Consultant's Report
Audit of an IRIX 6.5 email server
for GIAC Enterprises

GIAC GCUX Practical version 1.9

Sean Singh

Executive summary

This document details the results of a security audit of GIAC Enterprises' electronic mail server. The audit compared GIAC's system administration practices with established, industry standards. At the time of the audit, the system in question had been "in production" for three years. The system functions as an integral part of GIAC's fortune cookie sayings division, handling transactions between GIAC and it's suppliers and distributors. This server is "mission critical"; it's security is very important.

The services offered by GIAC's server include shell access through telnet and ssh, web services through HTTP and HTTPS, email services through shell access, POP, and IMAP (via a web page), file transfer services through FTP, and directory services through LDAP.

In order to ensure business continuity, this audit reviewed the following areas: operating system vulnerabilities, patch installation and management, configuration vulnerabilities, risks from installed third-party software, and administrative practices. Based on the findings of the audit, the following actions are recommended:

- update the operating system and keep it current
- install operating system patches in a timely fashion
- remove telnet
- remove ftp
- remove rsh
- remove rlogin
- turn off unneeded services
- upgrade third party software
- lock accounts after invalid login attempts
- disable ssh1
- enforce better password policies
- development services should be moved to a non-production server

Since this machine is offering so many services it has a large exposure profile. This is of particular concern since this machine has been labeled "mission critical" and is not behind a firewall. Given the exposure profile and the number of missing operating system patches and un-upgraded applications, this machine is at grave risk of compromise. These are critical deficiencies. Before any other work is done, the operating system and applications must be made current.

Description of system

The system is a cluster of two Silicon Graphics Inc. Origin 200s. Both machines have two 270 MHz processors, 1 GB of RAM and share mirrored EMC CLARiiON Fibre Channel disk arrays. Both systems are running SGI IRIX version 6.5.11. Clustering is achieved through SGI's Failsafe software. For the purposes of this document the entire cluster will be referred to as "the system".

This cluster of machines is the company's primary email server located in the company's data center. It provides access to mailboxes via web, POP, and shell access. Shell users may connect using telnet or ssh (versions 1 or 2). The web server also provides access to personal web pages. This server acts as an email forwarder for divisions of the institution that have legacy email systems. It also houses a small LDAP database that is used for testing new technologies. It also provides FTP access for shell users and web providers. In order to provide these services a number of third party applications have been added to the system. These packages include Apache version 1.3.19 , Sendmail version 8.12, qpopper version 3.1, webIMAP version 2.0k. Backups of the system are achieved via Veritas Netbackup to a remote host.

Physical access to the data center where this system is located, is limited to GIAC system administrators. Access is restricted through the use of identification cards with magnetic stripes and card readers. The card reader is strictly maintained by the data center staff. Tcp_wrappers restricts access to the services on this system (as evidenced in inetd.conf below).

Audit Methodology:

This audit will use automated security scanners, both network and host based. The system was also checked by hand for a number of known vulnerabilities and attack vectors. SARA (version 3.5.5), recognized by the Center for Internet Security for being able to identify the major vulnerabilities in several flavors of Unix, was used to identify possible network based vulnerabilities. TARA (by the same developers as SARA) is a host-based tool designed to expose vulnerabilities. Whisker (version 1.4) was used to check for CGI scripts with known vulnerabilities. Additionally, security alerts from SGI and SecurityFocus were used to identify other possible vulnerabilities.

Detailed Analysis

Operating System Vulnerabilities

The OS installed on the server is IRIX 6.5.11. At the time of this writing the current IRIX version is 6.5.15. There have been several vulnerabilities (both locally and remotely exploitable) addressed by SGI since IRIX 6.5.11 has been published. For more information see: http://www.sgi.com/support/security/advisories.html

Netstat, a program generally used to display statistics regarding network interfaces and network traffic, can be exploited to reveal to an attacker whether or not files exist on the system. While this vulnerability is a local exploit, there are still thousands of shell accounts that could take advantage of this vulnerability. This issue has been addressed in later versions of the OS. For more information see: http://archives.neohapsis.com/archives/vendor/2002-q2/0028.html

XFS, the default file system on most SGI workstations, contains a vulnerability that leaves it open to Denial of Service (DOS) attacks. Carefully crafted file names can crash the host. As with the previous vulnerability, this is a local exploit that should be handled immediately because of the number of shell accounts on the system. For more information see: http://archives.neohapsis.com/archives/vendor/2002-q2/0007.html

RPC, the remote procedure call subsystem of the installed version of IRIX, is vulnerable to a denial of service attack. Carefully crafted RPC requests can cause the portmap and rpcbind programs to crash. Loss of these services may lead to a denial of service. It is also possible that improper use of the HOSTALIASES environment variable could cause applications that use name services to dump core. Since core dumps may reveal information in memory, this vulnerability may expose sensitive information on the system (e.g. passwords). For more information see: http://archives.neohapsis.com/archives/vendor/2002-q1/0074.html

NSD, the IRIX name service daemon, also has a bug that may lead to a denial of service. The name service daemon caches name resolution requests. This cache is stored on disk without checking the available disk space. This can lead to the cache consuming all free space on the disk. This bug may be exploited remotely. For more information see: http://archives.neohapsis.com/archives/vulnwatch/2002-q1/0024.html

Nedit, a GUI based programmer's editor, is vulnerable to a race condition. Because of the way files are created (without properly checking permissions on the file or it's directory), it is possible for an attacker to insert a symbolic link to a file on the system that would be overwritten, or a least corrupted, by an unsuspecting user. Since there is no graphical console on this system and all development of software for this system generally occurs on other systems, this package should be removed. For more information see: http://archives.neohapsis.com/archives/vendor/2001-q4/0039.html

Some of the shells that ship with IRIX (bash, tcsh, sh and ksh) are vulnerable to a race condition when files are being written to through redirection, specifically the "<<" style redirection. These shells create files in /tmp without checking for pre-existing files of the same name. A malicious user could create a symbolic link to another file on the system and corrupt files writable by the shell process. Any processes run by root that use this style of redirection may be taken advantage of and used to gain elevated privileges on the system. For more information see: http://online.securityfocus.com/bid/2006/discussion/

All of the above vulnerabilities apply to the system. If there is a business reason not to upgrade the system OS, patches for these vulnerabilities must be applied.

Security patch installation/management

There are currently two sets of security patches applied to the system, patch 4270 and patch 4354. Patch 4270 fixes an FTP Denial of Service vulnerability. Patch 4354 fixes a root compromise in telnetd. This was verified with the following command:

```
% showprods | grep patch
I  patchSG0004270       09/13/2001  Patch SG0004270: FTP glob buffer overflows and denial of
service
I  patchSG0004270.eoe_sw  09/13/2001  IRIX Execution Environment Software
I  patchSG0004270.eoe_sw.base  09/13/2001  IRIX Base Execution Environment
I  patchSG0004354       08/23/2001  Patch SG0004354: Fix for telnetd security bug 830781 - root
exploit
I  patchSG0004354.eoe_sw  08/23/2001  IRIX Execution Environment Software
I  patchSG0004354.eoe_sw.base  08/23/2001  IRIX Base Execution Environment
```

There should be a few other patches applied to the system as well.

Patch 4469 addresses several issues with shells including predictable temporary file names and gratuitous use of memory. If for some reason the OS can't be upgraded, this patch must be applied.

Patch 4383 addresses issues with Nedit including a race condition occurring when files are created in /tmp (see discussion above). If Nedit is deemed necessary, this patch must be installed.

Patch 4193 addresses 4 different vulnerabilities in bind. All but one of these vulnerabilities allow remote root compromises. CERT vulnerability report VU#196945 warns of a buffer overflow condition that arises from improper handling of transaction signatures. CERT reports VU#572183 and VU#868916 warn of "malformed" DNS requests that could cause buffer overflows. CERT report VU#325431 warns that the name service daemon may be fooled into revealing the contents of environment or program variables to a remote attacker. This information may then be used in another attack. Exploits taking advantage of these vulnerabilities have been published (e.g. "erkms" toolkit – see: http://www.cert.org/incident_notes/IN-2001-03.html). Since bind is installed and running on this system, this patch must be installed.

```
% showprods | grep -i bind
I  fw_bind              06/21/1999  bind-8.1.2 with IP aliasing & scalability Fix
I  fw_bind.man          06/21/1999  bind-8.1.2 man pages
I  fw_bind.man.bind     06/21/1999  bind-8.1.2 man pages
I  fw_bind.man.relnotes 06/21/1999  bind-8.1.2-sgipl1 Release Notes
I  fw_bind.sw           06/21/1999  bind-8.1.2 execution only env
I  fw_bind.sw.bind      06/21/1999  bind-8.1.2 execution only env
% ps -ef | grep named
root       743         1  0 12:02:18 ?       0:00 /usr/sbin/named
```

Patch 4508 fixes a problem that could facilitate a DOS attack on RPC services and prevents the use of a specific environment variable (HOSTALIASES) from causing core dumps.

Patch 4236 fixes a problem with nsd in which a remote attacker could force the nsd cache to grow without limit. This could crash the machine or present a denial of service. If the machine were upgraded to the current version of the OS, this patch would not be needed.

It seems that there has not been a methodical application of patches on this system. It would be prudent to stay abreast of new vulnerabilities and apply the appropriate patches as they become available. Again, it is imperative that these patches be applied if the OS can't be upgraded.

Configuration Vulnerabilites

Rack mounting issues

While the system was purchased as a highly available system it isn't necessarily built to be highly available. The system is currently located in a data-center in the basement of a building, which also contains business offices. The offices directly above the data-center have working washrooms and the data-center itself has no special provisions to prevent water leaks from the floors above. To compound this hazard, the primary and secondary CPUs for the fault tolerant system are installed in the same rack. The same theoretical water leak that would disable the primary system would also disable the backup CPU and disk arrays.

Chkconfig issues

By running chkconfig we can see which services are enabled on this system.

```
% /sbin/chkconfig
        Flag                 State
        ====                 =====

        appletalk            off
        array                off
        autoconfig_ipaddress off
        autofs               off
        automount            off
        cleanpowerdown       on
        cpumeter             on
        desktop              on
        esp                  on
        failsafe             on
        fcagent              off
        fontserver           off
        gated                off
        ipaliases            on
        lockd                on
        lp                   on
        mediad               off
        mkpd                 on
        mmscd                on
        mrouted              off
        named                on
        nds                  off
        network              on
        networker            on
        netwr_client         off
        nfs                  off
        noiconlogin          off
```

```
nostickytmp          off
nsd                  on
nss_fasttrack        off
pmcd                 on
pmie                 off
privileges           on
proclaim_relayagent  off
proclaim_server      off
proxymngr            off
quickpage            off
quotacheck           on
quotas               on
rarpd                off
routed               off
rsvpd                off
rtmond               on
rwhod                off
sar                  on
savecore             on
sdpd                 on
sendmail             off
sendmail_cf          off
sesdaemon            on
snetd                on
soundscheme          on
sysevent             on
timed                off
timeslave            off
ts                   off
verbose              on
videod               off
visuallogin          on
vswap                off
webface              off
windowsystem         off
xdm                  off
xlv                  on
yp                   off
ypmaster             off
ypserv               off
```

Chkconfig reveals that Legato's Networker software is installed on this system. According to the system administrators, the Legato software was tested on the box but never put into production. Since the software is not used, it should be turned off or better yet, removed.

