Global Information Assurance Certification Paper

Intranet Web Server Security

Jeff Schaller

August 14, 2000

Contents

Executive Summary

Security is an on-going challenge for both management and system administrators. On the one hand, management pays for hardware, software, and administrator positions in order to gain functionality (such as a web server). On the other hand, a security-conscious system administrator must constantly restrict the functionality of each server to include only what it needs to provide. Fortunately, an agreed-upon level of security can be achieved through detailed understanding of the purpose of each server. By knowing what needs to be provided, system administrators can focus their efforts on a smaller set of programs and patches. Limiting the purpose of a server to a well-defined area also limits exposure to new security holes. In this way, management has a guarantee of what services are being provided, and administrators have a guide for securing the servers.

The two servers that were analyzed in this report are web servers. Snnyroch56 provides web service with CGI (Common Gateway Interface), SSI (Server-side Includes), Frontpage extensions, and Coldfusion; it is also an ftp server. Snnyroch08 provides web service with CGI (Common Gateway Interface), SSI (Server-side Includes), Frontpage extensions, and Coldfusion; it is also an ftp server and an LDAP (Lightweight Directory Access Protocol) server.

Unfortunately, even these minimal definitions can allow for compromise: CGI scripts are the most common avenue of attack on web servers; a recent defacement of http://www.apache.org[1] demonstrated the dangers of running unsafe configurations of ftp and web services on the same server. Above and beyond these

services, though, the company's web servers are running services and software that are both outside their service definition and vulnerable to attack.

It should be noted that the web servers in question are behind a corporate firewall, accessible only to employees. While this provides a measure of protection (it reduces the number of possible attackers), it is not a cure-all for security concerns. Security violations often occur from within a company - employees know more about the company's computer systems, and so can be that much more dangerous.

Two steps need to be taken immediately: audit and tighten security on scripts and services, and remove extraneous services and packages. While the bulk of the work now may appear to be a one-time effort, security is really an on-going project. Administrators need to keep current with patches and software updates, as well as maintain secure configurations of each software package, including their interactions with other packages on the system. Management needs to interact with the appropriate team members when requesting additional functionality as well as provide administrators with sufficient time to complete these tasks.

Detailed Analysis

Installed packages

Snnyroch08 has 268 packages installed; many of these are extraneous to web server operations. A compromise in one of these 268 packages could lead to a system compromise. Snnyroch56 has 283 packages installed; many of these are extraneous to web server operations. A compromise in one of the 283 packages could lead to a system compromise. Having more packages than are required on a system also means needing more patches, which means more wasted system administrator time and effort.

The following installed programs have had security-related bugs found in them recently (CVE numbers refer to the Common Vulnerability Database at http://cve.mitre.org):

- 2000-08-08: Solaris AnswerBook2 Administration Interface Access Vulnerability
  http://securityfocus.com/vdb/bottom.html?vid=1554
- 2000-08-07: Solaris AnswerBook2 Remote Command Execution Vulnerability
  http://securityfocus.com/vdb/bottom.html?vid=1556
- 2000-06-14: Solaris ufsrestore Buffer Overflow Vulnerability
  http://securityfocus.com/vdb/bottom.html?vid=1348
  CVE-1999-0069
- 2000-05-12: Solaris netpr Buffer Overflow Vulnerability
  http://securityfocus.com/vdb/bottom.html?vid=1200
  CVE-2000-0407
- 2000-04-24: Solaris lp -d Option Buffer Overflow Vulnerability
  http://securityfocus.com/vdb/bottom.html?vid=1143
- 2000-04-24: Solaris Xsun Buffer Overrun Vulnerability
  http://securityfocus.com/vdb/bottom.html?vid=1140
- 2000-04-24: Solaris lpset -r Buffer Overflow Vulnerability
  http://securityfocus.com/vdb/bottom.html?vid=1138
- 2000-01-06: Solaris chkperm Buffer Overflow Vulnerability
  http://securityfocus.com/vdb/bottom.html?vid=918
- 1999-12-22: Solaris DMI Denial of Service Vulnerabilities

