10881|NOTE|The remote SSH daemon supports the following
versions of the;SSH protocol :;;  . 1.33;  . 1.5;  . 1.99;  . 2.0;;
172.16.1.253|nessus (1241/tcp)|10147|INFO|A Nessus Daemon is listening on this port.;
172.16.1.253|ssh (22/tcp)|11574|INFO|;You are running OpenSSH-portable 3.6.1p1 or
older.;;If PAM support is enabled, an attacker may use a flaw in this version;to
determine the existence or a given login name by comparing the times;the remote sshd
daemon takes to refuse a bad password for a non-existant;login compared to the time it
```

```
takes to refuse a bad password for a;valid login.;;An attacker may use this flaw to
set up  a brute force attack against;the remote host.;;*** Nessus did not check
whether the remote SSH daemon is actually;*** using PAM or not, so this might be a
false positive;;Solution : Upgrade to OpenSSH-portable 3.6.1p2 or newer;Risk Factor :
Low;CVE : CAN-2003-0190;BID : 7482, 7467, 7342;
172.16.1.253|nessus (1241/tcp)|10863|NOTE|This TLSv1 server does not accept SSLv2
connections.;This TLSv1 server does not accept SSLv3 connections.;;
172.16.1.253|nessus (1241/tcp)|10863|NOTE|Here is the TLSv1 server
certificate:;Certificate:;    Data:;        Version: 3 (0x2);        Serial Number: 1
(0x1);        Signature Algorithm: md5WithRSAEncryption;        Issuer: C=US, ST=CA,
L=Hayward, O=My Company, OU=Certification Authority for localhost.localdomain,
CN=localhost.localdomain/emailAddress=ca@localhost.localdomain;        Validity;
Not Before: Nov 16 00:44:15 2003 GMT;            Not After : Nov 15 00:44:15 2004 GMT;
Subject: C=US, ST=CA, L=Hayward, O=My Company, OU=Server certificate for
localhost.localdomain,
CN=localhost.localdomain/emailAddress=nessusd@localhost.localdomain;        Subject
Public Key Info:;            Public Key Algorithm: rsaEncryption;            RSA
Public Key: (1024 bit);                Modulus (1024 bit):;
00:c2:f9:a9:09:b1:93:35:c3:3a:85:ff:4b:28:8f:;
68:38:e6:af:0e:13:4f:05:29:60:a2:4a:4e:d1:49:;
12:d7:c3:a6:cd:19:4c:86:61:4c:58:f7:51:25:d9:;
a7:bd:94:41:64:2e:f4:85:1a:06:c0:17:b5:3f:78:;
e6:82:db:15:64:db:27:00:fd:62:58:d9:dc:71:43:;
e9:2b:3c:3e:f2:42:39:9f:ac:72:c8:ef:e4:fe:df:;
cc:45:81:6c:0f:84:2e:31:b3:85:61:4e:7b:f9:d0:;
88:6a:57:97:f5:98:0c:4e:ab:36:9f:cb:60:ab:60:;
89:fc:30:a9:70:f6:e9:e7:8b;                Exponent: 65537 (0x10001);        X509v3
extensions:;            Netscape Cert Type: ;            SSL Server;            X509v3
Key Usage: ;            Digital Signature, Non Repudiation, Key Encipherment;
Netscape Comment: ;            OpenSSL Generated Certificate;            X509v3
Subject Key Identifier: ;
6A:15:6E:B1:96:69:B6:95:53:A6:11:F4:A3:A0:35:C6:B8:2E:82:6A;            X509v3
Authority Key Identifier: ;
keyid:07:A8:B8:BE:C3:44:E8:EF:98:D7:CB:74:59:DF:BB:2F:CC:81:A0:2B;
DirName:/C=US/ST=CA/L=Hayward/O=My Company/OU=Certification Authority for
localhost.localdomain/CN=localhost.localdomain/emailAddress=ca@localhost.localdomain;
serial:00;;            X509v3 Subject Alternative Name: ;
email:nessusd@localhost.localdomain;            X509v3 Issuer Alternative Name: ;
<EMPTY>;;    Signature Algorithm: md5WithRSAEncryption;
4b:eb:02:df:6b:72:33:66:e7:6f:27:08:c9:02:54:a8:24:b5:;
cf:15:85:e2:a7:fa:d0:80:9d:df:55:82:c8:9f:96:54:b1:7b:;
af:f5:4d:ed:b1:b7:e4:6f:47:c4:eb:fc:1e:bc:cf:d9:5a:c1:;
ae:f9:18:eb:aa:7d:1b:bb:55:18:e0:6a:56:40:36:f3:09:80:;
e0:3d:3c:82:4b:6b:a6:4a:27:57:a7:81:90:de:c9:f0:4f:44:;
ca:1e:21:50:1b:7c:6c:76:77:82:8d:92:6d:4a:fb:77:ea:ff:;
31:50:79:fc:3c:03:44:c7:d7:26:4c:8b:40:3b:de:ad:65:a7:;        98:b2;;
172.16.1.253|ssh (22/tcp)|11837|REPORT|;You are running a version of OpenSSH which is
older than 3.7.1;;Versions older than 3.7.1 are vulnerable to a flaw in the buffer
management;functions which might allow an attacker to execute arbitrary commands on
this ;host.;;An exploit for this issue is rumored to exist.;;;Note that several
distribution patched this hole without changing;the version number of OpenSSH. Since
Nessus solely relied on the;banner of the remote SSH server to perform this check,
this might;be a false positive.;;If you are running a RedHat host, make sure that the
command :;          rpm -q openssh-server;   ;Returns :; openssh-server-3.1p1-13
(RedHat 7.x); openssh-server-3.4p1-7  (RedHat 8.0); openssh-server-3.5p1-11 (RedHat
9);;Solution : Upgrade to OpenSSH 3.7.1;See also :
http://marc.theaimsgroup.com/?l=openbsd-misc&m=106375452423794&w=2;
http://marc.theaimsgroup.com/?l=openbsd-misc&m=106375456923804&w=2;Risk factor :
High;CVE : CAN-2003-0693, CAN-2003-0695;BID : 8628;
172.16.1.253|ssh (22/tcp)|10267|NOTE|Remote SSH version : SSH-1.99-OpenSSH_3.5p1;
172.16.1.253|nessus (1241/tcp)|10330|NOTE|A TLSv1 server answered on this port;;
172.16.1.253|mysql (3306/tcp)|10330|NOTE|An unknown service is running on this
port.;It is usually reserved for MySQL;
```

```
172.16.1.253|ssh (22/tcp)|10330|NOTE|An ssh server is running on this port;
172.16.1.253|mysql (3306/tcp)
172.16.1.253|nessus (1241/tcp)
172.16.1.253|ssh (22/tcp)
[root@localhost membrich]#
```

2.2.4.5.6. Disable SSH Version 1 Support.

To remove ssh version 1 support, edit /etc/ssh/sshd_config:

```
[root@localhost membrich]# vi /etc/ssh/sshd_config
```

Changed the protocol setting from:

```
#Protocol 2,1
```

To:

```
Protocol 2
```

Restart sshd:

```
[root@localhost membrich]# pkill -HUP sshd
```

2.2.4.5.7. Disable Mysql Port.

We don't need mysql to listen for input from any other host.
Fixed mysql open port (TCP 3306)
Edited /etc/my.cnf:

Found the setting that I wanted in the "man mysqld" output:

```
       --skip-networking
              Don't  listen  for  TCP/IP  connections at all. All
              interaction with mysqld must be made via Unix sock-
              ets.  This option is highly recommended for systems
              where only local  requests  are  allowed.  However,
              this  option  is  unsuitable  for  systems that use
              MIT-pthreads,  because  the  MIT-pthreads   package
              doesn't support Unix sockets.
```

The way to implement this option is to add it to the /etc/my.cnf file.

Change it from:

```
[mysqld]
datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock

[mysql.server]
user=mysql
basedir=/var/lib
```

```
[safe_mysqld]
err-log=/var/log/mysqld.log
pid-file=/var/run/mysqld/mysqld.pid
```

To:

```
[mysqld]
datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock
skip-networking

[mysql.server]
user=mysql
basedir=/var/lib

[safe_mysqld]
err-log=/var/log/mysqld.log
pid-file=/var/run/mysqld/mysqld.pid
```

Restart mysqld:

```
[root@localhost membrich]# /etc/init.d/mysqld restart
Stopping MySQL:                                            [  OK  ]
Starting MySQL:                                            [  OK  ]
[root@localhost membrich]#
```

Check it:
Make sure mysql is running:

```
[root@localhost membrich]# ps -eaf | grep mysql
root     30529     1  0 17:13 pts/1    00:00:00 /bin/sh /usr/bin/safe_mysqld --
defaults-file=/etc/my.cnf
mysql    30559 30529  0 17:13 pts/1    00:00:00 /usr/libexec/mysqld --defaults-
file=/etc/my.cnf --basedir=/usr --datadir=/var/lib/mysql --user=mysql --pid-
file=/var/run/mysqld/mysqld.pid --skip-locking
root     30564 30484  0 17:14 pts/1    00:00:00 grep mysql
```

It is running, so check if the port is still open:

```
[root@localhost membrich]# netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:1241            0.0.0.0:*               LISTEN
tcp        0      0 172.16.1.253:22         172.16.1.33:2938        ESTABLISHED
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node Path
unix  2      [ ACC ]     STREAM     LISTENING     36144  /var/lib/mysql/mysql.sock
unix  4      [ ]         DGRAM                    1437   /dev/log
unix  3      [ ]         STREAM     CONNECTED     36044
unix  3      [ ]         STREAM     CONNECTED     36043
unix  2      [ ]         DGRAM                    1587
unix  2      [ ]         DGRAM                    1447
[root@localhost membrich]#
```

TCP 3306 is no longer open.

2.2.4.5.8. Run Nessus Again.

```
[root@localhost membrich]# nessus -q localhost 1241 nessus nessus hosts test2
*** The plugins that have the ability to crash remote services or hosts
have been disabled. You should activate them if you want your security
audit to be complete
[root@localhost membrich]#
```

```
[root@localhost membrich]# cat test2
172.16.1.253|ssh (22/tcp)|11712|INFO|;You are running OpenSSH-portable 3.6.1 or
older.;;There is a flaw in this version which may allow an attacker to;bypass the
access controls set by the administrator of this server.;;OpenSSH features a mechanism
which can restrict the list of;hosts a given user can log from by specifying a
pattern;in the user key file (ie: *.mynetwork.com would let a user;connect only from
the local network).;;However there is a flaw in the way OpenSSH does reverse DNS
lookups.;If an attacker configures his DNS server to send a numeric IP address;when a
reverse lookup is performed, he may be able to circumvent;this mechanism.;;Solution :
Upgrade to OpenSSH 3.6.2 when it comes out;Risk Factor : Low;CVE : CAN-2003-0386;BID :
7831;
172.16.1.253|ssh (22/tcp)|10881|NOTE|The remote SSH daemon supports the following
versions of the;SSH protocol :;;  . 1.99;  . 2.0;;
172.16.1.253|nessus (1241/tcp)|10147|INFO|A Nessus Daemon is listening on this port.;
172.16.1.253|ssh (22/tcp)|11574|INFO|;You are running OpenSSH-portable 3.6.1p1 or
older.;;If PAM support is enabled, an attacker may use a flaw in this version;to
determine the existence or a given login name by comparing the times;the remote sshd
daemon takes to refuse a bad password for a non-existant;login compared to the time it
takes to refuse a bad password for a;valid login.;;An attacker may use this flaw to
set up  a brute force attack against;the remote host.;;*** Nessus did not check
whether the remote SSH daemon is actually;*** using PAM or not, so this might be a
false positive;;Solution : Upgrade to OpenSSH-portable 3.6.1p2 or newer;Risk Factor :
Low;CVE : CAN-2003-0190;BID : 7482, 7467, 7342;
172.16.1.253|nessus (1241/tcp)|10863|NOTE|This TLSv1 server does not accept SSLv2
connections.;This TLSv1 server does not accept SSLv3 connections.;;
172.16.1.253|nessus (1241/tcp)|10863|NOTE|Here is the TLSv1 server
certificate:;Certificate:;    Data:;        Version: 3 (0x2);        Serial Number: 1
(0x1);        Signature Algorithm: md5WithRSAEncryption;        Issuer: C=US, ST=CA,
L=Hayward, O=My Company, OU=Certification Authority for localhost.localdomain,
CN=localhost.localdomain/emailAddress=ca@localhost.localdomain;        Validity;
Not Before: Nov 16 00:44:15 2003 GMT;            Not After : Nov 15 00:44:15 2004 GMT;
Subject: C=US, ST=CA, L=Hayward, O=My Company, OU=Server certificate for
localhost.localdomain,
CN=localhost.localdomain/emailAddress=nessusd@localhost.localdomain;        Subject
Public Key Info:;            Public Key Algorithm: rsaEncryption;            RSA
Public Key: (1024 bit);                Modulus (1024 bit):;
00:c2:f9:a9:09:b1:93:35:c3:3a:85:ff:4b:28:8f:;
68:38:e6:af:0e:13:4f:05:29:60:a2:4a:4e:d1:49:;
12:d7:c3:a6:cd:19:4c:86:61:4c:58:f7:51:25:d9:;
a7:bd:94:41:64:2e:f4:85:1a:06:c0:17:b5:3f:78:;
e6:82:db:15:64:db:27:00:fd:62:58:d9:dc:71:43:;
e9:2b:3c:3e:f2:42:39:9f:ac:72:c8:ef:e4:fe:df:;
cc:45:81:6c:0f:84:2e:31:b3:85:61:4e:7b:f9:d0:;
88:6a:57:97:f5:98:0c:4e:ab:36:9f:cb:60:ab:60:;
89:fc:30:a9:70:f6:e9:e7:8b;                Exponent: 65537 (0x10001);        X509v3
extensions:;            Netscape Cert Type: ;            SSL Server;            X509v3
Key Usage: ;            Digital Signature, Non Repudiation, Key Encipherment;
Netscape Comment: ;            OpenSSL Generated Certificate;            X509v3
Subject Key Identifier: ;
6A:15:6E:B1:96:69:B6:95:53:A6:11:F4:A3:A0:35:C6:B8:2E:82:6A;            X509v3
Authority Key Identifier: ;
keyid:07:A8:B8:BE:C3:44:E8:EF:98:D7:CB:74:59:DF:BB:2F:CC:81:A0:2B;
DirName:/C=US/ST=CA/L=Hayward/O=My Company/OU=Certification Authority for
localhost.localdomain/CN=localhost.localdomain/emailAddress=ca@localhost.localdomain;
```

```
serial:00;;            X509v3 Subject Alternative Name: ;
email:nessusd@localhost.localdomain;           X509v3 Issuer Alternative Name: ;
<EMPTY>;;    Signature Algorithm: md5WithRSAEncryption;
4b:eb:02:df:6b:72:33:66:e7:6f:27:08:c9:02:54:a8:24:b5:;
cf:15:85:e2:a7:fa:d0:80:9d:df:55:82:c8:9f:96:54:b1:7b:;
af:f5:4d:ed:b1:b7:e4:6f:47:c4:eb:fc:1e:bc:cf:d9:5a:c1:;
ae:f9:18:eb:aa:7d:1b:bb:55:18:e0:6a:56:40:36:f3:09:80:;
e0:3d:3c:82:4b:6b:a6:4a:27:57:a7:81:90:de:c9:f0:4f:44:;
ca:1e:21:50:1b:7c:6c:76:77:82:8d:92:6d:4a:fb:77:ea:ff:;
31:50:79:fc:3c:03:44:c7:d7:26:4c:8b:40:3b:de:ad:65:a7:;        98:b2;;
172.16.1.253|ssh (22/tcp)|11837|REPORT|;You are running a version of OpenSSH which is
older than 3.7.1;;Versions older than 3.7.1 are vulnerable to a flaw in the buffer
management;functions which might allow an attacker to execute arbitrary commands on
this ;host.;;An exploit for this issue is rumored to exist.;;;Note that several
distribution patched this hole without changing;the version number of OpenSSH. Since
Nessus solely relied on the;banner of the remote SSH server to perform this check,
this might;be a false positive.;;If you are running a RedHat host, make sure that the
command :;          rpm -q openssh-server;   ;Returns :; openssh-server-3.1p1-13
(RedHat 7.x); openssh-server-3.4p1-7  (RedHat 8.0); openssh-server-3.5p1-11 (RedHat
9);;Solution : Upgrade to OpenSSH 3.7.1;See also :
http://marc.theaimsgroup.com/?l=openbsd-misc&m=106375452423794&w=2;
http://marc.theaimsgroup.com/?l=openbsd-misc&m=106375456923804&w=2;Risk factor :
High;CVE : CAN-2003-0693, CAN-2003-0695;BID : 8628;
172.16.1.253|ssh (22/tcp)|10267|NOTE|Remote SSH version : SSH-2.0-OpenSSH_3.5p1;
172.16.1.253|ssh (22/tcp)|10330|NOTE|An ssh server is running on this port;
172.16.1.253|nessus (1241/tcp)|10330|NOTE|A TLSv1 server answered on this port;;
172.16.1.253|nessus (1241/tcp)
172.16.1.253|ssh (22/tcp)
[root@localhost membrich]#
```

2.2.5. Apache + Mod_ssl.

Got most recent version from http://httpd.apache.org/download.cgi.

2.2.5.1. Check the MD5 Signature.

```
[membrich@localhost membrich]$ cat httpd-2.0.48.tar.gz.md5.txt
466c63bb71b710d20a5c353df8c1a19c  httpd-2.0.48.tar.gz
[membrich@localhost membrich]$ md5sum httpd-2.0.48.tar.gz
466c63bb71b710d20a5c353df8c1a19c  httpd-2.0.48.tar.gz
```

2.2.5.2. Install Apache.

```
[membrich@localhost membrich]$ gunzip httpd-2.0.48.tar.gz
[membrich@localhost membrich]$ tar -xvf httpd-2.0.48.tar
[membrich@localhost membrich]$ cd httpd-2.0.48
[membrich@localhost httpd-2.0.48]$ CFLAGS="-I/usr/kerberos/include" ./configure --
enable-ssl
[membrich@localhost httpd-2.0.48]$ make
[membrich@localhost httpd-2.0.48]$ su
Password:
[root@localhost httpd-2.0.48]# make install
```

*** There's a problem with the configure script because Redhat moved the location of some header files needed for --enable-ssl.

More info here:

http://mt.ernie.org/archives/000001.html

> So anyways, this didn't solve the problem either. krb5 and openssl rpms are all installed fine and apache just won't behave. SO I rip open that krb5-devel rpm and check out whether it has krb5.h, and where. Lo and behold:
>
> [root@nigel httpd-2.0.45]# rpm -ql krb5-devel | grep /krb5.h
> /usr/kerberos/include/krb5.h
> [root@nigel httpd-2.0.45]#
>
> Yet nothing in the failing build command is referencing that non standard include directory! AHA! I reconfigure with CFLAGS="-I/usr/kerberos/include"
> and it finally compiled.
>
> Here's my complete configure line:
>
> CFLAGS="-I/usr/kerberos/include -
> DSECURITY_HOLE_PASS_AUTHORIZATION"
> ./configure --prefix=/usr/local/apache-2.0.45 --enable-mods-shared=all
> --enable-ssl
>
> (Ernie 2003)

Check to make sure ssl is built in:

```
[membrich@localhost httpd-2.0.48]$ /usr/local/apache2/bin/httpd -l
Compiled in modules:
  core.c
  mod_access.c
  mod_auth.c
  mod_include.c
  mod_log_config.c
  mod_env.c
  mod_setenvif.c
  mod_ssl.c
  prefork.c
  http_core.c
  mod_mime.c
  mod_status.c
  mod_autoindex.c
  mod_asis.c
  mod_cgi.c
  mod_negotiation.c
  mod_dir.c
  mod_imap.c
  mod_actions.c
  mod_userdir.c
  mod_alias.c
  mod_so.c
[membrich@localhost httpd-2.0.48]$
```

2.2.5.3. Setup Certificates.

Following instructions from apache.org
http://httpd.apache.org/docs-2.0/ssl/ssl_faq.html

NOTE:
It is important that the Common Names be different for the CA key and the Server key. If they are the same, you'll get an error when you sign the server key.

2.2.5.3.1. Generate Server Key.

```
[root@localhost membrich]# openssl genrsa -des3 -out server.key 1024
Generating RSA private key, 1024 bit long modulus
......++++++
...........++++++
e is 65537 (0x10001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:
[root@localhost membrich]#
```

2.2.5.3.2. Create Certificate Signing Request.

> Create a Certificate Signing Request (CSR) with the server RSA private key (output will be PEM formatted):
>
> Make sure you enter the FQDN ("Fully Qualified Domain Name") of the server when OpenSSL prompts you for the "CommonName", i.e. when you generate a CSRfor a website which will be later accessed via https://www.foo.dom/, enter "www.foo.dom" here.
>
> (Apache HTTP Server Documentation Project 2003)

```
[root@localhost membrich]# openssl req -new -key server.key -out server.csr
Enter pass phrase for server.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:California
Locality Name (eg, city) [Newbury]:Hayward
Organization Name (eg, company) [My Company Ltd]:My Company
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:server.membrich.com
Email Address []:admin@membrich.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

```
[root@localhost membrich]#
```

2.2.5.3.3. Generate a CA Key.

Create a CA to sign the Cert request (created above)

```
[root@localhost membrich]# openssl genrsa -des3 -out ca.key 1024
Generating RSA private key, 1024 bit long modulus
.................++++++
.............++++++
e is 65537 (0x10001)
Enter pass phrase for ca.key:
Verifying - Enter pass phrase for ca.key:
[root@localhost membrich]#
```

2.2.5.3.4. Create a CA Certificate.

Create a self-signed CA Certificate (X509 structure) with the RSA key of the CA (output will be PEM formatted). (Apache HTTP Server Documentation Project 2003)

```
[root@localhost membrich]# openssl req -new -x509 -days 365 -key ca.key -out ca.crt
Enter pass phrase for ca.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:California
Locality Name (eg, city) [Newbury]:Hayward
Organization Name (eg, company) [My Company Ltd]:My Company
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:server1.membrich.com
Email Address []:admin@ebsonline.com
[root@localhost membrich]#
```

2.2.5.4.5. Sign the Server's CSR with your CA Key.

> Prepare a script for signing which is needed because the ``openssl ca" command has some strange requirements and the default OpenSSL config doesn't allow one easily to use ``openssl ca" directly. So a script named sign.sh is distributed with the mod_ssl distribution (subdir pkg.contrib/). Use this script for signing.
>
> (Apache HTTP Server Documentation Project 2003)

NOTE: This script is in the mod_ssl tarball, available at: http://www.modssl.org/

```
[root@localhost membrich]# ./sign.sh server.csr
CA signing: server.csr -> server.crt:
Using configuration from ca.config
Enter pass phrase for ./ca.key:
Check that the request matches the signature
Signature ok
```

```
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'US'
stateOrProvinceName   :PRINTABLE:'California'
localityName          :PRINTABLE:'Hayward'
organizationName      :PRINTABLE:'My Company'
commonName            :PRINTABLE:'server.membrich.com'
emailAddress          :IA5STRING:'admin@membrich.com'
Certificate is to be certified until Nov 15 02:37:56 2004 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
CA verifying: server.crt <-> CA cert
server.crt: OK
[root@localhost membrich]#
```

2.2.5.4.6. Place the Certificates in the Appropriate Location.

The /usr/local/apache2/conf/ssl.conf specifies where it looks for the certificates.

```
#   Server Certificate:
#   Point SSLCertificateFile at a PEM encoded certificate.  If
#   the certificate is encrypted, then you will be prompted for a
#   pass phrase.  Note that a kill -HUP will prompt again.  Keep
#   in mind that if you have both an RSA and a DSA certificate you
#   can configure both in parallel (to also allow the use of DSA
#   ciphers, etc.)
SSLCertificateFile /usr/local/apache2/conf/ssl.crt/server.crt
#SSLCertificateFile /usr/local/apache2/conf/ssl.crt/server-dsa.crt

#   Server Private Key:
#   If the key is not combined with the certificate, use this
#   directive to point at the key file.  Keep in mind that if
#   you've both a RSA and a DSA private key you can configure
#   both in parallel (to also allow the use of DSA ciphers, etc.)
SSLCertificateKeyFile /usr/local/apache2/conf/ssl.key/server.key
#SSLCertificateKeyFile /usr/local/apache2/conf/ssl.key/server-dsa.key

#   Server Certificate Chain:
#   Point SSLCertificateChainFile at a file containing the
#   concatenation of PEM encoded CA certificates which form the
#   certificate chain for the server certificate. Alternatively
#   the referenced file can be the same as SSLCertificateFile
#   when the CA certificates are directly appended to the server
#   certificate for convinience.
#SSLCertificateChainFile /usr/local/apache2/conf/ssl.crt/ca.crt

#   Certificate Authority (CA):
#   Set the CA certificate verification path where to find CA
#   certificates for client authentication or alternatively one
#   huge file containing all of them (file must be PEM encoded)
#   Note: Inside SSLCACertificatePath you need hash symlinks
#         to point to the certificate files. Use the provided
#         Makefile to update the hash symlinks after changes.
#SSLCACertificatePath /usr/local/apache2/conf/ssl.crt
#SSLCACertificateFile /usr/local/apache2/conf/ssl.crt/ca-bundle.crt
```

We'll set up that path structure and moving the certificates to the appropriate places:

```
[root@localhost membrich]# mkdir /usr/local/apache2/conf/ssl.crt
[root@localhost membrich]# chmod 700 /usr/local/apache2/conf/ssl.crt
[root@localhost membrich]# mkdir /usr/local/apache2/conf/ssl.key
[root@localhost membrich]# chmod 700 /usr/local/apache2/conf/ssl.key
[root@localhost membrich]# cp server.crt /usr/local/apache2/conf/ssl.crt/server.crt
[root@localhost membrich]# cp server.key /usr/local/apache2/conf/ssl.key/server.key
```

2.2.5.4.7. Test the Certificates.

```
[root@localhost membrich]# /usr/local/apache2/bin/apachectl startssl
Apache/2.0.48 mod_ssl/2.0.48 (Pass Phrase Dialog)
Some of your private key files are encrypted for security reasons.
In order to read them you have to provide us with the pass phrases.

Server www.example.com:443 (RSA)
Enter pass phrase:

Ok: Pass Phrase Dialog successful.
[root@localhost membrich]#


[root@localhost membrich]# netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:1241            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN
tcp        0      0 172.16.1.253:22         172.16.1.33:2938        ESTABLISHED
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node Path
unix  2      [ ACC ]     STREAM     LISTENING     36144  /var/lib/mysql/mysql.sock
unix  4      [ ]         DGRAM                    1437   /dev/log
unix  3      [ ]         STREAM     CONNECTED     36044
unix  3      [ ]         STREAM     CONNECTED     36043
unix  2      [ ]         DGRAM                    1587
unix  2      [ ]         DGRAM                    1447
[root@localhost membrich]#
```

The Apache server is running, listening on both TCP 80 (HTTP) and TCP 443 (HTTPS). We don't want Apache listening on TCP 80, that's one of the things we still need to change.

