# Global Information Assurance Certification Paper

**System Security Audit**
*Submitted by:* Jason Everett

## Executive Summary

This report contains the following sections: System Review, Administrative Summary, Physical Security Summary, Perimeter Defense Summary, Internal Defense and Monitoring Summary, and finally References. Sections will contain a "checklist" that can be used to review security concerns.

The System Review contains information about the hardware and network of this particular machine. In some instances, it can prove useful as a documented baseline of hardware currently installed. You may want to go one step further and document every piece of hardware including serial numbers, model numbers, etc. This will help disaster recovery if it were needed.

The Administrative Summary has information regarding the paper side of the shop. Policies are something no one wants to write, but will help as a planning and goal guide for not only the system but the organization as well. An organization should consider a security policy and, if collecting information about users, a privacy policy. Security policies are for internal use and guidance as administrators of the system do their day to day tasks. It provides them with the documentation and guidance they need to do their jobs. A security policy will likely include access information, network, software development, and disaster recovery procedures. A privacy policy will contain information regarding the use of the information collected about each individual user to the system and what is done with this information.

The Physical Security Summary details how and where the system is located physically. We look mostly at the building that the server is located and the vulnerabilities of the structure. We look at the design of the walls and ceilings, the fire suppression systems, and backup power. We also look at any security systems and other security procedures in the building. We found in this case that the building is relatively insecure as people flow in and out of the building on a regular basis. The doors are not kept locked and the locks are the same throughout the building so that any person having access to the building has access to the servers.

The Perimeter Defense Summary has information regarding outside penetration into the system. It describes what an intruder from the outside will see when he/she probes the system. In this case there were several ports open that didn't need to be and several of these ports had vulnerabilities that would let the intruder gain root access. We also found that some software was giving more information in the form of banners that could be eliminated. This will give the intruder one more hurdle in getting the correct information he/she needs to crack the system. We also found that administrators are communicating with the server using unencrypted communications. Although the local network is switched, those using the Internet could sniff the traffic to gain passwords or other useful information. ssh should be implemented in place of telnet and ftp.

The Internal Defense and Monitoring Summary is a review of the software running on the system and patches that need to be installed from vendors. This system is running an older version of RedHat (v5.2). Several patches are available and need to be installed. We went through each patch and determined if the 1) the software was installed, 2) if the software was needed or could be removed and 3) whether or not the patch was needed.

**System Review**

This section contains the hardware specifications of the system being audited. There is no checklist.

Network:

- Internal - Ethernet 100base-T switched network
- External - Internet via 3 T-1's
- Firewall – Limited packet filtering on the router
- Cisco routers and switches

Hardware:

- Intel Pentium II 266
- 128 Meg RAM
- 2 x 2gig SCSI Drives
- DDS II DAT tape drive

Software:

- OS - RedHat Linux 5.2
- deamons:
  - ESU 10 Media Catalog (custom c software)
  - PostgreSQL 6.1
  - Apache 1.3.3
  - sshd 2.0.13
  - lpd
  - portmap
  - syslogd
  - inetd

**Administrative Summary**

Currently no written security or privacy policies exist for this system. Policies used are 'traditional ways of handling the system' and thus are not enforced in any manner.

*Security Policy:*
The security policy could contain access, network, development, and disaster recovery information.

The access policy should note that access is given in three areas: system maintenance, database maintenance, database user. Currently, there are 26 accounts, of which nine have system maintenance and database maintenance accounts. Database users have little access and thus are not as much of a threat. Password procedures should include information on the rules and regulations for creating and changing the password. Passwords should not be based on personal information and should never use common words that would be found in a dictionary. Good passwords have combinations of letters, numbers, and special characters. They should also have a combination of upper and lower case letters that can easily be remembered so that the user will not write them down.

The network policy should include how the machine's network is configured, what network addresses have access, firewall information, network baselines, and other network specifics. The network policy should also contain information on how information is encrypted or passed from the server to the client. Procedure on IDS monitoring should include log reviews and logging of network traffic. One should also consider a syslog server to store logs off of the server.

The development policy is not as important, as there is only one developer. However, the policy should include items such as documentation, version tracking, and procedures for developing, installing, and running software on the machine. As a general rule, development should be done and tested on a separate machine before it is installed on the main server. This keeps the main server free of the development tools that the intruders will need to install much of the software they use.

A disaster recovery policy is needed as the data on this machine is very valuable to our customers and the jobs of the people maintaining and using it. It should include software backup procedures, hardware backup procedure, hardware replacement procedure, and compromise procedure. Software backup procedure should include restoring the system incase of disk failure or another incident that would render the software unusable. Hardware backups would include such things as RAID systems or redundant systems. Hardware replacement would include the procedure needed in the rare case that the hardware is destroyed. A compromise procedure would include those pre-incident planning ideas contained in the SANS book UNIX Forensics. It includes information on the tools needed, training that a systems administrator should have, and a good broad background. It also includes information on what happens when a compromise occurs.

*Privacy Policy:*

This machine does contain user and tracking information in a postgres database. The information stored is the users name, password, customer information, and what and when items are checked out, thus a privacy policy is in order. The privacy policy would include information on how the data is processed, who has access to it, when it is destroyed, and any other pertinent information.