Checkconfig also reports that sdpd is enabled. Sdpd is the multicast session directory server. Sdpd is used to check the network for SGI Radio announcements. It appears to be related to the webface package, which is also unused. Since this machine does not need this service, this service should be turned off or removed.

Soundscheme, a service that allows applications to mix and play audio streams on the computers audio port, is also turned on. The soundscheme audio cue server, as with sdpd and other programs to support streaming media, is not supported on this system. This service should be removed.

Visuallogin is also enabled on this system. Since this system does not have a graphical console, there is no need to enable graphical logins. The standard login program will suffice. While this does not pose an immediate threat it is a service that is not required. Removing it will reduce the exposure profile of this system.

Bind, the Berkley Internet Name Daemon, is also enabled on the system. Looking at /var/named we see that there are basically no data files for named. In fact, the only file is root.cache. We can also see in the file /etc/resolv.conf that the system uses it's version of bind for name resolution before any others.

```
# ls /var/named
root.cache
# more /etc/resolv.conf
domain  giac.com

search giac.com

nameserver      127.0.0.1
nameserver      192.0.0.44
nameserver      192.0.0.45
nameserver      192.0.0.46
```

DNS service is not a stated mission of this system. This policy is supported by the evidence that this system is the only machine on the network that can access it's name server.

```
# grep listen /etc/named.conf
        listen-on { 127.0.0.1; };
```

Since this machine does not need to run bind it should be removed from the system.

Third party software

Sometimes the greatest threat to a system does not come from software native to the OS (e.g. rsh, telnet, or ftp). Sometimes vulnerabilities are introduced by commercial or third party software that is just as (or more) worrisome as those introduced by the misconfigured OS. GIAC employs a homegrown method of software distribution that simplifies the identification of installed packages.

```
%manifest
MHonArc-2.4.6 installed by run on Wed Jun 28 13:22:05 EDT 2000
User-Utmp-1.0 installed by run on Fri Mar 10 13:44:23 EST 2000
apache-1.2.5 installed by dmc on Thu Jun 17 21:02:47 EDT 1999
apache_1.3.19 installed by run on Thu May 17 13:24:02 EDT 2001
apache_ssl-2.6.4-1.3.12 installed by run on Thu Jul 13  6:18:26 EDT 2000
bash-1.14.7pl1 installed by run on Mon Mar 19 11:24:34 EST 2001
bb-1.4h2 installed by run on Fri Sep 21  9:27:26 EDT 2001
chkdist-1.0 installed by run on Tue Jul 20 16:10:22 EDT 1999
chklogs-1.2 installed by dmc on Tue Jun 15 14:05:47 EDT 1999
cops-1.04a installed by dmc on Tue Jun 15 13:40:08 EDT 1999
elm-2.4.25 installed by dmc on Fri Jan  7  9:55:19 EST 2000
emacs-19.29 installed by rev on Wed Jun 23 17:08:44 EDT 1999
gdbm-1.8.0 installed by run on Wed May  9 14:51:13 EDT 2001
gnudiff-2.2 installed by dmc on Tue Jun 15 13:37:04 EDT 1999
hobgoblin-1.6 installed by dmc on Tue Jun 15 13:58:02 EDT 1999
inews-2.2 installed by rev on Tue Sep 28  9:48:37 EDT 1999
ispell-3.1.20 installed by run on Mon Jun 28  9:23:57 EDT 1999
joe-2.8 installed by dmc on Tue Jun 15 16:32:22 EDT 1999
kermit-5A-190 installed by dmc on Fri Jun 25 17:11:28 EDT 1999
killprocs-2.1.1 installed by run on Wed Jul 21 15:14:17 EDT 1999
less-178 installed by dmc on Tue Jun 15 16:27:09 EDT 1999
```

```
lynx-2.8 installed by dmc on Thu Jun 17 20:57:15 EDT 1999
giac.dotfiles installed by rev on Wed Jun  7 11:22:50 EDT 2000
majordomo-1.94.4 installed by dmc on Fri Jun 18 15:13:13 EDT 1999
metamail-2.5 installed by run on Mon Jun 28 11:45:50 EDT 1999
moduser-0.9 installed by dmc on Tue Sep 14 12:13:08 EDT 1999
mrtg-2.9.17 installed by run on Mon Mar 18 14:38:36 EST 2002
msgs-5.2pl2-bozo installed by run on Mon Jun 28 10:04:20 EDT 1999
oldpw_warn-0.0 installed by run on Fri Mar 24 11:13:58 EST 2000
openldap-1.2.11 installed by run on Fri Jul  7 14:07:41 EDT 2000
openldap-2.0.15 installed by run on Tue Nov 20  9:21:27 EST 2001
openssl-0.9.5a installed by run on Tue Jan  2 10:41:19 EST 2001
perl-5.4.4 installed by run on Wed Jul  7 16:27:30 EDT 1999
pidentd-3.0.4 installed by dmc on Mon Nov 29 15:21:53 EST 1999
pine-4.10 installed by dmc on Fri Jun 18 14:16:02 EDT 1999
pine-4.21 installed by run on Tue Dec 19  7:40:29 EST 2000
poppassd-irix installed by dmc on Wed Oct  6 16:24:42 EDT 1999
pwdist-2.0 installed by dmc on Mon Jun 21 19:32:37 EDT 1999
qi-2.2 installed by dmc on Fri Jun 25 17:15:39 EDT 1999
qpopper-2.53 installed by run on Wed May  9 14:27:57 EDT 2001
qpopper-3.1 installed by run on Fri Aug 31  9:54:59 EDT 2001
sendmail-8.10.1 installed by run on Tue May  9 12:22:30 EDT 2000
sendmail-8.11.1 installed by run on Tue Jan  9 11:13:56 EST 2001
sendmail-8.11.6 installed by run on Thu Nov 29 13:58:32 EST 2001
sendmail-8.12.1 installed by run on Thu Dec 20 15:04:18 EST 2001
ssh-1.2.27 installed by dmc on Mon Feb 14 14:00:30 EST 2000
ssh-1.2.31 installed by run on Fri Feb 16 10:09:45 EST 2001
ssh-2.1.0 installed by run on Fri Oct  6 16:17:24 EDT 2000
sudo-1.5.3 installed by dmc on Tue Jun 15 16:41:54 EDT 1999
syswatch-2.29 installed by dmc on Tue Jun 15 14:43:58 EDT 1999
tcp_wrappers-7.6 installed by run on Fri Jul 21  9:57:59 EDT 2000
tin-1.22 installed by run on Wed Jun 23 15:55:43 EDT 1999
tripwire-1.2 installed by dmc on Tue Jun 15 16:47:03 EDT 1999
trn-3.6 installed by dmc on Thu Jul  1 15:56:27 EDT 1999
uccdist-3.6 installed by run on Fri Feb 16 10:53:42 EST 2001
vim-5.6 installed by run on Mon Jun 19  8:15:15 EDT 2000
vips-1.1 installed by run on Mon Jun 28 16:56:06 EDT 1999
watcher-1.3 installed by dmc on Tue Jun 15 14:45:04 EDT 1999
wgrep-1.3 installed by dmc on Tue Jun 15 14:47:25 EDT 1999
wps-1.3 installed by dmc on Tue Jun 15 14:46:47 EDT 1999
ytalk-3.2 installed by dmc on Thu Jun 17 20:46:22 EDT 1999
zmodem-3.48 installed by dmc on Fri Jun 25 17:08:43 EDT 1999
```

Listserv

In order to manage mailing lists for clients, the L-Soft Listserv package was installed on this system. This package, specifically versions 1.8c and 1.8d, are subject to a buffer overflow condition that may allow remote attackers to run malicious code on this system.

The attacker would be able to run code with the permissions of the user running the Listserv package. While this limits the damage that the attacker can do, there are 779 users who are all in the same group as the Listserv user. If possible the listserv user's group should be changed to one that is not shared by any other users of this system. For more information on this vulnerability, see http://online.securityfocus.com/bid/1490

Mhonarc

Mhonarc is a package used to create web pages from email messages for the purposes making web accessible mail archives. It is possible to embed dangerous HTML and Javascript code into a mail message that is destined for Mhonarc that may compromise the system. More recent versions of Mhonarc have implemented filters to strip out dangerous HTML and Javascript. The version installed on this system, 2.4.6, does not check for dangerous HTML or Javascript. This is a feature that was added in version 2.4.9. Mhonarc should be upgraded to the latest version. For more information on this vulnerability, see http://online.securityfocus.com/bid/4546

Shells
Bash, tcsh, sh and ksh are all vulnerable to race conditions, when files are being written to through redirection, specifically the "<<" style redirection. These shells create files in /tmp without checking to see if a file of that name already exists. A malicious user could create a symbolic link to another file on the system and corrupt files writable by the shell process. Any processes run by root that use this style of redirection may be taken advantage of and used to gain elevated privileges on the system. For more information see: http://online.securityfocus.com/bid/2006/discussion/

Elm
Each email message contains an ID that can be found in that message's header. Elm does not handle long message IDs well. If a message contains an excessively long message ID, it will cause a buffer overflow. By attaching code to the end of an abnormally long message ID, a malicious user could force their code to be run, taking advantage of the buffer overflow. For more information see: http://online.securityfocus.com/bid/3037/discussion/

Emacs
In versions of emacs before and including 20.6 if the persmissions on terminals are not set properly, it is possible for users to access information in other users' editing sessions. It may also be possible for the malicious user to insert responses to editor events. Since the version of emacs on this system is 19.29, it should be upgraded immediately. The permissions should also be checked on all terminals. For more information see: http://www.securityfocus.com/bid/2164

Ispell
Ispell, like the shells mentioned earlier, creates temporary files with predictable names. Anyone who knows or can predict when a privileged user will run ispell could corrupt important files on the system. More likely, since uses have shell access, the malicious user may corrupt files edited by other users. Ispell should be upgraded. For more information see: http://online.securityfocus.com/bid/2827/discussion

Joe
Upon startup, the joe editor reads information from the configuration file .joerc. Joe can read this file from the current working directory. One of the things joe can do while reading this file is set key bindings. By manipulating the key binding process a malicious user could set up a key binding that could gain them the privileges of the user running joe. There is no published patch for this vulnerability. For more information see: http://online.securityfocus.com/bid/2437/discussion