2.2.5.4.8. Configure Apache.

We still need to change a few things:

- Turn off HTTP.
- Set up logging.
- Set up the email address that appears on error documents.
- Set up the server's name.

Edit httpd.conf

Made a copy of the original httpd.conf:

```
[root@localhost membrich]# cp /usr/local/apache2/conf/httpd.conf
/usr/local/apache2/conf/httpd.conf.original
```

Then edited the real one:

```
[root@localhost membrich]# vi /usr/local/apache2/conf/httpd.conf
```

Made the following changes:

2.2.5.4.8.1. Turn Off HTTP.

Comment out the "Listen 80" line.

```
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses (0.0.0.0)
#
#Listen 12.34.56.78:80

#Listen 80
```

2.2.5.4.8.2. Setup Server Admin Email Address.

Change the "Server Admin" setting to your administrator email address on this server.

```
# ServerAdmin: Your address, where problems with the server should be
# e-mailed.  This address appears on some server-generated pages, such
# as error documents.  e.g. admin@your-domain.com
#
#ServerAdmin you@example.com
ServerAdmin admin@membrich.com
```

2.2.5.4.8.3. Setup Server Name.

Change the "ServerName" setting to the name of this HTTPS server.

```
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If this is not set to valid DNS name for your host, server-generated
# redirections will not work.  See also the UseCanonicalName directive.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
# You will have to access it by its address anyway, and this will make
# redirections work in a sensible way.
#
#ServerName www.example.com:80
ServerName server.membrich.com
```

2.2.5.4.8.4. Setup Logging.

The default is to write the Apache logs to /usr/local/apache2/logs. It's not a good idea to have logs writing to this file system because it'll cause problems for you if the log files grow out of control and fill it up. It's better to send the logs to the /var file system, which is much harder to fill up, and causes less problems if it gets full. The worst that'll happen is hang services that can no longer write to their logs.

To do this, we change the "ErrorLog" and "CustomLog" settings.

```
# ErrorLog: The location of the error log file.
# If you do not specify an ErrorLog directive within a <VirtualHost>
# container, error messages relating to that virtual host will be
# logged here.  If you *do* define an error logfile for a <VirtualHost>
# container, that host's errors will be logged there and not here.
#
#ErrorLog logs/error_log
ErrorLog /var/log/apache/error_log

# The location and format of the access logfile (Common Logfile Format).
# If you do not define any access logfiles within a <VirtualHost>
# container, they will be logged here.  Contrariwise, if you *do*
# define per-<VirtualHost> access logfiles, transactions will be
# logged therein and *not* in this file.
#
#CustomLog logs/access_log common
CustomLog /var/log/apache/access_log common
```

We need to create this directory.

```
[root@localhost membrich]# mkdir /var/log/apache
```

2.2.5.4.8.5. Same Changes for /usr/local/apache2/conf/ssl.conf.

Change the ServerName, ServerAdmin, ErrorLog, TransferLog settings.

```
[root@localhost membrich]# vi /usr/local/apache2/conf/ssl.conf

## SSL Virtual Host Context
##

<VirtualHost _default_:443>

#  General setup for the virtual host
DocumentRoot "/usr/local/apache2/htdocs"
#ServerName www.example.com:443
ServerName server.membrich.com:443
#ServerAdmin you@example.com
ServerAdmin admin@membrich.com
#ErrorLog /usr/local/apache2/logs/error_log
ErrorLog /var/log/apache/error_log
#TransferLog /usr/local/apache2/logs/access_log
TransferLog /var/log/apache/access_log
```

2.2.5.4.8.6. Test it.

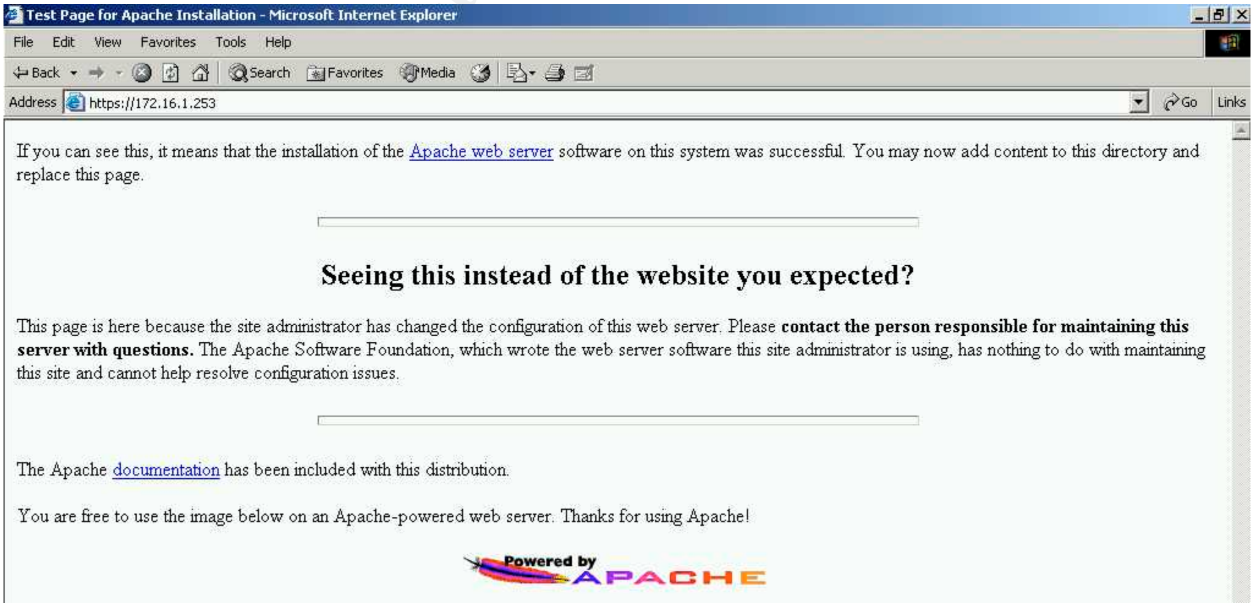
```
[root@localhost membrich]# /usr/local/apache2/bin/apachectl stop
[root@localhost membrich]# /usr/local/apache2/bin/apachectl startssl
```

```
Apache/2.0.48 mod_ssl/2.0.48 (Pass Phrase Dialog)
Some of your private key files are encrypted for security reasons.
In order to read them you have to provide us with the pass phrases.

Server server.membrich.com:443 (RSA)
Enter pass phrase:

Ok: Pass Phrase Dialog successful.
[root@localhost membrich]#
```

Check if we're still listening on TCP 80 (HTTP).

```
[root@localhost membrich]# netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:1241            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN
tcp        0      0 172.16.1.253:22         172.16.1.33:2938        ESTABLISHED
tcp        0      0 172.16.1.253:22         172.16.1.33:3366        ESTABLISHED
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node Path
unix  2      [ ACC ]     STREAM     LISTENING     36144  /var/lib/mysql/mysql.sock
unix  4      [ ]         DGRAM                    1437   /dev/log
unix  3      [ ]         STREAM     CONNECTED     71211
unix  3      [ ]         STREAM     CONNECTED     71210
unix  3      [ ]         STREAM     CONNECTED     36044
unix  3      [ ]         STREAM     CONNECTED     36043
unix  2      [ ]         DGRAM                    1587
unix  2      [ ]         DGRAM                    1447
[root@localhost membrich]#
```

You should now be able to bring up the Apache default index.html.
For example:



If you can see this, it means that the installation of the Apache web server software on this system was successful. You may now add content to this directory and replace this page.

Seeing this instead of the website you expected?

This page is here because the site administrator has changed the configuration of this web server. Please **contact the person responsible for maintaining this server with questions.** The Apache Software Foundation, which wrote the web server software this site administrator is using, has nothing to do with maintaining this site and cannot help resolve configuration issues.

The Apache documentation has been included with this distribution.

You are free to use the image below on an Apache-powered web server. Thanks for using Apache!

2.2.6. PHP

Downloaded the latest version from http://www.php.net/downloads.php
The MD5 signature is also posted on this page.

Here is the signature for the latest version (4.3.3):

```
PHP 4.3.4 (tar.gz) [4,522Kb] - 03 November 2003
md5: c0e7f7388fadacbf4948391c6d93dc5e
```

2.2.6.1. Check the MD5 Signature.

```
[membrich@localhost membrich]$ md5sum php-4.3.4.tar.gz
8963a382c8108a431e94bcfc49dbc4a5  php-4.3.4.tar.gz
```

Woops, didn't match, something is wrong!
Checked the file sizes, I didn't download the whole file:

```
[membrich@localhost membrich]$ ls -l php-4.3.4.tar.gz
-rw-rw-r--    1 membrich membrich   206242 Nov 15 23:41 php-4.3.4.tar.gz
```

Downloaded the file from a different mirror, tried the md5sum again.

```
[membrich@localhost membrich]$ md5sum php-4.3.4.tar.gz
c0e7f7388fadacbf4948391c6d93dc5e  php-4.3.4.tar.gz
```

2.2.6.2. Install PHP.

```
[membrich@localhost membrich]$ gunzip php-4.3.4.tar.gz
[membrich@localhost membrich]$ tar -xvf php-4.3.4.tar
[membrich@localhost membrich]$ cd php-4.3.4
[membrich@localhost php-4.3.4]$ ./configure --with-apxs2=/usr/local/apache2/bin/apxs -
-with-config-file-path=/usr/local/apache2/conf --enable-versioning --enable-bcmath --
with-mysql --disable-debug --enable-memory-limit-yes --enable-track-vars --with-gd --
with-jpeg-dir=/usr/lib --with-png-dir=/usr/lib --with-zlib-dir=/usr/lib --with-
freetype-dir=/usr/lib
[membrich@localhost php-4.3.4]$ make
[membrich@localhost php-4.3.4]$ su
Password:
[root@localhost php-4.3.4]# make install
```

2.2.6.3. Add the .php Type to httpd.conf.

We need to edit the /usr/local/apache2/conf/httpd.conf to make sure Apache knows how to handle web pages with the .php extension. I only added the last line, but included the rest to give you a reference point.

```
# AddType allows you to add to or override the MIME configuration
# file mime.types for specific file types.
#
#AddType application/x-tar .tgz
#
# AddEncoding allows you to have certain browsers uncompress
# information on the fly. Note: Not all browsers support this.
# Despite the name similarity, the following Add* directives have nothing
# to do with the FancyIndexing customization directives above.
#
#AddEncoding x-compress .Z
#AddEncoding x-gzip .gz .tgz
#
# If the AddEncoding directives above are commented-out, then you
# probably should define those extensions to indicate media types:
#
AddType application/x-compress .Z
AddType application/x-gzip .gz .tgz
AddType application/x-httpd-php .php
```

We need to restart the Apache server to make the changes take effect.

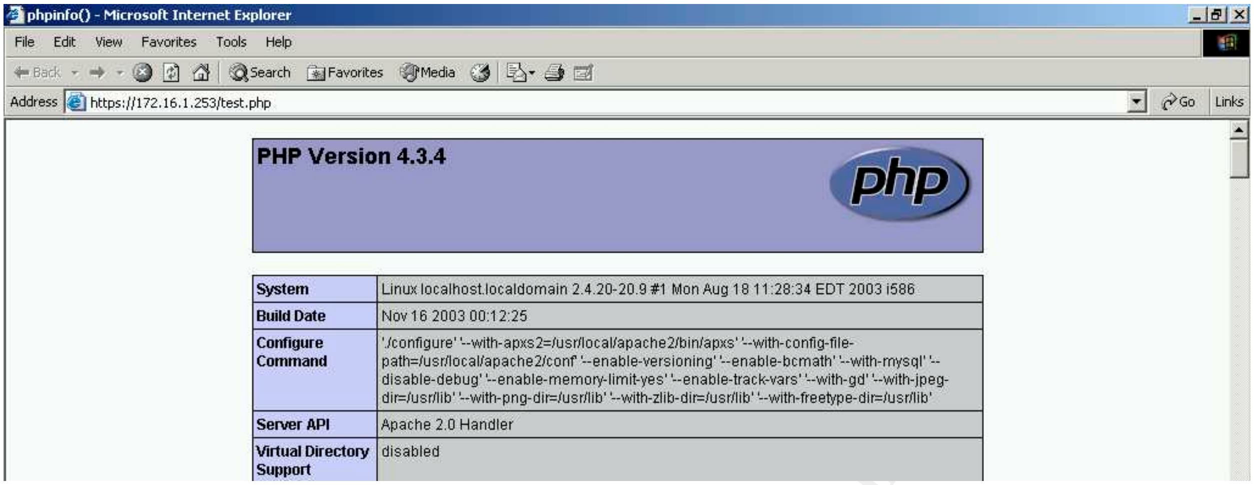
```
[root@localhost php-4.3.4]# /usr/local/apache2/bin/apachectl stop
[root@localhost php-4.3.4]# /usr/local/apache2/bin/apachectl startssl
Apache/2.0.48 mod_ssl/2.0.48 (Pass Phrase Dialog)
Some of your private key files are encrypted for security reasons.
In order to read them you have to provide us with the pass phrases.

Server server.membrich.com:443 (RSA)
Enter pass phrase:

Ok: Pass Phrase Dialog successful.
[root@localhost php-4.3.4]#
```

2.2.6.4. Test it.

Test PHP install:
Create a file test.php in /usr/local/apache2/htdocs (or anywhere that your web server will look for files to serve):

```
[root@localhost php-4.3.4]# cat /usr/local/apache2/htdocs/test.php
<?php phpinfo(); ?>
[root@localhost php-4.3.4]#
```

Then use your browser to open the page, in my case:


phpinfo() - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go
Links

Address: https://172.16.1.253/test.php

PHP Version 4.3.4

System	Linux localhost.localdomain 2.4.20-20.9 #1 Mon Aug 18 11:28:34 EDT 2003 i586
Build Date	Nov 16 2003 00:12:25
Configure Command	'./configure' '--with-apxs2=/usr/local/apache2/bin/apxs' '--with-config-file-path=/usr/local/apache2/conf' '--enable-versioning' '--enable-bcmath' '--with-mysql' '--disable-debug' '--enable-memory-limit-yes' '--enable-track-vars' '--with-gd' '--with-jpeg-dir=/usr/lib' '--with-png-dir=/usr/lib' '--with-zlib-dir=/usr/lib' '--with-freetype-dir=/usr/lib'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled

2.2.7. PHPlot.

Checked www.phplot.com for the latest version, but the site appeared to be down. However, I was able to find it also at: http://sourceforge.net/project/showfiles.php?group_id=14653&release_id=28664

2.2.7.1. Install PHPlot.

```
[membrich@localhost membrich]$ gunzip phplot-4.4.6.tar.gz
```

Unpack the phplot files in the /usr/local/apache2 directory.

```
[membrich@localhost membrich]$ su
Password:
[root@localhost membrich]# cd /usr/local/apache2
[root@localhost apache2]# tar -xvf /home/membrich/phplot-4.4.6.tar
```

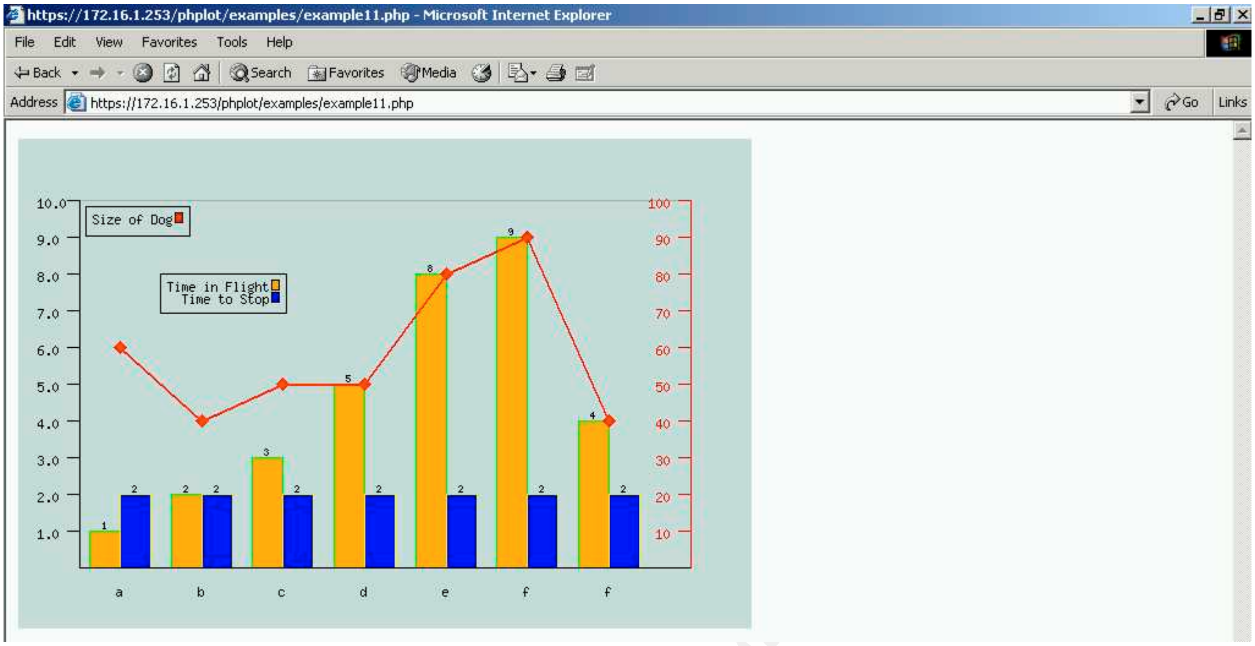
Created a link to the resulting /usr/local/apache/phplot-4.4.6 directory into the /usr/local/apache/htdocs directory:

```
[root@localhost apache2]# cd htdocs
[root@localhost htdocs]# ln -s ../phplot-4.4.6 phplot
[root@localhost htdocs]#
```

2.2.7.2. Test PHPlot.

After making that link, I pull up all of the examples, /usr/local/apache2/htdocs/phplot/examples/example1.php through /usr/local/apache2/htdocs/phplot/examples/example13.php.

Here’s one of the examples:


https://172.16.1.253/phplot/examples/example11.php - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://172.16.1.253/phplot/examples/example11.php
Go Links
Size of Dog
Time in Flight
Time to Stop
10.0
9.0
8.0
7.0
6.0
5.0
4.0
3.0
2.0
1.0
100
90
80
70
60
50
40
30
20
10
1 2 2 2 3 2 5 2 8 2 9 2 4 2
a b c d e f f

2.2.7. ADODB.

We need ADODB for ACID.

Downloaded latest stable version from: http://php.weblogs.com/ADOdb#downloads

```
[root@localhost membrich]# gunzip adodb404.tgz
[root@localhost membrich]# cd /usr/local/apache2
[root@localhost apache2]# tar -xvf /home/membrich/adodb404.tar
```

2.2.8. ACID.

Checked for the latest version:
http://www.andrew.cmu.edu/~rdanyliw/snort/snortacid.html

2.2.8.1. Check the MD5 Signature.

Posted on the download page:

acid-0.9.6b23.tar.gz
d8c49614393fa05ac140de349f57e438

```
[membrich@localhost membrich]$ md5sum acid-0.9.6b23.tar.gz
d8c49614393fa05ac140de349f57e438  acid-0.9.6b23.tar.gz
[membrich@localhost membrich]$
```

2.2.8.2. Install ACID.

```
[membrich@localhost membrich]$ gunzip acid-0.9.6b23.tar.gz
```

```
[membrich@localhost membrich]$ su
Password:
[root@localhost membrich]# cd /usr/local/apache2/htdocs
[root@localhost htdocs]# tar -xvf /home/membrich/acid-0.9.6b23.tar
```

2.2.8.3. Create the Snort Tables in Mysql.

```
[root@localhost htdocs]# cd ~membrich/snort-2.0.4
[root@localhost snort-2.0.4]# echo "create database snort;" | mysql -u root -p
Enter password:
[root@localhost snort-2.0.4]#

[root@localhost snort-2.0.4]# mysql -u root -p snort < ./contrib/create_mysql
Enter password:
[root@localhost snort-2.0.4]#

[root@localhost snort-2.0.4]# mysql -u root -p snort <
/usr/local/apache2/htdocs/acid/create_acid_tbls_mysql.sql
Enter password:
[root@localhost snort-2.0.4]#
```

2.2.8.4. Create the Snort User for Mysql and Give it Permissions.

```
[root@localhost snort-2.0.4]# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 6 to server version: 3.23.58

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> grant select, insert, update, delete on snort.* to snort@localhost identified
by 'snort';
Query OK, 0 rows affected (0.03 sec)

mysql> quit;
Bye
[root@localhost snort-2.0.4]#
```

2.2.8.5. Create and Setup an Archive Database.

```
[root@localhost snort-2.0.4]# echo "create database snort_archive;" | mysql -u root -p
Enter password:
[root@localhost snort-2.0.4]# mysql -u root -p snort_archive < ./contrib/create_mysql
Enter password:
[root@localhost snort-2.0.4]# mysql -u root -p snort_archive <
/usr/local/apache2/htdocs/acid/create_acid_tbls_mysql.sql
Enter password:
[root@localhost snort-2.0.4]# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 10 to server version: 3.23.58

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> grant select, insert, update, delete on snort_archive.* to snort@localhost
identified by 'snort';
Query OK, 0 rows affected (0.00 sec)

mysql> quit;
Bye
```

```
[root@localhost snort-2.0.4]#
```

2.2.8.6. Set the Password for the Mysql Snort User.

```
[root@localhost membrich]# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 11 to server version: 3.23.58

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> set password for snort@localhost = password('<your password>');
Query OK, 0 rows affected (0.01 sec)

mysql>
```

Test snort user on snort database:

```
mysql> use snort
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> select count(*) from event;
+----------+
| count(*) |
+----------+
|        0 |
+----------+
1 row in set (0.03 sec)

mysql> quit
Bye
[root@localhost membrich]#
```

That's what we wanted to see.

2.2.8.7. Configure ACID.

Following the instructions from:
http://www.andrew.cmu.edu/~rdanyliw/snort/acid_config.html, the following are settings we need to change:

```
      o $DBlib_path     : full path to the ADODB installation
                          (Note: do not include a trailing '\' character)

       o $DBtype         : type of the database used ("mysql", "postgres")

       o $alert_dbname   : alert database name
       o $alert_host     : alert database server
       o $alert_port     : port where the database is stored
       o $alert_user     : username for the alert database
       o $alert_password : password for the username

       [OPTIONAL for alert archiving support]

       o $archive_dbname   : archive/backup database name
       o $archive_host     : archive database server
```

```
        o $archive_port     :
        o $archive_user     : "root";
        o $archive_password : "mypassword";

        [OPTIONAL for chart support]

        o $ChartLib_path     : full path to the PHPlot install
                               (Note: do not include a trailing '\' character)

        o $chart_file_format : graphic format to use for generated charts
                               ("png", "jpeg", "gif").  The selected format should
                               have displayed correctly with the PHPlot diagnostic
                               page (see Step 8)

        [OPTIONAL for Snort portscan pre-processor support]

        o $portscan_file  : full path to a Snort portscan log file
```

(Danyliw 2003)

Here's what we need to change:

```
[root@localhost membrich]# vi /usr/local/apache2/htdocs/acid/acid_conf.php
```

From:

```
$DBlib_path = "";
```

To:

```
$DBlib_path = "/usr/local/apache2/adodb";
```

From:

```
$alert_dbname   = "snort_log";
$alert_host     = "localhost";
$alert_port     = "";
$alert_user     = "root";
$alert_password = "mypassword";
```

To:

```
$alert_dbname   = "snort";
$alert_host     = "localhost";
$alert_port     = "";
$alert_user     = "snort";
$alert_password = "<your password>";
```

From:

```
/* Archive DB connection parameters */
$archive_dbname   = "snort_archive";
$archive_host     = "localhost";
$archive_port     = "";
$archive_user     = "root";
$archive_password = "mypassword";
```

To:

```
/* Archive DB connection parameters */
$archive_dbname   = "snort_archive";
$archive_host     = "localhost";
$archive_port     = "";
$archive_user     = "snort";
$archive_password = "<your password>";
```

From:

```
$ChartLib_path = "";
```

To:

```
$ChartLib_path = "/usr/local/apache2/htdocs/phplot";
```

2.2.8.8. Set up ACID for the Archive Database.

We'll just copy what we set up for the main snort database.

```
[root@localhost membrich]# cp -r /usr/local/apache2/htdocs/acid
/usr/local/apache2/htdocs/acid_archive
[root@localhost membrich]# vi /usr/local/apache2/htdocs/acid_archive/acid_conf.php
```

We only need to change the "$alert_dbname" setting.
From:

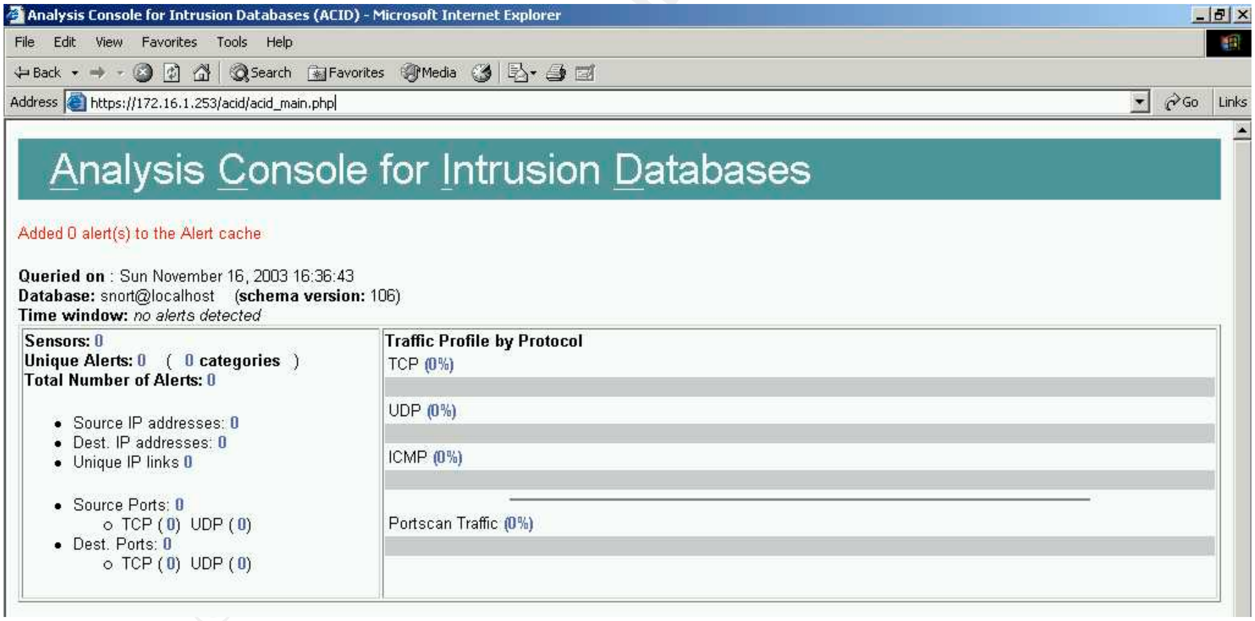
```
$alert_dbname   = "snort";
```

To:

```
$alert_dbname   = "snort_archive";
```

2.2.8.9. Test ACID.

Tested main ACID page: https://172.16.1.253/acid/acid_main.php.
Looks good:


Analysis Console for Intrusion Databases (ACID) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://172.16.1.253/acid/acid_main.php
Go Links

Analysis Console for Intrusion Databases

Added 0 alert(s) to the Alert cache

Queried on : Sun November 16, 2003 16:36:43
Database: snort@localhost   **(schema version:** 106)
Time window: *no alerts detected*

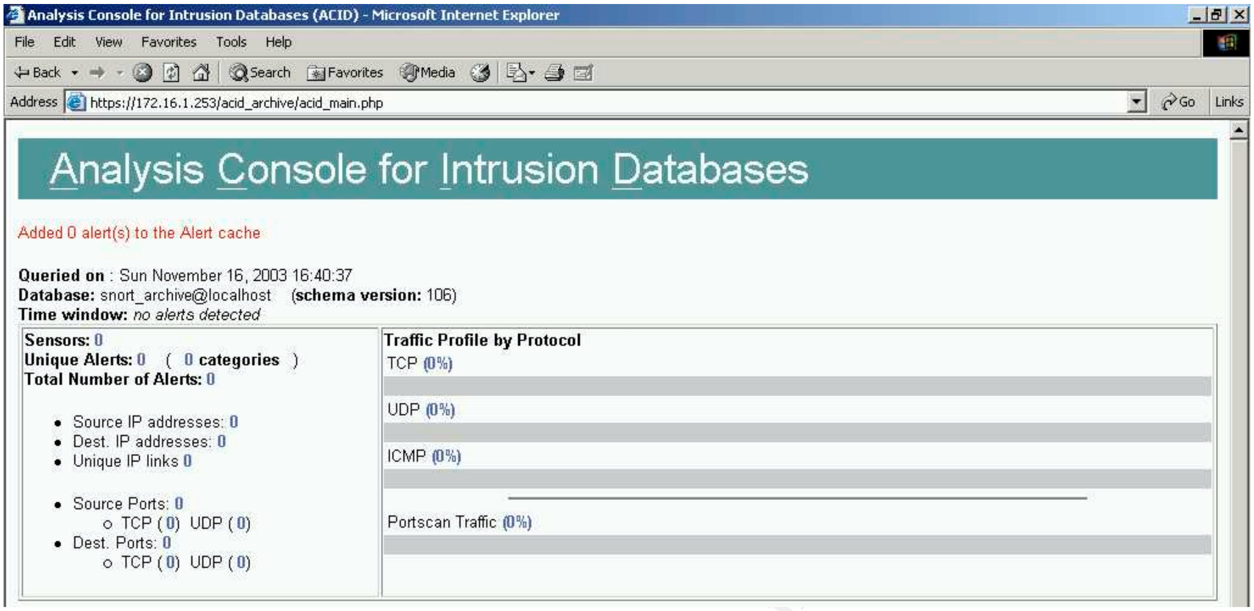
Sensors: 0
Unique Alerts: 0 (0 **categories**)
Total Number of Alerts: 0

- Source IP addresses: 0
- Dest. IP addresses: 0
- Unique IP links 0

- Source Ports: 0
  - TCP (0) UDP (0)
- Dest. Ports: 0
  - TCP (0) UDP (0)

Traffic Profile by Protocol
TCP (0%)
UDP (0%)
ICMP (0%)
Portscan Traffic (0%)

Tested archive ACID page: https://172.16.1.253/acid_archive/acid_main.php.
Looks good:


Analysis Console for Intrusion Databases (ACID) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://172.16.1.253/acid_archive/acid_main.php
Go Links

Analysis Console for Intrusion Databases

Added 0 alert(s) to the Alert cache

Queried on : Sun November 16, 2003 16:40:37
Database: snort_archive@localhost (**schema version:** 106)
Time window: *no alerts detected*

Sensors: 0
Unique Alerts: 0 (0 **categories**)
Total Number of Alerts: 0

- Source IP addresses: 0
- Dest. IP addresses: 0
- Unique IP links 0

- Source Ports: 0
  - TCP (0) UDP (0)
- Dest. Ports: 0
  - TCP (0) UDP (0)

Traffic Profile by Protocol
TCP (0%)
UDP (0%)
ICMP (0%)
Portscan Traffic (0%)

2.3. Tighten Down the Server.

2.3.1. Bastille Linux.

The creators of Bastille Linux describe it better than I can:
(from http://www.bastille-linux.org/)

> The Bastille Hardening System attempts to "harden" or "tighten" Unix operating systems. It currently supports the Red Hat, Debian, Mandrake, SuSE and TurboLinux Linux distributions along with HP-UX and Mac OS X. We attempt to provide the most secure, yet usable, system possible. The project is run by Jon Lasser, Lead Coordinator and Jay Beale, Lead Developer, and involves a number of developers, beta-testers and concept-creators. Bastille Linux was developed with several major goals:
>
> COMPREHENSIVENESS
> Bastille Linux draws from every available major reputable source on Linux Security. The initial development integrated Jay Beale's existing O/S hardening experience for Solaris and Linux with most major points from the SANS' Securing Linux Step by Step, Kurt Seifried's Linux Administrator's Security Guide, and countless other sources.
>
> (Lasser 2003)

2.3.1.1. Install Bastille Linux.

Since we do not have a GUI installed on this sensor, we need to use the text-only version of Bastille Linux. Which means installing perl-Curses (instead of perl-TK).

perl-Curses is available at: http://www.bastille-linux.org/perl-rpm-chart.html
Bastille Linux is available at: http://www.bastille-linux.org/

```
[root@localhost membrich]# rpm -ivh perl-Curses-1.06-219.i586.rpm
warning: only V3 signatures can be verified, skipping V4 signature
Preparing...                ########################################### [100%]
   1:perl-Curses            ########################################### [100%]
[root@localhost membrich]# rpm -ivh Bastille-2.1.1-1.0.i386.rpm
Preparing...                ########################################### [100%]
   1:Bastille               ########################################### [100%]
[root@localhost membrich]#
```

2.3.1.2. Running Bastille Linux.

```
[root@localhost membrich]# /usr/sbin/bastille -c
NOTE:    Using Curses user interface module.
NOTE:    Only displaying questions relevant to the current configuration.

Copyright (C) 1999-2002 Jay Beale
Copyright (C) 1999-2001 Peter Watkins
Copyright (C) 2000 Paul L. Allen
Copyright (C) 2001-2003 Hewlett Packard Company
Bastille is free software; you are welcome to redistribute it under
certain conditions.  See the 'COPYING' file in your distribution for terms.

DISCLAIMER.  Use of Bastille can help optimize system security, but does not
guarantee system security. Information about security obtained through use of
Bastille is provided on an AS-IS basis only and is subject to change without
notice. Customer acknowledges they are responsible for their system's security.
TO THE EXTENT ALLOWED BY LOCAL LAW, Bastille (SOFTWARE) IS PROVIDED TO YOU
AS IS WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, WHETHER ORAL OR WRITTEN,
EXPRESS OR IMPLIED.  JAY BEALE, THE BASTILLE DEVELOPERS, AND THEIR SUPPLIERS
DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.
Some countries, states and provinces do not allow exclusions of implied
warranties or conditions, so the above exclusion may not apply to you. You may
have other rights that vary from country to country, state to state, or province
to province.  EXCEPT TO THE EXTENT PROHIBITED BY LOCAL LAW, IN NO EVENT WILL
JAY BEALE, THE BASTILLE DEVELOPERS, OR THEIR SUBSIDIARIES, AFFILIATES OR
SUPPLIERS BE LIABLE FOR DIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL OR OTHER
DAMAGES (INCLUDING LOST PROFIT, LOST DATA, OR DOWNTIME COSTS), ARISING OUT OF
THE USE, INABILITY TO USE, OR THE RESULTS OF USE OF THE SOFTWARE, WHETHER BASED
IN WARRANTY, CONTRACT, TORT OR OTHER LEGAL THEORY, AND WHETHER OR NOT ADVISED
OF THE POSSIBILITY OF SUCH DAMAGES. Your use of the Software is entirely at your
own risk. Should the Software prove defective, you assume the entire cost of all
service, repair or correction. Some countries, states and provinces do not allow
the exclusion or limitation of liability for incidental or consequential
damages, so the above limitation may not apply to you.

You must accept the terms of this disclaimer to use
Bastille.  Type "accept" (without quotes) within 5
minutes to accept the terms of the above disclaimer
> accept

---------------------------
```

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  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 >
```

Chose "Next"

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                    •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•FilePermissions.pm Module 2 of 0•••••••••••••••••••••••••••••••••••••••••••••••
•Q: Would you like to set more restrictive permissions on the administration   •
•utilities? [N]                                                                •
•In general, the default file permissions set by most vendors are fairly secure•
•.  To make them more secure, though, you can remove non-root user access to   •
•some administrator functions.                                                 •
•                                                                              •
•If you choose this option, you'll be changing the permissions on some common  •
•system administration utilities so that they're not readable or executable by •
•users other than root.  These utilities (which include linuxconf, fsck,       •
•ifconfig, runlevel and portmap) are ones that most users should never have a  •
•need to access.  This option will increase your system security, but there's a•
•chance it will inconvenience your users.                                      •
•                                                                              •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                   •••••••
                                   •Yes  •
                                   •No   •
                                   •••••••
               < Back >     < Next >     < Explain Less >
```

Chose "Yes"

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                    •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•FilePermissions.pm Module 2 of 0••••••••••••••••••••••••••••••••••••••••••••••
•The following questions all pertain to disabling "SUID root" permission for   •
•particular programs. This permission allows non-root users to run these       •
•programs, increasing convenience but decreasing security.  If a security      •
•weakness or vulnerability is found in these programs, it can be exploited to  •
•gain root-level access to your computer through any user account.             •
•                                                                              •
•If you answer "Yes" and then realize later that you do need SUID permissions  •
•on a specific program, you can always turn it back on later with chmod u+s <  •
•file name>.                                                                   •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••



                < Back >     < Next >     < Explain Less >
```

Chose "Next"

```
---------------------------

••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                    •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•FilePermissions.pm Module 2 of 0••••••••••••••••••••••••••••••••••••••••••••••
•Q: Would you like to disable SUID status for mount/umount?                    •
•Mount and umount are used for mounting (activating) and unmounting (          •
•deactivating) drives that were not automatically mounted at boot time.  This  •
•can include floppy and CD-ROM drives.  Disabling SUID would still allow anyone•
•with the root password to mount and unmount drives.                           •
•                                                                              •
•Would you like to disable SUID status for mount/umount?                       •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                   •••••••
                                   •Yes  •
                                   •No   •
                                   •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "Yes"

```
---------------------------
```

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                    •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•FilePermissions.pm Module 2 of 0•••••••••••••••••••••••••••••••••••••••••••••••
•Q: Would you like to disable SUID status for ping? [Y]                        •
•Ping is used for testing network connectivity.  Specifically it's for testing •
•the  ability of the network to get a packet from this machine to another and  •
•back.  The ping program is SUID since only the root user can open a raw socket•
•. Since, however, it is often used only by the person responsible for         •
•networking the host, who normally has root access, we recommend disabling SUID•
•status for it.                                                                •
•                                                                              •
•Would you like to disable SUID status for ping? [Y]                           •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "Yes"

```
---------------------------
```

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                    •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•FilePermissions.pm Module 2 of 0•••••••••••••••••••••••••••••••••••••••••••••••
•Q: Would you like to disable SUID status for usernetctl? [Y]                  •
•usernetctl is a utility that allows ordinary users to control the network     •
•interfaces.  In general, there's no reason for anyone other than the system   •
•administrator to control network interfaces.                                  •
•                                                                              •
•Would you like to disable SUID status for usernetctl? [Y]                     •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "Yes"

```
---------------------------
```

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                   Bastille                                   •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•FilePermissions.pm Module 2 of 0•••••••••••••••••••••••••••••••••••••••••••••••
•Q: Would you like to disable SUID status for traceroute? [Y]                  •
•The traceroute utility is used to test network connectivity. It is useful for •
•debugging network problems, but it is generally not necessary, especially for •
•non-privileged users.  If non-root users will be needing to debug network     •
•connections, you can leave the SUID bit on traceroute.  Otherwise, you should •
•disable it.                                                                   •
•                                                                              •
•Would you like to disable SUID status for traceroute? [Y]                     •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "Yes"

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                   Bastille                                   •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•AccountSecurity.pm Module 3 of 0•••••••••••••••••••••••••••••••••••••••••••••••
•Q: Would you like to enforce password aging? [Y]                              •
•Your operating system's default behavior, which we would change here, is to   •
•disable an account when the password hasn't changed in 99,999 days.  This     •
•interval is too long to be useful.  We can set the default to 180 days.  At   •
•some point before the 180 days have passed, the system will ask the user to   •
•change his or her password.  At the end of the 180 days, if the password has  •
•not been changed, the account will be temporarily disabled.  We would make    •
•this change in /etc/login.defs.                                               •
•                                                                              •
•Would you like to enforce password aging? [Y]                                 •
•                                                                              •
•                                                                              •
•                                                                              •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "Yes"

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                    •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•AccountSecurity.pm Module 3 of 0••••••••••••••••••••••••••••••••••••••••••••••
•Q: Would you like to restrict the use of cron to administrative accounts? [Y] •
•Cron can be particularly useful for admins, giving them the ability to have   •
•the system check logs every night at midnight or confirm file integrity every •
•hour.  On the other hand, being able to execute jobs later or automatically   •
•represents an abusable privilege for users and also makes their actions       •
•slightly harder to track.                                                     •
•                                                                              •
•Many sites choose to restrict cron to administrative accounts.  We suggest    •
•this action to new admins especially, until they understand more about how    •
•cron can be abused and know more about which users need access to cron. We    •
•would like to create the /etc/cron.allow file of users who may use cron. You  •
•can add to that later.  If we don't create this file, all users will be       •
•allowed to use cron.                                                          •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "Yes"

```
---------------------------
```

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                    •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•AccountSecurity.pm Module 3 of 0••••••••••••••••••••••••••••••••••••••••••••••
•Q: Do you want to set the default umask? [Y]                                  •
•The umask sets the default permission for files that you create. Bastille can •
•set one of several umasks in the default login configuration files.  These    •
•cover standard shells like csh and most bourne shell variants like bash, sh,  •
•and ksh.  If you are going to install other shells, you may have to configure •
•them yourself.  The only reason not to set at least a minimal default umask is•
•if you are sure that you have already set one.                                •
•                                                                              •
•Do you want to set the default umask? [Y]                                     •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "Yes"

```
---------------------------
```

```
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                   •
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•AccountSecurity.pm Module 3 of 0•••••••••••••••••••••••••••••••••••••••••••••
•Q: What umask would you like to set for users on the system? [077]           •
•The umask sets a default permission for files that you create. Bastille can  •
•set one of several umasks.  Please select one of the following or create your •
•own:                                                                         •
•                                                                             •
•002  - Everyone can read your files & people in your group can alter them.   •
•                                                                             •
•022  - Everyone can read your files, but no one can write to them.           •
•                                                                             •
•027  - Only people in your group can read your files, no one can write to them•
•.                                                                            •
•                                                                             •
•077  - No one on the system can read or write your files.                    •
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
 •••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
 •Answer: 077                                                                 •
 •                                                                            •
 •••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
               < Back >     < Next >     < Explain Less >
```

Chose "Next"

```
---------------------------
```

```
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                   •
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•AccountSecurity.pm Module 3 of 0•••••••••••••••••••••••••••••••••••••••••••••
•Q: Should we disallow root login on tty's 1-6? [N]                           •
•You can restrict which tty's root can login on.  Some sites choose to restrict•
•root logins, so that an admin must login with an ordinary user account and   •
•then use su to become root.                                                  •
•                                                                             •
•This can stop an attacker who has only been able to steal the root password  •
•from logging in directly.  He has to steal a second account's password to make•
•use of the root password via the ttys.                                       •
•                                                                             •
•Should we disallow root login on tty's 1-6? [N]                              •
•                                                                             •
•                                                                             •
•                                                                             •
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                   •••••••
                                   •Yes  •
                                   •No   •
                                   •••••••
               < Back >     < Next >     < Explain Less >
```

Chose "Yes"

```
---------------------------
```

```
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                   •
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•BootSecurity.pm Module 4 of 0••••••••••••••••••••••••••••••••••••••••••••••••••
•Q: Would you like to password-protect the GRUB prompt? [N]                   •
•If an attacker has physical access to this machine, and particularly to the  •
•keyboard, s/he could get super-user access through the Grand Unified         •
•Bootloader (GRUB) command line.  We will look at other ways to prevent this  •
•later, but one easy way is to password-protect the GRUB prompt.  If GRUB is  •
•password-protected, any user can reboot the machine normally, but only users •
•with the password can pass arguments to the GRUB prompt.                     •
•                                                                             •
•Note that this option can interfere dual-booting with a second operating     •
•system, since dual booting often requires that type an O/S name to boot one of•
•the two operating systems.  If this machine sits in a general purpose lab and •
•dual boots, you probably shouldn't choose this option.                       •
•                                                                             •
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "No"
(we have physical security)

```
---------------------------
```

```
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                   •
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•BootSecurity.pm Module 4 of 0••••••••••••••••••••••••••••••••••••••••••••••••••
•Q: Would you like to disable CTRL-ALT-DELETE rebooting? [N]                  •
•Disabling CTRL-ALT-DELETE rebooting is designed to prevent an attacker with  •
•access to the machine's keyboard from being able to reboot the machine.  A   •
•reboot done in this manner should not damage the file system, as it shuts the •
•machine down cleanly, writing out all pending data in the disk cache to disk •
•first.  Even with this functionality disabled, however, an attacker could just•
•power cycle machine or pull the power cord.                                  •
•                                                                             •
•Unless the power line, switch and case of the machine can be physically      •
•protected, this precaution is wholly unnecessary.  Given the fact that the   •
•attacker _can_ reboot the machine, would you prefer that s/he do it in a way •
•potentially damages the file system? Think carefully here, as maintaining the •
•integrity of the machine's file system may be secondary to the goal of keeping•
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "No"

```
---------------------------
```

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                   Bastille                                   •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•BootSecurity.pm Module 4 of 0••••••••••••••••••••••••••••••••••••••••••••••••••
•Q: Would you like to password protect single-user mode? [Y]                   •
•Anyone who can physically interact with your system can tell the bootloader to•
•bring your machine up in "single user mode", where s/he is  given root        •
•privileges and everyone else is locked out of the system.  This doesn't       •
•require a password on most Unix systems.  The method differs with the         •
•bootloader being used, thus on each operating system revision and             •
•architecture.  You can test this attack on a Linux system that uses LILO by   •
•typing "linux single" at the LILO: prompt.                                    •
•                                                                              •
•Bastille can password-protect the bootprompt for you.  You won't have to      •
•remember another password--single user mode, or "root" mode, will require  the•
•root password.                                                                •
•                                                                              •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "Yes"

```
---------------------------
```

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                   Bastille                                   •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•SecureInetd.pm Module 5 of 0•••••••••••••••••••••••••••••••••••••••••••••••••••
•Q: Would you like to set a default-deny on TCP Wrappers and xinetd? [N]       •
•Not recommended for most users:                                               •
•                                                                              •
•Many network services can be configured to restrict access to certain network •
•addresses (and in the case of 'xinetd' services in Linux-Mandrake 8.0 and Red •
•Hat 7.x, other criteria as well). For services running under the older 'inetd •
•' super-server (found in older versions of Linux-Mandrake and Red Hat, and    •
•current versions of some other distributions), some standalone services like  •
•OpenSSH, and --unless otherwise configured-- services running under Red Hat's •
•xinetd super-server, you can configure restrictions based on network address  •
•in /etc/hosts.allow. The services using inetd or xinetd typically include     •
•telnet, ftp, pop, imap, finger, and a number of other services.               •
•                                                                              •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "Yes"

```
---------------------------
```

```
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                   Bastille                                    •
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•SecureInetd.pm Module 5 of 0••••••••••••••••••••••••••••••••••••••••••••••••••••
•Q: Should Bastille ensure the telnet service does not run on this system? [y] •
•Telnet is not secure.                                                          •
•                                                                               •
•Telnet is shipped on most operating systems for backward compatibility, and it•
•should not be used in an untrusted network.                                    •
•                                                                               •
•Telnet is a clear-text protocol, meaning that any data transferred, including •
•passwords, can be monitored by anyone else on your network (even if you use a •
•switching router, as switches were designed for performance, not security and •
•can be made to broadcast).  Other networks can monitor this information too if•
•the telnet session crosses multiple LANs.                                      •
•                                                                               •
•There are also other more active attacks.  For example, anyone who can        •
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "Yes"

```
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                   Bastille                                    •
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•SecureInetd.pm Module 5 of 0••••••••••••••••••••••••••••••••••••••••••••••••••••
•Q: Should Bastille ensure inetd's FTP service does not run on this system? [y]•
•Ftp is another problematic protocol.  First, it is a clear-text protocol, like•
•telnet -- this allows an attacker to eavesdrop on sessions and steal passwords•
•. This also allows an attacker to take over an FTP session, using a clear-text•
•-takeover tool like Hunt or Ettercap.  Second, it can make effective          •
•firewalling difficult due to the way FTP requires many ports to stay open.    •
•Third, every major FTP daemon has had a long history of security vulnerability•
•-- they represent one of the major successful attack vectors for remote root  •
•attacks.                                                                       •
•                                                                               •
•FTP can be replaced by Secure Shell's scp and sftp programs.                   •
•                                                                               •
•NOTE: Answering "yes" to this question will also prevent the use of this      •
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "Yes"

```
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                   •
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•SecureInetd.pm Module 5 of 0••••••••••••••••••••••••••••••••••••••••••••••••••
•Q: Would you like to display "Authorized Use" messages at log-in time? [Y]    •
•At this point you can create "Authorized Use Only" messages for your site.    •
•These may be very helpful in prosecuting system crackers you may catch trying •
•to break into your system.  Bastille can make default messages which you may  •
•then later edit.  This is sort of like an "anti-welcome mat" for your computer•
•.                                                                             •
•                                                                              •
•Would you like to display "Authorized Use" messages at log-in time? [Y]       •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "Yes"

```
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                   •
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                           <Press TAB to go on>                               •
•                                                                              •
•A default login/telnet/ftp "Authorized Use Only" banner will be created, and  •
•will be found in /etc/issue.  You should modify this banner to apply more     •
•specifically to your organization (for instance, adding any site-specific     •
•information to the default warnings).  If this is a corporate site, check with•
•your corporate counsel to determine the most appropriate warning for the      •
•banner.  These banners, according to CIAC's bulletin                          •
•                                                                              •
•   (http://ciac.llnl.gov/ciac/bulletins/j-043.shtml)                          •
•                                                                              •
•may make it much easier to prosecute intruders.  By including this default    •
•banner, neither the Bastille development team nor Hewlett-Packard Company take•
•any responsibility for your ability to prosecute system crackers. Please,     •
•especially if you run a corporate site, review/replace this with more specific•
•language.                                                                     •
•                                                                              •
•                                                                              •
•                                                                              •
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
```

Hit the TAB key

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                   Bastille                                   •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•SecureInetd.pm Module 5 of 0••••••••••••••••••••••••••••••••••••••••••••••••••••
•Q: Who is responsible for granting authorization to use this machine?        •
•Bastille will start to make the banner more specific by telling the user who  •
•is responsible for this machine.  This will state explicitly from whom the    •
•user needs to obtain authorization to use this machine.  Please type in the   •
•name of the company, person, or other organization who owns or is responsible •
•for this machine.                                                             •
•                                                                              •
•Who is responsible for granting authorization to use this machine?           •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
 ••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
 •Answer: Membrich.com                                                        •
 •                                                                             •
 ••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                < Back >     < Next >     < Explain Less >
```

Entered Membrich.com
Chose "Next"

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                   Bastille                                   •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•DisableUserTools.pm Module 6 of 0•••••••••••••••••••••••••••••••••••••••••••••••
•Q: Would you like to disable the gcc compiler? [N]                            •
•The most common technique for the bulk of the system crackers out there is to •
•gain access to your system, often through a regular user account, and then use•
•that access to compile exploits against your system or other systems.         •
•Disabling the gcc compiler on your system will slow these crackers down, and  •
•may even prevent some attacks entirely.                                       •
•                                                                              •
•If this machine is a dedicated server/firewall, which does not have users who •
•need to compile programs, this action is strongly recommended.  Otherwise, you•
•should very carefully consider whether you will be inconveniencing your users •
•by disabling the compiler.  If you do chose to disable it, we'll do so by only•
•allowing root access to the compiler.                                         •
•                                                                              •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                   •••••••
                                   •Yes  •
                                   •No   •
                                   •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "No"
(Just in case I need to install something later.)