***Administrative checklist:***

1) **Consult with administrative team to develop a:**
   Security Policy containing access, network, development and disaster recovery information.
   Privacy Policy informing users of what is happening with the information collected on the system.
2) **Educate administrative team on the Security Policy**
3) **Publish the Privacy Policy**

**Physical Security Summary**

*The Room:*
The hardware for the server is in an unlocked room located in a building that has many people in and out of the building attending conferences and classes. At night, the building is armed with a security system, but the room containing the server does not have a motion detector or any other security sensors. This particular room has a window to the and a window in the hallway door, which is the only exit to the room. False walls and ceilings pose little protection from getting into the room if it is locked. The building has a wet sprinkler system and no fire extinguishers in this server room. The closest dry chemical extinguisher is within 40 feet and the closest haylon extinguisher is 200 feet away. A fire in the room would set off the wet sprinkler system at 115 degrees and likely ruin the hardware.

*Hardware:*
The hardware has little protection from intruders once they gain access to the room. The case does not lock. The console is available to anyone who sits down at the machine. It is frequently logged into the root account for maintenance purposes. There is no protection on the BIOS. lilo bootloader security is not enforced.

*Backups:*
Backups are stored unencrypted on a shelf above the machine. These are not locked in anyway. Offsite backups are taken to an residential home, but not locked in a fireproof safe or similar enclosure.

*Precautions taken:*
Security precautions taken have included covering the windows to the room. Someone is also scheduled to be in the room during the normal workday. Power is conditioned using UPS systems. There are banks of machines for each UPS with each bank on a separate breaker. This machine is in a WAN bank.

***Physical Security checklist:***

**1) Password protect the BOIS**
**2) Enable lilo bootloader security**
**3) Lock the server room**
**4) Don't allow unattended sessions (Security Policy)**
**5) Store onsite backups in a safe**
**6) Encrypt onsite and offsite backups**
**7) Store offsite backups in a fireproof safe**
**8) Consider a more secure case that will lock**
**9) Install a hylon extinguisher in the server room**
**10) Increase the temperature of the sprinker heads**
**11) Consider building a more secure room or cage that will enclose the systems**

**Perimeter Defense Summary**

*Packet filtering router firewall.*

The router is blocking well-known security flaws and DoS attacks. There are three separate networks in the building. They are being separated so that there is a DMZ that the Internet servers will reside in a 'closed' network and an internal network the the workstations and LAN servers will reside. The third network is for internal testing. This machine is administered from the internal network, but is accessed from the external network via a web interface to the database.

*nmap report:*
Running nmap details open ports: (1)

```
Port        State       Service
21/tcp      open        ftp
22/tcp      open        ssh
23/tcp      open        telnet
37/tcp      open        time
80/tcp      open        http
98/tcp      open        linuxconf
111/tcp     open        sunrpc
113/tcp     open        auth
515/tcp     open        printer
```

Remote operating system guess: Linux 2.0.35-38

*Review of the software accessible externally:*
ftp:

This service can be turned off. There are dedicated servers on the network for anonymous ftp access and should the need arise that software or data needs to be transferred to the machine, sftp or asimilar service can be used.

- A security bug in wu-ftpd can permit remote users, even without an account, to gain root access. (1)
(http://www.redhat.com/support/errata/RHSA-2000-039-02.html)
- in.ftpd is behind wrappers letting only the local network have access
- The FTP service allows anonymous logins.(2)
- It is possible to gather the real path of the public area of the ftp server (like /home/ftp) by issuing the following command : CWD (2)
- Remote FTP server banner : (2)

```
xxx.xxx.xxx.xxx ftp server (version wu-2.4.2-academ[beta-18](1)
mon aug 3 19:17:20 edt 1998) ready.
```

- Anonymous FTP (3)
  ~ftp/pub/RedHat is writable by 'ftp'.
  ~ftp/pub/squid is writable by 'ftp'.
  ~ftp/pub/ntp is writable by 'ftp'.

~ftp/pub/Caldera is writable by 'ftp'.
- Network sniffing can compromise password and/or data

ssh:

This service was recently installed so that telnet and ftp could be removed. Newer releases of sshd have come out and should be investigated.

- Remote sshd server banner: (2)

```
Remote SSH version : SSH-2.0-2.0.13 (non-commercial)
```

- ssh configuration allows root login

telnet:

The database maintenance personnel currently use this service. ssh software will need to be installed on the individuals workstation so that this service can be removed.

- DoS fix: (1)
(http://www.redhat.com/support/errata/rh52-errata-general.html#in.telnetd)
- in.telnetd is behind wrappers letting only the local network have access
- Network sniffing can compromise password and/or data

time:

This service can be turned off as a cron job runs ntpdate periodically.

- The remote host answers to an ICMP timestamp request. (2)
- in.timed is behind wrappers letting only the local network have access

http:

Apache is the user interface to access the database running on the system. This needs to be updated to the current release.

-A vulnerability in the mod_rewrite module and vulnerabilities in the virtual hosting facility in versions of Apache prior to 1.3.14 may allow attackers to view files on the server which are meant to be inaccessible.(1)
(http://www.redhat.com/support/errata/RHSA-2000-088-04.html)
- Remote httpd server banner: (2)

```
Apache/1.3.3 (Unix)  (Red Hat/Linux)
```

- Passwords and data flow over the wire in clear text. Install an SSL module or similar software.

linuxconf:

- Service not currently being used and can be removed.

sunrpc:

- Service not currently being used and can be removed.

auth :

- in.identd could safely be turned off. The information is not used internally for anything.

lpr:

lpr is used to print reports on a daily basis. It will need to be updated.