http://securityfocus.com/vdb/bottom.html?vid=878
- 1999-12-10: Solaris sadmind Buffer Overflow Vulnerability
  http://securityfocus.com/vdb/bottom.html?vid=866
  CVE-1999-0977
- 1999-12-09: Solaris snoop (GETQUOTA) Buffer Overflow Vulnerability
  http://securityfocus.com/vdb/bottom.html?vid=864
  CVE-1999-0974
- 1999-12-07: Solaris snoop (print_domain_name) Buffer Overflow Vulnerability
  http://securityfocus.com/vdb/bottom.html?vid=858
  CVE-1999-0973
- 1999-12-01: Solaris arp Vulnerabilities
  http://securityfocus.com/vdb/bottom.html?vid=837
  CVE-1999-0859
- 1999-11-30: Solaris kcms_configure
  http://securityfocus.com/vdb/bottom.html?vid=831
  CVE-1999-0321
- 1999-11-19: Solaris rpc.ttdbserver Denial of Service Vulnerability
  http://securityfocus.com/vdb/bottom.html?vid=811
- 1999-11-03: Multiple Vendor CDE dtappgather Vulnerabilities
  http://securityfocus.com/vdb/bottom.html?vid=131
- 1999-09-22: Solaris Profiling File Creation Vulnerability
  http://securityfocus.com/vdb/bottom.html?vid=659
- 1999-09-13: Multiple Vendor CDE dtspcd Vulnerability
  http://securityfocus.com/vdb/bottom.html?vid=636
- 1999-09-13: Multiple Vendor CDE TT_SESSION Buffer Overflow Vulnerability
  http://securityfocus.com/vdb/bottom.html?vid=641
- 1999-09-13: Multiple Vendor CDE dtaction Userflag Buffer Overflow Vulnerability
  http://securityfocus.com/vdb/bottom.html?vid=635
- 1999-09-12: Solaris /usr/bin/mail -m Local Buffer Overflow Vulnerability
  http://securityfocus.com/vdb/bottom.html?vid=672
- 1999-08-09: Solaris sdtcm_convert File Creation Vulnerability
  http://securityfocus.com/vdb/bottom.html?vid=575
  CVE-1999-0676
- 1999-07-13: Multiple Vendor rpc.cmsd Buffer Overflow Vulnerability
  http://securityfocus.com/vdb/bottom.html?vid=524
- 1999-05-18: Solaris libX11 Vulnerabilities
  http://securityfocus.com/vdb/bottom.html?vid=238
- 1999-05-11: Solaris lpset Buffer Overflow Vulnerability
  http://securityfocus.com/vdb/bottom.html?vid=251
  CVE-1999-0773
- 1999-05-10: Solaris rmmount Setuid Files Vulnerability
  http://securityfocus.com/vdb/bottom.html?vid=250
- 1999-05-10: Solaris dtprintinfo Buffer Overflow Vulnerability
  http://securityfocus.com/vdb/bottom.html?vid=249
  CVE-1999-0806
- 1999-03-09: Solaris procfs Vulnerability
  http://securityfocus.com/vdb/bottom.html?vid=448
- 1999-03-05: Solaris cancel Vulnerability
  http://securityfocus.com/vdb/bottom.html?vid=293
- 1999-02-19: Solaris/SunOS man/catman Vulnerability

http://securityfocus.com/vdb/bottom.html?vid=165
- 1999-01-07: Solaris ff.core Vulnerability
  http://securityfocus.com/vdb/bottom.html?vid=327
  CVE-1999-0442
- 1998-12-24: Solaris kcms Buffer Overflow Vulnerability
  http://securityfocus.com/vdb/bottom.html?vid=452
  CVE-1999-0136
- 1998-12-17: Solaris dtmail Vulnerability
  http://securityfocus.com/vdb/bottom.html?vid=175
- 1998-12-17: Solaris passwd DoS Vulnerability
  http://securityfocus.com/vdb/bottom.html?vid=174
  CVE-1999-0188
- 1998-11-02: BMC Patrol Symbolic Link Vulnerability
  http://securityfocus.com/vdb/bottom.html?vid=534
- 1998-10-23: Solaris sdtcm_convert Vulnerability
  http://securityfocus.com/vdb/bottom.html?vid=166
- 1998-10-12: Solaris CDE/NIS+ screenlock Vulnerability
  http://securityfocus.com/vdb/bottom.html?vid=294
- 1998-07-16: Solaris SUNWadmap Vulnerability
  http://securityfocus.com/vdb/bottom.html?vid=430
  CVE-1999-0263
- 1998-06-10: Solaris rpc.nisd Vulnerability
  http://securityfocus.com/vdb/bottom.html?vid=677
- CVE-1999-0101 Buffer overflow in AIX and Solaris "gethostbyname" library call allows root access through corrupt DNS host names.
- CVE-1999-0134 vold in Solaris 2.x allows local users to gain root access.
- CVE-1999-0135 admintool in Solaris allows a local user to write to arbitrary files and gain root access.
- CVE-1999-0164 A race condition in the Solaris ps command allows an attacker to overwrite critical files.
- CVE-1999-0189 Solaris rpcbind listens on a high numbered UDP port, which may not be filtered since the standard port number is 111.
- CVE-1999-0190 Solaris rpcbind can be exploited to overwrite arbitrary files and gain root access.
- CVE-1999-0210 Automount daemon automountd allows local or remote users to gain privileges via shell metacharacters.
- CVE-1999-0295 Solaris sysdef command allows local users to read kernel memory, potentially leading to root privileges.
- CVE-1999-0296 Solaris volrmmount program allows attackers to read any file.
- CVE-1999-0300 nis_cachemgr for Solaris NIS+ allows attackers to add malicious NIS+ servers.
- CVE-1999-0315 Buffer overflow in Solaris fdformat command gives root access to local users.
- CVE-1999-0339 Buffer overflow in the libauth library in Solaris allows local use rs to gain additional privileges, possibly root access.
- CVE-1999-0773 Buffer overflow in Solaris lpset program allows local users to gai n root access.
- CVE-1999-0786 The dynamic linker in Solaris allows a local user to create arbitr ary files via the LD_PROFILE environmental variable and a symlink attack.
- CVE-1999-0908 Denial of service in Solaris TCP streams driver via a malicious connection that causes the server to panic as a result of recursiv e calls to mutex_enter.
- CVE-1999-0966 Buffer overflow in Solaris getopt in libc allows local users to ga in root privileges via a long argv[0].
- CVE-2000-0030 Solaris dmispd dmi_cmd allows local users to fill up restricted di sk space by adding