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                    •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•ConfigureMiscPAM.pm Module 7 of 0•••••••••••••••••••••••••••••••••••••••••••••
•Q: Would you like to put limits on system resource usage? [N]                 •
•Denial of Service attacks are often very difficult to defend against, since   •
•they don't require access of any kind to the target machine. Since several    •
•major daemons, including the web, name, and FTP servers, may run as a         •
•particular user, you can limit the effectiveness of many Denial of Service    •
•attacks by modifying /etc/security/limits.conf.  If you restrict the resources•
•available in this manner, you can effectively cripple most Denial of Service  •
•attacks.                                                                      •
•                                                                              •
•If you choose this option, you'll be setting the following initial limits on  •
•resource usage:                                                               •
•                                                                              •
•   - The number of allowed core files will be set to zero.  Core files        •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "No"

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                    •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•ConfigureMiscPAM.pm Module 7 of 0•••••••••••••••••••••••••••••••••••••••••••••
•Q: Should we restrict console access to a small group of user accounts? [N]   •
•Under some distributions, users logged in at the console have some special    •
•access rights (like the ability to mount the CD-ROM drive).  You can disable  •
•this special access entirely, but a more flexible option is to restrict       •
•console access to a small group of trusted user accounts.                     •
•                                                                              •
•Should we restrict console access to a small group of user accounts? [N]      •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "No"
There is only one user, membrich.

```
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                   •
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•Logging.pm Module 8 of 0••••••••••••••••••••••••••••••••••••••••••••••••••••••
•Q: Would you like to add additional logging? [Y]                             •
•We would like to configure additional logging for your system. We will give  •
•you the option to log to a remote host, if your site already has one.  We will•
•add two additional logging files to the default setup and will also log some •
•status messages to the 7th and 8th virtual terminals (the ones you'll see when•
•you hit ALT-F7 and ALT-F8).  This additional logging will not change the     •
•existing log files at all, so this is by no means a "risky" move.            •
•                                                                             •
•Would you like to add additional logging? [Y]                                •
•                                                                             •
•                                                                             •
•                                                                             •
•                                                                             •
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "Yes"

```
---------------------------
```

```
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                   •
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                           <Press TAB to go on>                              •
•                                                                             •
•This script is adding additional logging files:                              •
•                                                                             •
•/var/log/kernel       --    kernel messages /var/log/syslog       --         •
•messages of severity "warning" and "error"                                   •
•                                                                             •
•Also, if you check the 7th and 8th TTY's, by hitting ALT-F7 or ALT-F8, you'll •
•find that we are now logging to virtual TTY's as well.  If you try this,     •
•remember that you can use ALT-F1 to get back to the first virtual TTY.       •
•                                                                             •
•                                                                             •
•                                                                             •
•                                                                             •
•                                                                             •
•                                                                             •
•                                                                             •
•                                                                             •
•                                                                             •
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
```

Hit the TAB key.

```
---------------------------
```

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                    •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•Logging.pm Module 8 of 0••••••••••••••••••••••••••••••••••••••••••••••••••••••
•Q: Do you have a remote logging host? [N]                                    •
•If you already have a remote logging host, we can set this machine to log to •
•it.                                                                          •
•                                                                             •
•Do you have a remote logging host? [N]                                       •
•                                                                             •
•                                                                             •
•                                                                             •
•                                                                             •
•                                                                             •
•                                                                             •
•                                                                             •
•                                                                             •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "No"
(Haven't set up a remote logging host, not yet at least.)

```
---------------------------
```

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                    •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•MiscellaneousDaemons.pm Module 9 of 0•••••••••••••••••••••••••••••••••••••••••
•To make the operating system more secure, we try to deactivate all system    •
•daemons, especially those running at a high/unlimited level of privilege.    •
•Each active system daemon serves as a potential point of break-in, which might•
•allow an attacker illegitimate access to your system.  An attacker can use   •
•these system daemons to gain access if they are later found to have a bug or •
•security vulnerability.                                                      •
•                                                                             •
•We practice a minimalist principle here: minimize the number of privileged   •
•system daemons and you can decrease your chances of being a victim should one •
•of the standard daemons be found later to have a vulnerability.  This section •
•will require careful attention, but if you have doubts, you should be able to •
•safely select the default value in most cases.                               •
•                                                                             •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••



                < Back >     < Next >     < Explain Less >
```

Chose "Next"

```
---------------------------
```

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                    •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•TMPDIR.pm Module 17 of 0•••••••••••••••••••••••••••••••••••••••••••••••••••••••
•Q: Would you like to install TMPDIR/TMP scripts? [N]                          •
•Many programs use the /tmp directory in ways that are dangerous on multi-user •
•systems. Many of those programs will use an alternate directory if one is     •
•specified with the TMPDIR or TMP environment variables. We can install scripts•
•that will be run when users log in that safely create suitable temporary      •
•directories and set the TMPDIR and TMP environment variables. This depends on •
•your system supporting /etc/profile.d scripts.                                •
•                                                                              •
•Would you like to install TMPDIR/TMP scripts? [N]                             •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                <  Back  >     <  Next  >     < Explain Less >
```

Chose "No"
Don't need it.

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                    •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•Firewall.pm Module 18 of 0•••••••••••••••••••••••••••••••••••••••••••••••••••••
•Q: Would you like to run the packet filtering script? [N]                     •
•Using the packet filtering script, you will be able to do packet filtering/   •
•modification via the Linux kernel.  You can use this to block certain types of•
•connections to or from your machine, to turn your machine into a small        •
•firewall, and to do Network Address Translation (also known as "IP            •
•masquerading"), which lets several machines share a single IP address.        •
•                                                                              •
•If you install the packet filtering script, it will create firewalling        •
•instructions for you. You will be prompted to make various choices (with      •
•suggested defaults), but you may need to edit it for your particular site and •
•WILL need to individually activate it.                                        •
•                                                                              •
•This script supports both kernel 2.2 (ipchains) and 2.4 (iptables if available•
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                <  Back  >     <  Next  >     < Explain Less >
```

Chose "No"
We can set this up at a later date.

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                    •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•End of 0•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•Q: Are you finished answering the questions, i.e. may we make the changes?    •
•We will now implement the choices you have made here.                         •
•                                                                              •
•Answer NO if you want to go back and make changes!                            •
•                                                                              •
•                                                                              •
•Are you finished answering the questions, i.e. may we make the changes?       •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "Yes"

```
---------------------------

•Bastille Credits     (press TAB to go on)••••••••••••••••••••••••••••••••••••••
•    Jon Lasser                 - Lead Coordinator                             •
•    Jay Beale                  - Lead Developer                               •
•    Peter Watkins              - Core Developer, Major Contributor            •
•    Mike Rash                  - Developer - Bastille IDS                     •
•    Sweth Chandramouli         - Developer - Bastille Automation              •
•    HP Bastille Dev Team       - Developers - HP-UX Port, Design/Arch.        •
•    Paul Allen                 - Developer - User Interface                   •
•    Javier Fdez-Sanguino       - Developer - Debian Port                      •
•    Niki Rahimi (IBM)         - Developer - SuSE and TurboLinux Ports         •
•    Bruce Meyer, Donald Wilder - Beta Testers Extraordinaire v1&v1.2          •
•    James Durkin              - Testing and Ideas                             •
•    Yoann Vandoorselaere       - Developer - msec creator                     •
•    Don E Groves, Jr           - Design Contributor                           •
•    Manuel Caphina             - Developer -- Bastille IDS/NADS               •
•    Peter Friedman             - Developer -- webget                          •
•    Rob Sherwood               - Developer -- process accounting              •
•    Thomas Mangin              - Contributor - Beta Testing, Suggestions      •
•    Susan Marie Groppi        - Text and Documentation Coordinator            •
•    David A. Wheeler          - Contributor -- Miscellaneous Suggestions      •
•    Ben Woodard                - Infrastructure Liaison                       •
•    Kurt Seifried             - Gadfly                                        •
•    F.Soderblom, T.Lovqvist, K.Steves - HP-UX content from Armor              •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
```

Hit the TAB key.

```
---------------------------

[root@localhost membrich]#
```

Before rebooting, we need to make some changes to the /etc/hosts.allow file or we won't be able to connect with ssh.

Changing /etc/hosts.allow from:

```
#
# hosts.allow   This file describes the names of the hosts which are
#               allowed to use the local INET services, as decided
#               by the '/usr/sbin/tcpd' server.
#

# Bastille: default deny
# no safe_finger for in.fingerd (prevent loops)
in.fingerd : ALL : DENY
# but everything else is denied & reported with safe_finger
ALL : ALL : spawn (/usr/sbin/safe_finger -l @%h | /bin/mail -s "Port Denial noted %d-
%h" root) & : DENY
```

To:

```
#
# hosts.allow   This file describes the names of the hosts which are
#               allowed to use the local INET services, as decided
#               by the '/usr/sbin/tcpd' server.
#

sshd : 172.16.1.33
# Bastille: default deny
# no safe_finger for in.fingerd (prevent loops)
in.fingerd : ALL : DENY
# but everything else is denied & reported with safe_finger
ALL : ALL : spawn (/usr/sbin/safe_finger -l @%h | /bin/mail -s "Port Denial noted %d-
%h" root) & : DENY
```

Where 172.16.1.33 is my workstation.

Rebooted.

2.3.2. Disable Unnecessary SetUID and SetGID Files.

The concept of disabling SetUID and SetGID files came from Sean Boran, available at: http://www.boran.com/security/sp/Solaris_hardening3.html. Boran's instructions are specifically for Solaris, but we can adapt them to a RedHat 9 machine:

> Files which have the SUID bit set (an "s" where the execute bit for the owner/group is shown in 'ls' listings) allow the user executing the program to assume the identity/group of the owner of the program. This is typically used to allow normal users to access certain function typically only allowed to root, for example binding to low ports, mounting a floppy disk, etc. The problem is that historically, many security weakness have been found in such programs allowing attackers with local accounts to become root by exploiting buffer over flows, race conditions etc.

- Solaris has many "SUID root" binaries and each one presents a risk, so when hardening systems it is advisable to disable as many SUID program as possible.
- The purpose of this section is to provide a brief overview of the subject, a list of documents and scripts for disabling SUID files is provided.
- See [8] for SUID references and further reading.

What SUID files are on the system?

The find command can be used to list all SUID files:
find / -perm -u+s -ls

or all SGID files:
find / -perm -g+s -ls

How should we handle SUID files? Possible courses of action, in order of preference, are:

- Remove the package containing the offending file
- Disable the program (e.g. chmod 000 FILENAME)
- The SUID bit can be removed (e.g. chmod ug-s FILENAME)
- Restrict the file to a group of users (first remove world access: "chmod o-rwx", then allow a group "chgrp MYGROUP MYFILE") .

(Boran 2001)

2.3.2.1. Find SetUID and SetGID Files.

Following Boran's instructions, find the files that have the SUID or SGID bit set:

```
[root@localhost membrich]# find / -perm -u+s -ls > suid_files
find: /proc/651/fd/4: No such file or directory
[root@localhost membrich]# find / -perm -g+s -ls > sgid_files
find: /proc/652/fd/4: No such file or directory
[root@localhost membrich]#
```

The SetUID files are:

```
 32641   36 -rwsr-xr-x   1 root     root        35376 Feb 12  2003 /usr/bin/chage
 32643   36 -rwsr-x---   1 root     root        36216 Feb 12  2003 /usr/bin/gpasswd
 33219   16 -rws--x--x   1 root     root        14140 Feb 24  2003 /usr/bin/chfn
 33220   12 -rws--x--x   1 root     root        11644 Feb 24  2003 /usr/bin/chsh
 33239    8 -rws--x--x   1 root     root         4728 Feb 24  2003 /usr/bin/newgrp
 33376   16 -r-s--x--x   1 root     root        16336 Feb 13  2003 /usr/bin/passwd
 34453  112 -rwsr-xr-x   1 root     root       110114 Feb 19  2003 /usr/bin/crontab
 97098  152 -rws--x--x   1 root     root       150688 Sep 17 09:13
/usr/libexec/openssh/ssh-keysign
 33382   28 -rwsr-x---   1 root     root        26680 Feb 24  2003
/usr/sbin/userhelper
 59883  100 -rwsr-xr-x   1 root     root        97260 Oct 29 06:44 /bin/su
 47076    8 -r-s--x--x   1 root     root         7088 Feb 10  2003
/sbin/pam_timestamp_check
 47077  124 -r-sr-xr-x   1 root     root       119528 Feb 10  2003 /sbin/pwdb_chkpwd
 47078   20 -r-sr-xr-x   1 root     root        17220 Feb 10  2003 /sbin/unix_chkpwd
```

The SetGID files are:

```
 33205    8 -r-xr-sr-x   1 root     tty          6908 Feb 10  2003 /usr/bin/wall
 33250   44 -rwxr-sr-x   1 root     tty         43593 Feb 24  2003 /usr/bin/write
 34452   36 -rwxr-sr-x   1 root     utmp        34186 Feb 18  2003 /usr/sbin/utempter
 47155   28 -rwxr-s---   1 root     root        28538 Mar 12  2003 /sbin/netreport
```

2.3.2.2. Removing SetUID and SetGID Bits.

```
[root@localhost membrich]# chmod ug-s /usr/bin/chage
[root@localhost membrich]# chmod ug-s /usr/bin/gpasswd
[root@localhost membrich]# chmod ug-s /usr/bin/chfn
[root@localhost membrich]# chmod ug-s /usr/bin/chsh
[root@localhost membrich]# chmod ug-s /usr/bin/newgrp
[root@localhost membrich]# chmod ug-s /usr/bin/crontab
[root@localhost membrich]# chmod ug-s /usr/libexec/openssh/ssh-keysign
[root@localhost membrich]# chmod ug-s /sbin/unix_chkpwd
[root@localhost membrich]#
[root@localhost membrich]# chmod ug-s /usr/bin/wall
[root@localhost membrich]# chmod ug-s /usr/bin/write
[root@localhost membrich]# chmod ug-s /sbin/netreport
[root@localhost membrich]#
```

This is what is left over:

```
[root@localhost membrich]# find / -perm -u+s -ls
find: /proc/666/fd/4: No such file or directory
 33376   16 -r-s--x--x   1 root     root        16336 Feb 13  2003 /usr/bin/passwd
 33382   28 -rwsr-x---   1 root     root        26680 Feb 24  2003
/usr/sbin/userhelper
 59883  100 -rwsr-xr-x   1 root     root        97260 Oct 29 06:44 /bin/su
 47076    8 -r-s--x--x   1 root     root         7088 Feb 10  2003
/sbin/pam_timestamp_check
 47077  124 -r-sr-xr-x   1 root     root       119528 Feb 10  2003 /sbin/pwdb_chkpwd
[root@localhost membrich]# find / -perm -g+s -ls
find: /proc/667/fd/4: No such file or directory
 34452   36 -rwxr-sr-x   1 root     utmp        34186 Feb 18  2003 /usr/sbin/utempter
[root@localhost membrich]#
```

3. Sensor.

3.1. Install Linux.

Redhat has a pretty neat automated install system called Kickstart. An automated install file is created for you automatically each time you install the O/S. Therefore, for each server I build, I can use Kickstart and the server's Kickstart file to build my sensors.

It is done by adding a ks.cfg file to a Redhat boot disk, then running the install from the boot disk.

3.1.1. Create Redhat Boot Disk.

http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/install-guide/s1-steps-install-cdrom.html#S2-STEPS-MAKE-DISKS

From my Windows workstation, inserted the first Redhat 9 CD,
Brought up a Command Prompt,

```
E:\cd \dosutils
E:\dosutils> rawrite
Enter disk image source file name: ..\images\bootdisk.img
Enter target diskette drive: a:
Please insert a formatted diskette into drive A: and
press --ENTER-- : [Enter]
E:\dosutils>
```

3.1.2. Get Kickstart File from Server.

The Kickstart file is found in the root user's home dir:

```
[root@localhost membrich]# ls /root
anaconda-ks.cfg  install.log  install.log.syslog
[root@localhost membrich]#
```

The file anaconda-ks.cfg is a record of what was done during the install.

3.1.3. Edit the Kickstart File.

Since this is for a different type of machine (snort sensor vs. snort server), we want a different set of packages installed. We no longer need mysql, php, nessus, etc.

3.1.3.1. Edit Partition Table.

The anaconda-ks.cfg file has the disk partitioning info used on the previous machine, but it is commented out:

```
# The following is the partition information you requested
# Note that any partitions you deleted are not expressed
# here so unless you clear all partitions first, this is
# not guaranteed to work
#clearpart --linux
#part /boot --fstype ext3 --size=150 --ondisk=hda --asprimary
#part /usr --fstype ext3 --size=1000 --ondisk=hda
#part /home --fstype ext3 --size=1000 --ondisk=hda
#part / --fstype ext3 --size=700 --ondisk=hda --asprimary
#part /tmp --fstype ext3 --size=500 --ondisk=hda
#part swap --size=256 --ondisk=hda --asprimary
#part /var --fstype ext3 --size=100 --grow --ondisk=hda
```

My snort sensor has a smaller hard drive of 4 GB, so I need to change the sizes of the partitions, here's what I'm using:

```
# The following is the partition information you requested
# Note that any partitions you deleted are not expressed
# here so unless you clear all partitions first, this is
# not guaranteed to work
clearpart --linux
part /boot --fstype ext3 --size=150 --ondisk=hda --asprimary
part /usr --fstype ext3 --size=700 --ondisk=hda
part /home --fstype ext3 --size=700 --ondisk=hda
part / --fstype ext3 --size=500 --ondisk=hda --asprimary
part /tmp --fstype ext3 --size=300 --ondisk=hda
part swap --size=256 --ondisk=hda --asprimary
part /var --fstype ext3 --size=100 --grow --ondisk=hda
```

3.1.3.2. Edit "packages" Section.

The default install packages are not listed unless I asked that they be removed (denoted with a minus sign). Additional packages are listed (no minus sign).

Commenting out records is sufficient to cause unwanted additional packages to not be installed.

Changed from:

```
%packages
@ Dialup Networking Support
-libtool-libs
-elfutils
openssl-devel
-kernel-pcmcia-cs
mysql-devel
m4
-statserial
-portmap
-jfsutils
-lha
-libwvstreams
-dhclient
-ftp
-gpm
-setuptool
-lrzsz
-isdn4k-utils
perl-DBD-MySQL
-wireless-tools
-quota
```

```
-stunnel
-unix2dos
-dump
-nss_ldap
-finger
libpng
binutils
glibc-kernheaders
-specspo
-nfs-utils
libpng10
-pam_krb5
-irda-utils
tripwire
freetype-devel
mysql
libpcap
-lokkit
libpng-devel
-redhat-config-network-tui
-bc
-devlabel
-wget
-cyrus-sasl-plain
-rp-pppoe
-attr
-mtr
-ppp
-jwhois
-rsync
-dos2unix
-python-optik
gd
-lftp
-apmd
-fbset
-reiserfs-utils
-pinfo
libjpeg-devel
-sudo
-rdist
glibc-devel
gcc
-tcsh
-pspell
zlib-devel
-talk
-hesiod
-wvdial
flex
krb5-devel
libjpeg
bzip2-devel
-sendmail
-procmail
-rdate
-slocate
-mt-st
-pam_smb
-mtools
-rmt
-rsh
-ypbind
```

```
-up2date
-ethtool
freetype
bison
-vconfig
-mailcap
-krbafs
-autofs
-nscd
-lockdev
perl-DBI
mysql-server
-yp-tools
-rhnlib
-pax
-rpm-python
-aspell
-pyOpenSSL
-minicom
-anacron
perl-CGI
-star
-telnet
cpp
```

To:

```
%packages
@ Dialup Networking Support
-libtool-libs
-elfutils
openssl-devel
-kernel-pcmcia-cs
#mysql-devel
m4
-statserial
-portmap
-jfsutils
-lha
-libwvstreams
-dhclient
-ftp
-gpm
-setuptool
-lrzsz
-isdn4k-utils
#perl-DBD-MySQL
-wireless-tools
-quota
-stunnel
-unix2dos
-dump
-nss_ldap
-finger
#libpng
binutils
glibc-kernheaders
-specspo
-nfs-utils
#libpng10
-pam_krb5
-irda-utils
tripwire
```

```
#freetype-devel
#mysql
libpcap
-lokkit
#libpng-devel
-redhat-config-network-tui
-bc
-devlabel
-wget
-cyrus-sasl-plain
-rp-pppoe
-attr
-mtr
-ppp
-jwhois
-rsync
-dos2unix
-python-optik
#gd
-lftp
-apmd
-fbset
-reiserfs-utils
-pinfo
#libjpeg-devel
-sudo
-rdist
glibc-devel
gcc
-tcsh
-pspell
zlib-devel
-talk
-hesiod
-wvdial
flex
krb5-devel
#libjpeg
bzip2-devel
-sendmail
-procmail
-rdate
-slocate
-mt-st
-pam_smb
-mtools
-rmt
-rsh
-ypbind
-up2date
-ethtool
#freetype
bison
-vconfig
-mailcap
-krbafs
-autofs
-nscd
-lockdev
#perl-DBI
#mysql-server
-yp-tools
-rhnlib
```

```
-pax
-rpm-python
-aspell
-pyOpenSSL
-minicom
-anacron
#perl-CGI
-star
-telnet
cpp
```

3.1.4. Add the Edited Kickstart File to the Boot Floppy.

Save the Kickstart file (was anaconda-ks.cfg) to the boot floppy's root dir as ks.cfg.

3.1.5. Use the Boot Floppy to Run Kickstart Install.

Boot from the boot floppy.
When you get the "boot:" prompt, type in "linux ks=floppy" to run the Kickstart install.

3.1.6. Disk Size Warning.

I received a warning about the disk geometry not matching. The suggested geometry was wrong too, so I chose to Ignore. After the install, went back to check the partition sizes, looks good:

```
[membrich@localhost membrich]$ df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/hda2             485M   61M  399M  14% /
/dev/hda1             146M  9.0M  129M   7% /boot
/dev/hda5             689M   17M  638M   3% /home
none                   31M     0   31M   0% /dev/shm
/dev/hda7             291M  8.1M  268M   3% /tmp
/dev/hda6             689M  340M  315M  52% /usr
/dev/hda8             1.5G   43M  1.4G   4% /var
[membrich@localhost membrich]$
```

3.1.7. Post Install Cleanup.

3.1.7.1. Added Myself as a User.

```
[root@localhost root]# useradd -c "Mark Embrich" -m -d /home/membrich -u 1101 membrich
[root@localhost root]# passwd membrich
Changing password for user membrich.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost root]#
```

3.1.7.2. Set up eth1 Interface.

Edited /etc/sysconfig/network-scripts/ifcfg-eth1:

```
[membrich@localhost membrich]$ cat /etc/sysconfig/network-scripts/ifcfg-eth1
```

```
DEVICE=eth1
BOOTPROTO=static
BROADCAST=172.16.255.255
IPADDR=172.16.1.252
NETMASK=255.255.0.0
NETWORK=172.16.0.0
ONBOOT=yes
[membrich@localhost membrich]$
```

Restarted eth1 interface by running:

```
[root@localhost root]# /etc/init.d/network restart
```

3.1.7.3. Remove Unnecessary Packages.

```
[membrich@localhost membrich]$ rpm -qa > packages
[membrich@localhost membrich]$ sort packages > sorted_pkgs
[membrich@localhost membrich]$ wc -l sorted_pkgs
    149 sorted_pkgs

[membrich@localhost membrich]$ su
Password:
[root@localhost membrich]# rpm -e ash
[root@localhost membrich]# rpm -e at
[root@localhost membrich]# rpm -e authconfig
[root@localhost membrich]# rpm -e comps
[root@localhost membrich]# rpm -e cpio
[root@localhost membrich]# rpm -e ed
[root@localhost membrich]# rpm -e hdparm
[root@localhost membrich]# rpm -e hotplug
[root@localhost membrich]# rpm -e lilo
[root@localhost membrich]# rpm -e redhat-config-mouse
[root@localhost membrich]# rpm -e rhpl
[root@localhost membrich]# rpm -e pyxf86config
[root@localhost membrich]# rpm -e python
[root@localhost membrich]# rpm -e raidtools
[root@localhost membrich]# rpm -e redhat-logos
[root@localhost membrich]# rpm -e usbutils
[root@localhost membrich]#

[root@localhost membrich]# rpm -qa > packages1
[root@localhost membrich]# sort packages1 > sort_pkgs1
[root@localhost membrich]# wc -l sort_pkgs1
    133 sort_pkgs1
[root@localhost membrich]#
```

3.1.7.4. Fix grub.conf.

Removing the redhat-logos messes up the grub splashimage. We'll fix that by commenting out the splashimage line.

Change /boot/grub/grub.conf from:

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/hda2
#          initrd /initrd-version.img
#boot=/dev/hda
default=0
timeout=10
splashimage=(hd0,0)/grub/splash.xpm.gz
title Red Hat Linux (2.4.20-8)
        root (hd0,0)
        kernel /vmlinuz-2.4.20-8 ro root=LABEL=/ hdb=ide-scsi
        initrd /initrd-2.4.20-8.img
```

To:

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/hda2
#          initrd /initrd-version.img
#boot=/dev/hda
default=0
timeout=10
#splashimage=(hd0,0)/grub/splash.xpm.gz
title Red Hat Linux (2.4.20-8)
        root (hd0,0)
        kernel /vmlinuz-2.4.20-8 ro root=LABEL=/ hdb=ide-scsi
        initrd /initrd-2.4.20-8.img
```

Rebooted to make sure I didn't break anything.

```
[root@localhost membrich]# /sbin/shutdown -r now

Broadcast message from root (pts/0) (Sat Oct 27 23:54:40 2001):

The system is going down for reboot NOW!
```

3.1.8. Install Patches.

Since the sensor has no packages that are not already installed on the server, we don't need to do any research to find out which patches are needed. We'll just install the same patches.