- lpr has a format string security bug, LPRng compat issues, and a race cond. [1] (http://www.redhat.com/support/errata/RHSA-2000-066-05.html)

***Perimeter Defense checklist:***

**1) Close ports that are not needed**

ftp, telnet, in.timed, linuxconf, sunrpc, auth
inetd could be turned off completely

**2) Update software**

apache, lpr, sshd

**3) Fix banner messages**

ftp, sshd

**4) Review network encryption**

Use ssh for connection to the machine
Review use of apache 'basic' authentication for database access
Use ssl for web connections

**5) Complete the installation and configuration of the firewall network**

## Internal Defense and Monitoring Summary

OS patches for RedHat 5.2 [1]

```
20-Nov-2000: joe (RHSA-2000:110-06)
12-Nov-2000: bind (RHSA-2000:107-02)
10-Nov-2000: pine, imap (RHSA-2000:102-04)
02-Nov-2000: dump (RHSA-2000:100-02)
26-July-2000: apache, php, mod_perl, auth_ldap (RHSA-2000:088-04)
26-July-2000: ypbind (RHSA-2000:086-05)
06-Oct-2000: traceroute (RHSA-2000:078-02)
04-Oct-2000: lpr (RHSA-2000:066-05)
26-July-2000: glint (RHSA-2000:062-03)
26-July-2000: sysklogd (RHSA-2000:061-02)
14-Sep-2000: xpdf (RHSA-2000:060-03)
11-Sep-2000: megetty (RHSA-2000:059-02)
07-Sep-2000: screen (RHSA-2000:058-03)
07-Sep-2000: glibc (RHSA-2000:057-04)
30-Aug-2000: mailx and perl (RHSA-2000:048-03)
09-Aug-2000: rpm (RHEA-2000:051-01)
28-July-2000: Netscape (RHSA-2000:046-02)
26-July-2000: gpm (RHSA-2000:045-01)
03-July-2000: man security fix (RHSA-2000:041-02)
23-June-2000: wu-ftpd security fix (RHSA-2000:039-02)
12-April-2000: gpm-root security fix (RHSA-2000:009-02)
30-Mar-2000: ircii-4.4M-1 (RHSA-2000:008-01)
06-Mar-2000: Netscape-4.72 (RHSA-2000:007-02)
06-Mar-2000: nmh-1.0.3-5x (RHSA-2000:006-01)
07-Jan-2000: lpr (RHSA-2000:002-01)
03-Jan-2000: sharutils (RHBA-1999:063-02)
31-Dec-1999: libtiff, groff (RHBA-1999:061-01)
19-Nov-1999: syslogd (RHSA-1999:055-01)
11-Nov-1999: bind (RHSA-1999:054-01)
11-Nov-1999: NFS (RHSA-1999:053-01)
27-Oct-1999: ypserv (RHSA-1999:046-01)
21-Oct-1999: wu-ftpd (RHSA-1999:043-01)
13-Sept-1999: mars_nwe (RHSA-1999:037-01)
07-Sept-1999: XFree86 (RHSA-1999:035-02)
01-Sept-1999: inews (RHSA-1999:033-01)
30-Aug-1999: amd (RHSA-1999:032-01)
25-Aug-1999: vixie-cron (RHSA-1999:030-02)
19-Aug-1999: in.telnetd (RHSA-1999:029-01)
17-Aug-1999: libtermcap (RHSA-1999:028-01)
29-Jul-1999: squid (RHSA-1999:025-01)
29-Jul-1999: samba (RHSA-1999:022-02)
07-Jul-1999: rpm (RHEA-1999:018-01)
11-Jun-1999: timetool
10-Jun-1999: imap
27-May-1999: mod_perl
16-Apr-1999: rsync
16-Apr-1999: procmail
01-Apr-1999: pine
01-Apr-1999: mutt
06-Nov-1998: zgv
19-Feb-1999: lsof
09-Feb-1999: minicom
02-Feb-1999: dump
```

```
02-Feb-1999: perl
02-Feb-1999: Xconfigurator
19-Jan-1999: fvwm2
03-Jan-1999: kernel
03-Jan-1999: pam
03-Jan-1999: New Boot Images
22-Dec-1998: ftp client
13-Nov-1998: Security: libc5
13-Nov-1998: Unable to Select PackagesDuring Install (Alpha)
06-Nov-1998: Security: svgalib
```

*Updates needed:*

pine - Pine is a very full featured text based mail and news client. It is aimed at both novice and expert users. It includes an easy to use editor, pico, for composing messages. Pico has gained popularity as a stand alone text editor in its own right. It features MIME support, address books, and support for IMAP, mail, and MH style folders. (4)

- This package is not used and can safely be removed.

dump - dump and restore can be used to backup extended 2 (ext2) partitions in a variety of ways. (4)

- dump is used to back the system up to tape.

apache - Apache is a full featured web server that is freely available, and also happens to be the most widely used. (4)

- Apache is the user interface to the database.

ypbind - This is a daemon which runs on NIS/YP clients and binds them to a NIS domain. It must be running for systems based on glibc to behave as NIS clients.(4)

- This package is not used and can safely be removed.

traceroute - Traceroute prints the route packets take across a TCP/IP. The names (or IP numbers if names are not available) of the machines which are routing packets from the machine traceroute is running on to the destination machine are printed, along with the time is took to receive a packet acknowledgement from that machine. This tool can be very helpfull in diagnosing networking problems. (4)

- This is a useful diagnostic tool when users cannot connect to the system.