Lynx
Lynx, a text based web browser, is installed on this system. Because of the way Lynx handles long URLs, it is possible for a malicious user to craft a URL that would cause a buffer overflow. The buffer overflow would then enable the user to run malicious code. Upgrade Lynx to the latest version. For more information see: http://online.securityfocus.com/bid/1012/info/

Majordomo
Majordomo, the public domain mailing list manager, is installed on this system (version 1.94.4). Since the primary purpose of this machine is to facilitate email, this may be considered a mission critical service. However, majordomo does have a weakness. Due to predictable configuration filenames (i.e. listname.passwd) for mailing lists and an error in the way majordomo deals with mailing list password files it may be possible for a malicious user to issue list administration commands. Specifically, majordomo will use the filename as the admin password for a list. While this is not a direct threat to the system, it may enable “social engineering” that may be used to subvert other security measures. For example, an attacker might utilize this vulnerability to pose as system administrator and ask users to set their passwords to one provided in email. There is no vendor-supplied patch for this issue. For more information see: http://online.securityfocus.com/bid/2028/info/

MRTG
MRTG (Multi Router Traffic Grapher), typically used to give historical information on router traffic is installed on this machine. This installation of MRTG instead of displaying router statistics shows the level of email traffic on the system. While it is useful to gather these statistics the use of MRTG does introduce a problem. Because MRTG allows the use relative paths, it allows the viewing of any file on the system. The version of MRTG that is installed is 2.9.17. There is no vendor-supplied patch for this vulnerability. There is a workaround that should be investigated for use of this system. At the very least, if this a mission critical service, access the MRTG CGI(s) should be limited to only those people who need access through the use of .htaccess files. For more information see: http://online.securityfocus.com/bid/4017/info/

Pine
Pine, a very popular email client on this system, is vulnerable to a buffer overflow condition. A user may send a well-crafted mail message with an excessively long “From” header line that includes malicious code. When an unsuspecting user tries to read that message, the specially crafted “From” line would create a buffer overflow and run the malicious code placed in the buffer. The version of Pine installed is 4.21. Upgrade the version of Pine. For more information see: http://online.securityfocus.com/bid/1709/info/

Qpopper
Qpopper, distributed by Qualcomm, is the mechanism by which POP users connect to this system to retrieve their email. Qpopper has a bulletin feature which allows system administrators to provide updates to users. The problem occurs when bulletins are

created with long names. Long filenames, due to improper checking, create a buffer overflow. This problem exists in version 4.0. The version installed on this system is version 3.1. While it is not verified that the problem exists in this version, version 3.1 does support bulletins. It is highly unlikely that bounds checking would be removed in the upgrade from versions 3.x to version 4.0. The Qpopper software should be upgraded to version 4.03 (or later) to avoid this problem. For more information see: http://online.securityfocus.com/bid/2811/info/

Vim

Several versions of vim, an enhanced version of vi, contain a race condition. Proper safeguards are not taken when swap files are created. If a malicious user can guess or anticipate the names of files that will be created by another user, they can create files will be set to an unsuspecting user's permissions. Needless to say, this would be especially bad if the user were the root user. It is possible that this version of vim contains another vulnerability that would allow the execution of arbitrary code.   For more information on this see: http://online.securityfocus.com/bid/2927/info/
and http://online.securityfocus.com/bid/2510

Talkd

Talkd, the protocol, behind talk, ntalk, and ytalk, has no mechanism for authenticating the user initiating the "conversation". Since no authentication is employed by the talk protocol, users receiving a talk request can never be sure of the identity of the person initiating a talk request. The talk program, according to system administrators, is popular on this system. Talk may be used in a social engineering attack and may be exploited remotely. There is no work around or solution to this problem. Limit exposure by not allowing remote talk sessions through TCP_wrappers. For more information on this see: http://online.securityfocus.com/bid/4419/info/

Ssh

Ssh1 should not be used anymore because of some serious flaws in the protocol. From the list of installed software above, we can see that ssh has been installed on this system (both versions 1 and 2). By using 'ls' we can easily verify that both versions are still installed on the system.

```
% ls -l sshd1 sshd2
-rwxr-xr-x    1 root     staff     1625536 Feb 13  2001 sshd1
-rwxr-xr-x    1 root     staff     2057588 Jun 13  2000 sshd2
```

We can also see that ssh2 has been installed with ssh1 support.

```
% grep "        Ssh" ssh2/sshd2_config
        Ssh1Compatibility               yes
        Sshd1Path                       /usr/giac/etc/sshd1
```

According to CERT Vulnerability Note VU#665372, ssh1, when using RC4 and password authentication, is vulnerable to session replays. The conversation between server and client is encrypted. These keys used in the ssh1 encryption scheme are regenerated every hour. Because of a flaw in the way keys are generated and the fact that session ids are not used to identify sessions when password authentication is used, an attacker may replay a sessions within the window of a given session key.

In Vulnerability Note VU#565052, CERT reveals that attackers can utilize VU#665372 to reverse engineer a user's password. When an attacker captures the initialization of an ssh1 session, the password may be "easily" computed. By replaying the session and carefully manipulating the password packets and their related error checking bits, the attacker can determine a user's password. Similarly, VU#25309 shows that the error correcting bits can be modified leading to altered packets.

CERT Vulnerability Note VU# 684820 states that client authentication may be forwarded. This presents itself as a "man in the middle" attack. The attacker basically inserts himself (or herself) in the middle of an ssh1 session. By doing this, the ssh1 session id may be recorded and used to reverse engineer a new public key. Based on the new public key, a new private key can be generated. The attacker can now use the same session id for multiple connections.

Ssh2 is not without flaws either. As reported in CERT Vulnerability Note VU#596827, passwords may be guessed by attackers monitoring an ssh session even though it is encrypted. This is due to the predictability of the physical act of typing and some knowledge of the operating system. When a user types the command "su" the system echoes those characters back to the user and issues a predictable password prompt. At this point the su program waits for the user's input. The su program however does not echo the entered password back to the user. If the session were not encrypted, the attacker would know that the string that follows is a password. Since the session is encrypted, the attacker must glean information about the session by other means. It turns out that the interval between keystrokes is predictable. Using this data, the attacker can greatly narrow the scope of passwords that must be tried in a brute force attack. While this is a vulnerability, there is no practical defense against this type of attack at this time.

Administrative practices

Foreign executables

GIAC maintains a policy against 'foreign' binaries. The only programs allowed on the system, are those installed by a system administrator. A cron job scans for executables nightly and forwards the results to the system administrator. The accounts of users found with foreign executables are promptly locked.

Log review

The systems staff at GIAC over the years have developed a system of reviewing log files. Tripwire, hobgoblin, syslog and other log files are either diff-ed or emailed to a central email address. From there the logs are sent to an admin (or that persons backup depending on the administrator's availability: i.e. conferences and/or vacations). The administrator reviews the logs daily for abnormalities and respond to those abnormalities. While this system works it may be improved with the use of a central log host.

A central log host combined with automated log scanning, some problems may be detected that would otherwise go undetected. Putting aside the issue of overworked system administrators that are not able to review all logs in a single day, an automated scan of all GIAC logs may

- reveal the methodical probing of ports across machines.
- give a secure secondary host for logs in case of compromise
- allow administrators to care for machines instead of reading logs

Backup policies
Using Veritas' Netbackup the system is backed up nightly. Once a week a full backup is done of all file systems. On the other days, cumulative backups are done. Once a month one set of backup tapes are pulled out of rotation and sent to a remote location for storage. Once that set goes off site, the previous off site tape set gets reinserted into the set of available tapes.

Disaster Recovery
An adequate disaster recovery plan does not exist for this system. This system does not have duplicate hardware in a remote site in case of a disaster. In the case of a disaster a comparable system would need to be located. Once located, DNS entries would have to be changed to reflect the new host. Once the new machine was set up, the offsite tapes would have to be loaded onto the new host. Any third party software that is keyed to the machine's hostid would not function properly if at all.

Time Synchronization
In the event of a system compromise it will be very important to correlate information between other systems both locally and remotely. The correlation effort will be impeded if the time on each system is slightly different. In order to aid in the correlation of logs these systems should use a coordinated strategy for keeping their time synchronized. The cluster consists on an active and a passive computer. Currently the passive machine of the cluster updates its clock from the active. The active host however, does not synchronize time with any other host. This is evident because both timed and timeslave have been chkconfig'ed off (see above).

Surely if there were an intrusion, there would most likely be issues synchronizing logs between sites. GIAC should poll at least 3 (local and remote) very stable and reliable NTP timeservers. If it cannot afford to deploy an NTP server (either cesium atomic clock or GPS based), arrangements should be made to synchronize clocks with other organizations that run accurate timeservers.

Core files
A sweep of the machine reveals core files in several locations including user directories.

```
%find / -name core
/u/b/user003/core
/u/b/user001/core
/u/b/user003/core
/u/b/user003/core
/u/c/user009/core
/u/c/user001/core
/u/c/user001/core
/u/d/user007/core
/u/d/user001/core
/u/e/user014/core
/etc/core
/etc/init.d/core
/var/ha/script/core
/var/giac/adm/security/core
/core
```

Unless the machine is crashing regularly or you are trying to debug a particular problem, do not save core files. Since core files are a snapshot of memory, they may contain information that should not be revealed to users (like passwords). Use the systune command to limit core files:

```
%systune rlimit_core_cur 0.
```

This effectively sets the Maximum core file size to zero. This limit can be temporarily lifted on a per user basis with the use of the limit or ulimit shell commands. For more information on using systune to limit resources see www.techpubs.sgi.com

Password policies

GIAC does have policies to help ensure that trivial passwords are not used.
The policy however, is not readily available to users when they run the password command. When using the web interface for changing passwords, they are informed what the requirements of a "good" password are only if the password they chose does not meet the requirements. Currently, the requirements are

- password longer than 5 characters
- login name not included in the password
- at least 2 letters
- at least one number or special character

This very basic guideline encourages easily cracked passwords. Better policies need to be implemented and enforced. The password command in use is the system native passwd command. We can verify this because the file size and checksum match those of the files from the installation media.

```
% showfiles | grep bin/passwd
f 17050 41312 eoe.sw.base            usr/bin/passwd
% ls -l /usr/bin/passwd
-rwsr-sr-x    1 root     sys        41312 Aug  1  2001 /usr/bin/passwd
% sum -r /usr/bin/passwd
17050     81 /usr/bin/passwd
```

Since the system native command does minimal checking of passwords, it should be upgraded to something better like npasswd which has many dictionaries. Not only will npasswd enforce good passwords by checking its rules, dictionaries, and previously used passwords, it can also contain a help file that could contain the password policy and hints for creating a good password. Since the web interface would not use npasswd, it should be upgraded to use ‘cracklib’ so that it can follow the same rules as npasswd.

Incident response

There is no documented procedure on how to deal with security incidents. In order to assure that incidents are handled consistently, GIAC should develop a policy regarding incident response. Having the policy is not good enough. All system administrators must know and practice it.