files to the /var/dmi/db database.
- CVE-2000-0032 Solaris dmi_cmd allows local users to crash the dmispd daemon by adding a malformed file to the /var/dmi/db database.

Patch list

The following patches come from Sun's recommended patch cluster[2]. The patches listed are the ones that apply to each system. Most of these patches are Sun's response to the previously-listed vulnerabilities. Patches needed on snnyroch08:

- 105407-01
- 105464-02
- 105558-04
- 105562-03
- 105665-03
- 105926-01
- 106049-01
- 106222-01
- 106226-01
- 106242-02
- 106301-01
- 106448-01
- 106828-01
- 107434-01

Patches needed on snnyroch56:

- 105357-04
- 105395-06
- 105407-01
- 105464-02
- 105558-04
- 105562-03
- 105665-03
- 105667-02
- 105837-03
- 105926-01
- 106049-01
- 106123-04
- 106222-01
- 106226-01
- 106242-02
- 106271-06
- 106301-01
- 106415-03
- 106437-03
- 106448-01
- 106495-01
- 106569-01

- 106648-01
- 106649-01
- 106828-01
- 106834-01
- 106894-01
- 107336-01
- 107434-01
- 107618-01
- 107758-01
- 107766-01
- 107774-01
- 107991-01
- 108199-01
- 108201-01

Open ports

Using nmap[3], the following TCP ports were found open on snnyroch08:

- 7/tcp echo
- 9/tcp discard
- 13/tcp daytime
- 19/tcp chargen
- 21/tcp ftp
- 22/tcp ssh
- 23/tcp telnet
- 25/tcp smtp
- 37/tcp time
- 79/tcp finger
- 80/tcp http
- 111/tcp sunrpc
- 389/tcp ldap
- 512/tcp exec
- 513/tcp login
- 514/tcp shell
- 515/tcp printer
- 540/tcp uucp
- 707/tcp unknown
- 708/tcp unknown
- 1103/tcp xaudio
- 4045/tcp lockd
- 6000/tcp X11
- 6112/tcp dtspc
- 7100/tcp font-service
- 32771/tcp sometimes-rpc5
- 32772/tcp sometimes-rpc7
- 32773/tcp sometimes-rpc9
- 32774/tcp sometimes-rpc11
- 32775/tcp sometimes-rpc13

- 32776/tcp sometimes-rpc15
- 32777/tcp sometimes-rpc17
- 32778/tcp sometimes-rpc19
- 32779/tcp sometimes-rpc21
- 32780/tcp sometimes-rpc23

The following UDP ports were found open on snnyroch08:

- 32771/udp sometimes-rpc6
- 32772/udp sometimes-rpc8
- 32773/udp sometimes-rpc10
- 32774/udp sometimes-rpc12
- 32775/udp sometimes-rpc14
- 32776/udp sometimes-rpc16
- 32777/udp sometimes-rpc18
- 32778/udp sometimes-rpc20
- 32779/udp sometimes-rpc22
- 32789/udp unknown
- 32790/udp unknown
- 32799/udp unknown
- 32800/udp unknown

The following TCP ports were found open on snnyroch56:

- 7/tcp echo
- 9/tcp discard
- 13/tcp daytime
- 19/tcp chargen
- 21/tcp ftp
- 22/tcp ssh
- 23/tcp telnet
- 25/tcp smtp
- 37/tcp time
- 79/tcp finger
- 80/tcp http
- 111/tcp sunrpc
- 512/tcp exec
- 513/tcp login
- 514/tcp shell
- 515/tcp printer
- 540/tcp uucp
- 723/tcp unknown
- 724/tcp unknown
- 1103/tcp xaudio
- 4045/tcp lockd
- 6112/tcp dtspc
- 7100/tcp font-service
- 32771/tcp sometimes-rpc5
- 32772/tcp sometimes-rpc7
- 32773/tcp sometimes-rpc9
- 32774/tcp sometimes-rpc11

- 32775/tcp sometimes-rpc13
- 32776/tcp sometimes-rpc15
- 32777/tcp sometimes-rpc17
- 32778/tcp sometimes-rpc19
- 32786/tcp sometimes-rpc25

The following UDP ports were found open on snnyroch56:

- 32771/udp sometimes-rpc6
- 32772/udp sometimes-rpc8
- 32773/udp sometimes-rpc10
- 32774/udp sometimes-rpc12
- 32775/udp sometimes-rpc14
- 32776/udp sometimes-rpc16
- 32777/udp sometimes-rpc18
- 32778/udp sometimes-rpc20
- 32779/udp sometimes-rpc22
- 32797/udp unknown
- 32798/udp unknown
- 32799/udp unknown

A total of 48 ports were found open on snnyroch08; 44 ports were found open on snnyroch56. Since these machines should only be listening on one or two ports, the vast majority of these ports should not be open; providing extra services means providing an extra avenue of attack. Of these extra services, the following have been shown to be exploitable:

- 7/tcp: Can be used to flood the network
- 19/tcp: Can be used to flood the network
- 25/tcp: Sendmail
- 111/tcp: sunrpc: CVE-1999-0189
- 512/tcp: rexec: provides remote execution capability
- 513/tcp: login: provides remote login capability
- 514/tcp: shell: provides trusted remote login capability
- 515/tcp: printer: provides remote printing ability
- 6000/tcp: Xsun Buffer Overrun Vulnerability. Bugtraq ID 1140
- 6112/tcp: dtspc: provides remote access to CDE
- 32771 through 32790/tcp,udp: provides RPC capability

All of the above exploitable services can be safely turned off on both web servers. The ``small'' TCP services, 7, 9, 13, and 19, are only used for debugging purposes, and never required in a production environment. Since neither server functions as a mail hub, sendmail should be inactivated. Since neither of the web servers need to provide remote login service, 512, 513, and 514 can be safely turned off, and ssh (which is already installed) used instead. Print services are also outside the scope of the two servers. Beyond just listening on port 515, the print subsystem has had a rash of security holes, and should be removed.

Filesystem permissions

World-writable files

Snnyroch08 has 4,601 world-writable files; 3,455 of these are in a cgi-bin directory. Snnyroch56 has 1,732 world-writeable files; 766 in a cgi-bin directory. World-writable files are a security hazard because a malicious (or careless) user can cause a denial of service by filling up the partition that the file resides on. Once the partition is full, system behavior becomes erratic and unstable. World-writable files in a cgi-bin directory are doubly-dangerous because then the denial of service becomes available to anyone on the network. Other malicious activities are possible if a cgi program is compromised: overwritten files, trojan horses, mistrusted information, etc. Webpage defacement (such as what happened to www.apache.org) becomes possible in this scenario as well.

Setuid and setgid files

Snnyroch08 has 1,413 setuid and setgid files; 1,288 are Frontpage-related. Snnyroch56 has 363 setuid and setgid files; 235 of them are Frontpage-related. Xsun is setgid, and listening on both snnyroch08 and snnyroch56, port 6000. Of the 72 setid binaries on snnyroch08, 14 were not found in the Solaris fingerprint database[4]. These were: sudo, ssh, top, and files in two other 3rd-party software programs: bgs and patrol. Of the 60 setid binaries on snnyroch56, 3 were not found in the Solaris fingerprint database: sudo, ssh, and top. Sudo, ssh, and top are all recently-installed 3rd-party programs.

Setuid binary files are particularly dangerous because they run as a different user than the one who executed it. If the current user can cause the setid binary to misbehave, then they may gain elevated privileges. Buffer overflows and symlink attacks are two current methods for attacking setid programs, with others sure to come. For the list of setid files on each system, see Appendix A.

Accounts and passwords

Passwords

Crack[5] guessed the passwords to 14 of the 38 accounts on snnyroch08. It also guessed the passwords to 7 of the 28 accounts on snnyroch56. John the Ripper[6] found one additional password on snnyroch08 and two additional passwords on snnyroch56. Weak passwords allow a malicious user to gain access to additional accounts; with this access comes an extra layer of obscurity and possibly elevated privileges.