lpr - This package manages printing services. It manages print queues, sends jobs to local printers and remote pritners, and accepts jobs from remote clients. (4)

- lpr is used to create reports on a daily basis.

sysklogd - This is the Linux system and kernel logging program. It is run as a daemon (background process) to log messages to different places. These are usually things like sendmail logs, security logs, and errors from other daemons. (4)

- sysklogd is used extensively for logging.

glibc - Contains the standard libraries that are used by multiple programs on the system. In order to save disk space and memory, as well as to ease upgrades, common system code is kept in one place and shared between programs. This package contains the most important sets of shared libraries, the standard C library and the standard math library. Without these, a Linux system will not function. It also contains national language (locale) support and timezone databases. (4)

mailx - The /bin/mail program can be used to send quick mail messages, and is often used in shell scripts. (4)

- This package is not used and can safely be removed.

perl - Perl is an interpreted language optimized for scanning arbitrary text files, extracting information from those text files, and printing reports based on that information. It's also a good language for many system management tasks. The language is intended to be practical (easy to use, efficient, complete) rather than beautiful (tiny, elegant, minimal). (4)

- Perl is used in a few of the cgi's and some maintenance scripts. This will need an update.

rpm - RPM is a powerful package manager, which can be used to build, install, query, verify, update, and uninstall individual software packages. A package consists of an archive of files, and package information, including name, version, and description. (4)

- rpm is used as an easy way to install security updates.

man - The man page suite, including man, apropos, and whatis. These programs are used to read most of the documentation available on a Linux system. The whatis and apropos programs can be used to find documentation related to a particular subject. (4)

- man is used extensively in documentation review. Although it could be removed the convenience outweighs the risks.

wu-ftpd - wu-ftpd is the daemon (background) program which serves FTP files to ftp clients. It is useful if you wish to exchange programs between computers without running a network filesystem such as NFS, or if you with to run an anonymous FTP site (in which case, you will want to install the anonftp package). (4)

- This is currently being used to transfer reports to a print workstation to print labels. It can be removed if labels can be printed without transferring them to the workstation via ftp. The problem lies in the fact that the workstation that prints the labels is a dos machine and thus is very limited in its abilities.

nmh - nmh mail handling system (with POP support). nmh is a popular mail handling system but includes only a command line interface. It is an important base, however, for programs like xmh and exmh. (4)

- This package is not used and can safely be removed.

sharutils - The shar utilities can be used to encode and package a number of files, binary and/or text, in a special plain text format. This format can safely be sent through email or other means where sending binary files is difficult. (4)

- This package is not used and can safely be removed.

libtiff - This package is a library of functions that manipulate TIFF images. (4)
- This package is not used and can safely be removed.

groff - The groff text formatting system can be used to create professional looking documents on both paper and a computer screen. All the man pages are processed with groff, so you'll need this package to read man pages. (4)
- This will be used for documentation review.

NFS - The NFS and mount daemons are used to create an NFS server which can export filesystems to other machines. This package is not needed to mount NFS filesystems -- that functionality is already in the Linux kernel. (4)
- This can be removed as nfs is being used as a client to backup data files. These data files will eventually be transferred using sftp.

vixie-cron - cron is a standard UNIX program that runs user-specified programs at periodic scheduled times. vixie cron adds a number of features to the basic UNIX cron, including better security and more powerful configuration options. (4)
- cron is being used in several system maintenance functions and also in creating the reports to be printed daily.

in.telnetd - Telnet is a popular protocol for remote logins across the Internet. This package provides a command line telnet client as well as a telnet daemon which allows remote logins into the machine it is running on. The telnet daemon is enabled by default, and may be disabled by editing /etc/inetd.conf. (4)
- Telnet is currently being used but plans are in place to replace it with ssh.

libtermcap - This is the library for accessing the termcap database. It is necessary to be installed for a system to be able to do much of anything. (4)
- This package needs to be updated.

timetool - Timetool is a graphical interface for setting the current date and time for your system. (4)
- This package can be safely removed, as there is no graphical interface used on the machine.

procmail - Red Hat Linux uses procmail for all local mail delivery. In addition to regluar mail delivery duties, procmail can be used to do many different automatic filtering, presorting, and mail handling jobs. It is the basis for the SmartList mailing list processor. (4)
- This system handle some mail and thus this package needs to be updated.

Xconfigurator - This is the Red Hat X Configuration tool. It is based on the sources for xf86config, a utility from XFree86. It has a nicer user interface added to make it easier for the end user. (4)

- This package can be safely removed, as there is no graphical interface used on the system.

fvwm2 - fvwm is a version of the popular "Feeble Virtual Window Manager" (4)

- This package can be safely removed, as there is no graphical interface used on the system.

pam - PAM (Pluggable Authentication Modules) is a powerful, flexible, extensible authentication system which allows the system administrator to configure authentication services individually for every pam-compliant application without recompiling any of the applications. (4)

- This package is used for authentication to the machine. It will need to be updated.

ftp client - This provides the standard Unix command-line ftp client. ftp is the standard Internet file transfer protocol, which is extremely popular for both file archives and file transfers between individuals. (4)

- Most ftp transactions will use sftp but a few will require ftp. It will need to be updated.

libc5 - Older Linux systems (including all Red Hat Linux releases between 2.0 and 4.2, inclusive) were based on libc 5. This package includes these libraries and other libraries based on libc 5, allowing old applcications to run on glibc (libc 6) based systems. (4)

- This system has a legacy software system installed that needs the libc5 libraries. A full test of the libraries will be needed before it is updated.

svgalib - SVGAlib is a library which allows applications to use full screen graphics on a variety of hardware platforms. Many games and utilities are available which take advantage of SVGAlib for graphics access, as it is more suitable for machines with little memory than X Windows is. (4)

- This package can be safely removed, as there is no graphical interface used on the system.