Identification and Protection of sensitive data

The procedure used at GIAC to create accounts includes the accumulation of client info including SSN. The file used to track the SSN is accessible by all system administrators (approx 11 people). Care should be taken not to expand that group. If possible that number should be smaller. Check the protections on the file and its directory. A separate file is used to track the accounts and billing information. The file used to track billing information is accessible by all system administrators and the billing clerks. Care should be taken not to expand that group.

Protection of data traversing the network

Because this machine plays a crucial role in the day to day operations and communications of GIAC staff and clients, it is important that all network traffic going to this machine should be secure. It is imperative that all demographic, billing, strategic planning and other mission critical data be kept as secure as possible. The easiest way to start this process is to remove all mechanisms of communications that do not encrypt their traffic over the network where possible.

Replace telnet/ftp with ssh/sftp

The biggest culprits in this arena are telnet and FTP. By checking /etc/inetd.conf we can see that telnet and FTP are enabled.

```
% grep -v "^#" /etc/inetd.conf
imap2   stream  tcp     nowait  root    /usr/giac/etc/tcpd       /usr/ucc/etc/imapd
poppassd        stream  tcp     nowait  root    /usr/giac/etc/tcpd       /usr/ucc/etc/poppassd
pop3    stream  tcp     nowait  root    /usr/giac/etc/tcpd       /usr/ucc/etc/qpopper -s  -b
/var/popbulls
ftp     stream  tcp     nowait  root    /usr/giac/etc/tcpd       ftpd -l
telnet  stream  tcp     nowait  root    /usr/giac/etc/tcpd       telnetd
shell   stream  tcp     nowait  root    /usr/giac/etc/tcpd       rshd -L
login   stream  tcp     nowait  root    /usr/giac/etc/tcpd       rlogind
finger  stream  tcp     nowait  nobody  /usr/giac/etc/tcpd       fingerd
ntalk   dgram   udp     wait    root    /usr/giac/etc/tcpd       talkd
time    stream  tcp     nowait  root    internal
time    dgram   udp     wait    root    internal
bpcd    stream  tcp     nowait  root    /usr/openv/netbackup/bin/bpcd bpcd
vopied  stream  tcp     nowait  root    /usr/openv/bin/vopied vopied
bpjava-msvc     stream  tcp     nowait  root    /usr/openv/netbackup/bin/bpjava-msvc bpjava-msvc
-transient
```

These unsecured protocols are the biggest vulnerabilities on the system aside from the un-patched operating system. Let's say that an attacker socially engineers access to one account on the system. In a matter of seconds that attacker can determine the operating system installed on the server. In a matter of minutes after that, the attacker can download a precompiled binary to gather network traffic. Tools such as this are very good at isolating username/password pairs. These protocols can be exploited remotely as well as locally.

Compromised hosts, whether they are local or on other ISP networks, whose interfaces are in promiscuous mode may also give up access to your system. Valid users of the system may have their password 'sniffed' if their network traffic crosses the compromised ISP's network. There is nothing you can do to safeguard against this if you continue to allow these protocols on your system.

Instead of using telnet and/or ftp, which send all information (including usernames and passwords) in the clear, use ssh (secure shell) and sftp (secure ftp). Ssh encrypts it's network traffic including the login sequence. Sftp implements traditional FTP functionality over a communication 'pipe' secured via ssh. Doing this will secure the majority of the traffic on your network. While ssh is installed on this system, the majority of the interactive sessions on this system use telnet. GIAC system administrators should begin a campaign of user education about ssh and remove telnetd and ftpd as soon as possible.

Similarly, rlogin and rsh are enabled in /etc/inetd.conf. These should be disabled as well for the same reasons. Ssh and scp can be used to replace these functions. Newer versions of the rdist program can also use ssh (for more information see: http://www.magnicomp.com/rdist/rdist.shtml). Even though rsh and rlogin access is limited to a few machines through the use of tcp_wrappers, there is no reason to continue using 'r' programs.

```
%grep rsh /var/giac/etc/hosts.allow
rshd : operator@machine.giac.com EXCEPT PARANOID
rshd : root@machina.giac.com EXCEPT PARANOID
rshd : operator@machina.giac.com EXCEPT PARANOID
rshd : carro.giac.com EXCEPT PARANOID
rshd : automivil.giac.com EXCEPT PARANOID

%grep rlogin /var/giac/etc/hosts.allow
rlogin: operator@machine.giac.com EXCEPT PARANOID
rlogin: root@machina.giac.com EXCEPT PARANOID
rlogin: operator@machina.giac.com EXCEPT PARANOID
rlogin: carro.giac.com EXCEPT PARANOID
rlogin: automivil.giac.com EXCEPT PARANOID
```

Even though access is limited, a malicious user with access to snoop or a similar tool could easily grab passwords for any rsh or rlogin session to this system. Additionally, an attacker finding this information in the hosts.allow would know that root rlogins are allowed from carro.giac.com. A successful attack on carro.giac.com would then yield two compromised hosts.

Not all functions or applicatios can be totally replaced with a secure version. Sendmail, for example, is a mission critical application on this host that can't be removed entirely. The good news is that current versions of sendmail support SASL (Simple Authentication and Security Layer - http://www.sendmail.org/~ca/email/auth.html) or TLS (Transport Layer Security - http://www.sendmail.org/~ca/email/extensions.html#PGPSMIME). The TLS technology allows the encryption of data over the network. While client software that supports this functionality is not universal, users should be strongly encouraged to use email clients that do offer this feature.

SASL use would also allow for the authentication of email users. This would greatly reduce the occurrence of spoofed email. System administrators should begin planning a transition away from unencrypted and unauthenticated email. This will not be a quick fix as it involves a revamp of the entire organizations email infrastructure. In other words, every email client on every desktop PC in the organization needs to be reconfigured (probably upgraded as well to support the configuration).

Since many GIAC staff and clients access their email through the web, it is essential that the web access to email, and any other critical information, be secured via SSL Secure Socket Layer). It is imperative that this information be secured. The rationale here is the same as that used for telnet and FTP. There are enough web browsers available on the market today that support SSL that offering all web content via secure web pages is feasible.

Detection of promiscuous interfaces

Normally, a computer's network interface only listens to traffic that is destined for that computer. It is possible however to change the behavior of the network interface. When trying to debug network problems software such as 'snoop' allows the network interface (NIC) to gather all traffic on the network segment to which it is connected. When the NIC does this, it is said to be in promiscuous mode. Attackers who have compromised a machine sometimes install snoop-like software that watches the network for username/password pairs. Once identified, attackers use these accounts to either further elevate their privileges on the compromised system or launch attacks on other hosts.

This system should be checked periodically to ensure that its Ethernet interfaces are not in promiscuous mode. Checking for this is fairly simple. The 'ifconfig' command will report on the status of all interfaces. If an interface is in promiscuous mode, it will be clearly labeled "PROMISC".

```
% /usr/etc/ifconfig -a
ef1: flags=415d43<UP,BROADCAST,RUNNING,PROMISC,FILTMULTI,MULTICAST,CKSUM,DRVRLOCK,LINK0,IPALIAS>
        inet 192.0.0.31 netmask 0xffffff00 broadcast 192.0.0.255
        inet 192.0.0.17 netmask 0xffffff00 broadcast 192.0.0.255
ef0: flags=415c47<UP,BROADCAST,DEBUG,RUNNING,FILTMULTI,MULTICAST,CKSUM,DRVRLOCK,LINK0,IPALIAS>
        inet 192.0.3.1 netmask 0xffffff00 broadcast 192.0.3.255
lo0: flags=1849<UP,LOOPBACK,RUNNING,MULTICAST,CKSUM>
        inet 127.0.0.1 netmask 0xff000000
```

If the data traversing the network has been secured using a mechanism such as SSL or TLS, a simple snoop will yield no valuable information.

Access controls

General access controls

Disable or remove ‘unused’ or ‘inactive’ accounts on the system. Because disgruntled ex-employees (or clients) are possibly the most motivated attackers against any site, it is important to delete unnecessary user accounts from the system as soon as possible. The GIAC Human Resources department should notify system administrators immediately when a staff member is no longer associated with the organization. Currently, that notification process is left to the departmental managers who may or may not remember to notify a system administrator. While there is a yearly review of all accounts on the system, this could leave a several month window in which an unauthorized person has access to the system. GIAC should develop a policy which allows for more timely account deletion.

Root login

Brute force attacks on the root password from remote hosts can be denied if the root account is limited to logging in from the console only.

```
% grep CONSOLE  /etc/default/login

CONSOLE=/dev/ttyd1
```

Non-interactive admin accounts

Certain accounts on the system do not need to have a shell set in /etc/passwd. Accounts such as smtp, bin, uucp, nuucp, listen and rfindd do not need shells. Set the shell for these account to /dev/null. This will limit exposure. Better yet remove accounts like rfindd if they are not needed. Similarly, if these accounts are non-interactive, they don’t need to use FTP. Since FTP is enabled on this system, make sure that these non-interactive accounts (and root) appear in the /etc/ftpusers file. This will prevent these accounts from being used in an FTP attack.

Least privilege

Users should only have access to only the functions they need. For example the average user does not need access to the ifconfig or netstat commands. The Netstat vulnerability previously mentioned perfectly illustrates the need to limit access to certain functions. System administrators should minimally look at /usr/etc and /usr/diags. Users who need access to ‘restricted’ functions (e.g. helpdesk staff that need to reset other users’ passwords) should be given access only to those functions through the use of ‘sudo’. The ‘sudoers’ file should be reviewed periodically to ensure that each user still require access to functions/services.

Separation of duties

The concept of separation of duties in system administration is fairly simple. For certain activities, a higher level of authorization must be obtained before the action can take place (see the related article: http://www.nwfusion.com/newsletters/sec/2000/0612sec2.html) For example, a help desk staff person might request a file restore. However to make sure that the user is not requesting /etc/shadow to be restored to a user directory, the request is verified by a system operator or administrator. Processes around granting elevated privileges or account creation or billing are natural candidates for implementing separation of duty safeguards. GIAC should review its procedures to ensure that the individuals performing functions of authority are monitored.

Shared accounts

Generally the use of shared accounts is discouraged for reasons of accountability. There are a few accounts on this system that are 'shared.' Through the use of some homegrown scripts and sudo users are jointly able to maintain certain email accounts. Since sudo is used to access these accounts, there is an audit trail. As mentioned above, system administrators should review the sudoers file.