Rhosts

Two accounts on both snnyroch08 and snnyroch56 had .rhosts files in their home directory. Trusted relationships can be used by an attacker to compromise additional servers - they should not be used. Ssh, which is already installed, provides a secure replacement for the rhosts functionality.

Tools

- rcs: A useful tool for modifying configuration files; it provides version control and an audit log. It is installed but not widely used.
- xntpd: Time synchronization is important for coordinating log files across multiple machines. Xntpd is installed and being used.
- sudo: An extremely valuable tool for granting fine-grained super-user access. Sudo is installed and

being used.
- logfile watcher: A logfile watching program needs to be used for syslog files for summarized reporting of abnormal system behavior.

Other vulnerabilities

This section lists other areas of vulnerability that the web servers are currently not susceptible to. Physical access to a server is akin to superuser access, and so should be strictly controlled and monitored. Currently, both web servers are located in a data center behind electronic card access doors. Several popular packages are not currently installed; they fall outside the scope of the servers' purpose. Security issues recently been found with each package, so installation of any of them requires close analysis and careful configuration: BIND, NFS, IMAP, POP.

List of Issues

1. Too many packages
2. Too many services
3. Weak passwords
4. Open filesystem permissions
5. OS patches
6. Scripts in cgi-bin directories
7. Scripts run from cron
8. Third-party software
9. RPC programs
10. Sendmail
11. Sadmind

List of Solutions

1. Too many packages
   Having extra packages installed on a system contributes to three security concerns:

   (a) More filesystem permissions to worry about

(b)
Possibly more programs listening to open ports on the network
(c)
Another vector for local exploitation

The list of packages should be reviewed with the ``pkginfo'' command and packages which do not fit the system's service definition should be removed. Since a large number of packages are installed, a significant amount of time will need to be invested. The estimated time required to remedy the issue is 20 hours for each server. On an ongoing basis, 1 hour per week per server will be required, depending on the number of new packages installed.

2.
Too many services
There are too many programs listening to open ports on the web servers. Comment out the unecessary ones from /etc/inetd.conf, restart inetd, and remove the package if possible. The estimated time required to complete these steps is 2 hours per server. The ongoing time requirement is 1 hour per week per server to analyze service requirements, depending on the number of new services.
3.
Weak passwords
Accounts with easily-guessed passwords provide a vector for attack. Limiting access to known, trusted users limits the threat of attackers gaining escalated privileges. Run ``Crack'' and ``John the Ripper'' periodically to catch accounts with weak passwords. Occasionally search for accounts with .rhosts files and inactive accounts. The estimated time required to check account security is 1 hour per server. The ongoing time requirement is 1 hour per week.
4.
Open filesystem permissions
Check the filesystem periodically with the ``find / -perm o+w ! -type l'' command. Tighten permissions with the appropriate ``chmod'' commands. Due to the large number of offending files, the initial time requirement estimate is quite high: 190 hours. The ongoing time requirement is estimated at 5 hours per week per server, again depending on the number of new files installed.
5.
OS patches
Keeping the OS patched keeps OS bugs from becoming exploitable vulnerabilities. Check http://sunsolve.sun.com periodically and schedule a regular maintenance time to install patches and reboot the servers. The estimated time required to patch the systems is 8 hours per server, plus reboot time. The ongoing time requirement to choose and install relevant patches is 1 hour per week, plus any required reboot time.
6.
Scripts in cgi-bin directories
These need to be audited for known CGI vulnerabilities: buffer overflows, using untrusted data in system calls, file locking, etc. Places to look for good CGI programming tips are:

- http://www.go2net.com/people/paulp/cgi-security
- http://www.cert.org/security-improvement/practices/p078.html
- http://www.cert.org/security-improvement/practices/p079.html

The estimated time required to audit the scripts is 40 hours. The ongoing time requirement is estimated at 1 hour per week per server, depending on the number of new scripts.

7.
Scripts run from cron

All the scripts in root's crontab need to be audited and regularly checked for changes or additions. The estimated time required to review the scripts is 8 hours per server. The ongoing time requirement is 1 hour per week, depending on the number of changes to the crontab.

8. Third-party software
   Schedule time to check each vendor's site for bugfixes and updates. Estimated time required to initially investigate is 8 hours. Ongoing time requirement is 1 hour per week.
9. RPC programs
   Disable and/or remove all RPC programs. Estimated time required is 2 hours. Ongoing time requirement is 1 hour per week.
10. Sendmail
    Remove from /etc/inetd.conf and restart inetd. Estimated time required is less than 1 hour. There are no ongoing requirements.
11. Sadmind
    Remove from /etc/inetd.conf and restart inetd. Estimated time required is less than 1 hour. There are no ongoing requirements.