*Cron jobs:*

root

ntpdate

postgres

daily reports

*Accounts/passwords:*

[/etc/password removed from report.]

A review of the password file shows that there are accounts that can be removed. Accounts that can be removed include news, uucp, games, gopher, ftp, isaacson, and announce. Passwords are also vulnerable. Although we have not perfomed a scan using crack or some other method to crack the password, two generic accounts have easy to guess passwords. The password policy needs to be enforced.

*suid/sgid files:*

SUID and SGID files on your system are a potential security risk, and should be monitored closely. Because these programs grant special privileges to the user who is executing them, it is necessary to ensure that insecure programs are not installed. [5]

Results of: find / -type f \( -perm -04000 -o -perm -02000 \)

```
/usr/bin/rcp
/usr/bin/rlogin
/usr/bin/rsh
/usr/bin/wall
/usr/bin/at
/usr/bin/dos
/usr/bin/lpq
/usr/bin/lpr
/usr/bin/lprm
/usr/bin/man
/usr/bin/passwd
/usr/bin/suidperl
/usr/bin/lockfile
/usr/bin/procmail
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/write
/usr/bin/crontab
/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/inc
/usr/bin/sperl5.00404
/usr/X11R6/bin/xterm
/usr/X11R6/bin/Xwrapper
/usr/X11R6/bin/nxterm
/usr/local/bin/ssh-signer2
/usr/sbin/usernetctl
/usr/sbin/lpc
/usr/sbin/sendmail
/usr/sbin/traceroute
/usr/sbin/wsmbconf
/usr/sbin/userhelper
/bin/ping
/bin/mount
/bin/umount
/bin/su
/bin/login
/bin/.login
/sbin/pwdb_chkpwd
/sbin/cardctl
/sbin/dump
/sbin/restore
/sbin/netreport
/data/ftp/pub/RedHat/instimage/usr/bin/ping
/misc/bin/ping
/misc/bin/mount
/misc/bin/umount
/misc/bin/su
/misc/bin/login
/misc/bin/.login
```

```
/misc/sbin/pwdb_chkpwd
/misc/sbin/cardctl
/misc/sbin/dump
/misc/sbin/restore
/misc/sbin/netreport
```

*Unowned files:*
Unowned files may also be an indication an intruder has accessed your system. (5)

Results of: find / -nouser -o -nogroup –print
/media-backup

World-writable files, particularly system files, can be a security hole if a cracker gains access to your system and modifies them. Additionally, world-writable directories are dangerous, since they allow a cracker to add or delete files as he wishes. (5)