Setuid/setgid programs

Take care that any program that is setuid or setgid needs to have that privilege. Since attackers will often use those programs to elevate their privilege on a host, it is important to turn off the setuid/setgid bits on programs and scripts when possible. The following command will help you find setuid programs:

```
% find / -perm –4000
```

The following command will help you find setuid programs:

```
% find / -perm –2000
```

Un-owned files

When users are removed from the system it is important that all of the files belonging to that user are removed. If the uid of a removed user is ever reused, file ownership will be transferred (effectively) to the new account. This could lead to a various number of problems ranging from inaccurate disk utilization charges to the disclosure of sensitive information. On this system, GIAC utilized a uid 'registry' which helps to ensure that uids are not reused. However, a routine scan of the machine might reveal gaps in the user management procedures and might identify disk space that may be recovered. The following command will help you find unowned files:

```
% find / -nouser
```

World writeable files/directories

The presence of world writable files presents a problem with regard to data integrity. If a file is world writable, it is impossible to guarantee that the data in that file is authentic. This is especially true for any programs or scripts that users may run. There should never be any world writable scripts on any system. While tools such as tripwire might notify the system administrator of the file's alteration, there is no accountability. We can't go to a person (or even a group of people) to determine why the file might have been changed. There may be a need for some files to be world writeable. Care must be taken to ensure that only those files that need to be world writeable are world writeable. The following command will help you find world writable files:

```
% find / -perm -0002 -type f
```

Similarly, world writable directories should be monitored. Users looking to avoid "over quota" warnings often move files into any world writable directories that they can find. This might be 'innocent' or it could be used as a denial of service. Users seeking to elevate their privileges may also use these directories to store configuration files for programs that do not do proper checking on configuration files. Programs such as vim can read configuration files from arbitrary directories (http://online.securityfocus.com/bid/2510). Use of this 'feature' may lead to social engineering attacks where the program may be tricked to run other programs or scripts on the system.

The following command will help you find world writable directories:

```
% find / -perm -0002 -type d
```

The TARA scan attached as Appendix A contains some other suggestions regarding files. Read and implement the changes suggested in Appendix A.

Critical issues and recommendations

The following are the top 10 issues related to this machine's security

1) Update the OS & keep it current
Many important security patches are incorporated into the operating system updates. In order to ensure that you have the most current set of patches the operating system must be kept up to date. This must be addressed before all other problems because the operating system is the foundation upon which the rest of the system is built. A service contract from the hardware vendor may be obtained via the web at http://www.sgi.com/support/suppserv.html. Updates should be applied on a regular basis.

2) Install security patches & stay current
From time to time SGI releases patches to correct vulnerabilities (http://www.sans.org/newlook/digests/SAC/SGI.htm) in the operating system. These patches should be installed shortly after their release. Often these patches are developed in response to a recent exploit or attack. Installing these patches will help to ensure the integrity of the system. System administrators can join the SGI security advisory mailing list by going to the following web page: http://www.sgi.com/support/security/wiretap.html

3) Remove telnet
Because telnet sends username and password information over the network using clear text, it is a very large risk to the system. With so many users of the system using telnet, it wouldn't be difficult for an attacker to 'sniff' passwords on the network. Since this system already has ssh installed, the telnetd line can be commented out of (or preferably removed from) /etc/inet/inetd.conf. Of course, users must be warned before this occurs. System administrators should work with the help desk staff on this transition.

4) Remove ftp
Just like telnet, FTP also sends usernames and passwords over the network in the clear. While it is possible that fewer people use FTP than telnet, it is still a very big vulnerability. Since this system already has ssh installed, the ftpd line can be commented out of (or preferably removed from) /etc/inet/inetd.conf. Users should transition to sftp. Again, users must be warned before this occurs and system administrators should work with help desk staff on this transition.

5) Remove rsh/rlogin
Rsh and rlogin, like telnet and ftp, are programs that send username/password combinations over the network in the clear. Comment rsh and rlogin out of (or remove them entirely from) /etc/inet/inetd.conf.

6) Trivial passwords
Since the system default password program (/usr/bin/passwd) only does the most basic checks on the users' passwords, there is a high probability that many users' passwords are easy to guess. This leaves the system much more vulnerable to brute force password guessing. Download, compile and install Npasswd. It is available on the web at http://www.utexas.edu/cc/unix/software/npasswd/

7) Turn off unneeded services
Turn off services that are not needed. Services like networker, sdpd and soundscheme, and visuallogon are not used on this host. At best they steal CPU cycles from other applications. At worst they introduce vulnerabilities into the system. For each of these services, run "chkconfig *service* off" to turn the service off. It would be better to remove programs/packages if possible. Legato Networker for example can be removed with no ill side effects. Use inst to remove that package.

```
%showprods | grep networker
%inst
inst> from none
inst> remove networker5.*
inst> go
inst> quit
```

8) Upgrade third party software
Several of the third party applications installed on this system contain vulnerabilities. These packages should be upgraded as soon as possible. Local and remote attackers can use these packages to elevate their privileges. The current, secure versions of the

third party applications must be downloaded, compiled (where necessary), and installed.

9) Lock accounts with failed logins
This system is vulnerable to brute force password guessing. Since accounts are not locked after unsuccessful logins, an attacker can automate the process of stepping through passwords in an attempt to gain access to the system. While

10) Disable ssh version 1
By initiating an ssh session on an already compromised host, a "man in the middle" attack may be initiated by an attacker seeking to gain access to the system. Since ssh version 2 (which is not vulnerable to this type of attack) is already installed on the system, ssh2 should be configured not to fall back to ssh1. Change the word 'yes' in the "Ssh1Compatibility" line in the sshd2_config file to "no".

Other recommendations

Turn off named
Named is chkconfig'ed on on this system (see above). There are several bugs in named that might allow remote attackers to gain access to the box. While named is running on this system the only file in /var/named is the root.cache file. Apparently, bind is being run on this system to relieve congestion on the other name servers in the organization. This performance loss is minor compared to the downtime that would be incurred from a break-in due to a vulnerability in bind. Rather than run bind on this machine, the networks and name servers should be upgraded to handle the load.

Firewall/IDS
GIAC.com should consider putting a firewall between this machine and the Internet. With so many services being offered to so many clients, GIAC should consider streamlining its offerings and allowing only necessary protocols through the firewall. At the same time GIAC should consider the installation of an intrusion detection system (IDS). An IDS would be able to analyze network traffic and identify anomalies. With proper notification and action, this may prevent break-in attempts from becoming forensics cases.

References

1. SGI security coordinator. “IRIX netstat vulnerability.” Neohapsis Miscellaneous vendor alerts. May 07, 2002. http://archives.neohapsis.com/archives/vendor/2002-q2/0028.html (June 10,2002)

2. SGI security coordinator. “IRIX XFS filesystem denial of service attack” Neohapsis Miscellaneous vendor alerts. Apr 15 2002. http://archives.neohapsis.com/archives/vendor/2002-q2/0007.html (June 10,2002)

3. SGI security coordinator. “IRIX rpc/HOSTALIASES vulnerability” Neohapsis Miscellaneous vendor alerts. Mar. 28, 2002. http://archives.neohapsis.com/archives/vendor/2002-q1/0074.html (June 10,2002)

4. SGI security coordinator. “IRIX nsd vulnerability update” Neohapsis Miscellaneous vendor alerts. Jan. 16, 2002. http://archives.neohapsis.com/archives/vulnwatch/2002-q1/0024.html (June 10,2002)

5. SGI security coordinator. “IRIX nedit vulnerability” Neohapsis Miscellaneous vendor alerts. Nov. 30, 2001 http://archives.neohapsis.com/archives/vendor/2001-q4/0039.html (June 10,2002)

6. Szabo, Paul; Irlam, Gordon; proton@energymech.net. “Unix Shell Redirection Race Condition Vulnerability” Bugtraq vulnerabilities. Nov. 30, 2001 http://online.securityfocus.com/bid/2006/discussion/ (June 10,2002)

7. supportlib@sgi.com. “Patch 4469 : Shell security fixes : [IRIX 6.5.13m 6.5.12m 6.5.11m 6.5.10m]” Supportfolio Online http://support.sgi.com/irix/content/patches_nosupport/html/pinfo4469.html (June 10,2002)

8. supportlib@sgi.com. “Patch 4383 : nedit 5.1.1 security patch : [IRIX 6.5.13m 6.5.13f 6.5.12m 6.5.12f 6.5.11m 6.5.11f]” Supportfolio Online http://support.sgi.com/irix/content/patches_nosupport/html/pinfo4383.html (June 10,2002)

9. supportlib@sgi.com. “Patch 4193 : named security fix for 6.5.x : [IRIX 6.5.11m 6.5.11f 6.5.10m 6.5.10f 6.5.9m 6.5.9f 6.5.8m 6.5.8f 6.5.7m 6.5.7f 6.5.6m 6.5.6f 6.5.5m 6.5.5f 6.5.4m 6.5.4f 6.5.3m 6.5.3f 6.5.2m 6.5.2f 6.5.1 6.5]” Supportfolio Online http://support.sgi.com/irix/content/patches_nosupport/html/pinfo4193.html (June 10,2002)

10. cert@cert.org. “ISC BIND 8 contains buffer overflow in transaction signature (TSIG) handling code” Vulnerability Notes Database http://www.kb.cert.org/vuls/id/196945 (June 10,2002)

11. cert@cert.org. “ISC BIND 4 contains buffer overflow in nslookupComplain()” Vulnerability Notes Database http://www.kb.cert.org/vuls/id/572183 (June 10,2002)

12. cert@cert.org. “ISC BIND 4 contains input validation error in nslookupComplain()” Vulnerability Notes Database http://www.kb.cert.org/vuls/id/868916 (June 10,2002)

13. cert@cert.org. “Queries to ISC BIND servers may disclose environment variables” Vulnerability Notes Database http://www.kb.cert.org/vuls/id/325431 (June 10,2002)

14. cert@cert.org. “Queries to ISC BIND servers may disclose environment variables” Vulnerability Notes Database http://www.kb.cert.org/vuls/id/325431 (June 10,2002)

15. supportlib@sgi.com. “Patch 4508 : libc fix for SIGSEGV in gethostsbyname if HOSTALIASES is set for 6.5.11m : [IRIX 6.5.11m]” Supportfolio Online http://support.sgi.com/irix/content/patches_nosupport/html/pinfo4508.html (June 10,2002)

16. supportlib@sgi.com. “Patch 4236 : Prevent nsd's cache from growing too large : [IRIX 6.5.11m 6.5.11f]” Supportfolio Online http://support.sgi.com/irix/content/patches_nosupport/html/pinfo4236.html (June 10,2002)

17. Network Associates. “L-Soft Listserv 1.8c and 1.8d Web Archives Long QUERY_STRING Buffer Overflow Vulnerability” Bugtraq vulnerabilities. July 17, 2000 http://online.securityfocus.com/bid/1490 (June 10,2002)

18. Molenda, Jason; Takagi, Hiromitsu. “MHonArc HTML Script Filter Bypass Vulnerability” Bugtraq vulnerabilities. Apr 18, 2002 http://online.securityfocus.com/bid/4546 (June 10,2002)

19. devjoe@bellatlantic.net. “Elm Message-ID Buffer Overflow Vulnerability” Bugtraq vulnerabilities. July 3, 2001. http://online.securityfocus.com/bid/3037/discussion/ (June 10,2002)