As the time of this writing, November 9, 2003, we need parts of the following patches:
rhsa-2003-091
rhba-2003-136
rhsa-2003-174
rhsa-2003-175
rhba-2003-140
rhsa-2003-199
rhba-2003-263
rhsa-2003-279
rhsa-2003-292

rhsa-2003-256
rhsa-2003-281
rhsa-2003-309

3.1.8.1. Install RedHat's Public Key.

Import redhat public key (for checking authenticity of patches):
RedHat Public Key can be found on the root directory of CD1.

```
[root@localhost membrich]# mount -t iso9660 /dev/cdrom /mnt/cdrom
mount: block device /dev/cdrom is write-protected, mounting read-only
[root@localhost membrich]# ls /mnt/cdrom
autorun               README.it              RELEASE-NOTES-fr.html
dosutils              README.ja              RELEASE-NOTES.html
EULA                  README.ko              RELEASE-NOTES-it.html
GPL                   README.pt              RELEASE-NOTES-ja.html
images                README.pt_BR           RELEASE-NOTES-ko.html
isolinux              README.zh_CN           RELEASE-NOTES-pt_BR.html
README                README.zh_TW           RELEASE-NOTES-pt.html
README-Accessibility  RedHat                 RELEASE-NOTES-zh_CN.html
README.de             RELEASE-NOTES          RELEASE-NOTES-zh_TW.html
README.es             RELEASE-NOTES-de.html  RPM-GPG-KEY
README.fr             RELEASE-NOTES-es.html  TRANS.TBL
[root@localhost membrich]# rpm --import /mnt/cdrom/RPM-GPG-KEY
[root@localhost membrich]#
```

3.1.8.2. Get the Patches to the Sensor.

I downloaded the necessary rpms to my workstation, then used scp to move them to our machine:

```
D:\download\redhat\patches>dir
 Volume in drive D is New Volume
 Volume Serial Number is 1C0E-19DB

 Directory of D:\download\redhat\patches

11/09/2003  05:04p      <DIR>          .
11/09/2003  05:04p      <DIR>          ..
11/09/2003  04:37p      <DIR>          rhba-2003-136
11/09/2003  04:40p      <DIR>          rhba-2003-140
11/10/2003  10:55p      <DIR>          rhba-2003-263
11/09/2003  04:34p      <DIR>          rhsa-2003-091
11/09/2003  04:38p      <DIR>          rhsa-2003-174
11/09/2003  04:40p      <DIR>          rhsa-2003-175
11/09/2003  04:42p      <DIR>          rhsa-2003-199
11/09/2003  05:01p      <DIR>          rhsa-2003-256
11/09/2003  04:53p      <DIR>          rhsa-2003-279
11/09/2003  05:03p      <DIR>          rhsa-2003-281
11/09/2003  04:57p      <DIR>          rhsa-2003-292
11/09/2003  05:05p      <DIR>          rhsa-2003-309
               0 File(s)              0 bytes
              14 Dir(s)   2,096,316,416 bytes free

D:\download\redhat\patches>pscp -r * membrich@172.16.1.252:/home/membrich
membrich@172.16.1.252's password:
glibc-2.3.2-27.9.i386.rpm |       3222 kB | 537.1 kB/s | ETA: 00:00:00 | 100%
glibc-common-2.3.2-27.9.i |      12148 kB | 506.2 kB/s | ETA: 00:00:00 | 100%
```

```
glibc-devel-2.3.2-27.9.i3 |       2285 kB | 571.4 kB/s | ETA: 00:00:00 | 100%
bash-2.05b-20.1.i386.rpm  |        737 kB | 368.7 kB/s | ETA: 00:00:00 | 100%
kernel-2.4.20-20.9.i586.r |      13468 kB | 498.8 kB/s | ETA: 00:00:00 | 100%
krb5-devel-1.2.7-14.i386. |        713 kB | 356.8 kB/s | ETA: 00:00:00 | 100%
krb5-libs-1.2.7-14.i386.r |        410 kB | 410.7 kB/s | ETA: 00:00:00 | 100%
tcpdump-3.7.2-1.9.1.i386. |        299 kB | 299.5 kB/s | ETA: 00:00:00 | 100%
gnupg-1.2.1-4.i386.rpm    |       1209 kB | 604.9 kB/s | ETA: 00:00:00 | 100%
unzip-5.50-33.i386.rpm    |        136 kB | 136.8 kB/s | ETA: 00:00:00 | 100%
perl-5.8.0-88.3.i386.rpm  |      14143 kB | 505.1 kB/s | ETA: 00:00:00 | 100%
perl-CGI-2.81-88.3.i386.r |        183 kB | 183.7 kB/s | ETA: 00:00:00 | 100%
openssh-3.5p1-11.i386.rpm |        177 kB | 177.6 kB/s | ETA: 00:00:00 | 100%
openssh-clients-3.5p1-11. |        300 kB | 300.0 kB/s | ETA: 00:00:00 | 100%
openssh-server-3.5p1-11.i |        177 kB | 177.1 kB/s | ETA: 00:00:00 | 100%
mysql-3.23.58-1.9.i386.rp |       5831 kB | 485.9 kB/s | ETA: 00:00:00 | 100%
mysql-devel-3.23.58-1.9.i |        567 kB | 567.4 kB/s | ETA: 00:00:00 | 100%
mysql-server-3.23.58-1.9. |       1097 kB | 365.7 kB/s | ETA: 00:00:00 | 100%
openssl-0.9.7a-20.i386.rp |       1103 kB | 552.0 kB/s | ETA: 00:00:00 | 100%
openssl-devel-0.9.7a-20.i |       1611 kB | 402.9 kB/s | ETA: 00:00:00 | 100%
coreutils-4.5.3-19.0.2.i3 |       2357 kB | 471.4 kB/s | ETA: 00:00:00 | 100%

D:\download\redhat\patches>
```

3.1.8.3. Install the Patches.

The order in which you install the patches is important.

I'll document this section by using two parts for each patch. First, I'll include the important information from the RedHat web site. Then I'll show you what I actually did to install the patch.

3.1.8.3.1. RHSA-2003-091.

> https://rhn.redhat.com/errata/RHSA-2003-091.html
> Updated kerberos packages fix various vulnerabilities
>
> Advisory: RHSA-2003:091-22
> Last updated on: 2003-04-02
>
> i386:
> krb5-devel-1.2.7-14.i386.rpm
> [via FTP] [via HTTP]   49e7783cb50c3694411b7856d098eff5
> krb5-libs-1.2.7-14.i386.rpm
> [via FTP] [via HTTP]   6cb5040d3a4bd21a801e8c1e5da6388d
>
> rpm -Fvh [filenames]
>
> (“Updated Kerberos Packages Fix Various Vulnerabilities.” 2003)

```
[root@localhost membrich]# rpm --checksig rhsa-2003-091/*.rpm
rhsa-2003-091/krb5-devel-1.2.7-14.i386.rpm: (sha1) dsa sha1 md5 gpg OK
rhsa-2003-091/krb5-libs-1.2.7-14.i386.rpm: (sha1) dsa sha1 md5 gpg OK
```

```
[root@localhost membrich]# rpm -Fvh rhsa-2003-091/*.rpm
Preparing...                ############################################ [100%]
   1:krb5-libs              ############################################ [ 50%]
   2:krb5-devel             ############################################ [100%]
[root@localhost membrich]#
```

3.1.8.3.2. RHBA-2003-136.

https://rhn.redhat.com/errata/RHBA-2003-136.html
glibc bugfix errata

Advisory: RHBA-2003:136-07
Last updated on: 2003-04-09

NOTE: Make sure you get the right glibc-2.3.27.9.iX86.rpm file. My server is a Pentium, so I'll use the i386 version.

i686:
glibc-2.3.2-27.9.i686.rpm
[via FTP] [via HTTP] 17698f5ff98d3cee2a72b2f206bc1589
i386:
glibc-2.3.2-27.9.i386.rpm
[via FTP] [via HTTP] 8fe9a661fd031b405d75a0e22a57925b
glibc-common-2.3.2-27.9.i386.rpm
[via FTP] [via HTTP] dc5b2aa636ff96c2ecfa144d373eac64
glibc-devel-2.3.2-27.9.i386.rpm
[via FTP] [via HTTP] 780dda739f56779fa953df64ddaeaeff

rpm -Fvh [filenames]

("Glibc Bugfix Errata." 2003)

```
[root@localhost membrich]# rpm --checksig rhba-2003-136/*.rpm
rhba-2003-136/glibc-2.3.2-27.9.i386.rpm: (sha1) dsa sha1 md5 gpg OK
rhba-2003-136/glibc-common-2.3.2-27.9.i386.rpm: (sha1) dsa sha1 md5 gpg OK
rhba-2003-136/glibc-devel-2.3.2-27.9.i386.rpm: (sha1) dsa sha1 md5 gpg OK
[root@localhost membrich]# rpm -Fvh rhba-2003-136/*.rpm
Preparing...                ############################################ [100%]
   1:glibc-common           ############################################ [ 33%]
   2:glibc                  ############################################ [ 67%]
Stopping sshd:[  OK  ]
Starting sshd:[  OK  ]
   3:glibc-devel            ############################################ [100%]
[root@localhost membrich]#
```

3.1.8.3.3. RHSA-2003-174.

https://rhn.redhat.com/errata/RHSA-2003-174.html
Updated tcpdump packages fix privilege dropping error

Advisory: RHSA-2003:174-04
Last updated on: 2003-05-15

i386:
tcpdump-3.7.2-1.9.1.i386.rpm
[via FTP] [via HTTP]   6cff8bf6b2425c361eec70ba3017d82b

(“Updated Tcpdump Packages Fix Privilege Dropping Error.” 2003)

Update instructions missing, assuming "rpm -Fvh".

```
[root@localhost membrich]# rpm --checksig rhsa-2003-174/*.rpm
rhsa-2003-174/tcpdump-3.7.2-1.9.1.i386.rpm: (sha1) dsa sha1 md5 gpg OK
[root@localhost membrich]# rpm -Fvh rhsa-2003-174/*.rpm
Preparing...                ########################################### [100%]
   1:tcpdump                ########################################### [100%]
[root@localhost membrich]#
```

3.1.8.3.4. RHSA-2003-175.

https://rhn.redhat.com/errata/RHSA-2003-175.html
Updated gnupg packages fix validation bug

Advisory: RHSA-2003:175-06
Last updated on: 2003-05-20

i386:
gnupg-1.2.1-4.i386.rpm
[via FTP] [via HTTP]   d0a0ad4a6e8708711d4bd5cae6118767

rpm -Fvh [filenames]

(“Updated Gnupg Packages Fix Validation Bug.” 2003)

```
[root@localhost membrich]# rpm --checksig rhsa-2003-175/*.rpm
rhsa-2003-175/gnupg-1.2.1-4.i386.rpm: (sha1) dsa sha1 md5 gpg OK
[root@localhost membrich]# rpm -Fvh rhsa-2003-175/*.rpm
Preparing...                ########################################### [100%]
   1:gnupg                  ########################################### [100%]
[root@localhost membrich]#
```

3.1.8.3.5. RHBA-2003-140.

https://rhn.redhat.com/errata/RHBA-2003-140.html
Updated bash packages fix several bugs

Advisory: RHBA-2003:140-05
Last updated on: 2003-06-23

i386:
bash-2.05b-20.1.i386.rpm
[via FTP] [via HTTP]   fa2aa425bd39ba4a9857dba700227dea

rpm -Fvh [filenames]

(“Updated Bash Packages Fix Several Bugs.” 2003)

```
[root@localhost membrich]# rpm --checksig rhba-2003-140/*.rpm
rhba-2003-140/bash-2.05b-20.1.i386.rpm: (sha1) dsa sha1 md5 gpg OK
[root@localhost membrich]# rpm -Fvh rhba-2003-140/*.rpm
Preparing...                ########################################### [100%]
   1:bash                   ########################################### [100%]
[root@localhost membrich]#
```

3.1.8.3.6. RHSA-2003-199.

https://rhn.redhat.com/errata/RHSA-2003-199.html
Updated unzip packages fix trojan vulnerability

Advisory: RHSA-2003:199-14
Last updated on: 2003-08-15

i386:
unzip-5.50-33.i386.rpm
[via FTP] [via HTTP]   e6d52c854a8ebba7dacb678a5edb5cb8

rpm -Fvh [filenames]

(“Updated Unzip Packages Fix Trojan Vulnerability.” 2003)

```
[root@localhost membrich]# rpm --checksig rhsa-2003-199/*.rpm
rhsa-2003-199/unzip-5.50-33.i386.rpm: (sha1) dsa sha1 md5 gpg OK
[root@localhost membrich]# rpm -Fvh rhsa-2003-199/*.rpm
Preparing...                ########################################### [100%]
   1:unzip                  ########################################### [100%]
[root@localhost membrich]#
```

3.1.8.3.7. RHBA-2003-263.

https://rhn.redhat.com/errata/RHBA-2003-263.html
Updated 2.4 kernel resolves obscure bugs.

Advisory: RHBA-2003:263-05
Last updated on: 2003-08-20

NOTE: Make sure you get the right kernel-2.4.20-20.9.iX86.rpm file. My server is a Pentium, so I'll use the i586 version. You can check your processor by using "uname -p":

```
[root@localhost membrich]# uname -p
i586
```

i386:
kernel-2.4.20-20.9.i386.rpm
[via FTP] [via HTTP]   7f855d126d0c66fa68c27b1b699d4d27
i586:
kernel-2.4.20-20.9.i586.rpm
[via FTP] [via HTTP]   0a5456524d186b2bf75325a2f843bd9f
i686:
kernel-2.4.20-20.9.i686.rpm
[via FTP] [via HTTP]   ed8725afb1fdaed2e3038d539043bff0

To install kernel packages manually, use "rpm -ivh <package>" and modify system settings to boot the kernel you have installed. To do this, edit /boot/grub/grub.conf and change the default entry to "default=0" (or, if you have chosen to use LILO as your boot loader, edit /etc/lilo.conf and run lilo)

Do not use "rpm -Uvh" as that will remove your running kernel binaries from your system. You may use "rpm -e" to remove old kernels after determining that the new kernel functions properly on your system.

(“Updated 2.4 Kernel Resolves Obscure Bugs.” 2003)

```
[root@localhost membrich]# rpm --checksig rhba-2003-263/*.rpm
rhba-2003-263/kernel-2.4.20-20.9.i586.rpm: (sha1) dsa sha1 md5 gpg OK
[root@localhost membrich]# rpm -ivh rhba-2003-263/*.rpm
Preparing...                ############################################ [100%]
   1:kernel                 ############################################ [100%]
[root@localhost membrich]#
```

Edited /boot/grub/grub.conf, changed default from 1 to 0.

```
[root@localhost membrich]# cp /boot/grub/grub.conf /boot/grub/grub.conf.old
[root@localhost membrich]# vi /boot/grub/grub.conf
```

Changed grub.conf from:

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/hda2
#          initrd /initrd-version.img
#boot=/dev/hda
default=1
timeout=10
#splashimage=(hd0,0)/grub/splash.xpm.gz
title Red Hat Linux (2.4.20-20.9)
        root (hd0,0)
        kernel /vmlinuz-2.4.20-20.9 ro root=LABEL=/ hdb=ide-scsi
        initrd /initrd-2.4.20-20.9.img
title Red Hat Linux (2.4.20-8)
        root (hd0,0)
        kernel /vmlinuz-2.4.20-8 ro root=LABEL=/ hdb=ide-scsi
        initrd /initrd-2.4.20-8.img
```

To:

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/hda2
#          initrd /initrd-version.img
#boot=/dev/hda
default=0
timeout=10
#splashimage=(hd0,0)/grub/splash.xpm.gz
title Red Hat Linux (2.4.20-20.9)
        root (hd0,0)
        kernel /vmlinuz-2.4.20-20.9 ro root=LABEL=/ hdb=ide-scsi
        initrd /initrd-2.4.20-20.9.img
title Red Hat Linux (2.4.20-8)
        root (hd0,0)
        kernel /vmlinuz-2.4.20-8 ro root=LABEL=/ hdb=ide-scsi
        initrd /initrd-2.4.20-8.img
```

Changing the "default" setting from 1 to 0 means it'll boot the first kernel listed rather than the second by default. You can still manually select the second kernel at boot time. We want to boot the first kernel because that's the newer one, the one we just installed.

Reboot the server:

```
[root@localhost membrich]# /sbin/shutdown -r now

Broadcast message from root (pts/0) (Fri Nov 21 01:09:37 2003):

The system is going down for reboot NOW!
```

Once we're satisfied that the new kernel works, we can remove the old kernel by simply removing the old kernel's package:

```
[root@localhost membrich]# rpm -qa | grep kernel
kernel-2.4.20-20.9
kernel-2.4.20-8
[root@localhost membrich]# rpm -e kernel-2.4.20-8
[root@localhost membrich]#
```

Removing the package also removes the entry from grub.conf:

```
[root@localhost membrich]# cat /boot/grub/grub.conf
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/hda2
#          initrd /initrd-version.img
#boot=/dev/hda
default=0
timeout=10
#splashimage=(hd0,0)/grub/splash.xpm.gz
title Red Hat Linux (2.4.20-20.9)
        root (hd0,0)
        kernel /vmlinuz-2.4.20-20.9 ro root=LABEL=/ hdb=ide-scsi
        initrd /initrd-2.4.20-20.9.img
[root@localhost membrich]#
```

Reboot again to make sure everything still works.

```
[root@localhost membrich]# /sbin/shutdown -r now

Broadcast message from root (pts/0) (Fri Nov 21 01:58:05 2003):

The system is going down for reboot NOW!
```

No problems.

3.1.8.3.8. RHSA-2003-279.

https://rhn.redhat.com/errata/RHSA-2003-279.html
Updated OpenSSH packages fix potential vulnerabilities

Advisory: RHSA-2003:279-17
Last updated on: 2003-09-17

i386:
openssh-3.5p1-11.i386.rpm
[via FTP] [via HTTP]   8598eddc12b2f06c34464a24d549d9af
openssh-clients-3.5p1-11.i386.rpm
[via FTP] [via HTTP]   922cf88933eeda965d6ad7534051c17e
openssh-server-3.5p1-11.i386.rpm
[via FTP] [via HTTP]   f58b37fc0290039448c450c3eb9630df

rpm -Fvh [filenames]

(“Updated OpenSSH Packages Fix Potential Vulnerabilities.” 2003)

```
[root@localhost membrich]# rpm --checksig rhsa-2003-279/*.rpm
rhsa-2003-279/openssh-3.5p1-11.i386.rpm: (sha1) dsa sha1 md5 gpg OK
rhsa-2003-279/openssh-clients-3.5p1-11.i386.rpm: (sha1) dsa sha1 md5 gpg OK
rhsa-2003-279/openssh-server-3.5p1-11.i386.rpm: (sha1) dsa sha1 md5 gpg OK
[root@localhost membrich]# rpm -Fvh rhsa-2003-279/*.rpm
Preparing...                ########################################### [100%]
   1:openssh                ########################################### [ 33%]
   2:openssh-clients        ########################################### [ 67%]
   3:openssh-server         ########################################### [100%]
[root@localhost membrich]#
```

3.1.8.3.9. RHSA-2003-292.

https://rhn.redhat.com/errata/RHSA-2003-292.html
Updated OpenSSL packages fix vulnerabilities

Advisory: RHSA-2003:292-12
Last updated on: 2003-09-30

i386:
openssl-0.9.7a-20.i386.rpm
[via FTP] [via HTTP]   91269d6393def01e0a796e40b74a970d
openssl-devel-0.9.7a-20.i386.rpm
[via FTP] [via HTTP]   957ff6ab058b3041a9995a93698a0cca
i686:
openssl-0.9.7a-20.i686.rpm
[via FTP] [via HTTP]   4fc16039f6893f039cd36b83c37a4fa6

To update all RPMs for your particular architecture, run:

rpm -Fvh [filenames]

(“Updated OpenSSL Packages Fix Vulnerabilities.” 2003)

```
[root@localhost membrich]# rpm --checksig rhsa-2003-292/*.rpm
rhsa-2003-292/openssl-0.9.7a-20.i386.rpm: (sha1) dsa sha1 md5 gpg OK
rhsa-2003-292/openssl-devel-0.9.7a-20.i386.rpm: (sha1) dsa sha1 md5 gpg OK
[root@localhost membrich]# rpm -Fvh rhsa-2003-292/*.rpm
Preparing...                ########################################### [100%]
   1:openssl                ########################################### [ 50%]
   2:openssl-devel          ########################################### [100%]
[root@localhost membrich]#
```

3.1.8.3.10. RHSA-2003-256.

https://rhn.redhat.com/errata/RHSA-2003-256.html
Updated Perl packages fix security issues.

Advisory: RHSA-2003:256-15
Last updated on: 2003-10-03

i386:
perl-5.8.0-88.3.i386.rpm
[via FTP] [via HTTP]   0ac800e33acab6522169d72dac29721b
perl-CGI-2.81-88.3.i386.rpm
[via FTP] [via HTTP]   cc53faea268b17b68d1494e9cd4d442b

To update all RPMs for your particular architecture, run:

rpm -Fvh [filenames]

("Updated Perl Packages Fix Security Issues." 2003)

```
[root@localhost membrich]# rpm --checksig rhsa-2003-256/*.rpm
rhsa-2003-256/perl-5.8.0-88.3.i386.rpm: (sha1) dsa sha1 md5 gpg OK
rhsa-2003-256/perl-CGI-2.81-88.3.i386.rpm: (sha1) dsa sha1 md5 gpg OK
[root@localhost membrich]# rpm -Fvh rhsa-2003-256/*.rpm
Preparing...                ########################################### [100%]
   1:perl                   ########################################### [100%]
[root@localhost membrich]#
```

3.1.8.3.11. RHSA-2003-281.

https://rhn.redhat.com/errata/RHSA-2003-281.html
Updated MySQL packages fix vulnerability

Advisory: RHSA-2003:281-08
Last updated on: 2003-10-09

i386:
mysql-3.23.58-1.9.i386.rpm
[via FTP] [via HTTP]   aa674d9d284788f8c354f3f20b6aec57
mysql-devel-3.23.58-1.9.i386.rpm
[via FTP] [via HTTP]   8eac37417227bf2c0c7d13a2eafcb80f
mysql-server-3.23.58-1.9.i386.rpm
[via FTP] [via HTTP]   78b516147ff717a2db347260e85e6688

("Updated MySQL Packages Fix Vulnerability." 2003)

Update instructions missing, assuming "rpm -Fvh".

```
[root@localhost membrich]# rpm --checksig rhsa-2003-281/*.rpm
rhsa-2003-281/mysql-3.23.58-1.9.i386.rpm: (sha1) dsa sha1 md5 gpg OK
rhsa-2003-281/mysql-devel-3.23.58-1.9.i386.rpm: (sha1) dsa sha1 md5 gpg OK
rhsa-2003-281/mysql-server-3.23.58-1.9.i386.rpm: (sha1) dsa sha1 md5 gpg OK
[root@localhost membrich]# rpm -Fvh rhsa-2003-281/*.rpm
[root@localhost membrich]#
```

Mysql is not installed, so nothing to patch.

3.1.8.3.12. RHSA-2003-309.

https://rhn.redhat.com/errata/RHSA-2003-309.html
Updated fileutils/coreutils package fix ls vulnerabilities

Advisory: RHSA-2003:309-08
Last updated on: 2003-11-03

i386:
coreutils-4.5.3-19.0.2.i386.rpm
[via FTP] [via HTTP]   da3fc5f54917452a4fa704330e193e24

To update all RPMs for your particular architecture, run:

rpm -Fvh [filenames]

(“Updated Fileutils/Coreutils Package Fix ls Vulnerabilities.” 2003)

```
[root@localhost membrich]# rpm --checksig rhsa-2003-309/*.rpm
rhsa-2003-309/coreutils-4.5.3-19.0.2.i386.rpm: (sha1) dsa sha1 md5 gpg OK
[root@localhost membrich]# rpm -Fvh rhsa-2003-309/*.rpm
Preparing...                ########################################### [100%]
   1:coreutils              ########################################### [100%]
[root@localhost membrich]#
```

3.2. Install 3rd Party Applications.

3.2.1. Snort.

Got latest version from http://www.snort.org/dl/
At the time of this writing, the latest version is 2.0.4.
Get the MD5 file too, so you can check the signature.

3.2.1.1. Check the MD5 Signature.

```
[membrich@localhost membrich]$ md5sum snort-2.0.4.tar.gz
8cff1ab5b6ab0ff507fb7264a05be05b  snort-2.0.4.tar.gz
[membrich@localhost membrich]$ cat snort-2.0.4.tar.gz.gz
md5  : 8cff1ab5b6ab0ff507fb7264a05be05b  snort-2.0.4.tar.gz
sha1 : 9ae95612d05c8bd605c689353f38d919a0d753ba  snort-2.0.4.tar.gz
[membrich@localhost membrich]$
```

Looks good.

3.2.1.2. Install Snort.

```
[membrich@localhost membrich]$ gunzip snort-2.0.4.tar.gz
[membrich@localhost membrich]$ tar -xvf snort-2.0.4.tar
[membrich@localhost membrich]$ cd snort-2.0.4
[membrich@localhost snort-2.0.4]$ ./configure --enable-flexresp
```

Got this error:

```
ERROR!  Libnet header not found, go get it from
   http://www.packetfactory.net/projects/libnet/
   or use the --with-libnet-* options, if you have it installed
   in unusual place
```

I tried installing the most recent stable version of libnet, but received this error on configuring snort:

```
checking for libnet.h... yes
checking for libnet version 1.0.2a... ./configure: line 1: libnet-config: command not
found
no


**********************************************
  ERROR: unable to find libnet 1.0.2a (libnet.h)
  checked in the following places
**********************************************
```

3.2.1.2.1. Install Libnet-1.0.2a.

Libnet-1.0.2a is available at: http://www.packetfactory.net/Projects/Libnet/.

```
[membrich@localhost membrich]$ gunzip libnet-1.0.2a.tar.gz
[membrich@localhost membrich]$ tar -xvf libnet-1.0.2a.tar
[membrich@localhost membrich]$ cd Libnet-1.0.2a/
[membrich@localhost Libnet-1.0.2a]$ ./configure
[membrich@localhost Libnet-1.0.2a]$ make
[membrich@localhost Libnet-1.0.2a]$ su
Password:
[root@localhost Libnet-1.0.2a]# make install
```

3.2.1.2.2. Back to Snort.

To make sure the configure and make go cleanly, I'll delete the prior attempt:

```
[membrich@localhost membrich]$ rm -rf snort-2.0.4
[membrich@localhost membrich]$ tar -xvf snort-2.0.4.tar
[membrich@localhost membrich]$ cd snort-2.0.4
[membrich@localhost snort-2.0.4]$ ./configure --enable-flexresp
[membrich@localhost snort-2.0.4]$ make
[membrich@localhost snort-2.0.4]$ su
Password:
[root@localhost snort-2.0.4]# make install

`--enable-flexresp'
     Enable the 'Flexible Response' code, that allows you to
     cancel hostile connections on IP-level when a rule matches.
     When you enable this feature, you also need the 'libnet'-library
     that can be found at http://www.packetfactory.net/libnet.
     See README.FLEXRESP for details.
     This function is still ALPHA, so use with caution.
```

3.2.1.3. Test it.

3.2.1.3.1. Enable the eth0 Interface.

We want the interface to have no IP address, so I changed the /etc/sysconfig/network-scripts/ifcfg-eth0 file to:

```
[root@localhost membrich]# cat /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
BOOTPROTO=static
ONBOOT=yes
```

Then we need to start it up by doing:

```
[root@localhost membrich]# /etc/init.d/network restart
Shutting down interface eth1:                              [  OK  ]
Shutting down loopback interface:                          [  OK  ]
Setting network parameters:                                [  OK  ]
Bringing up loopback interface:                            [  OK  ]
Bringing up interface eth0:                                [  OK  ]
Bringing up interface eth1:                                [  OK  ]
[root@localhost membrich]#
```

3.2.1.3.2. Test Snort.

```
[root@localhost membrich]# mkdir test
[root@localhost membrich]# snort -i eth0 -b -l test
Running in packet logging mode
Log directory = test

Initializing Network Interface eth0
OpenPcap() device eth0 network lookup:
        eth0: no IPv4 address assigned

        --== Initializing Snort ==--
Initializing Output Plugins!
Decoding Ethernet on interface eth0

        --== Initialization Complete ==--

-*> Snort! <*-
```

```
Version 2.0.4 (Build 96)
By Martin Roesch (roesch@sourcefire.com, www.snort.org)


===============================================================================
Snort analyzed 29 out of 29 packets, dropping 0(0.000%) packets

Breakdown by protocol:                Action Stats:
    TCP: 25         (86.207%)         ALERTS: 0
    UDP: 1          (3.448%)          LOGGED: 28
   ICMP: 2          (6.897%)          PASSED: 0
    ARP: 0          (0.000%)
  EAPOL: 0          (0.000%)
   IPv6: 0          (0.000%)
    IPX: 0          (0.000%)
  OTHER: 0          (0.000%)
DISCARD: 0          (0.000%)
===============================================================================
Wireless Stats:
Breakdown by type:
    Management Packets: 0          (0.000%)
    Control Packets:    0          (0.000%)
    Data Packets:       0          (0.000%)
===============================================================================
Fragmentation Stats:
Fragmented IP Packets: 0          (0.000%)
    Fragment Trackers: 0
   Rebuilt IP Packets: 0
   Frag elements used: 0
Discarded(incomplete): 0
   Discarded(timeout): 0
  Frag2 memory faults: 0
===============================================================================
TCP Stream Reassembly Stats:
        TCP Packets Used: 0          (0.000%)
         Stream Trackers: 0
          Stream flushes: 0
           Segments used: 0
   Stream4 Memory Faults: 0
===============================================================================
Snort exiting
[root@localhost membrich]#

[root@localhost membrich]# ls -l test
total 8
-rw-------    1 root     root         4473 Nov 21 15:54 snort.log.1069458849
[root@localhost membrich]#
```

Looks good.