Results of: find / -perm -2 ! -type l –ls |grep –v dev

```
  4033    1 drwxrwxrwt   3 root     root         1024 Nov 21 15:37 /tmp
 50402    1 drwxrwxrwx   2 root     root         1024 Aug 13  1999 /tmp/.X11-unix
 50403    0 srwxrwxrwx   1 root     root            0 Aug 13  1999 /tmp/.X11-unix/X9
 30268    1 drwxrwxrwt   2 root     root         1024 Aug 24  1999 /var/lib/texmf
 30263    1 drwxrwxrwx   2 root     root         1024 Oct 12  1998 /var/spool/samba
 60481    1 drwxrwxrwt   2 root     root         1024 Aug 28 13:42 /var/tmp
277480   57 -rw-rw-rw-   1 postgres postgres    58300 Nov 24  1997 /data/postgresql-
6.2.1/src/test/regress/results/onek.data
277497    1 -rw-rw-rw-   1 postgres postgres      208 Nov 24  1997 /data/postgresql-
6.2.1/src/test/regress/results/stud_emp.data
350882    2 -rw-rw-rw-   1 1002     root         1664 Jan  2  1997 /data/postgresql-
6.2.1/medcat/create.sql
352921    1 drw-rw-rw-   2 1002     root         1024 Feb 24  1997 /data/postgresql-
6.2.1/medcat/logs
350883    2 -rw-rw-rw-   1 1002     root         1248 Mar  6  1997 /data/postgresql-
6.2.1/medcat/conflicts.c
350884    8 -rw-rw-rw-   1 1002     root         7176 Mar  6  1997 /data/postgresql-
6.2.1/medcat/media_items
350885    8 -rw-rw-rw-   1 1002     root         7190 Mar 17  1997 /data/postgresql-
6.2.1/medcat/check_out.c
350886    1 -rw-rw-rw-   1 1002     root          812 Feb  5  1997 /data/postgresql-
6.2.1/medcat/perl1
350887    1 -rw-rw-rw-   1 1002     root          279 Feb  5  1997 /data/postgresql-
6.2.1/medcat/perl2
350888    5 -rw-rw-rw-   1 1002     root         4875 Mar 17  1997 /data/postgresql-
6.2.1/medcat/co-extend2.c
350889   48 -rw-rw-rw-   1 1002     root        49152 Feb 21  1997 /data/postgresql-
6.2.1/medcat/testlibpq3
350891    7 -rw-rw-rw-   1 1002     root         7114 Sep 13 13:22 /data/postgresql-
6.2.1/medcat/mi-maint.c
350892   48 -rw-rw-rw-   1 1002     root        49152 Feb 21  1997 /data/postgresql-
6.2.1/medcat/medcat
350893    1 -rw-rw-rw-   1 1002     root          648 Feb 11  1997 /data/postgresql-
6.2.1/medcat/db.h
350894    2 -rw-rw-rw-   1 root     root         1259 Apr 15  1997 /data/postgresql-
6.2.1/medcat/import-mi.c
350895    2 -rw-rw-rw-   1 1002     root         1314 Aug 17  1998 /data/postgresql-
6.2.1/medcat/medcat.h
```

```
350896    6 -rw-rw-rw-   1 1002     root         5674 Jan 16  1997 /data/postgresql-
6.2.1/medcat/html.c
350897    1 -rw-rw-rw-   1 1002     root          504 Oct 14  1996 /data/postgresql-
6.2.1/medcat/html.h
350898    5 -rw-rw-rw-   1 1002     root         4748 Dec  1  1997 /data/postgresql-
6.2.1/medcat/db.c
350899    2 -rw-rw-rw-   1 1002     root         1769 Dec 13  1996 /data/postgresql-
6.2.1/medcat/r-add2.c
350900    1 -rw-rw-rw-   1 1002     root           78 Nov 15  1996 /data/postgresql-
6.2.1/medcat/mci
350901    1 -rw-rw-rw-   1 1002     root          316 Dec  9  1996 /data/postgresql-
6.2.1/medcat/backup.sql
350902    1 -rw-rw-rw-   1 1002     root          143 Oct  8  1996 /data/postgresql-
6.2.1/medcat/mc7.awk
350903    1 -rw-rw-rw-   1 1002     root          764 Feb  5  1997 /data/postgresql-
6.2.1/medcat/perl3
350904    3 -rw-rw-rw-   1 1002     root         2955 Feb 12  1997 /data/postgresql-
6.2.1/medcat/route.c
350906   17 -rw-rw-rw-   1 1002     root        16986 Aug 10  1999 /data/postgresql-
6.2.1/medcat/mi-search.c
350907    9 -rw-rw-rw-   1 1002     root         8513 Feb 21  1997 /data/postgresql-
6.2.1/medcat/mi-change1.c
350909    1 -rw-rw-rw-   1 1002     root          950 Feb  7  1997 /data/postgresql-
6.2.1/medcat/r-change2.c
350910    4 -rw-rw-rw-   1 1000     root         4081 May 30  1997 /data/postgresql-
6.2.1/medcat/util.c
350911    1 -rw-rw-rw-   1 1002     root          398 Nov 15  1996 /data/postgresql-
6.2.1/medcat/util.h
350912    3 -rw-rw-rw-   1 1002     root         2785 Aug 11  1999 /data/postgresql-
6.2.1/medcat/user.c
350913   11 -rw-rw-rw-   1 1002     root        11058 Aug 10  1999 /data/postgresql-
6.2.1/medcat/mi-display.c
350914    4 -rw-rw-rw-   1 1002     root         3290 Nov 26  1997 /data/postgresql-
6.2.1/medcat/passwd.c
350915    7 -rw-rw-rw-   1 1002     root         6782 Mar  6  1997 /data/postgresql-
6.2.1/medcat/mi-change2.c
350917    5 -rw-rw-rw-   1 1002     root         4472 Feb  7  1997 /data/postgresql-
6.2.1/medcat/r-change1.c
350918    1 -rw-rw-rw-   1 1002     root          476 Dec 16  1996 /data/postgresql-
6.2.1/medcat/user.h
350919    6 -rw-rw-rw-   1 1002     root         5635 Feb 12  1997 /data/postgresql-
6.2.1/medcat/school.c
350920    1 -rw-rw-rw-   1 1002     root          579 Oct 21  1996 /data/postgresql-
6.2.1/medcat/school.h
350921    2 -rw-rw-rw-   1 1002     root         1504 Oct 25  1996 /data/postgresql-
6.2.1/medcat/mi-delete.c
350922    7 -rw-rw-rw-   1 1002     root         6510 Mar  6  1997 /data/postgresql-
6.2.1/medcat/book3-user.c
350923   12 -rw-rw-rw-   1 1000     root        11287 Aug 21  1998 /data/postgresql-
6.2.1/medcat/book2-admin.c
350924    6 -rw-rw-rw-   1 1002     root         5272 Feb 18  1997 /data/postgresql-
6.2.1/medcat/check-in.c.old
350925    1 -rw-rw-rw-   1 1002     root          744 Oct 25  1996 /data/postgresql-
6.2.1/medcat/mi-delete2.c
350926    7 -rw-rw-rw-   1 1002     root         6601 Sep 15  1998 /data/postgresql-
6.2.1/medcat/book1-admin.c
350928    2 -rw-rw-rw-   1 1002     root         1059 Nov 11  1996 /data/postgresql-
6.2.1/medcat/sids.c
350929    3 -rw-rw-rw-   1 1002     root         2783 Dec 13  1996 /data/postgresql-
6.2.1/medcat/r-add.c
350930    2 -rw-rw-rw-   1 1002     root         1629 Nov 26  1997 /data/postgresql-
6.2.1/medcat/u-add.c
```

```
350931    2 -rw-rw-rw-   1 1002     root         1285 Feb  7  1997 /data/postgresql-
6.2.1/medcat/r-delete1.c
350932    1 -rw-rw-rw-   1 1002     root          586 Nov  4  1996 /data/postgresql-
6.2.1/medcat/s-delete2.c
350933    2 -rw-rw-rw-   1 1002     root         1420 Dec  1  1997 /data/postgresql-
6.2.1/medcat/check-in2.c
350939   80 -rw-rw-rw-   1 1002     root        81920 May 21  1997 /data/postgresql-
6.2.1/medcat/clean-up