20. Mandrake Security Advisory. “Emacs Inadequate PTY Permissions Vulnerability” Bugtraq vulnerabilities. Dec 31, 2000 http://www.securityfocus.com/bid/2164 (June 10,2002)

21. Huuskonen, Jarno. “Ken Stevens ispell Symbolic Link Vulnerability” Bugtraq vulnerabilities. May 24, 2001. http://online.securityfocus.com/bid/2827/discussion (June 10,2002)

22. Wkit Security AB. “Joe Text Editor .joerc Arbitrary Command Execution Vulnerability” Bugtraq vulnerabilities. February 28, 2001. http://online.securityfocus.com/bid/2437/discussion (June 10,2002)

23. Zalewski, Michal. “Lynx Long URL Buffer Overflow Vulnerabilities” Bugtraq vulnerabilities. February 27, 2000. http://online.securityfocus.com/bid/1012/info/ (June 10,2002)

24. marvin@nss.nu. “Majordomo Config-file admin_password Configuration Vulnerability” Bugtraq vulnerabilities. December 1, 2000. http://online.securityfocus.com/bid/2028/info/ (June 10,2002)

25. UkR Security Team. “MRTG CGI Arbitrary File Display Vulnerability” Bugtraq vulnerabilities. February 02, 2002. http://online.securityfocus.com/bid/4017/info/ (June 10,2002)

26. Arkane. “Pine "From:" Field Buffer Overflow Vulnerability” Bugtraq vulnerabilities. September 23, 2000. http://online.securityfocus.com/bid/1709/info/ (June 10,2002)

27. Deraison, Renaud. “Qualcomm qpopper Username Buffer Overflow Vulnerability” Bugtraq vulnerabilities. Jun 02, 2001. http://online.securityfocus.com/bid/2811/info/ (June 10,2002)

28. SuSE Security Advisory. “Vim Swap File Race Condition Vulnerability” Bugtraq vulnerabilities. April 11, 2001. http://online.securityfocus.com/bid/2811/info/ (June 10,2002)

29. Red Hat advisory: RHSA-2001:008-02. “VIM statusline Text-Embedded Command Execution Vulnerability” Bugtraq vulnerabilities. Mar 26, 2001. http://online.securityfocus.com/bid/2510 (June 10,2002)

30. tek@superw00t.com. “Multiple Vendor TalkD User Validation Vulnerability” Bugtraq vulnerabilities. Apr 03, 2002. http://online.securityfocus.com/bid/4419/info/ (June 10,2002)

31. cert@cert.org. “SSH connections using RC4 and password authentication can be replayed” Vulnerability Notes Database http://www.kb.cert.org/vuls/id/665372 (June 10,2002)

32. cert@cert.org. “Passwords sent via SSH encrypted with RC4 can be easily cracked” Vulnerability Notes Database http://www.kb.cert.org/vuls/id/565052 (June 10,2002)

33. cert@cert.org. “SSH-1 allows client authentication to be forwarded by a malicious server to another server” Vulnerability Notes Database http://www.kb.cert.org/vuls/id/684820 (June 10,2002)

34. cert@cert.org. “Weaknesses in the SSH protocol simplify brute-force attacks against passwords typed in an existing SSH session” Vulnerability Notes Database http://www.kb.cert.org/vuls/id/596827 (June 10,2002)

35. Aßmann, Claus. “SMTP AUTH in sendmail 8.10-8.12” Links to e-mail related informations. Jun. 11, 2002. http://www.sendmail.org/~ca/email/auth.html (June 10,2002)

36. Aßmann, Claus. “More features of e-mail” Links to e-mail related informations. Sep. 16, 2000. http://www.sendmail.org/~ca/email/extensions.html#PGPSMIME (June 10,2002)

37. SGI. “Support for MIPS® Processor-Based Systems with the IRIX® Operating System “ http://www.sgi.com/support/suppserv.html (June 10,2002)

38. SGI. “Security Advisory Mailing List” http://www.sgi.com/support/security/wiretap.html (June 10,2002)

39. SGI. “Advisories” http://www.sgi.com/support/security/advisories.html (June 10,2002)

40. cert@cert.org. “Exploitation of BIND Vulnerabilities” CERT® Incident Note IN-2001-03 http://www.cert.org/incident_notes/IN-2001-03.html (June 10,2002)

41. MagniComp. “RDist Home Page” http://www.magnicomp.com/rdist/rdist.shtml (June 10,2002)

42. Kabay, M. E. “Personnel and security: Separation of duties” Jun. 14 2000. http://www.nwfusion.com/newsletters/sec/2000/0612sec2.html (June 10,2002)

43. Network Computing and SANS.org “SGI Alerts” Security Alert Consensus http://www.sans.org/newlook/digests/SAC/SGI.htm (June 10,2002)

Appendix A
Output from TARA scan

```
Security scripts *** 2.0.9 ARC, 1999.0907.2100 ***
Tue Apr 30 15:10:57 EDT 2002
15:10> Beginning security report for GIAC1 (IP27 IRIX 6.5).

# Performing check of passwd files...
--WARN-- [pass002w] UID 0 exists multiple times in /etc/passwd.

# Performing check of group files...
--WARN-- [grp002w] GID 0 exists multiple times in /etc/group.

# Performing check of user accounts...
# Checking accounts from /etc/passwd.
--WARN-- [acc012w] Login ID diag has uid == 0.
--WARN-- [acc012w] Login ID smtp has uid == 0.
--WARN-- [acc012w] Login ID sysadm has uid == 0.

# Performing check of /etc/hosts.equiv and .rhosts files...

# Checking accounts from /etc/passwd...

# Performing check of .netrc files...

# Checking accounts from /etc/passwd...

# Performing check of /etc/default/login, /securetty, and /etc/ttytab...


# Performing check of PATH components...
# Only checking user 'root'

# Performing check of anonymous FTP...

# Performing checks of mail aliases...
# Checking aliases from /usr/lib/aliases.


# Performing check of `cron' entries...

# Performing check of 'services' and 'inetd'...
# Checking services from /etc/services.
--FAIL-- [inet003f] The port for service pop-3 is assigned to service pop3.
# Checking inetd entries from /usr/etc/inetd.conf
--WARN-- [inet005w] Service finger is using /usr/ucc/etc/tcpd instead of
         /usr/etc/fingerd.
--WARN-- [inet005w] Service ftp is using /usr/ucc/etc/tcpd instead of
         /usr/etc/ftpd.
--WARN-- [inet005w] Service login is using /usr/ucc/etc/tcpd instead of
         /usr/etc/rlogind.
--WARN-- [inet005w] Service ntalk is using /usr/ucc/etc/tcpd instead of
         /usr/etc/talkd.
--WARN-- [inet005w] Service shell is using /usr/ucc/etc/tcpd instead of
         /usr/etc/rshd.
--WARN-- [inet005w] Service telnet is using /usr/ucc/etc/tcpd instead of
```

```
         /usr/etc/telnetd.

# Performing NFS exports check...

# Performing check of system file permissions...
--WARN-- [perm001w] /unix should not have group execute.
--WARN-- [perm001w] /unix should not have world execute.
--WARN-- [perm001w] The owner of /var/tmp should be root (owned by sys).
--WARN-- [perm001w] /etc/exports should not have group read.
--WARN-- [perm001w] /etc/fstab should not have group read.
--WARN-- [perm001w] /etc/hosts.equiv should not have group read.
--FAIL-- [perm001w] /etc/netgroup should not have group read.

# Checking for known intrusion signs...

# Performing check of files in system mail spool...
--WARN-- [kis008w] File ".user1.pop.bak" in the mail spool, owned by
         `user1'.
--WARN-- [kis008w] File ".user2.pop.bak" in the mail spool, owned by
         `user2'.

# Performing system specific checks...
# Running './scripts/check_sendmail'...

# Checking sendmail...

# Checking setuid executables...


# Checking setgid executables...

--CONFIG-- [fsys003c] No setgid list... listing all setgid files

# Checking unusual file names...

# Looking for unusual device files...

# Checking symbolic links...
```

Appendix B
Details from SARA scan

Host: giac.com

General host information:

- Host type: IRIX 6
- Subnet 168.0.0
- FTP server (GREEN)
- LDAP over SSL server (GREEN)
- WWW (Secure) server (GREEN)

Vulnerability information:

- SSH may be vulnerable(RED)
- Apache (less than 1.3.21) is vulnerable to multiple exploits (http)(YELLOW)
- Probable smtp relay (spam)(YELLOW)
- IRIX telnetd version may be vulnerable(YELLOW)
- printer version may be vulnerable to buffer overflow(BROWN)
- sendmail EXPN command may provide hacker information(BROWN)
- Check login banner for telnet connections(BROWN)
- sgi pmcd (Co Pilot) provides system information to the world(BROWN)

Excessive finger information(BROWN)