3.3. Tighten Down the Sensor.

3.3.1. Bastille Linux.

The creators of Bastille Linux describe it better than I can:
(from http://www.bastille-linux.org/)

The Bastille Hardening System attempts to "harden" or "tighten" Unix operating systems. It currently supports the Red Hat, Debian, Mandrake, SuSE and TurboLinux

Linux distributions along with HP-UX and Mac OS X. We attempt to provide the most secure, yet usable, system possible. The project is run by Jon Lasser, Lead Coordinator and Jay Beale, Lead Developer, and involves a number of developers, beta-testers and concept-creators. Bastille Linux was developed with several major goals:

COMPREHENSIVENESS
Bastille Linux draws from every available major reputable source on Linux Security. The initial development integrated Jay Beale's existing O/S hardening experience for Solaris and Linux with most major points from the SANS' Securing Linux Step by Step, Kurt Seifried's Linux Administrator's Security Guide, and countless other sources.

3.3.1.1. Install Bastille Linux.

Since we do not have a GUI installed on this sensor, we need to use the text-only version of Bastille Linux. Which means installing perl-Curses (instead of perl-TK).

perl-Curses is available at: http://www.bastille-linux.org/perl-rpm-chart.html
Bastille Linux is available at: http://www.bastille-linux.org/

```
[root@localhost membrich]# rpm -ivh perl-Curses-1.06-219.i586.rpm
warning: only V3 signatures can be verified, skipping V4 signature
Preparing...                ########################################### [100%]
   1:perl-Curses            ########################################### [100%]
[root@localhost membrich]# rpm -ivh Bastille-2.1.1-1.0.i386.rpm
Preparing...                ########################################### [100%]
   1:Bastille               ########################################### [100%]
[root@localhost membrich]#
```

3.3.1.2. Running Bastille Linux.

```
[root@localhost membrich]# /usr/sbin/bastille -c
NOTE:    Using Curses user interface module.
NOTE:    Only displaying questions relevant to the current configuration.

Copyright (C) 1999-2002 Jay Beale
Copyright (C) 1999-2001 Peter Watkins
Copyright (C) 2000 Paul L. Allen
Copyright (C) 2001-2003 Hewlett Packard Company
Bastille is free software; you are welcome to redistribute it under
certain conditions.  See the 'COPYING' file in your distribution for terms.

DISCLAIMER.  Use of Bastille can help optimize system security, but does not
guarantee system security. Information about security obtained through use of
Bastille is provided on an AS-IS basis only and is subject to change without
notice. Customer acknowledges they are responsible for their system's security.
TO THE EXTENT ALLOWED BY LOCAL LAW, Bastille (SOFTWARE) IS PROVIDED TO YOU
AS IS WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, WHETHER ORAL OR WRITTEN,
EXPRESS OR IMPLIED.  JAY BEALE, THE BASTILLE DEVELOPERS, AND THEIR SUPPLIERS
DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.
Some countries, states and provinces do not allow exclusions of implied
warranties or conditions, so the above exclusion may not apply to you. You may
have other rights that vary from country to country, state to state, or province
to province.  EXCEPT TO THE EXTENT PROHIBITED BY LOCAL LAW, IN NO EVENT WILL
JAY BEALE, THE BASTILLE DEVELOPERS, OR THEIR SUBSIDIARIES, AFFILIATES OR
```

```
SUPPLIERS BE LIABLE FOR DIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL OR OTHER
DAMAGES (INCLUDING LOST PROFIT, LOST DATA, OR DOWNTIME COSTS), ARISING OUT OF
THE USE, INABILITY TO USE, OR THE RESULTS OF USE OF THE SOFTWARE, WHETHER BASED
IN WARRANTY, CONTRACT, TORT OR OTHER LEGAL THEORY, AND WHETHER OR NOT ADVISED
OF THE POSSIBILITY OF SUCH DAMAGES. Your use of the Software is entirely at your
own risk. Should the Software prove defective, you assume the entire cost of all
service, repair or correction. Some countries, states and provinces do not allow
the exclusion or limitation of liability for incidental or consequential
damages, so the above limitation may not apply to you.

You must accept the terms of this disclaimer to use
Bastille.  Type "accept" (without quotes) within 5
minutes to accept the terms of the above disclaimer
> accept

---------------------------

••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  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 >
```

Chose "Next"

```
---------------------------
```

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                   Bastille                                    •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•FilePermissions.pm Module 2 of 0••••••••••••••••••••••••••••••••••••••••••••••••
•Q: Would you like to set more restrictive permissions on the administration   •
•utilities? [N]                                                                 •
•In general, the default file permissions set by most vendors are fairly secure•
•.  To make them more secure, though, you can remove non-root user access to   •
•some administrator functions.                                                  •
•                                                                               •
•If you choose this option, you'll be changing the permissions on some common  •
•system administration utilities so that they're not readable or executable by •
•users other than root.  These utilities (which include linuxconf, fsck,       •
•ifconfig, runlevel and portmap) are ones that most users should never have a  •
•need to access.  This option will increase your system security, but there's a•
•chance it will inconvenience your users.                                      •
•                                                                               •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                <  Back  >     <  Next  >     < Explain Less >
```

Chose "Yes"

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                   Bastille                                    •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•FilePermissions.pm Module 2 of 0••••••••••••••••••••••••••••••••••••••••••••••••
•The following questions all pertain to disabling "SUID root" permission for   •
•particular programs. This permission allows non-root users to run these       •
•programs, increasing convenience but decreasing security.  If a security      •
•weakness or vulnerability is found in these programs, it can be exploited to  •
•gain root-level access to your computer through any user account.             •
•                                                                               •
•If you answer "Yes" and then realize later that you do need SUID permissions  •
•on a specific program, you can always turn it back on later with chmod u+s <  •
•file name>.                                                                    •
•                                                                               •
•                                                                               •
•                                                                               •
•                                                                               •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••



                <  Back  >     <  Next  >     < Explain Less >
```

Chose "Next"

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                    •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•FilePermissions.pm Module 2 of 0••••••••••••••••••••••••••••••••••••••••••••••••
•Q: Would you like to disable SUID status for mount/umount?                    •
•Mount and umount are used for mounting (activating) and unmounting (          •
•deactivating) drives that were not automatically mounted at boot time.  This  •
•can include floppy and CD-ROM drives.  Disabling SUID would still allow anyone•
•with the root password to mount and unmount drives.                           •
•                                                                              •
•Would you like to disable SUID status for mount/umount?                       •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "Yes"

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                    •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•FilePermissions.pm Module 2 of 0••••••••••••••••••••••••••••••••••••••••••••••••
•Q: Would you like to disable SUID status for ping? [Y]                        •
•Ping is used for testing network connectivity.  Specifically it's for testing •
•the  ability of the network to get a packet from this machine to another and  •
•back.  The ping program is SUID since only the root user can open a raw socket•
•. Since, however, it is often used only by the person responsible for         •
•networking the host, who normally has root access, we recommend disabling SUID•
•status for it.                                                                •
•                                                                              •
•Would you like to disable SUID status for ping? [Y]                           •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "Yes"

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                    •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•FilePermissions.pm Module 2 of 0•••••••••••••••••••••••••••••••••••••••••••••••
•Q: Would you like to disable SUID status for usernetctl? [Y]                  •
•usernetctl is a utility that allows ordinary users to control the network     •
•interfaces.  In general, there's no reason for anyone other than the system   •
•administrator to control network interfaces.                                  •
•                                                                              •
•Would you like to disable SUID status for usernetctl? [Y]                     •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "Yes"

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                    •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•FilePermissions.pm Module 2 of 0•••••••••••••••••••••••••••••••••••••••••••••••
•Q: Would you like to disable SUID status for traceroute? [Y]                  •
•The traceroute utility is used to test network connectivity. It is useful for •
•debugging network problems, but it is generally not necessary, especially for •
•non-privileged users.  If non-root users will be needing to debug network     •
•connections, you can leave the SUID bit on traceroute.  Otherwise, you should •
•disable it.                                                                   •
•                                                                              •
•Would you like to disable SUID status for traceroute? [Y]                     •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "Yes"

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                    •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•AccountSecurity.pm Module 3 of 0••••••••••••••••••••••••••••••••••••••••••••••
•Q: Would you like to enforce password aging? [Y]                              •
•Your operating system's default behavior, which we would change here, is to   •
•disable an account when the password hasn't changed in 99,999 days.  This     •
•interval is too long to be useful.  We can set the default to 180 days.  At   •
•some point before the 180 days have passed, the system will ask the user to   •
•change his or her password.  At the end of the 180 days, if the password has  •
•not been changed, the account will be temporarily disabled.  We would make    •
•this change in /etc/login.defs.                                               •
•                                                                              •
•Would you like to enforce password aging? [Y]                                 •
•                                                                              •
•                                                                              •
•                                                                              •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "Yes"

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                    •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•AccountSecurity.pm Module 3 of 0••••••••••••••••••••••••••••••••••••••••••••••
•Q: Would you like to restrict the use of cron to administrative accounts? [Y] •
•Cron can be particularly useful for admins, giving them the ability to have   •
•the system check logs every night at midnight or confirm file integrity every •
•hour.  On the other hand, being able to execute jobs later or automatically   •
•represents an abusable privilege for users and also makes their actions       •
•slightly harder to track.                                                     •
•                                                                              •
•Many sites choose to restrict cron to administrative accounts.  We suggest    •
•this action to new admins especially, until they understand more about how    •
•cron can be abused and know more about which users need access to cron. We    •
•would like to create the /etc/cron.allow file of users who may use cron. You  •
•can add to that later.  If we don't create this file, all users will be      •
•allowed to use cron.                                                          •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "Yes"

```
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                   •
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•AccountSecurity.pm Module 3 of 0•••••••••••••••••••••••••••••••••••••••••••••
•Q: Do you want to set the default umask? [Y]                                 •
•The umask sets the default permission for files that you create. Bastille can •
•set one of several umasks in the default login configuration files.  These    •
•cover standard shells like csh and most bourne shell variants like bash, sh,  •
•and ksh.  If you are going to install other shells, you may have to configure •
•them yourself.  The only reason not to set at least a minimal default umask is•
•if you are sure that you have already set one.                               •
•                                                                             •
•Do you want to set the default umask? [Y]                                    •
•                                                                             •
•                                                                             •
•                                                                             •
•                                                                             •
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "Yes"

```
---------------------------
```

```
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                   •
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•AccountSecurity.pm Module 3 of 0•••••••••••••••••••••••••••••••••••••••••••••
•Q: What umask would you like to set for users on the system? [077]           •
•The umask sets a default permission for files that you create. Bastille can  •
•set one of several umasks.  Please select one of the following or create your •
•own:                                                                         •
•                                                                             •
•002  - Everyone can read your files & people in your group can alter them.   •
•                                                                             •
•022  - Everyone can read your files, but no one can write to them.           •
•                                                                             •
•027  - Only people in your group can read your files, no one can write to them•
•.                                                                            •
•                                                                             •
•077  - No one on the system can read or write your files.                    •
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
 •••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
 •Answer: 077                                                                •
 •                                                                           •
 •••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                < Back >     < Next >     < Explain Less >
```

Chose "Next"

```
---------------------------
```

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                    •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•AccountSecurity.pm Module 3 of 0•••••••••••••••••••••••••••••••••••••••••••••••
•Q: Should we disallow root login on tty's 1-6? [N]                            •
•You can restrict which tty's root can login on.  Some sites choose to restrict•
•root logins, so that an admin must login with an ordinary user account and    •
•then use su to become root.                                                   •
•                                                                              •
•This can stop an attacker who has only been able to steal the root password   •
•from logging in directly.  He has to steal a second account's password to make•
•use of the root password via the ttys.                                        •
•                                                                              •
•Should we disallow root login on tty's 1-6? [N]                               •
•                                                                              •
•                                                                              •
•                                                                              •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "Yes"

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                    •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•BootSecurity.pm Module 4 of 0••••••••••••••••••••••••••••••••••••••••••••••••••
•Q: Would you like to password-protect the GRUB prompt? [N]                    •
•If an attacker has physical access to this machine, and particularly to the   •
•keyboard, s/he could get super-user access through the Grand Unified          •
•Bootloader (GRUB) command line.  We will look at other ways to prevent this   •
•later, but one easy way is to password-protect the GRUB prompt.  If GRUB is   •
•password-protected, any user can reboot the machine normally, but only users  •
•with the password can pass arguments to the GRUB prompt.                      •
•                                                                              •
•Note that this option can interfere dual-booting with a second operating      •
•system, since dual booting often requires that type an O/S name to boot one of•
•the two operating systems.  If this machine sits in a general purpose lab and •
•dual boots, you probably shouldn't choose this option.                        •
•                                                                              •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "No"
(we have physical security)

```
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                   Bastille                                    •
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•BootSecurity.pm Module 4 of 0•••••••••••••••••••••••••••••••••••••••••••••••••••
•Q: Would you like to disable CTRL-ALT-DELETE rebooting? [N]                    •
•Disabling CTRL-ALT-DELETE rebooting is designed to prevent an attacker with    •
•access to the machine's keyboard from being able to reboot the machine.  A     •
•reboot done in this manner should not damage the file system, as it shuts the  •
•machine down cleanly, writing out all pending data in the disk cache to disk   •
•first.  Even with this functionality disabled, however, an attacker could just•
•power cycle machine or pull the power cord.                                    •
•                                                                               •
•Unless the power line, switch and case of the machine can be physically        •
•protected, this precaution is wholly unnecessary.  Given the fact that the     •
•attacker _can_ reboot the machine, would you prefer that s/he do it in a way   •
•potentially damages the file system? Think carefully here, as maintaining the  •
•integrity of the machine's file system may be secondary to the goal of keeping•
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "No"

```
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                   Bastille                                    •
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•BootSecurity.pm Module 4 of 0•••••••••••••••••••••••••••••••••••••••••••••••••••
•Q: Would you like to password protect single-user mode? [Y]                    •
•Anyone who can physically interact with your system can tell the bootloader to•
•bring your machine up in "single user mode", where s/he is  given root         •
•privileges and everyone else is locked out of the system.  This doesn't        •
•require a password on most Unix systems.  The method differs with the          •
•bootloader being used, thus on each operating system revision and              •
•architecture.  You can test this attack on a Linux system that uses LILO by    •
•typing "linux single" at the LILO: prompt.                                     •
•                                                                               •
•Bastille can password-protect the bootprompt for you.  You won't have to       •
•remember another password--single user mode, or "root" mode, will require  the•
•root password.                                                                 •
•                                                                               •
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "Yes"

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                    •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•SecureInetd.pm Module 5 of 0•••••••••••••••••••••••••••••••••••••••••••••••••••
•Q: Would you like to set a default-deny on TCP Wrappers and xinetd? [N]       •
•Not recommended for most users:                                               •
•                                                                              •
•Many network services can be configured to restrict access to certain network •
•addresses (and in the case of 'xinetd' services in Linux-Mandrake 8.0 and Red •
•Hat 7.x, other criteria as well). For services running under the older 'inetd •
•' super-server (found in older versions of Linux-Mandrake and Red Hat, and    •
•current versions of some other distributions), some standalone services like  •
•OpenSSH, and --unless otherwise configured-- services running under Red Hat's •
•xinetd super-server, you can configure restrictions based on network address  •
•in /etc/hosts.allow. The services using inetd or xinetd typically include     •
•telnet, ftp, pop, imap, finger, and a number of other services.               •
•                                                                              •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "Yes"

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                    •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•SecureInetd.pm Module 5 of 0•••••••••••••••••••••••••••••••••••••••••••••••••••
•Q: Should Bastille ensure the telnet service does not run on this system? [y] •
•Telnet is not secure.                                                         •
•                                                                              •
•Telnet is shipped on most operating systems for backward compatibility, and it•
•should not be used in an untrusted network.                                   •
•                                                                              •
•Telnet is a clear-text protocol, meaning that any data transferred, including •
•passwords, can be monitored by anyone else on your network (even if you use a •
•switching router, as switches were designed for performance, not security and •
•can be made to broadcast).  Other networks can monitor this information too if•
•the telnet session crosses multiple LANs.                                     •
•                                                                              •
•There are also other more active attacks.  For example, anyone who can        •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "Yes"

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                    •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•SecureInetd.pm Module 5 of 0••••••••••••••••••••••••••••••••••••••••••••••••••••
•Q: Should Bastille ensure inetd's FTP service does not run on this system? [y]•
•Ftp is another problematic protocol.  First, it is a clear-text protocol, like•
•telnet -- this allows an attacker to eavesdrop on sessions and steal passwords•
•. This also allows an attacker to take over an FTP session, using a clear-text•
•-takeover tool like Hunt or Ettercap.  Second, it can make effective          •
•firewalling difficult due to the way FTP requires many ports to stay open.    •
•Third, every major FTP daemon has had a long history of security vulnerability•
•-- they represent one of the major successful attack vectors for remote root  •
•attacks.                                                                      •
•                                                                              •
•FTP can be replaced by Secure Shell's scp and sftp programs.                  •
•                                                                              •
•NOTE: Answering "yes" to this question will also prevent the use of this      •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                <  Back  >    <  Next  >    < Explain Less >
```

Chose "Yes"

```
---------------------------
```

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                    •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•SecureInetd.pm Module 5 of 0••••••••••••••••••••••••••••••••••••••••••••••••••••
•Q: Would you like to display "Authorized Use" messages at log-in time? [Y]    •
•At this point you can create "Authorized Use Only" messages for your site.    •
•These may be very helpful in prosecuting system crackers you may catch trying •
•to break into your system.  Bastille can make default messages which you may  •
•then later edit.  This is sort of like an "anti-welcome mat" for your computer•
•.                                                                             •
•                                                                              •
•Would you like to display "Authorized Use" messages at log-in time? [Y]       •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                <  Back  >    <  Next  >    < Explain Less >
```

Chose "Yes"

```
---------------------------
```

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                    •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                           <Press TAB to go on>                               •
•                                                                              •
•A default login/telnet/ftp "Authorized Use Only" banner will be created, and  •
•will be found in /etc/issue.  You should modify this banner to apply more     •
•specifically to your organization (for instance, adding any site-specific     •
•information to the default warnings).  If this is a corporate site, check with•
•your corporate counsel to determine the most appropriate warning for the      •
•banner.  These banners, according to CIAC's bulletin                          •
•                                                                              •
•   (http://ciac.llnl.gov/ciac/bulletins/j-043.shtml)                          •
•                                                                              •
•may make it much easier to prosecute intruders.  By including this default    •
•banner, neither the Bastille development team nor Hewlett-Packard Company take•
•any responsibility for your ability to prosecute system crackers. Please,     •
•especially if you run a corporate site, review/replace this with more specific•
•language.                                                                     •
•                                                                              •
•                                                                              •
•                                                                              •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
```

Hit the TAB key

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                    •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•SecureInetd.pm Module 5 of 0••••••••••••••••••••••••••••••••••••••••••••••••••••
•Q: Who is responsible for granting authorization to use this machine?         •
•Bastille will start to make the banner more specific by telling the user who  •
•is responsible for this machine.  This will state explicitly from whom the    •
•user needs to obtain authorization to use this machine.  Please type in the   •
•name of the company, person, or other organization who owns or is responsible •
•for this machine.                                                             •
•                                                                              •
•Who is responsible for granting authorization to use this machine?            •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
 ••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
 •Answer: Membrich.com                                                        •
 •                                                                            •
 ••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
               < Back >     < Next >     < Explain Less >
```

Entered Membrich.com
Chose "Next"

```
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                     •
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•DisableUserTools.pm Module 6 of 0••••••••••••••••••••••••••••••••••••••••••••••••
•Q: Would you like to disable the gcc compiler? [N]                             •
•The most common technique for the bulk of the system crackers out there is to •
•gain access to your system, often through a regular user account, and then use•
•that access to compile exploits against your system or other systems.          •
•Disabling the gcc compiler on your system will slow these crackers down, and  •
•may even prevent some attacks entirely.                                        •
•                                                                               •
•If this machine is a dedicated server/firewall, which does not have users who •
•need to compile programs, this action is strongly recommended.  Otherwise, you•
•should very carefully consider whether you will be inconveniencing your users •
•by disabling the compiler.  If you do chose to disable it, we'll do so by only•
•allowing root access to the compiler.                                          •
•                                                                               •
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "Yes"

```
---------------------------
```

```
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                     •
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•ConfigureMiscPAM.pm Module 7 of 0••••••••••••••••••••••••••••••••••••••••••••••••
•Q: Would you like to put limits on system resource usage? [N]                  •
•Denial of Service attacks are often very difficult to defend against, since   •
•they don't require access of any kind to the target machine. Since several    •
•major daemons, including the web, name, and FTP servers, may run as a         •
•particular user, you can limit the effectiveness of many Denial of Service    •
•attacks by modifying /etc/security/limits.conf.  If you restrict the resources•
•available in this manner, you can effectively cripple most Denial of Service  •
•attacks.                                                                       •
•                                                                               •
•If you choose this option, you'll be setting the following initial limits on  •
•resource usage:                                                                •
•                                                                               •
•   - The number of allowed core files will be set to zero.  Core files        •
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "No"

```
---------------------------
```

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                    •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•ConfigureMiscPAM.pm Module 7 of 0•••••••••••••••••••••••••••••••••••••••••••••
•Q: Should we restrict console access to a small group of user accounts? [N]   •
•Under some distributions, users logged in at the console have some special    •
•access rights (like the ability to mount the CD-ROM drive).  You can disable  •
•this special access entirely, but a more flexible option is to restrict      •
•console access to a small group of trusted user accounts.                     •
•                                                                              •
•Should we restrict console access to a small group of user accounts? [N]      •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "No"
There is only one user, membrich.

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                    •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•Logging.pm Module 8 of 0••••••••••••••••••••••••••••••••••••••••••••••••••••••
•Q: Would you like to add additional logging? [Y]                              •
•We would like to configure additional logging for your system. We will give   •
•you the option to log to a remote host, if your site already has one.  We will•
•add two additional logging files to the default setup and will also log some  •
•status messages to the 7th and 8th virtual terminals (the ones you'll see when•
•you hit ALT-F7 and ALT-F8).  This additional logging will not change the      •
•existing log files at all, so this is by no means a "risky" move.             •
•                                                                              •
•Would you like to add additional logging? [Y]                                 •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "Yes"

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                    •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                           <Press TAB to go on>                               •
•                                                                              •
•This script is adding additional logging files:                               •
•                                                                              •
•/var/log/kernel       --    kernel messages /var/log/syslog       --          •
•messages of severity "warning" and "error"                                    •
•                                                                              •
•Also, if you check the 7th and 8th TTY's, by hitting ALT-F7 or ALT-F8, you'll •
•find that we are now logging to virtual TTY's as well.  If you try this,      •
•remember that you can use ALT-F1 to get back to the first virtual TTY.        •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
```

Hit the TAB key.

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                    •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•Logging.pm Module 8 of 0•••••••••••••••••••••••••••••••••••••••••••••••••••••••
•Q: Do you have a remote logging host? [N]                                     •
•If you already have a remote logging host, we can set this machine to log to  •
•it.                                                                           •
•                                                                              •
•Do you have a remote logging host? [N]                                        •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "No"
(Haven't set up a remote logging host, not yet at least.)

```
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                   •
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•MiscellaneousDaemons.pm Module 9 of 0••••••••••••••••••••••••••••••••••••••••
•To make the operating system more secure, we try to deactivate all system    •
•daemons, especially those running at a high/unlimited level of privilege.    •
•Each active system daemon serves as a potential point of break-in, which might•
•allow an attacker illegitimate access to your system.  An attacker can use   •
•these system daemons to gain access if they are later found to have a bug or •
•security vulnerability.                                                       •
•                                                                              •
•We practice a minimalist principle here: minimize the number of privileged   •
•system daemons and you can decrease your chances of being a victim should one •
•of the standard daemons be found later to have a vulnerability.  This section •
•will require careful attention, but if you have doubts, you should be able to •
•safely select the default value in most cases.                                •
•                                                                              •
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••



                < Back >     < Next >     < Explain Less >
```

Chose "Next"

```
---------------------------
```

```
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                   •
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•TMPDIR.pm Module 17 of 0•••••••••••••••••••••••••••••••••••••••••••••••••••••
•Q: Would you like to install TMPDIR/TMP scripts? [N]                          •
•Many programs use the /tmp directory in ways that are dangerous on multi-user •
•systems. Many of those programs will use an alternate directory if one is     •
•specified with the TMPDIR or TMP environment variables. We can install scripts•
•that will be run when users log in that safely create suitable temporary      •
•directories and set the TMPDIR and TMP environment variables. This depends on •
•your system supporting /etc/profile.d scripts.                                •
•                                                                              •
•Would you like to install TMPDIR/TMP scripts? [N]                             •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                   •••••••
                                   •Yes  •
                                   •No   •
                                   •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "No"
Don't need it.