350934    3 -rw-rw-rw-   1 1002     root         2499 Oct 25  1996 /data/postgresql-
6.2.1/medcat/u-change1.c
350935    2 -rw-rw-rw-   1 1002     root         1212 Feb 14  1997 /data/postgresql-
6.2.1/medcat/s-delete1.c
350936    1 -rw-rw-rw-   1 1002     root          138 Oct 23  1996 /data/postgresql-
6.2.1/medcat/u-change.h
350937   13 -rw-rw-rw-   1 1000     root        12938 Jan  8  1998 /data/postgresql-
6.2.1/medcat/book2-user.c
350938    1 -rw-rw-rw-   1 1002     root          466 Oct 23  1996 /data/postgresql-
6.2.1/medcat/u-change3.c
350940    3 -rw-rw-rw-   1 1002     root         2973 Feb 12  1997 /data/postgresql-
6.2.1/medcat/u-stuff.c
350941    3 -rw-rw-rw-   1 1002     root         2168 Feb 12  1997 /data/postgresql-
6.2.1/medcat/u-change.c
361081    1 drw-rw-rw-   2 1002     root         1024 Nov 15  1999 /data/postgresql-
6.2.1/medcat/convert
350942    1 -rw-rw-rw-   1 1002     root          138 Oct 23  1996 /data/postgresql-
6.2.1/medcat/u-stuff.h
350943    5 -rw-rw-rw-   1 1002     root         4641 Feb 20  1997 /data/postgresql-
6.2.1/medcat/co-list.c
350945    2 -rw-rw-rw-   1 1002     root         1793 Nov 26  1997 /data/postgresql-
6.2.1/medcat/u-change2.c
350946    2 -rw-rw-rw-   1 1002     root         1825 Mar  6  1997 /data/postgresql-
6.2.1/medcat/media_items.c
350947    3 -rw-rw-rw-   1 1002     root         2221 Jan 13  1998 /data/postgresql-
6.2.1/medcat/new-labels.c
350948    6 -rw-rw-rw-   1 1002     root         5699 May 20  1997 /data/postgresql-
6.2.1/medcat/check-in.c
350949    2 -rw-rw-rw-   1 1002     root         1637 Oct 25  1996 /data/postgresql-
6.2.1/medcat/u-delete1.c
350950    1 -rw-rw-rw-   1 1002     root          539 Oct 25  1996 /data/postgresql-
6.2.1/medcat/u-delete2.c
350951    1 -rw-rw-rw-   1 1002     root          476 Jan  6  1997 /data/postgresql-
6.2.1/medcat/check-in.h
350952    1 -rw-rw-rw-   1 1002     root          751 Feb 24  1997 /data/postgresql-
6.2.1/medcat/check_out.h
350953   82 -rw-rw-rw-   1 1002     root        83271 Feb  7  1997 /data/postgresql-
6.2.1/medcat/query.out
350954    1 -rw-rw-rw-   1 1002     root          523 Dec 13  1996 /data/postgresql-
6.2.1/medcat/route.h
350955    1 -rw-rw-rw-   1 1002     root          843 Oct 27  1996 /data/postgresql-
6.2.1/medcat/media_items.h
350956    2 -rw-rw-rw-   1 1002     root         1165 Nov  7  1996 /data/postgresql-
6.2.1/medcat/double-book.pl
350957    8 -rw-rw-rw-   1 1002     root         7694 May 19  1997 /data/postgresql-
6.2.1/medcat/mi-search-all.c
350958    2 -rw-rw-rw-   1 1002     root         1756 Dec  2  1996 /data/postgresql-
6.2.1/medcat/s-add.c
350959   12 -rw-rw-rw-   1 1002     root        11286 Jan 16  1997 /data/postgresql-
6.2.1/medcat/file
350960    1 -rw-rw-rw-   1 1002     root          608 Feb 14  1997 /data/postgresql-
6.2.1/medcat/s-change1.c
350961    2 -rw-rw-rw-   1 1002     root         1914 Dec  2  1996 /data/postgresql-
6.2.1/medcat/s-change2.c
```

```
350962    4 -rw-rw-rw-   1 1002     root         4070 Dec 13  1996 /data/postgresql-
6.2.1/medcat/mi-display-all.c
350963    3 -rw-rw-rw-   1 1002     root         2412 Mar  5  1997 /data/postgresql-
6.2.1/medcat/co-extend.c
350964    2 -rw-rw-rw-   1 1002     root         1364 Dec  1  1997 /data/postgresql-
6.2.1/medcat/mi-id-change.c
350965    2 -rw-rw-rw-   1 1002     root         1168 Jan  9  1997 /data/postgresql-
6.2.1/medcat/co-delete.c
350966    5 -rw-rw-rw-   1 1002     root         4591 Jan 13  1998 /data/postgresql-
6.2.1/medcat/delivery.c
350967    1 -rw-rw-rw-   1 1002     root          721 Feb  5  1997 /data/postgresql-
6.2.1/medcat/perl4
350968    7 -rw-rw-rw-   1 1002     root         7082 Mar 17  1997 /data/postgresql-
6.2.1/medcat/mi-search.c.old
350969    4 -rw-rw-rw-   1 1002     root         3588 Mar  8  1997 /data/postgresql-
6.2.1/medcat/pickup.c
350970    2 -rw-rw-rw-   1 1002     root         2032 Mar  6  1997 /data/postgresql-
6.2.1/medcat/co-ckin.c
350971    2 -rw-rw-rw-   1 1002     root         1282 Apr 22  1999 /data/postgresql-
6.2.1/medcat/overdue.c
350972    1 -rw-rw-rw-   1 1002     root          390 May 22  1997 /data/postgresql-
6.2.1/medcat/query.sql
350973    1 -rw-rw-rw-   1 1002     root          714 Jan 16  1997 /data/postgresql-
6.2.1/medcat/updater.c
350974    7 -rw-rw-rw-   1 1002     root         7057 Mar 17  1997 /data/postgresql-
6.2.1/medcat/mi-search-all.c.old
350975   11 -rw-rw-rw-   1 1002     root        10374 Mar 17  1997 /data/postgresql-
6.2.1/medcat/book2-admin.c.old
350976    1 -rw-rw-rw-   1 1002     root          485 Feb  1  1997 /data/postgresql-
6.2.1/medcat/co-unlock.c
350978    2 -rw-rw-rw-   1 1002     root         1719 Feb 11  1997 /data/postgresql-
6.2.1/medcat/create2.sql
350979   13 -rw-rw-rw-   1 1000     root        12773 May  8  1997 /data/postgresql-
6.2.1/medcat/book2-user.c.old
350980    7 -rw-rw-rw-   1 1002     root         6599 Feb 12  1997 /data/postgresql-
6.2.1/medcat/book1-user.c.old
350981    3 -rw-rw-rw-   1 root     root         2582 May 21  1997 /data/postgresql-
6.2.1/medcat/clean-up.c
350982    4 -rw-rw-rw-   1 1000     root         3487 Dec  2  1997 /data/postgresql-
6.2.1/medcat/hand-book.c
350983    7 -rw-rw-rw-   1 1002     root         6304 Feb  7  1997 /data/postgresql-
6.2.1/medcat/u-change
350984    1 -rw-rw-rw-   1 1002     root          330 Feb 12  1997 /data/postgresql-
6.2.1/medcat/perl5
350985    1 -rw-rw-rw-   1 1002     root          324 Feb 12  1997 /data/postgresql-
6.2.1/medcat/perl6
350987    1 -rw-rw-rw-   1 1002     root           33 Feb  5  1997 /data/postgresql-
6.2.1/medcat/sed.script1
351016    8 -rw-rw-rw-   1 root     root         7856 Nov 26  1997 /data/postgresql-
6.2.1/medcat/Makefile.save
350944  190 -rw-rw-rw-   1 root     root       194560 Apr 15  1997 /data/postgresql-
6.2.1/backup/util.tar
  4081    1 drwxrwxrwt   2 root     root         1024 Aug  5  1999 /misc/tmp
 18361    1 drwxrwxrwt   2 root     root         1024 Mar  1  1999 /misc/var/lib/texmf
 55081    1 drwxrwxrwx   2 root     root         1024 Oct 12  1998
/misc/var/spool/samba
 63241    1 drwxrwxrwt   2 root     root         1024 Jul 20  1999 /misc/var/tmp
```