Along with the above immediate fixes, ongoing attention needs to be paid to keeping the system secure. Beware of interaction between programs, particularly when modifying one of their configuration files. Use lsof[7] and nmap to watch for programs unexpectedly listening to open ports.

Summary

Several areas of insecure configuration were found on both snnyroch08 and snnyroch56. After defining roles for the two systems, it becomes easy to secure them by comparing programs and services to their roles. Constant attention must be paid to the web and ftp server configurations to maintain system integrity. Any script that is run automatically or by the web server must be audited for unsafe practices.

The total estimated time per server to implement the fixes is 281 hours. The total ongoing time requirement per server per week is 13 hours, varying significantly depending on the number of changes to the systems (adding, removing, or modifying programs). Assuming an industry average of $45 per hour, the cost in man-hours to implement the changes is $12,645. Since most of the eleven suggested fixes do not overlap, the tasks could be split among multiple system administrators.

Appendix

Setid file listing

This file listing does not include the admin.exe and author.exe files that exist in every Frontpage web. List of setid files on snnyroch08:

- /usr/lib/lp/bin/netpr

- /usr/lib/fs/ufs/quota
- /usr/lib/fs/ufs/ufsdump
- /usr/lib/fs/ufs/ufsrestore
- /usr/lib/exrecover
- /usr/lib/pt_chmod
- /usr/lib/sendmail
- /usr/lib/utmp_update
- /usr/lib/acct/accton
- /usr/lib/uucp/remote.unknown
- /usr/lib/uucp/uucico
- /usr/lib/uucp/uusched
- /usr/lib/uucp/uuxqt
- /usr/openwin/lib/mkcookie
- /usr/openwin/bin/Xsun
- /usr/openwin/bin/xlock
- /usr/openwin/bin/ff.core
- /usr/openwin/bin/mailtool
- /usr/openwin/bin/kcms_configure
- /usr/openwin/bin/kcms_calibrate
- /usr/openwin/bin/sys-suspend
- /usr/platform/sun4u/sbin/eeprom
- /usr/platform/sun4u/sbin/prtdiag
- /usr/dt/bin/dtaction
- /usr/dt/bin/dtappgather
- /usr/dt/bin/sdtcm_convert
- /usr/dt/bin/dtmail
- /usr/dt/bin/dtmailpr
- /usr/dt/bin/dtprintinfo
- /usr/dt/bin/dtsession
- /usr/bin/at
- /usr/bin/atq
- /usr/bin/atrm
- /usr/bin/crontab
- /usr/bin/eject
- /usr/bin/fdformat
- /usr/bin/login
- /usr/bin/mail
- /usr/bin/mailx
- /usr/bin/netstat
- /usr/bin/newgrp
- /usr/bin/passwd
- /usr/bin/ps
- /usr/bin/rcp
- /usr/bin/rdist
- /usr/bin/rlogin
- /usr/bin/rsh
- /usr/bin/su
- /usr/bin/tip
- /usr/bin/uptime
- /usr/bin/write

- /usr/bin/w
- /usr/bin/yppasswd
- /usr/bin/admintool
- /usr/bin/ct
- /usr/bin/cu
- /usr/bin/uucp
- /usr/bin/uuglist
- /usr/bin/uuname
- /usr/bin/uustat
- /usr/bin/uux
- /usr/bin/ipcs
- /usr/bin/chkey
- /usr/bin/nispasswd
- /usr/bin/cancel
- /usr/bin/lp
- /usr/bin/lpset
- /usr/bin/lpstat
- /usr/bin/solstice
- /usr/bin/volcheck
- /usr/bin/volrmmount
- /usr/sbin/allocate
- /usr/sbin/arp
- /usr/sbin/fusage
- /usr/sbin/mkdevalloc
- /usr/sbin/mkdevmaps
- /usr/sbin/ping
- /usr/sbin/prtconf
- /usr/sbin/sacadm
- /usr/sbin/swap
- /usr/sbin/sysdef
- /usr/sbin/wall
- /usr/sbin/whodo
- /usr/sbin/deallocate
- /usr/sbin/list_devices
- /usr/sbin/dmesg
- /usr/sbin/m64config
- /usr/sbin/lpmove
- /usr/sbin/pmconfig
- /usr/sbin/static/rcp
- /usr/ucb/ps
- /usr/vmsys/bin/chkperm
- /usr/netscape/wwwdocs/cgi-bin/hazel/hamwrap.cgi
- /usr/netscape/wwwdocs/cgi-bin/hazel/hazel.cgi
- /usr/netscape/wwwdocs/cgi-bin/webadmin/addchangeuser.cgi
- /usr/netscape/wwwdocs/cgi-bin/webadmin/deletesubweb.cgi
- /usr/netscape/wwwdocs/cgi-bin/webadmin/newsubweb.cgi
- /usr/netscape/wwwdocs/cgi-bin/webadmin/archivesubweb.cgi
- /usr/netscape/wwwapps/coldfusion/coldfusion/btcats/program/dbconvrt
- /usr/netscape/wwwapps/coldfusion/coldfusion/btcats/program/probeurl
- /usr/netscape/wwwapps/coldfusion/coldfusion/btcats/program/regedtux