Appendix C
Output from Whisker

```
-- whisker / v1.4.0 / rain forest puppy / www.wiretrip.net --
- Loaded script database of 1968 lines

= - = - = - = - = - =
= Host: giac.com
= Server: Apache/1.3.19 (Unix) mod_ssl/2.8.2 OpenSSL/0.9.5a


+ 404 Not Found: GET /cfdocs/
+ 404 Not Found: GET /scripts/
+ 404 Not Found: GET /cfcache.map
+ 404 Not Found: GET /cfide/Administrator/startstop.html
+ 404 Not Found: GET /cfappman/index.cfm
+ 403 Forbidden: GET /cgi-bin/
+ 404 Not Found: GET /cgi-bin/dbmlparser.exe
+ 404 Not Found: HEAD /_vti_inf.html
+ 404 Not Found: HEAD /_vti_pvt/
+ 404 Not Found: HEAD /cgi-bin/webdist.cgi
+ 404 Not Found: HEAD /cgi-bin/handler
+ 404 Not Found: HEAD /cgi-bin/wrap
+ 404 Not Found: HEAD /cgi-bin/pfdisplay.cgi
+ 404 Not Found: HEAD /cgi-bin/MachineInfo
+ 404 Not Found: HEAD /mall_log_files/order.log
+ 404 Not Found: HEAD /PDG_Cart/
+ 404 Not Found: HEAD /quikstore.cfg
+ 404 Not Found: HEAD /orders/
+ 404 Not Found: HEAD /Admin_files/order.log
+ 404 Not Found: HEAD /WebShop/
+ 404 Not Found: HEAD /pw/storemgr.pw
+ 404 Not Found: HEAD /bigconf.cgi
+ 404 Not Found: HEAD /icat
+ 404 Not Found: HEAD /cgi-bin/icat
+ 404 Not Found: HEAD /cgi-local/
+ 404 Not Found: HEAD /htbin/
+ 404 Not Found: HEAD /cgibin/
+ 404 Not Found: HEAD /cgis/
+ 404 Not Found: HEAD /cgi/
+ 404 Not Found: HEAD /cgi-bin/flexform.cgi
+ 404 Not Found: HEAD /cgi-bin/flexform
+ 404 Not Found: HEAD /cgi-bin/LWGate
+ 404 Not Found: HEAD /cgi-bin/lwgate
+ 404 Not Found: HEAD /cgi-bin/LWGate.cgi
+ 404 Not Found: HEAD /cgi-bin/lwgate.cgi
+ 404 Not Found: HEAD /cgi-win/
+ 404 Not Found: HEAD /cgi-bin/pu3.pl
+ 404 Not Found: HEAD /cgi-bin/meta.pl
+ 404 Not Found: HEAD /cgi-bin/day5datacopier.cgi
+ 404 Not Found: HEAD /cgi-bin/webutils.pl
+ 404 Not Found: HEAD /cgi-bin/tigvote.cgi
+ 404 Not Found: HEAD /cgi-bin/tpgnrock
+ 404 Not Found: HEAD /cgi-bin/webwho.pl
+ 404 Not Found: HEAD /cgi-bin/form.cgi
+ 404 Not Found: HEAD /cgi-bin/message.cgi
+ 404 Not Found: HEAD /cgi-bin/.cobalt/siteUserMod/siteUserMod.cgi
+ 404 Not Found: HEAD /cgi-bin/.fhp
+ 404 Not Found: HEAD /cgi-bin/htsearch
+ 404 Not Found: HEAD /cgi-bin/plusmail
+ 404 Not Found: HEAD /manage/cgi/cgiproc
+ 404 Not Found: HEAD /cgi-bin/ultraboard.cgi
+ 404 Not Found: HEAD /cgi-bin/ultraboard.pl
+ 404 Not Found: HEAD /cgi-bin/perlshop.cgi
+ 404 Not Found: HEAD /cgi-bin/download.cgi
+ 404 Not Found: HEAD /cgi-bin/bnbform.cgi
+ 404 Not Found: HEAD /cgi-bin/bnbform
+ 404 Not Found: HEAD /cgi-bin/cgi-lib.pl
+ 404 Not Found: HEAD /cgi-bin/post_query
+ 404 Not Found: HEAD /cgi-bin/upload.pl
+ 404 Not Found: HEAD /cgi-bin/rwwwshell.pl
+ 404 Not Found: HEAD /cgi-bin/nlog-smb.pl
+ 404 Not Found: HEAD /cgi-bin/nlog-smb.cgi
+ 404 Not Found: HEAD /cgi-bin/wwwboard/
+ 404 Not Found: HEAD /wwwboard/
+ 404 Not Found: HEAD /cgi-bin/wwwboard.pl
+ 404 Not Found: HEAD /cgi-bin/wwwboard.cgi
+ 404 Not Found: HEAD /logs/
+ 404 Not Found: HEAD /database/
+ 404 Not Found: HEAD /databases/
+ 404 Not Found: HEAD /cgi-bin/cachemgr.cgi
+ 403 Forbidden: HEAD /.htaccess
+ 403 Forbidden: HEAD /cgi-bin/.htaccess
+ 404 Not Found: HEAD /docs/
+ 403 Forbidden: HEAD /~root/
+ 404 Not Found: HEAD /cgi-bin/htgrep.cgi
+ 404 Not Found: HEAD /cgi-bin/htgrep
+ 404 Not Found: HEAD /ws_ftp.ini
+ 404 Not Found: HEAD /cgi-bin/ws_ftp.ini
+ 404 Not Found: HEAD /WS_FTP.ini
+ 404 Not Found: HEAD /cgi-bin/WS_FTP.ini
+ 404 Not Found: HEAD /cgi-bin/ax-admin.cgi
+ 404 Not Found: HEAD /cgi-bin/axs.cgi
+ 404 Not Found: HEAD /cgi-bin/responder.cgi
+ 404 Not Found: HEAD /cgi-bin/w3-sql
+ 404 Not Found: HEAD /search97.vts
+ 404 Not Found: HEAD /search.vts
+ 404 Not Found: HEAD /search97cgi/s97_cgi
+ 404 Not Found: HEAD /cgi-bin/unlg1.1
+ 404 Not Found: HEAD /cgi-bin/unlg1.2
+ 404 Not Found: HEAD /cgi-bin/gH.cgi
+ 500 Internal Server Error: HEAD /cgi-bin/test-cgi
+ 500 Internal Server Error: GET /cgi-bin/test-cgi
+ 404 Not Found: HEAD /cgi-bin/campas
+ 404 Not Found: HEAD /cgi-bin/www-sql
+ 404 Not Found: HEAD /cgi-bin/w3-msql
+ 404 Not Found: HEAD /cgi-bin/view-source
+ 404 Not Found: HEAD /cgi-bin/add_ftp.cgi
+ 404 Not Found: HEAD /cgi-bin/cgiwrap
+ 404 Not Found: HEAD /cgi-bin/guestbook.cgi
+ 404 Not Found: HEAD /cgi-bin/guestbook.pl
+ 404 Not Found: HEAD /cgi-bin/edit.pl
+ 404 Not Found: HEAD /cgi-bin/webbbs.cgi
+ 404 Not Found: HEAD /cgi-bin/whois_raw.cgi
+ 404 Not Found: HEAD /webcart/
+ 404 Not Found: HEAD /webcart-lite/
+ 404 Not Found: HEAD /cgi-bin/AnyBoard.cgi
+ 404 Not Found: HEAD /cgi-bin/admin.php
+ 404 Not Found: HEAD /cgi-bin/code.php
+ 404 Not Found: HEAD /cgi-bin/dumpenv.pl
+ 404 Not Found: HEAD /cgi-bin/admin.php3
+ 404 Not Found: HEAD /cgi-bin/code.php3
+ 404 Not Found: HEAD /cgi-bin/login.cgi
+ 404 Not Found: HEAD /cgi-bin/login.pl
+ 404 Not Found: HEAD /reviews/newpro.cgi
+ 404 Not Found: HEAD /piranha/secure/passwd.php3
+ 404 Not Found: HEAD /cgi-bin/sojourn.cgi
+ 404 Not Found: HEAD /cgi-bin/dfire.cgi
+ 404 Not Found: HEAD /cgi-bin/spin_client.cgi
+ 404 Not Found: HEAD /cgi-bin/Count.cgi
+ 404 Not Found: HEAD /cgi-bin/stats.prf
+ 404 Not Found: HEAD /cgi-bin/statsconfig
+ 404 Not Found: HEAD /srchadm
+ 404 Not Found: HEAD /cgi-bin/count.cgi
+ 404 Not Found: HEAD /users/scripts/submit.cgi
+ 404 Not Found: HEAD /cgi-bin/nph-test-cgi
+ 404 Not Found: HEAD /cgi-bin/webgais
+ 404 Not Found: HEAD /cgi-bin/websendmail
+ 404 Not Found: HEAD /cgi-bin/bb-hist.sh
+ 404 Not Found: HEAD /bb-dnbd/
+ 404 Not Found: HEAD /cgi-bin/faxsurvey
+ 404 Not Found: HEAD /cgi-bin/htmlscript
+ 404 Not Found: HEAD /cgi-bin/aglimpse
+ 404 Not Found: HEAD /cgi-bin/glimpse
+ 404 Not Found: HEAD /cgi-bin/man.sh
+ 404 Not Found: HEAD /cgi-bin/architext_query.pl
+ 404 Not Found: HEAD /cgi-bin/architext_query.cgi
+ 404 Not Found: HEAD /cgi-bin/excite
+ 404 Not Found: HEAD /cgi-bin/getdoc.cgi
+ 404 Not Found: HEAD /cgi-bin/webplus
+ 404 Not Found: HEAD /cgi-bin/bizdb1-search.cgi
+ 404 Not Found: HEAD /cgi-bin/cart.pl
+ 404 Not Found: HEAD /cgi-bin/filemail.pl
+ 404 Not Found: HEAD /cgi-bin/filemail
+ 404 Not Found: HEAD /cgi-bin/php.cgi
+ 404 Not Found: HEAD /cgi-bin/jj
+ 404 Not Found: HEAD /cgi-bin/info2www
+ 404 Not Found: HEAD /cgi-bin/nph-publish
+ 404 Not Found: HEAD /cgi-bin/ax.cgi
+ 404 Not Found: HEAD /session/admnlogin
+ 404 Not Found: HEAD /cgi-bin/rpm_query
+ 404 Not Found: HEAD /cgi-bin/AnyForm2
+ 404 Not Found: HEAD /cgi-bin/AnyForm
+ 404 Not Found: HEAD /cgi-bin/textcounter.pl
+ 404 Not Found: HEAD /cgi-bin/wwwthreads/
+ 404 Not Found: HEAD /wwwthreads/
+ 404 Not Found: HEAD /cgi-bin/classified.cgi
+ 404 Not Found: HEAD /cgi-bin/classifieds.cgi
+ 404 Not Found: HEAD /cgi-bin/classifieds
+ 404 Not Found: HEAD /ss.cfg
+ 404 Not Found: HEAD /ncl_items.html
+ 404 Not Found: HEAD /cgi-bin/survey.cgi
+ 404 Not Found: HEAD /cgi-bin/survey
+ 404 Not Found: HEAD /test/test.cgi
+ 404 Not Found: HEAD /cgi-bin/search.cgi
+ 404 Not Found: HEAD /cgi-bin/c_download.cgi
+ 404 Not Found: HEAD /cgi-bin/ntitar.pl
+ 404 Not Found: HEAD /cgi-bin/enter.cgi
+ 404 Not Found: HEAD /cgi-bin/dig.cgi
+ 404 Not Found: HEAD /cgi-bin/tidfinder.cgi
+ 404 Not Found: HEAD /cgi-bin/tablebuild.pl
+ 404 Not Found: HEAD /cgi-bin/displayTC.pl
+ 404 Not Found: HEAD /cgi-bin/dasp/fm_shell.asp
+ 500 Internal Server Error: HEAD /cgi-bin/printenv
+ 500 Internal Server Error: GET /cgi-bin/printenv
+ 404 Not Found: HEAD /cgi-bin/environ.cgi
+ 404 Not Found: HEAD /cgi-bin/session/adminlogin
+ 404 Not Found: HEAD /cgi-bin/finger
+ 404 Not Found: HEAD /cgi-bin/finger.pl