A review of these files shows that the directory /data/postgresql-6.2.1/medcat was improperly installed. These files can be safely changed to 750. It also shows that the directory /misc can be cleaned out. It looks as if a back up of the system has been place in this location. The temporary

samba directory can be removed and the X11 directories can be removed also. This will get the system back in order.

*Umask Settings*
The umask command can be used to determine the default file creation mode on your system. It is the octal complement of the desired file mode. If files are created without any regard to their permissions settings, the user could inadvertently give read or write permission to someone that should not have this permission. Typical umask settings include 022, 027, and 077 (which is the most restrictive). Normally the umask is set in /etc/profile, so it applies to all users on the system. The file creation mask can be calculated by subtracting the desired value from 777. In other words, a umask of 777 would cause newly-created files to contain no read, write or execute permission for anyone. A mask of 666 would cause newly-created files to have a mask of 111. (5)

This system is using a umask of 002 set in /etc/profile.

***Internal Defense and Monitoring checklist:***

1) **Install patches for known problems**
2) **Remove packages that are not needed**
3) **Review and document cron jobs**
4) **Remove unneeded accounts**
5) **Review and enforce password policy**
6) **Document suid and sgid files**
7) **Document unowned files**
8) **Clean up world writable files**
9) **Document world writable files**
10) **Document umask settings**

## Referneces


(1) RedHat errata
http://www.redhat.com/errata/

(2) nessus scan

(3) tiger scan

(4) RPM query
Result of: rpm –qi package_name

(5) Linux Security HOWTO

Last Updated: May 25th, 2017

# Upcoming Training


| | | | |
|---|---|---|---|
| **SANS London July 2017** | **London, United Kingdom** | **Jul 03, 2017 - Jul 08, 2017** | **Live Event** |
| **SANSFIRE 2017** | **Washington, DC** | **Jul 22, 2017 - Jul 29, 2017** | **Live Event** |
| **SANS Network Security 2017** | **Las Vegas, NV** | **Sep 10, 2017 - Sep 17, 2017** | **Live Event** |
| **SANS OnDemand** | **Online** | **Anytime** | **Self Paced** |
| **SANS SelfStudy** | **Books & MP3s Only** | **Anytime** | **Self Paced** |