- /usr/netscape/frontpage/version3.0/admin/scripts/fpadmcgi.exe
- /usr/netscape/suitespot/userdb/ldap/db
- /usr/local/bin/sudo_Sun2.5
- /usr/local/bin/sudo_Sun2.6
- /usr/local/bin/ssh1
- /usr/local/bin/top
- /usr/nsc/sicom/si/svcinit
- /export/opt/bgs/best1_6.2/bgs/bin/bgsagent
- /export/opt/bgs/best1_6.2/bgs/bin/bgsagent_start
- /export/opt/bgs/best1_6.2/bgs/bin/bgsagent_stop
- /export/opt/bgs/best1_6.2/bgs/bin/bgsarmcollect
- /export/opt/bgs/best1_6.2/bgs/bin/bgscollect
- /export/opt/bgs/best1_6.2/bgs/bin/bgscollect.old
- /export/opt/bgs/best1_6.2/bgs/scripts/best1collect
- /export/opt/patrol/3209/Solaris25-sun4/bin/PatrolAgent
- /export/opt/patrol/3209/Solaris25-sun4/bin/snmpmagt
- /export/opt/patrol/3209/unix/AIX3.2-RS/bin/procstat
- /export/opt/patrol/3209/unix/AIX4.1-RS/bin/procstat
- /opt/SUNWadm/2.2/bin/stomgr
- /etc/lp/alerts/printer
- /proc/438/object/a.out
- /proc/372/object/a.out
- /proc/511/object/a.out
- /proc/572/object/a.out

List of setid files on snnyroch56:

- /usr/netscape/suitespot/userdb/ldap/db
- /usr/netscape/wwwdocs/cgi-bin/na_home/ce_to_cs.cgi
- /usr/netscape/wwwdocs/cgi-bin/na_home/cs_to_ce.cgi
- /usr/netscape/wwwdocs/cgi-bin/na_home/cs_to_is.cgi
- /usr/netscape/wwwdocs/cgi-bin/na_home/cs_to_p.cgi
- /usr/netscape/wwwdocs/cgi-bin/na_home/ie_to_is.cgi
- /usr/netscape/wwwdocs/cgi-bin/na_home/is_to_cs.cgi
- /usr/netscape/wwwdocs/cgi-bin/na_home/is_to_ie.cgi
- /usr/netscape/wwwdocs/cgi-bin/na_home/is_to_p.cgi
- /usr/netscape/wwwdocs/cgi-bin/na_home/p_to_cs.cgi
- /usr/netscape/wwwdocs/cgi-bin/na_home/p_to_is.cgi
- /usr/netscape/wwwdocs/cgi-bin/portal/ce_to_cs.cgi
- /usr/netscape/wwwdocs/cgi-bin/portal/cs_to_ce.cgi
- /usr/netscape/wwwdocs/cgi-bin/portal/cs_to_is.cgi
- /usr/netscape/wwwdocs/cgi-bin/portal/cs_to_p.cgi
- /usr/netscape/wwwdocs/cgi-bin/portal/ie_to_is.cgi
- /usr/netscape/wwwdocs/cgi-bin/portal/is_to_cs.cgi
- /usr/netscape/wwwdocs/cgi-bin/portal/is_to_ie.cgi
- /usr/netscape/wwwdocs/cgi-bin/portal/is_to_p.cgi
- /usr/netscape/wwwdocs/cgi-bin/portal/p_to_cs.cgi
- /usr/netscape/wwwdocs/cgi-bin/portal/p_to_is.cgi
- /usr/netscape/wwwdocs/cgi-bin/webadmin/addchangeuser.cgi
- /usr/netscape/wwwdocs/cgi-bin/webadmin/deletesubweb.cgi
- /usr/netscape/wwwdocs/cgi-bin/webadmin/newsubweb.cgi