+ 404 Not Found: HEAD /cgi-bin/finger.cgi
+ 404 Not Found: HEAD /cgi-bin/maillist.pl
+ 404 Not Found: HEAD /cgi-bin/maillist.cgi
+ 404 Not Found: HEAD /cgi-bin/sh
+ 404 Not Found: HEAD /cgi-bin/bash
+ 404 Not Found: HEAD /cgi-bin/ash
+ 404 Not Found: HEAD /cgi-bin/tcsh
+ 404 Not Found: HEAD /cgi-bin/ksh
+ 404 Not Found: HEAD /cgi-bin/csh
+ 404 Not Found: HEAD /cgi-bin/rksh
+ 404 Not Found: HEAD /cgi-bin/rsh
+ 404 Not Found: HEAD /cgi-bin/zsh
+ 404 Not Found: HEAD /cgi-bin/perl
+ 404 Not Found: HEAD /cgi-bin/test-cgi.tcl
+ 404 Not Found: HEAD /php/
+ 404 Not Found: HEAD /mlog.phtml
+ 404 Not Found: HEAD /cgi-bin/mlog.phtml
+ 404 Not Found: HEAD /mylog.phtml
+ 404 Not Found: HEAD /cgi-bin/mylog.phtml
+ 404 Not Found: HEAD /HyperStat/stat_what.log
+ 404 Not Found: HEAD /Stats/
+ 404 Not Found: HEAD /WebTrend/
+ 404 Not Found: HEAD /analog/
+ 404 Not Found: HEAD /cache-stats/
+ 404 Not Found: HEAD /easylog/easylog.html
+ 404 Not Found: HEAD /hit_tracker/
+ 404 Not Found: HEAD /hitmatic/
+ 404 Not Found: HEAD /hitmatic/analyse.cgi
+ 404 Not Found: HEAD /hyperstat/stat_what.log
+ 404 Not Found: HEAD /log/
+ 404 Not Found: HEAD /logfile/
+ 404 Not Found: HEAD /logfiles/
+ 404 Not Found: HEAD /logger/
+ 404 Not Found: HEAD /logging/
+ 404 Not Found: HEAD /logs/access_log
+ 404 Not Found: HEAD /ministats/admin.cgi
+ 404 Not Found: HEAD /scripts/weblog
+ 404 Not Found: HEAD /server_stats/
+ 404 Not Found: HEAD /stat/
+ 404 Not Found: HEAD /statistics/
+ 404 Not Found: HEAD /stats/
+ 404 Not Found: HEAD /super_stats/access_logs
+ 404 Not Found: HEAD /trafficlog/
+ 404 Not Found: HEAD /ustats/
+ 404 Not Found: HEAD /w3perl/admin
+ 404 Not Found: HEAD /webaccess/access-options.txt
+ 404 Not Found: HEAD /weblog/
+ 404 Not Found: HEAD /weblogs/
+ 404 Not Found: HEAD /webstats/
+ 404 Not Found: HEAD /wstats/
+ 404 Not Found: HEAD /wusage/
+ 404 Not Found: HEAD /wwwlog/
+ 404 Not Found: HEAD /wwwstats/
+ 404 Not Found: HEAD /access-log
+ 404 Not Found: HEAD /access.log
+ 404 Not Found: HEAD /awebvisit.stat
+ 404 Not Found: HEAD /dan_o.dat
+ 404 Not Found: HEAD /hits.txt
+ 404 Not Found: HEAD /log.htm
+ 404 Not Found: HEAD /log.html
+ 404 Not Found: HEAD /log.txt
+ 404 Not Found: HEAD /logfile
+ 404 Not Found: HEAD /logfile.htm
+ 404 Not Found: HEAD /logfile.html
+ 404 Not Found: HEAD /logfile.txt
+ 404 Not Found: HEAD /logger.html
+ 404 Not Found: HEAD /stat.htm
+ 404 Not Found: HEAD /stats.htm
+ 404 Not Found: HEAD /stats.html
+ 404 Not Found: HEAD /stats.txt
+ 404 Not Found: HEAD /webaccess.htm
+ 404 Not Found: HEAD /wwwstats.html
+ 404 Not Found: HEAD /bin/
+ 404 Not Found: HEAD /cgi-bin/log/
+ 404 Not Found: HEAD /cgi-bin/log/nether-log.pl?checkit
+ 404 Not Found: HEAD /cgi-bin/logs/
+ 404 Not Found: HEAD /cgi-bin/stat/
+ 404 Not Found: HEAD /cgi-bin/stats.pl
+ 404 Not Found: HEAD /cgi-bin/stats/
+ 404 Not Found: HEAD /cgi-bin/clickcount.pl?view=test
+ 404 Not Found: HEAD /cgi-bin/cstat.pl
+ 404 Not Found: HEAD /cgi-bin/ex-logger.pl
+ 404 Not Found: HEAD /cgi-bin/hitview.cgi
+ 404 Not Found: HEAD /cgi-bin/log-reader.cgi
+ 404 Not Found: HEAD /cgi-bin/logit.cgi
+ 404 Not Found: HEAD /cgi-bin/logs.pl
+ 404 Not Found: HEAD /cgi-bin/lookwho.cgi
+ 404 Not Found: HEAD /cgi-bin/mini_logger.cgi
+ 404 Not Found: HEAD /cgi-bin/ratlog.cgi
+ 404 Not Found: HEAD /cgi-bin/robadmin.cgi
+ 404 Not Found: HEAD /cgi-bin/show.pl
+ 404 Not Found: HEAD /cgi-bin/stats-bin-p/reports/index.html
+ 404 Not Found: HEAD /cgi-bin/statview.pl
+ 404 Not Found: HEAD /cgi-bin/viewlogs.pl
+ 404 Not Found: HEAD /cgi-bin/wwwstats.pl
+ 404 Not Found: HEAD /admin/
+ 404 Not Found: HEAD /Admin_files/
+ 404 Not Found: HEAD /DMR/
+ 404 Not Found: HEAD /StoreDB/
+ 404 Not Found: HEAD /Web_store/
+ 404 Not Found: HEAD /access/
+ 404 Not Found: HEAD /account/
+ 404 Not Found: HEAD /accounting/
+ 404 Not Found: HEAD /administrator/
+ 404 Not Found: HEAD /app/
+ 404 Not Found: HEAD /apps/
+ 404 Not Found: HEAD /archive/
+ 404 Not Found: HEAD /asp/
+ 404 Not Found: HEAD /atc/
+ 404 Not Found: HEAD /backup/
+ 404 Not Found: HEAD /bak/
+ 404 Not Found: HEAD /beta/
+ 404 Not Found: HEAD /buy/
+ 404 Not Found: HEAD /buynow/
+ 404 Not Found: HEAD /c/
+ 404 Not Found: HEAD /cart/
+ 404 Not Found: HEAD /ccard/
+ 404 Not Found: HEAD /config/
+ 404 Not Found: HEAD /counter/
+ 404 Not Found: HEAD /credit/
+ 404 Not Found: HEAD /customers/
+ 404 Not Found: HEAD /dat/
+ 404 Not Found: HEAD /data/
+ 404 Not Found: HEAD /db/
+ 404 Not Found: HEAD /dbase/
+ 404 Not Found: HEAD /doc-html/
+ 404 Not Found: HEAD /down/
+ 404 Not Found: HEAD /download/
+ 404 Not Found: HEAD /downloads/
+ 404 Not Found: HEAD /employees/
+ 404 Not Found: HEAD /exe/
+ 404 Not Found: HEAD /file/
+ 404 Not Found: HEAD /files/
+ 404 Not Found: HEAD /forum/
+ 404 Not Found: HEAD /fpadmin/
+ 404 Not Found: HEAD /ftp/
+ 404 Not Found: HEAD /guestbook/
+ 404 Not Found: HEAD /guests/
+ 404 Not Found: HEAD /home/
+ 404 Not Found: HEAD /htdocs/
+ 404 Not Found: HEAD /html/
+ 404 Not Found: HEAD /ibill/
+ 404 Not Found: HEAD /idea/
+ 404 Not Found: HEAD /ideas/
+ 404 Not Found: HEAD /incoming/
+ 404 Not Found: HEAD /info/
+ 404 Not Found: HEAD /install/
+ 404 Not Found: HEAD /intranet/
+ 404 Not Found: HEAD /jave/
+ 404 Not Found: HEAD /jdbc/
+ 404 Not Found: HEAD /lib/
+ 404 Not Found: HEAD /library/
+ 200 OK: HEAD /login/
+ 404 Not Found: HEAD /mail/
+ 404 Not Found: HEAD /mall_log_files/
+ 200 OK: HEAD /manual/
+ 404 Not Found: HEAD /marketing/
+ 404 Not Found: HEAD /msql/
+ 404 Not Found: HEAD /new/
+ 404 Not Found: HEAD /odbc/
+ 404 Not Found: HEAD /old/
+ 404 Not Found: HEAD /oracle/
+ 404 Not Found: HEAD /order/
+ 404 Not Found: HEAD /outgoing/
+ 404 Not Found: HEAD /pages/
+ 404 Not Found: HEAD /passwords/
+ 404 Not Found: HEAD /perl/
+ 404 Not Found: HEAD /private/
+ 404 Not Found: HEAD /pub/
+ 404 Not Found: HEAD /public/
+ 404 Not Found: HEAD /purchase/
+ 404 Not Found: HEAD /purchases/
+ 404 Not Found: HEAD /pw/
+ 404 Not Found: HEAD /register/
+ 404 Not Found: HEAD /registered/
+ 404 Not Found: HEAD /reseller/
+ 404 Not Found: HEAD /retail/
+ 404 Not Found: HEAD /root/
+ 404 Not Found: HEAD /sales/
+ 404 Not Found: HEAD /search/
+ 404 Not Found: HEAD /sell/
+ 404 Not Found: HEAD /setup/
+ 404 Not Found: HEAD /shop/
+ 404 Not Found: HEAD /shopper/
+ 404 Not Found: HEAD /site/iissamples/
+ 404 Not Found: HEAD /software/
+ 404 Not Found: HEAD /source/
+ 404 Not Found: HEAD /sql/
+ 404 Not Found: HEAD /store/
+ 404 Not Found: HEAD /support/
+ 404 Not Found: HEAD /temp/
+ 404 Not Found: HEAD /test/
+ 404 Not Found: HEAD /test-cgi/
+ 404 Not Found: HEAD /tmp/
+ 404 Not Found: HEAD /tools/
+ 404 Not Found: HEAD /tree/
+ 404 Not Found: HEAD /updates/
+ 404 Not Found: HEAD /usage/
+ 404 Not Found: HEAD /user/
+ 404 Not Found: HEAD /users/
+ 404 Not Found: HEAD /web/
+ 404 Not Found: HEAD /web800fo/
+ 404 Not Found: HEAD /webadmin/
+ 404 Not Found: HEAD /webboard/
+ 404 Not Found: HEAD /webdata/
+ 404 Not Found: HEAD /website/
+ 404 Not Found: HEAD /www/
+ 404 Not Found: HEAD /www-sql/
+ 404 Not Found: HEAD /wwwjoin/
+ 404 Not Found: HEAD /import/
+ 404 Not Found: HEAD /zipfiles/
+ 404 Not Found: HEAD /passwd
+ 404 Not Found: HEAD /cgi-bin/passwd
+ 404 Not Found: HEAD /passwd.txt
+ 404 Not Found: HEAD /cgi-bin/passwd.txt
+ 404 Not Found: HEAD /password
+ 404 Not Found: HEAD /cgi-bin/password
+ 404 Not Found: HEAD /password.txt
+ 404 Not Found: HEAD /cgi-bin/password.txt
+ 404 Not Found: HEAD /status/
```