```
---------------------------
```

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                    •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•Firewall.pm Module 18 of 0•••••••••••••••••••••••••••••••••••••••••••••••••••••
•Q: Would you like to run the packet filtering script? [N]                     •
•Using the packet filtering script, you will be able to do packet filtering/   •
•modification via the Linux kernel.  You can use this to block certain types of•
•connections to or from your machine, to turn your machine into a small        •
•firewall, and to do Network Address Translation (also known as "IP            •
•masquerading"), which lets several machines share a single IP address.        •
•                                                                              •
•If you install the packet filtering script, it will create firewalling        •
•instructions for you. You will be prompted to make various choices (with      •
•suggested defaults), but you may need to edit it for your particular site and •
•WILL need to individually activate it.                                        •
•                                                                              •
•This script supports both kernel 2.2 (ipchains) and 2.4 (iptables if available•
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "No"
We can set this up at a later date.

```
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•                                  Bastille                                    •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•End of 0•••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
•Q: Are you finished answering the questions, i.e. may we make the changes?    •
•We will now implement the choices you have made here.                         •
•                                                                              •
•Answer NO if you want to go back and make changes!                            •
•                                                                              •
•                                                                              •
•Are you finished answering the questions, i.e. may we make the changes?       •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
•                                                                              •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
                                    •••••••
                                    •Yes  •
                                    •No   •
                                    •••••••
                < Back >     < Next >     < Explain Less >
```

Chose "Yes"

```
•Bastille Credits     (press TAB to go on)••••••••••••••••••••••••••••••••••••••
•    Jon Lasser                 - Lead Coordinator                                •
•    Jay Beale                  - Lead Developer                                  •
•    Peter Watkins              - Core Developer, Major Contributor               •
•    Mike Rash                  - Developer - Bastille IDS                        •
•    Sweth Chandramouli         - Developer - Bastille Automation                 •
•    HP Bastille Dev Team       - Developers - HP-UX Port, Design/Arch.           •
•    Paul Allen                 - Developer - User Interface                      •
•    Javier Fdez-Sanguino       - Developer - Debian Port                         •
•    Niki Rahimi (IBM)         - Developer - SuSE and TurboLinux Ports           •
•    Bruce Meyer, Donald Wilder - Beta Testers Extraordinaire v1&v1.2             •
•    James Durkin              - Testing and Ideas                                •
•    Yoann Vandoorselaere       - Developer - msec creator                        •
•    Don E Groves, Jr           - Design Contributor                              •
•    Manuel Caphina             - Developer -- Bastille IDS/NADS                  •
•    Peter Friedman             - Developer -- webget                             •
•    Rob Sherwood               - Developer -- process accounting                 •
•    Thomas Mangin              - Contributor - Beta Testing, Suggestions         •
•    Susan Marie Groppi        - Text and Documentation Coordinator              •
•    David A. Wheeler          - Contributor -- Miscellaneous Suggestions        •
•    Ben Woodard                - Infrastructure Liaison                          •
•    Kurt Seifried             - Gadfly                                           •
•    F.Soderblom, T.Lovqvist, K.Steves - HP-UX content from Armor                 •
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••
```

Hit the TAB key.

```
---------------------------

[root@localhost membrich]#
```

Before rebooting, we need to make some changes to the /etc/hosts.allow file or we won't be able to connect with ssh.

Changing /etc/hosts.allow from:

```
#
# hosts.allow   This file describes the names of the hosts which are
#               allowed to use the local INET services, as decided
#               by the '/usr/sbin/tcpd' server.
#

# Bastille: default deny
# no safe_finger for in.fingerd (prevent loops)
in.fingerd : ALL : DENY
# but everything else is denied & reported with safe_finger
ALL : ALL : spawn (/usr/sbin/safe_finger -l @%h | /bin/mail -s "Port Denial noted %d-
%h" root) & : DENY
```

To:

```
#
# hosts.allow   This file describes the names of the hosts which are
#               allowed to use the local INET services, as decided
#               by the '/usr/sbin/tcpd' server.
#

sshd : 172.16.1.33, 172.16.1.253
# Bastille: default deny
# no safe_finger for in.fingerd (prevent loops)
```

```
in.fingerd : ALL : DENY
# but everything else is denied & reported with safe_finger
ALL : ALL : spawn (/usr/sbin/safe_finger -l @%h | /bin/mail -s "Port Denial noted %d-
%h" root) & : DENY
```

Where 172.16.1.33 is my workstation and 172.16.1.253 is the server.

Rebooted.

3.3.2. Disable Unnecessary SetUID and SetGID Files.

The concept of disabling SetUID and SetGID files came from Sean Boran, available at: http://www.boran.com/security/sp/Solaris_hardening3.html. Boran's instructions are specifically for Solaris, but we can adapt them to a RedHat 9 machine:

> Files which have the SUID bit set (an "s" where the execute bit for the owner/group is shown in 'ls' listings) allow the user executing the program to assume the identity/group of the owner of the program. This is typically used to allow normal users to access certain function typically only allowed to root, for example binding to low ports, mounting a floppy disk, etc. The problem is that historically, many security weakness have been found in such programs allowing attackers with local accounts to become root by exploiting buffer over flows, race conditions etc.

- Solaris has many "SUID root" binaries and each one presents a risk, so when hardening systems it is advisable to disable as many SUID program as possible.
- The purpose of this section is to provide a brief overview of the subject, a list of documents and scripts for disabling SUID files is provided.
- See [8] for SUID references and further reading.

> What SUID files are on the system?
>
> The find command can be used to list all SUID files:
> find / -perm -u+s -ls
>
> or all SGID files:
> find / -perm -g+s -ls
>
> How should we handle SUID files? Possible courses of action, in order of preference, are:
>
> - Remove the package containing the offending file
> - Disable the program (e.g. chmod 000 FILENAME)
> - The SUID bit can be removed (e.g. chmod ug-s FILENAME)
> - Restrict the file to a group of users (first remove world access: "chmod o-rwx", then allow a group "chgrp MYGROUP MYFILE") .
>
> (Boran)

3.3.2.1. Find SetUID and SetGID Files.

Following Boran's instructions, find the files that have the SUID or SGID bit set:

```
[root@localhost membrich]# find / -perm -u+s -ls > suid_files
find: /proc/722/fd/4: No such file or directory
[root@localhost membrich]# find / -perm -g+s -ls > sgid_files
find: /proc/723/fd/4: No such file or directory
[root@localhost membrich]#
```

The SetUID files are:

```
 30656   36 -rwsr-xr-x   1 root     root        35376 Feb 12  2003 /usr/bin/chage
 30658   36 -rwsr-x---   1 root     root        36216 Feb 12  2003 /usr/bin/gpasswd
 31762   16 -rws--x--x   1 root     root        14140 Feb 24  2003 /usr/bin/chfn
 31763   12 -rws--x--x   1 root     root        11644 Feb 24  2003 /usr/bin/chsh
 31782    8 -rws--x--x   1 root     root         4728 Feb 24  2003 /usr/bin/newgrp
 31817   16 -r-s--x--x   1 root     root        16336 Feb 13  2003 /usr/bin/passwd
 32404  112 -rwsr-xr-x   1 root     root       110114 Feb 19  2003 /usr/bin/crontab
 45509  152 -rws--x--x   1 root     root       150688 Sep 17 09:13
/usr/libexec/openssh/ssh-keysign
 61475   28 -rwsr-x---   1 root     root        26680 Feb 24  2003
/usr/sbin/userhelper
 42889   96 -rwsr-xr-x   1 root     root        97260 Oct 29 06:44 /bin/su
 73548    7 -r-s--x--x   1 root     root         7088 Feb 10  2003
/sbin/pam_timestamp_check
 73549  118 -r-sr-xr-x   1 root     root       119528 Feb 10  2003 /sbin/pwdb_chkpwd
 73550   18 -r-sr-xr-x   1 root     root        17220 Feb 10  2003 /sbin/unix_chkpwd
```

The SetGID files are:

```
 31754    8 -r-xr-sr-x   1 root     tty          6908 Feb 10  2003 /usr/bin/wall
 31793   44 -rwxr-sr-x   1 root     tty         43593 Feb 24  2003 /usr/bin/write
 62295   36 -rwxr-sr-x   1 root     utmp        34186 Feb 18  2003 /usr/sbin/utempter
 73594   29 -rwxr-s---   1 root     root        28538 Mar 12  2003 /sbin/netreport
```

3.3.2.2. Removing SetUID and SetGID Bits.

```
[root@localhost membrich]# chmod ug-s /usr/bin/chage
[root@localhost membrich]# chmod ug-s /usr/bin/gpasswd
[root@localhost membrich]# chmod ug-s /usr/bin/chfn
[root@localhost membrich]# chmod ug-s /usr/bin/chsh
[root@localhost membrich]# chmod ug-s /usr/bin/newgrp
[root@localhost membrich]# chmod ug-s /usr/bin/crontab
[root@localhost membrich]# chmod ug-s /usr/libexec/openssh/ssh-keysign
[root@localhost membrich]# chmod ug-s /sbin/unix_chkpwd
[root@localhost membrich]#
[root@localhost membrich]# chmod ug-s /usr/bin/wall
[root@localhost membrich]# chmod ug-s /usr/bin/write
[root@localhost membrich]# chmod ug-s /sbin/netreport
[root@localhost membrich]#
```

This is what is left over:

```
[root@localhost membrich]# find / -perm -u+s -ls
find: /proc/758/fd/4: No such file or directory
```

```
 31817   16 -r-s--x--x   1 root     root        16336 Feb 13  2003 /usr/bin/passwd
 61475   28 -rwsr-x---   1 root     root        26680 Feb 24  2003
/usr/sbin/userhelper
 42889   96 -rwsr-xr-x   1 root     root        97260 Oct 29 06:44 /bin/su
 73548    7 -r-s--x--x   1 root     root         7088 Feb 10  2003
/sbin/pam_timestamp_check
 73549  118 -r-sr-xr-x   1 root     root       119528 Feb 10  2003 /sbin/pwdb_chkpwd
[root@localhost membrich]# find / -perm -g+s -ls
find: /proc/759/fd/4: No such file or directory
 62295   36 -rwxr-sr-x   1 root     utmp        34186 Feb 18  2003 /usr/sbin/utempter
[root@localhost membrich]#
```

3.3.3. Nessus Check.

Since we have Nessus set up on our server, we can use it to check our sensor for vulnerabilities.

From the server, I did the following:

```
[root@localhost membrich]# rm hosts
rm: remove regular file `hosts'? y
[root@localhost membrich]# echo "172.16.1.252" > hosts
[root@localhost membrich]# cat hosts
172.16.1.252
[root@localhost membrich]# nessusd -D
[root@localhost membrich]# nessus -q localhost 1241 nessus nessus hosts sensor
*** The plugins that have the ability to crash remote services or hosts
have been disabled. You should activate them if you want your security
audit to be complete
[root@localhost membrich]# cat sensor
172.16.1.252|general/icmp|10114|INFO|;The remote host answers to an ICMP timestamp
request. This allows an attacker ;to know the date which is set on your machine.
;;This may help him to defeat all your time based authentication protocols.;;Solution
: filter out the ICMP timestamp requests (13), and the outgoing ICMP ;timestamp
replies (14).;;Risk factor : Low;CVE : CAN-1999-0524;
172.16.1.252|general/tcp|11618|INFO|;The remote host does not discard TCP SYN packets
which;have the FIN flag set.;;Depending on the kind of firewall you are using,
an;attacker may use this flaw to bypass its rules.;;See also :
http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html;
http://www.kb.cert.org/vuls/id/464113;    ;Solution : Contact your vendor for a
patch;Risk factor : Medium;BID : 7487;
172.16.1.252|ssh (22/tcp)|10330|NOTE|An unknown service is running on this port.;It is
usually reserved for SSH;
172.16.1.252|general/udp|10287|NOTE|For your information, here is the traceroute to
172.16.1.252 : ;172.16.1.253;172.16.1.252;;
172.16.1.252|ssh (22/tcp)
[root@localhost membrich]#
```

Looks good.

3.3.4. Disable SSH Version 1.

We know from the server install that the default configuration for sshd accepts SSH version 1. Here's how to disable SSH version 1:

To remove ssh version 1 support, edit /etc/ssh/sshd_config:

```
[root@localhost membrich]# vi /etc/ssh/sshd_config
```

Changed the protocol setting from:

```
#Protocol 2,1
```

To:

```
Protocol 2
```

Restart sshd:

```
[root@localhost membrich]# pkill -HUP sshd
```

Done, the sensor is ready for business.

4. Getting the Machines to Work Together.

4.1. SSH Keys.

4.1.1. Generate SSH Keys.

Create key with empty passphrase (to be used for controlling sensors).

```
[root@localhost membrich]# ssh-keygen -b 2048 -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
98:06:4e:eb:4d:f2:ee:12:1d:29:61:02:00:46:e7:7d root@localhost.localdomain
[root@localhost membrich]#
```

4.1.2. Copy the Server's Public Key to the Sensor.

```
[root@localhost membrich]# scp /root/.ssh/id_rsa.pub
root@172.16.1.252:/root/.ssh/authorized_keys
root@172.16.1.252's password:
scp: /root/.ssh/authorized_keys: No such file or directory
[root@localhost membrich]#
```

Found that the /root/.ssh directory doesn't exist on the sensor, we need to create it. On the sensor:

```
[root@localhost membrich]# mkdir /root/.ssh
```

Back to the server:

```
[root@localhost membrich]# scp /root/.ssh/id_rsa.pub
root@172.16.1.252:/root/.ssh/authorized_keys
root@172.16.1.252's password:
id_rsa.pub           100% |*****************************|   408       00:00
[root@localhost membrich]#
```

4.1.3. Test it.

```
[root@localhost membrich]# ssh 172.16.1.252
Last login: Sat Nov 22 00:13:17 2003 from 172.16.1.253
[root@localhost root]#
```

That means I can use ssh utilities, namely scp to move files between the server and sensor through scripts without encoding a password in those scripts.

NOTE: It also means that the private key on the server is not encrypted. This isn't a good thing, but better than including a password in the scripts.

4.2. Snort Scripts.

Now that we have the ability to move files between the server and sensor, we need the scripts to do it for us. In true system administrator fashion, I chose to use something somebody else already wrote rather than do the work myself. Paul Ritchey wrote scripts for doing exactly what I want in his Snorticus package, available at: http://snorticus.baysoft.net/snorticus.html.

From Ritchey's documentation:

> About Snorticus:
>
> Snorticus is a collection of useful scripts that are used support the automatic retrieval and processing of collected Snort data from multiple sensors as well as the rules files. The basic concept is to have multiple sensors deployed that collect data. That data is 'wrapped up' once an hour and pulled back to a box that is used to further analyze the collected data (SnortSnarf) and then is used by analysts to view it via a web interface. Snorticus gives you the ability to manage not only data from multiple sites, but also the ability to monitor multiple subnets at a time with the same sensor (accomplished by launching multiple instances of Snort on the same sensor). While individual sensor data (or 'site' data) is kept separated, if a sensor is monitoring multiple subnets, that data will be automatically combined down so that those multiple Snort instances monitoring multiple subnets on the same sensor appear as one. Snorticus supports sites across time zones - it detects the proper date/time it should retrieve from the sensor so that all data residing on the analyst box is at most 1 hour old. Snorticus also supports the use of multiple network interface cards in the sensor. Subnets can be 'bound' to any network interface which is usefull if you run redundant networks and need to monitor the same address space on separate feeds.
>
> (Ritchey)

The parts I am interested in are:

- A script that runs on the sensor that stops and starts snort every hour, managing the log files. This would be Ritchey's hourly_wrapup.sh.
- A script that runs on the server that retrieves the snort logs from the sensor every hour, running the log files through snort on the server and managing the log files. This would be Ritchey's retrieve_wrapup.sh.

However, I do require some changes. First of all, Ritchey's scripts run via csh. Neither the server nor the sensor have csh installed. More importantly, Ritchey's scripts run the snort log files through SnortSnarf. Instead, I want to run the snort log files through snort, which will enter the alerts into a mysql database to appear in ACID.

So I rewrote (rather badly I might add) Ritchey's scripts into perl scripts to serve my purposes.

4.2.1. Sensor Script -- hourly

```
#!/usr/bin/perl

#  020613 adapted from the csh Snorticus scripts created by
#      Paul Ritchey.
#
#      One big difference is that my sensor will not be aware
#             of rules, it'll capture everything.
#      Another big difference is that I'll be putting the
#             data into ACID.

################### User configuration section #############
$SENSOR_SITE = 'test';
$DATA_EXPIRES = '1';
$RULES_DIR = '';
$LOG_DIR = '/var/log/snort/LOGS';
#$NETWORK_LIST = '/var/log/snort/network.cfg';
################### END User configuration #################

################## flags ###############################
if (`uname -s` == 'Linux') {
       $TAR_FLAGS = 'Pcvf';
       $PS_FLAGS = 'aux';
}
else   {
       $TAR_FLAGS = 'cvf';
       $PS_FLAGS = '-ef';
}
################# END flags ###########################

################### other prelim stuff ###################
#$NETWORK_TO_WATCH = (`grep -v '#' $NETWORK_LIST`);

#print ("network to watch = $NETWORK_TO_WATCH\n");

chop($CURRENT_DATEHOUR = `date '+%Y%m%d.%H'`);
$CURRENT_DATE = $CURRENT_DATEHOUR;
substr($CURRENT_DATE, -3) = '';

chop($PREVIOUS_DATEHOUR = `date --date='1 hour ago' '+%Y%m%d.%H'`);
$PREVIOUS_DATE = $PREVIOUS_DATEHOUR;
substr($PREVIOUS_DATE, -3) = '';

#print ("Current date_hour = $CURRENT_DATEHOUR\n");
#print ("Previous date_hour = $PREVIOUS_DATEHOUR\n");
print "create dirs = $LOG_DIR/$SENSOR_SITE/$CURRENT_DATE\n";
print "create dirs 2 = $LOG_DIR/$SENSOR_SITE/$CURRENT_DATE/$CURRENT_DATEHOUR\n";

&chkdir("$LOG_DIR/$SENSOR_SITE/$CURRENT_DATE");
&chkdir("$LOG_DIR/$SENSOR_SITE/$CURRENT_DATE/$CURRENT_DATEHOUR");

#print ("created $LOG_DIR/$SENSOR_SITE/$CURRENT_DATEHOUR\n");

################# run snort and cleanup ###########################

@SNORT_PIDS = (`ps -C snort -o pid=`);
foreach $SNORT_PIDS (@SNORT_PIDS) {
       print "snort PID = $SNORT_PIDS\n";
       kill 9, $SNORT_PIDS;
}
```

```
#`snort -b -de -l "$LOG_DIR/$SENSOR_SITE/$CURRENT_DATE/$CURRENT_DATEHOUR" -D`;

#`snort -b -de -l "$LOG_DIR/$SENSOR_SITE/$CURRENT_DATE/$CURRENT_DATEHOUR" -D -i eth1 >
"$LOG_DIR/$SENSOR_SITE/$CURRENT_DATE/$CURRENT_DATEHOUR/out.$CURRENT_DATEHOUR`;
`/usr/local/bin/snort -b -de -l
"$LOG_DIR/$SENSOR_SITE/$CURRENT_DATE/$CURRENT_DATEHOUR" -D -i eth0`;

&cleanup;
exit 0;

################## sub cleanup ################################
sub cleanup {

       `tar "$TAR_FLAGS" "$LOG_DIR/$SENSOR_SITE/$PREVIOUS_DATE/$PREVIOUS_DATEHOUR.tar"
"$LOG_DIR/$SENSOR_SITE/$PREVIOUS_DATE/$PREVIOUS_DATEHOUR"`;
       `gzip "$LOG_DIR/$SENSOR_SITE/$PREVIOUS_DATE/$PREVIOUS_DATEHOUR.tar"`;
       `rm -rf "$LOG_DIR/$SENSOR_SITE/$PREVIOUS_DATE/$PREVIOUS_DATEHOUR"`;
       `find "$LOG_DIR/$SENSOR_SITE" -mtime +"$DATA_EXPIRES" -exec rm -rf {} \\;`;
}
################# END sub cleanup #############################

################# sub chkdir ##################################
sub chkdir {
#      print "passed value is $_[0]\n";
       if (!-d $_[0]) {
              `mkdir $_[0]`;
              print "creating directory $_[0]\n";
       }
}
################# END sub chkdir ##############################
```

4.2.1.1. Copy it to my Sensor.

```
D:\download\track1_prac>pscp hourly root@172.16.1.252:/usr/local/bin
root@172.16.1.252's password:
hourly                    |          2 kB |   2.9 kB/s | ETA: 00:00:00 | 100%

D:\download\track1_prac>
```

Make the script executable (also changed the permissions on /usr/local/bin/snort since it should only be run by root).

```
[root@localhost membrich]# ls -l /usr/local/bin
total 2148
-rw-r--r--    1 root     root         2949 Nov 22 04:11 hourly
-rwxr-xr-x    1 root     root      2191311 Nov 21 15:18 snort
[root@localhost membrich]# chmod 700 /usr/local/bin/*
[root@localhost membrich]# ls -l /usr/local/bin
total 2148
-rwx------    1 root     root         2949 Nov 22 04:11 hourly
-rwx------    1 root     root      2191311 Nov 21 15:18 snort
[root@localhost membrich]#
```

4.2.1.2. Set up a cron Job to Run the Script Every Hour.

```
[root@localhost membrich]# crontab -l
no crontab for root
[root@localhost membrich]# crontab -e
```

Added the following:

```
[root@localhost membrich]# crontab -l
# DO NOT EDIT THIS FILE - edit the master and reinstall.
# (/tmp/crontab.1779 installed on Sat Nov 22 04:22:58 2003)
# (Cron version -- $Id: crontab.c,v 2.13 1994/01/17 03:20:37 vixie Exp $)
#################################################
# The following job runs snort each hour.
#################################################
00 * * * *      /usr/local/bin/hourly   > /dev/null 2>&1
[root@localhost membrich]#
```

Set up the directory structure needed by the /usr/local/bin/hourly script.

```
[root@localhost membrich]# mkdir /var/log/snort
[root@localhost membrich]# mkdir /var/log/snort/LOGS
[root@localhost membrich]# mkdir /var/log/snort/LOGS/test
```

4.2.1.3. Start the /usr/local/bin/hourly Script.

```
[root@localhost membrich]# /usr/local/bin/hourly
create dirs = /var/log/snort/LOGS/test/20031122
create dirs 2 = /var/log/snort/LOGS/test/20031122/20031122.04
creating directory /var/log/snort/LOGS/test/20031122
creating directory /var/log/snort/LOGS/test/20031122/20031122.04
tar: /var/log/snort/LOGS/test/20031122/20031122.03: Cannot stat: No such file or
directory
tar: Error exit delayed from previous errors
```

Check to make sure the snort log file has been created.

```
[root@localhost membrich]# ls -l /var/log/snort/LOGS/test
total 4
drwxr-xr-x    3 root     root         4096 Nov 22 04:28 20031122
[root@localhost membrich]# ls -l /var/log/snort/LOGS/test/20031122/
total 8
-rw-r--r--    1 root     root           61 Nov 22 04:28 20031122.03.tar.gz
drwxr-xr-x    2 root     root         4096 Nov 22 04:28 20031122.04
[root@localhost membrich]# ls -l /var/log/snort/LOGS/test/20031122/20031122.04
total 60
-rw-------    1 root     root        54266 Nov 22 04:32 snort.log.1069504100
[root@localhost membrich]#
```

Check to make sure it's running.

```
[root@localhost membrich]# ps -eaf | grep snort
root      1812     1  0 04:28 ?        00:00:00 /usr/local/bin/snort -b -de -l
/var/log/snort/LOGS/test/20031122/20031122.04 -D -i eth0
root      1820  1299  0 04:29 pts/0    00:00:00 grep snort
[root@localhost membrich]#
```

4.2.2. Server Script.

```
#!/usr/bin/perl

#  020613 adapted from the csh Snorticus scripts created by
#      Paul Ritchey.
#
#      One big difference is that my sensor will not be aware
#             of rules, it'll capture everything.
#      Another big difference is that I'll be putting the
#             data into ACID.

############# User Configuration Section ######################
$LOG_DIR = '/var/log/snort/LOGS';
$DATA_EXPIRES = 10;
$NETWORK_LIST_FILE = '/var/log/snort/rules/network.cfg';
$GNUDATE_PATH = '/bin';
$RETRIEVE_ACCOUNT = 'root';
$RETRIEVE_FILE = '/root/.ssh/id_rsa';
############# END User Configuration Section ##################

if (`uname -s` == 'Linux') {
       $TAR_FLAGS = 'Pxvf';
}
else {
       $TAR_FLAGS = 'xvf';
}

if ($#ARGV < 1) {
       print "\n";
       print "Incorrect number of parameters passed.  Usage:\n";
       print "retrieve <site_name> <hostname || ip> [yyyymmdd.hh]\n";
       print "\n";
       exit 0;
}

$SITE_NAME = $ARGV[0];
$HOSTNAME = $ARGV[1];
$NETWORK_TO_WATCH=(`grep -v '#' $NETWORK_LIST_FILE`);

print "site_name = $SITE_NAME\n";
print "hostname = $HOSTNAME\n";

if ($#ARGV > 1) {
       $PREVIOUS_DATEHOUR = $ARGV[2];
       $PREVIOUS_DATE = $ARGV[2];
       substr($PREVIOUS_DATE, -3) = '';
}
else   {
       chop($PREVIOUS_DATEHOUR = `ssh -i $RETRIEVE_FILE $HOSTNAME "$GNUDATE_PATH/date
--date='1 hour ago' '+%Y%m%d.%H'"`);
       $PREVIOUS_DATE = $PREVIOUS_DATEHOUR;
       substr($PREVIOUS_DATE, -3) = '';
}

#print "ARGV #2 = $ARGV[2]\n";
#print "Previous date hour = $previous_datehour\n";
#print "Previous date = $previous_date\n";

################ Prepare logging directory ####################

&chkdir("$LOG_DIR/$SITE_NAME");
&chkdir("$LOG_DIR/$SITE_NAME/$PREVIOUS_DATE");

############### Retrieve the data ############################

#chdir "$LOG_DIR/$SITE_NAME/$PREVIOUS_DATE" || die "Can't cd to
$LOG_DIR/$SITE_NAME/$PREVIOUS_DATE: $!\n";
```

```
`scp -B -q -i $RETRIEVE_FILE
"$HOSTNAME:$LOG_DIR/$SITE_NAME/$PREVIOUS_DATE/$PREVIOUS_DATEHOUR.tar.gz"
"$LOG_DIR/$SITE_NAME/$PREVIOUS_DATE/$PREVIOUS_DATEHOUR.tar.gz"`;
`gunzip -c "$LOG_DIR/$SITE_NAME/$PREVIOUS_DATE/$PREVIOUS_DATEHOUR.tar.gz" | tar
$TAR_FLAGS -`;
`rm "$LOG_DIR/$SITE_NAME/$PREVIOUS_DATE/$PREVIOUS_DATEHOUR.tar.gz"`;

@LOG_FILES = (`ls "$LOG_DIR/$SITE_NAME/$PREVIOUS_DATE/$PREVIOUS_DATEHOUR" | grep
snort`);
foreach $LOG_FILES (@LOG_FILES) {
        chop($LOG_FILES);
        `/usr/local/bin/snort -de -l
$LOG_DIR/$SITE_NAME/$PREVIOUS_DATE/$PREVIOUS_DATEHOUR -c /usr/local/snort/snort.conf -
r $LOG_DIR/$SITE_NAME/$PREVIOUS_DATE/$PREVIOUS_DATEHOUR/$LOG_FILES >
$LOG_DIR/$SITE_NAME/$PREVIOUS_DATE/$PREVIOUS_DATEHOUR/marklog`;
}

################# sub chkdir ###################################
sub chkdir {

        print "argv[0] = $_[0]\n";
        if (!-d $_[0]) {
                print "couldn't find the directory $_[0]\n";
                `mkdir $_[0]`;
                if ($? != 0) {
                        print "\n";
                        print "Unable to continue...\n";
                        print "Unable to create needed directory:\n";
                        print "  $_[0]\n";
                        print "\n";
                        exit 0;
                }
                else    {
                        print "created the directory $_[0]\n";
                }
        }

} ### End chkdir
```

4.2.2.1. Copied it to my Server.