- /usr/netscape/wwwapps/coldfusion/btcats/program/dbconvrt
- /usr/netscape/wwwapps/coldfusion/btcats/program/probeurl
- /usr/netscape/wwwapps/coldfusion/btcats/program/regedtux
- /usr/lib/lp/bin/netpr
- /usr/lib/fs/ufs/quota
- /usr/lib/fs/ufs/ufsdump
- /usr/lib/fs/ufs/ufsrestore
- /usr/lib/exrecover
- /usr/lib/pt_chmod
- /usr/lib/sendmail
- /usr/lib/utmp_update
- /usr/lib/acct/accton
- /usr/lib/uucp/remote.unknown
- /usr/lib/uucp/uucico
- /usr/lib/uucp/uusched
- /usr/lib/uucp/uuxqt
- /usr/platform/sun4u/sbin/eeprom
- /usr/platform/sun4u/sbin/prtdiag
- /usr/openwin/lib/mkcookie
- /usr/openwin/bin/Xsun
- /usr/openwin/bin/xlock
- /usr/openwin/bin/ff.core
- /usr/openwin/bin/mailtool
- /usr/openwin/bin/kcms_configure
- /usr/openwin/bin/kcms_calibrate
- /usr/openwin/bin/sys-suspend
- /usr/dt/bin/dtaction
- /usr/dt/bin/dtappgather
- /usr/dt/bin/sdtcm_convert
- /usr/dt/bin/dtmail
- /usr/dt/bin/dtmailpr
- /usr/dt/bin/dtprintinfo
- /usr/dt/bin/dtsession
- /usr/bin/at
- /usr/bin/atq
- /usr/bin/atrm
- /usr/bin/crontab
- /usr/bin/eject
- /usr/bin/fdformat
- /usr/bin/login
- /usr/bin/mail
- /usr/bin/mailx
- /usr/bin/netstat
- /usr/bin/newgrp
- /usr/bin/passwd
- /usr/bin/ps
- /usr/bin/rcp
- /usr/bin/rdist
- /usr/bin/rlogin
- /usr/bin/rsh

- /usr/bin/su
- /usr/bin/tip
- /usr/bin/uptime
- /usr/bin/write
- /usr/bin/w
- /usr/bin/yppasswd
- /usr/bin/admintool
- /usr/bin/ct
- /usr/bin/cu
- /usr/bin/uucp
- /usr/bin/uuglist
- /usr/bin/uuname
- /usr/bin/uustat
- /usr/bin/uux
- /usr/bin/ipcs
- /usr/bin/chkey
- /usr/bin/nispasswd
- /usr/bin/cancel
- /usr/bin/lp
- /usr/bin/lpset
- /usr/bin/lpstat
- /usr/bin/volcheck
- /usr/bin/volrmmount
- /usr/sbin/allocate
- /usr/sbin/arp
- /usr/sbin/fusage
- /usr/sbin/mkdevalloc
- /usr/sbin/mkdevmaps
- /usr/sbin/ping
- /usr/sbin/prtconf
- /usr/sbin/sacadm
- /usr/sbin/swap
- /usr/sbin/sysdef
- /usr/sbin/wall
- /usr/sbin/whodo
- /usr/sbin/deallocate
- /usr/sbin/list_devices
- /usr/sbin/dmesg
- /usr/sbin/lpmove
- /usr/sbin/pmconfig
- /usr/sbin/static/rcp
- /usr/ucb/ps
- /usr/vmsys/bin/chkperm
- /usr/local/bin/sudo_Sun2.5
- /usr/local/bin/sudo_Sun2.6
- /usr/local/bin/ssh1
- /usr/local/bin/top
- /usr/nsc/sicom/user/server
- /usr/nsc/sicom/si/svcinit
- /usr/nsc/sicom/cam/nserver

- /etc/lp/alerts/printer
- /proc/241/object/a.out
- /proc/281/object/a.out

About this document ...

Intranet Web Server Security

This document was generated using the **LaTeX**2HTML translator Version 98.1 release (February 19th, 1998)

The command line arguments were:
latex2html `-local_icons -dir giac_html1 -split 0 giac_report.tex`.

The translation was initiated by Jeff Schaller on 2000-08-14

Footnotes

... http://www.apache.org[1]
Article at http://www.securityfocus.com in the Bugtraq archives entitled ``How we defaced www.apache.org''

... cluster[2]
http://sunsolve.Sun.COM/pub-cgi/show.pl?target=patches/patch-access

... nmap[3]
http://www.insecure.org/nmap/

... database[4]
http://sunsolve.Sun.COM/pub-cgi/fileFingerprints.pl

... Crack[5]
http://www.crypto.dircon.co.uk/download/c50-faq.html

... Ripper[6]
http://www.openwall.com/john

... lsof[7]
ftp://vic.cc.purdue.edu/pub/tools/unix/lsof/README

Jeff Schaller
2000-08-14