```
D:\download\track1_prac>pscp retrieve root@172.16.1.253:/usr/local/bin
root@172.16.1.253's password:
retrieve                  |          3 kB |   3.6 kB/s | ETA: 00:00:00 | 100%

D:\download\track1_prac>
```

Make the script executable.

```
[root@localhost membrich]# ls -l /usr/local/bin/retrieve
-rw-r--r--    1 root     root         3655 Nov 23 05:57 /usr/local/bin/retrieve
[root@localhost membrich]# chmod 700 /usr/local/bin/retrieve
[root@localhost membrich]# ls -l /usr/local/bin/retrieve
-rwx------    1 root     root         3655 Nov 23 05:57 /usr/local/bin/retrieve
[root@localhost membrich]#
```

4.2.2.2. Set up a cron Job to Run the Script Every Hour.

```
[root@localhost membrich]# crontab -l
```

```
no crontab for root
[root@localhost membrich]# crontab -e
```

Added the following:

```
[root@localhost membrich]# crontab -l
# DO NOT EDIT THIS FILE - edit the master and reinstall.
# (/tmp/crontab.4749 installed on Sun Nov 23 06:03:38 2003)
# (Cron version -- $Id: crontab.c,v 2.13 1994/01/17 03:20:37 vixie Exp $)
##################################################
# The next job runs the snort retrieve script.
##################################################
10 * * * *      /usr/local/bin/retrieve test 172.16.1.252 > /dev/null 2>&1
[root@localhost membrich]#
```

Note that we want to give the sensor a bit of time to process it's snort log files before we try to retrieve it.

Set up the directory structure needed by the /usr/local/bin/retrieve script.

```
[root@localhost membrich]# mkdir /var/log/snort
[root@localhost membrich]# mkdir /var/log/snort/LOGS
[root@localhost membrich]# mkdir /var/log/snort/LOGS/test
```

Give the sensor a few hours to create some snort logs, then we'll check on the server to make sure it's receiving the logs.

4.3. Tripwire.

4.3.1. Initialize the Tripwire Database.

Tripwire was already installed when we installed RedHat, but it's not exactly ready to run. In addition, we want to make some changes to the way Tripwire is run. Since the snort sensor machine is closer to the attackers, it is more vulnerable to attack. Therefore, we'll move the Tripwire database and executables to the server. Each night, we'll have the server move the executables and database over to the sensor, run a file integrity check, then pull the executables and database back to the server. This way the executables and database won't be available to attackers to corrupt (except a few minutes). This centralizing of Tripwire also has the added convenience of putting the Tripwire reports all on a single machine.

Sean Boran wrote scripts for centralizing Tripwire, available here: http://www.boran.com/security/sp/solaris/. I adapted the trip_host.sh script to my own use. I had some problems getting the Initialize functionality to work. However, since you only need to Initialize once, I do it manually and removed Initialize functionality from my trip_host.sh script.

RedHat's Reference Guide has instructions on how to Initialize the Tripwire database, available at: http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/ref-guide/ch-tripwire.html.

4.3.1.1. Set up /etc/hosts Files.

To simplify things for the Tripwire setup, we need to set hostnames on the server and sensor. Having a magnificent imagination, I'll use "sensor" for the sensor and "server" for the server.

Set the /etc/hosts file on the server to:

```
[root@localhost membrich]# cat /etc/hosts
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1               localhost.localdomain localhost
172.16.1.253            server
172.16.1.252            sensor
[root@localhost membrich]#
```

Set the /etc/hosts file on the sensor to:

```
[root@localhost membrich]# cat /etc/hosts
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1               localhost.localdomain localhost
172.16.1.252            sensor
172.16.1.253            server
[root@localhost membrich]#
```

Reboot both, then test it.
From the server:

```
[root@server membrich]# ssh sensor
The authenticity of host 'sensor (172.16.1.252)' can't be established.
RSA key fingerprint is 53:7b:49:b8:56:1f:53:13:1c:f8:b1:fc:db:7b:84:05.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'sensor' (RSA) to the list of known hosts.
Last login: Sat Nov 22 18:57:14 2003 from 172.16.1.253
[root@sensor root]#
```

That works.

4.3.1.2. Edit the HOSTNAME Setting in /etc/tripwire/twpol.txt.

The default setting for the HOSTNAME in /etc/tripwire/twpol.txt is:

```
HOSTNAME=localhost;
```

On the sensor, set it to make use of the hostname we just set:

```
HOSTNAME=sensor;
```

4.3.2. Run the twinstall.sh Script on the Sensor.

```
[root@sensor tripwire]# ./twinstall.sh
```

```
----------------------------------------------
The Tripwire site and local passphrases are used to
sign a variety of files, such as the configuration,
policy, and database files.

Passphrases should be at least 8 characters in length
and contain both letters and numbers.

See the Tripwire manual for more information.

----------------------------------------------
Creating key files...

(When selecting a passphrase, keep in mind that good passphrases typically
have upper and lower case letters, digits and punctuation marks, and are
at least 8 characters in length.)

Enter the site keyfile passphrase:
Verify the site keyfile passphrase:
Generating key (this may take several minutes)...Key generation complete.

(When selecting a passphrase, keep in mind that good passphrases typically
have upper and lower case letters, digits and punctuation marks, and are
at least 8 characters in length.)

Enter the local keyfile passphrase:
Verify the local keyfile passphrase:
Generating key (this may take several minutes)...Key generation complete.

----------------------------------------------
Signing configuration file...
Please enter your site passphrase:
Wrote configuration file: /etc/tripwire/tw.cfg

A clear-text version of the Tripwire configuration file
/etc/tripwire/twcfg.txt
has been preserved for your inspection.  It is recommended
that you delete this file manually after you have examined it.


----------------------------------------------
Signing policy file...
Please enter your site passphrase:
Wrote policy file: /etc/tripwire/tw.pol

A clear-text version of the Tripwire policy file
/etc/tripwire/twpol.txt
has been preserved for your inspection.  This implements
a minimal policy, intended only to test essential
Tripwire functionality.  You should edit the policy file
to describe your system, and then use twadmin to generate
a new signed copy of the Tripwire policy.

[root@sensor tripwire]#
```

4.3.3. Run the twinstall.sh Script on the Server.

We need the site and local keys to have the same passphrase on the server and the sensor. This is because we need the keys to access the Tripwire reports, but since we're manipulating the reports from the sensor on the server machine, the server's key needs to be able to unlock the sensor's reports.

```
[root@server membrich]# /etc/tripwire/twinstall.sh

----------------------------------------------
The Tripwire site and local passphrases are used to
sign a variety of files, such as the configuration,
policy, and database files.

Passphrases should be at least 8 characters in length
and contain both letters and numbers.

See the Tripwire manual for more information.

----------------------------------------------
Creating key files...

(When selecting a passphrase, keep in mind that good passphrases typically
have upper and lower case letters, digits and punctuation marks, and are
at least 8 characters in length.)

Enter the site keyfile passphrase:
Verify the site keyfile passphrase:
Generating key (this may take several minutes)...Key generation complete.

(When selecting a passphrase, keep in mind that good passphrases typically
have upper and lower case letters, digits and punctuation marks, and are
at least 8 characters in length.)

Enter the local keyfile passphrase:
Verify the local keyfile passphrase:
Generating key (this may take several minutes)...Key generation complete.

----------------------------------------------
Signing configuration file...
Please enter your site passphrase:
Wrote configuration file: /etc/tripwire/tw.cfg

A clear-text version of the Tripwire configuration file
/etc/tripwire/twcfg.txt
has been preserved for your inspection.  It is recommended
that you delete this file manually after you have examined it.


----------------------------------------------
Signing policy file...
Please enter your site passphrase:
Wrote policy file: /etc/tripwire/tw.pol

A clear-text version of the Tripwire policy file
/etc/tripwire/twpol.txt
has been preserved for your inspection.  This implements
a minimal policy, intended only to test essential
Tripwire functionality.  You should edit the policy file
to describe your system, and then use twadmin to generate
a new signed copy of the Tripwire policy.

[root@server membrich]#
```

4.3.4. Use Initialize to Dictate tw.pol.

There are two user-configurable files that determine how Tripwire runs. The tw.cfg file is a traditional configuration file, telling Tripwire where to find files and what options to enable. The tw.pol file tells Tripwire what files to check and how to check those files. Not being a Linux master, I can't set up the tw.pol file without some help. I'll use the Initialize function of Tripwire to help me out.

```
[root@sensor membrich]# /usr/sbin/tripwire --init
Please enter your local passphrase:
Parsing policy file: /etc/tripwire/tw.pol
Generating the database...
*** Processing Unix File System ***
```

Under the "Processing" section, Tripwire lists the files that do not exist. There are so many of them that I don't want to list them here, but here's an example of a few:

```
### Warning: File system error.
### Filename: /usr/sbin/fixrmtab
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /usr/bin/vimtutor
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /sbin/accton
### No such file or directory
```

4.3.5. Edit the /etc/tripwire/twpol.txt File.

For each of the files listed here, we want to comment them out in the tw.pol file. We can't edit the tw.pol file directly, so we make the changes to the /etc/tripwire/twpol.txt file and update the tw.pol file using twadmin. This is also in the RedHat documentation: http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/ref-guide/s1-tripwire-update-policy.html.

Edited /etc/tripwire/twpol.txt.

```
[root@sensor membrich]# vi /etc/tripwire/twpol.txt
```

Use twadmin to update tw.pol:

```
[root@sensor membrich]# /usr/sbin/twadmin --create-polfile -S /etc/tripwire/site.key
/etc/tripwire/twpol.txt
Please enter your site passphrase:
Wrote policy file: /etc/tripwire/tw.pol
[root@sensor membrich]#
```

4.3.6. Recreate the Tripwire Database.

Remove the old Tripwire database:

```
[root@sensor membrich]# rm /var/lib/tripwire/sensor.twd
rm: remove regular file `/var/lib/tripwire/sensor.twd'? y
[root@sensor membrich]#
```

Initialize again:

```
[root@sensor tripwire]# /usr/sbin/tripwire --init
Please enter your local passphrase:
Parsing policy file: /etc/tripwire/tw.pol
Generating the database...
*** Processing Unix File System ***
Wrote database file: /var/lib/tripwire/sensor.twd
The database was successfully generated.
[root@sensor tripwire]#
```

4.3.7. Move the Tripwire Files to the Server.

On the sensor:

```
[root@sensor membrich]# mkdir /etc/tripwire/sensor
[root@sensor membrich]# mv /var/lib/tripwire/sensor.twd /etc/tripwire/sensor
[root@sensor membrich]# mv /etc/tripwire/tw.pol /etc/tripwire/sensor
[root@sensor membrich]# mv /etc/tripwire/tw.cfg /etc/tripwire/sensor
[root@sensor membrich]# mv /etc/tripwire/site.key /etc/tripwire/sensor
[root@sensor membrich]# mv /etc/tripwire/sensor-local.key /etc/tripwire/sensor
[root@sensor membrich]# mv /var/lib/tripwire/report /etc/tripwire/sensor
[root@sensor membrich]# cd /etc/tripwire
[root@sensor tripwire]# tar -cf sensor.tar sensor
[root@sensor tripwire]# gzip sensor.tar
[root@sensor tripwire]#
```

On the server:

```
[root@server membrich]# scp sensor:/etc/tripwire/sensor.tar.gz /var/lib/tripwire
sensor.tar.gz        100% |*****************************|   392 KB    00:00
[root@server membrich]#
```

Back to the sensor:

```
[root@sensor tripwire]# cd ~membrich
[root@sensor membrich]# rm -rf /etc/tripwire
[root@sensor membrich]# rm -rf /var/lib/tripwire
[root@sensor membrich]# rm -rf /usr/sbin/tripwire
[root@sensor membrich]#
```

4.3.8. Test the triphost.sh Script.

First, we need to put the tripwire executable into the set of files we move to the sensor. On the server:

```
[root@server membrich]# cd /var/lib/tripwire
[root@server tripwire]# gunzip sensor.tar.gz
[root@server tripwire]# tar -xvf sensor.tar
sensor/
sensor/sensor.twd
```

```
sensor/tw.pol
sensor/tw.cfg
sensor/site.key
sensor/sensor-local.key
sensor/report/
[root@server tripwire]# cp /usr/sbin/tripwire sensor
[root@server tripwire]# rm sensor.tar
rm: remove regular file `sensor.tar'? y
[root@server tripwire]# tar -cf sensor.tar sensor
[root@server tripwire]# gzip sensor.tar
[root@server tripwire]# rm -rf sensor
```

We need to create the directory for the sensor's Tripwire reports.
On the server:

```
[root@server tripwire]# mkdir /var/log/tripwire/sensor
[root@server tripwire]# mkdir /var/lib/tripwire/report
[root@server tripwire]# mkdir /var/lib/tripwire/report/sensor
[root@server tripwire]#
```

Test triphost.sh.

```
[root@server membrich]# /usr/local/bin/triphost.sh -check sensor
### Warning: File system error.
### Filename: /usr/sbin/tripwire
### No such file or directory
### Continuing...
[root@server membrich]
```

The errors are no big deal. It couldn't find /usr/sbin/tripwire on the sensor because it's already been deleted. I left it in the script just in case the tripwire executable finds it's way back onto the sensor.

The report has been created in /var/lib/tripwire/report/sensor and the /usr/local/bin/triprpt.sh script converted that into a human-readable format in /var/log/tripwire.

```
[root@server membrich]# ls -l /var/lib/tripwire/report/sensor
total 12
-rw-r--r--    1 root     root        10038 Nov 26 02:15 sensor-20031127.twr

[root@server membrich]# ls -l /var/log/tripwire/sensor
total 20
-rw-r--r--    1 root     root        17664 Nov 27 02:18 sensor-20031127.txt
[root@server membrich]#
```

4.3.9. Set up a cron Job to run Tripwire Each Night.

Add a line to the root user's crontab to run our triphost.sh script every night.

Before:

```
[root@server membrich]# crontab -l
# DO NOT EDIT THIS FILE - edit the master and reinstall.
# (/tmp/crontab.4749 installed on Sun Nov 23 06:03:38 2003)
# (Cron version -- $Id: crontab.c,v 2.13 1994/01/17 03:20:37 vixie Exp $)
##################################################
# The next job runs the snort retrieve script.
##################################################
10 * * * *      /usr/local/bin/retrieve test 172.16.1.252 > /dev/null 2>&1
```

To edit crontab:

```
[root@server membrich]# crontab -e
```

After:

```
[root@server membrich]# crontab -l
# DO NOT EDIT THIS FILE - edit the master and reinstall.
# (/tmp/crontab.3663 installed on Thu Nov 27 02:51:23 2003)
# (Cron version -- $Id: crontab.c,v 2.13 1994/01/17 03:20:37 vixie Exp $)
##################################################
# The next job runs the snort retrieve script.
##################################################
10 * * * *      /usr/local/bin/retrieve test 172.16.1.252 > /dev/null 2>&1
# The next job runs Tripwire on the sensors.
0 0 * * *       /usr/local/bin/triphost.sh -check sensor
[root@server membrich]#
```

This will run the triphost.sh script at midnight every day.

4.3.10. triphost.sh Script.

```
#!/bin/sh
#
#
#
##########################################################
#      Initialize variables
##########################################################
#
DATE=`date "+%Y%m%d"`

ACTION="$1"
TARGET="$2"
SSH="/usr/bin/ssh -n -q -x"
SCP="/usr/bin/scp -B -q -i /root/.ssh/id_rsa"
ERRS=$0.err.$$;
#

##########################################################
#      check USAGE
##########################################################

#USAGE="USAGE: $0 [-h | -help | -init | -check] TARGET_HOST";
USAGE="USAGE: $0 [-h | -help | -check] TARGET_HOST";

if [ "$TARGET" = "" ] ; then
       echo $USAGE
       exit 1;
fi

if   [ "$ACTION" = "-h" ]  ; then echo $USAGE; exit 1;
elif [ "$ACTION" = "-help" ]     ; then echo $USAGE; exit 1;
```

```
#elif [ "$ACTION" = "-init" ]     ; then ACTION="-init";
elif [ "$ACTION" = "-check" ]     ; then ACTION="-check";
else
        echo "You must select an option:  -init or -check."
        echo $USAGE
        exit 1;
fi

##########################################################
#       functions
##########################################################

#######################################
check_err () {
        if [ $* -ne 0 ] ; then
                echo "SCRIPT $0 ABORTED: error."
                exit 1;
        fi
}
#######################################


#######################################
deliver_files () {

        # Copy necessary files to $TARGET, including binary
        $SSH $TARGET "mkdir /etc/tripwire; mkdir /var/lib/tripwire; mkdir
/var/lib/tripwire/report;" > /dev/null 2>&1

        $SCP $WORKDIR/$TARGET.tar.gz $TARGET:/$CFGDIR
        check_err "$?";
        $SSH $TARGET "cd $CFGDIR; /bin/gunzip -c $CFGDIR/$TARGET.tar.gz | tar xf -;" >
/dev/null 2>&1
        check_err "$?";
        $SSH $TARGET "mv $CFGDIR/$TARGET/$TARGET-local.key $CFGDIR; mv
$CFGDIR/$TARGET/site.key $CFGDIR; mv $CFGDIR/$TARGET/tw.cfg $CFGDIR; mv
$CFGDIR/$TARGET/tw.pol $CFGDIR; mv $CFGDIR/$TARGET/$TARGET.twd $DBDIR;"
        check_err "$?";
        rm -f $WORKDIR/$TARGET.tar.gz

#echo "end deliver_files"
}
#######################################


#######################################
get_files () {

        $SSH $TARGET "mv $DBDIR/$TARGET.twd $CFGDIR/$TARGET; mv $CFGDIR/tw.pol
$CFGDIR/$TARGET; mv $CFGDIR/tw.cfg $CFGDIR/$TARGET; mv $CFGDIR/site.key
$CFGDIR/$TARGET; mv $CFGDIR/$TARGET-local.key $CFGDIR/$TARGET; mv $RPTDIR
$CFGDIR/$TARGET; rm -f /usr/sbin/tripwire;"

#       echo "get_files, after mv commands"

        $SSH $TARGET "cd $CFGDIR; rm -f $CFGDIR/$TARGET.tar.gz; tar -cf $TARGET.tar
$TARGET; gzip $TARGET.tar;"
        $SCP $TARGET:$CFGDIR/$TARGET.tar.gz $WORKDIR
        $SSH $TARGET "rm -rf $CFGDIR; rm -rf $DBDIR;"

#       echo "end get_files"
}
#######################################
```

```
#######################################
check () {

#       $SSH $TARGET "cd $CFGDIR/$TARGET; $CFGDIR/$TARGET/tripwire -m c -n -s -r
$RPTDIR/$TARGET-$DATE.twr;" 2>$ERRS
        $SSH $TARGET "cd $CFGDIR/$TARGET; $CFGDIR/$TARGET/tripwire -m c -n -s -r
$RPTDIR/$TARGET-$DATE.twr;"
        MYERR=$?;
#       if [ -f $ERRS ] ; then cat $ERRS | egrep -v "No such file"; rm $ERRS; fi
#       check_err "$MYERR";
#       echo "ERRS = $ERRS";
#       echo "cat ERRS"
#       cat $ERRS
#       echo "done cat ERRS"
#       echo "done check" > /home/membrich/scripts/triph.txt

}
#######################################


#######################################
cleanup () {
#       echo "start cleanup"
#       echo "start cleanup" >> /home/membrich/scripts/triph.txt
# unzip the received files, put the report into the appropriate place
        cd $WORKDIR
        /bin/gunzip -c $TARGET.tar.gz | tar xf -
        rm -f $WORKDIR/$TARGET.tar.gz
#       mv $TARGET/$TARGET.twd.bak $WORKDIR/$TARGET

# get the file ready to deliver tomorrow
        mv $TARGET/report/*.twr $RPTDIR/$TARGET
        rm -rf $WORKDIR/$TARGET/report
        tar -cf $TARGET.tar $TARGET
        gzip $TARGET.tar
#       echo "end cleanup"
#       echo "end cleanup" >> /home/membrich/scripts/triph.txt
}
#######################################


#######################################

# Check connection to $TARGET
$SSH $TARGET date > /dev/null
if [ $? -ne 0 ] ; then
        echo "  ==> SCRIPT $0 ABORTED: cannot execute remote commands on $TARGET."
        exit 1;
fi

deliver_files
if [ "$ACTION" = "-check" ] ; then check; fi
get_files
cleanup
/usr/local/bin/triprpt.sh $TARGET
```

4.3.11. triprpt.sh Script.

```
#!/bin/sh
#
```

```
#  triprpt.sh 020716
#      The purpose of this script is to turn the
#      Tripwire reports from unreadable .twr files
#      into readable text files.
#
#      In the future I'd like to have these files
#      emailed to me (or the appropriate admins).
#
#######################################################
#      Initialize variables
#######################################################
#
DATE=`date "+%Y%m%d"`
TWRDIR='/var/lib/tripwire/report'
LOGDIR='/var/log/tripwire'
HOSTNAME="$1"
#
#######################################################
#      functions
#######################################################
#
/usr/sbin/twprint -m r -r $TWRDIR/$HOSTNAME/$HOSTNAME-$DATE.twr >
$LOGDIR/$HOSTNAME/$HOSTNAME-$DATE.txt
```

====================

That's your full Intrusion Detection System, featuring a sensor and a server.

5. References.

Apache HTTP Server Documentation Project. “SSL/TLS Strong Encryption: FAQ.” Apache HTTP Server Version 2.0 Documentation. <http://httpd.apache.org/docs-2.0/ssl/ssl_faq.html> (15 November 2003).

Boran, Sean. “Hardening Solaris with Yassp.” 18 April 2001. <http://www.boran.com/security/sp/Solaris_hardening3.html> (15 November 2003).

Danyliw, Roman. “ACID: Installation and Configuration.” 09 October 2002. <http://www.andrew.cmu.edu/~rdanyliw/snort/acid_config.html> (15 November 2003).

Ernie. “The Apache-2.0.45 Redhat 9, OpenSSL-0.9.7a Love Triangle.” Technical Travails. 11 April 2003. <http://mt.ernie.org/archives/000001.html> (15 November 2003).

Fyoder. “Nmap Hackers: Nmap 3.48: Service Fingerprints Galore!” Nmap Hackers Security List. 06 October 2003. <http://seclists.org/lists/nmap-hackers/2003/Oct-Dec/0000.html> (15 November 2003).

“Glibc Bugfix Errata.” RedHat Linux 9 General Advisories. 09 April 2003. <https://rhn.redhat.com/errata/RHBA-2003-136.html> (13 November 2003).

Lasser, Jon and Jay Beale. “Bastille Linux.” 05 May 2003. <http://www.bastille-linux.org> (15 November 2003).

Ranum, Marcus J. “The Network Police Blotter.” ;login:. June 2000. <http://www.usenix.org/publications/login/2000-6/features/police.html> (25 November 2003).

Ritchey, Paul. "Snorticus Documentation." <http://snorticus.baysoft.net/snorticus.html> (15 November 2003).

The SHADOW Team. “SHADOW Version 1.8 Installation Manual.” <http://www.nswc.navy.mil/ISSEC/CID/Install3-MS.htm> (26 November 2003).

“Updated 2.4 Kernel Resolves Obscure Bugs.” RedHat Linux 9 General Advisories. 20 August 2003. <https://rhn.redhat.com/errata/RHBA-2003-263.html> (13 November 2003).

“Updated Bash Packages Fix Several Bugs.” RedHat Linux 9 General Advisories. 23 June 2003. <https://rhn.redhat.com/errata/RHBA-2003-140.html> (13 November 2003).

"Updated Fileutils/Coreutils Package Fix ls Vulnerabilities." RedHat Linux 9 General Advisories. 03 November 2003. <https://rhn.redhat.com/errata/RHSA-2003-309.html> (13 November 2003).

"Updated Gnupg Packages Fix Validation Bug." RedHat Linux 9 General Advisories. 20 May 2003. <https://rhn.redhat.com/errata/RHSA-2003-175.html> (13 November 2003).

"Updated Kerberos Packages Fix Various Vulnerabilities." RedHat Linux 9 General Advisories. 02 April 2003. <https://rhn.redhat.com/errata/RHSA-2003-091.html> (13 November 2003).

"Updated MySQL Packages Fix Vulnerability." RedHat Linux 9 General Advisories. 09 October 2003. <https://rhn.redhat.com/errata/RHSA-2003-281.html> (13 November 2003).

"Updated OpenSSH Packages Fix Potential Vulnerabilities." RedHat Linux 9 General Advisories. 17 September 2003. <https://rhn.redhat.com/errata/RHSA-2003-279.html> (13 November 2003).

"Updated OpenSSL Packages Fix Vulnerabilities." RedHat Linux 9 General Advisories. 30 September 2003. <https://rhn.redhat.com/errata/RHSA-2003-292.html> (13 November 2003).

"Updated Perl Packages Fix Security Issues." RedHat Linux 9 General Advisories. 03 October 2003. <https://rhn.redhat.com/errata/RHSA-2003-256.html> (13 November 2003).

"Updated Tcpdump Packages Fix Privilege Dropping Error." RedHat Linux 9 General Advisories. 15 May 2003. <https://rhn.redhat.com/errata/RHSA-2003-174.html> (13 November 2003).

"Updated Unzip Packages Fix Trojan Vulnerability." RedHat Linux 9 General Advisories. 15 August 2003. <https://rhn.redhat.com/errata/RHSA-2003-199.html> (13 November 2003).