Global Information Assurance Certification Paper

SANS GIAC Certified UNIX Security Administrator (GCUX)
SANS 2002 Orlando, FL
GCUX Practical Assignment Version 1.9
Option 2 - Consultant's Report From Auditing Unix

Audit of Gauntlet 5.5 Firewall
(Running on Solaris 2.6 with BIND 8.2.3-REL)

Jeff Holland, GCUX/GCIA/GCIH/GSEC

Table of Contents

Typesetting Conventions Used

The following typesetting conventions were used in this practical:

1. Text written by the auditor is displayed using the Times New Roman 12 point font.

2. `Commands executed, resulting output and scripts are displayed using the Courier New 10 point font.`

3. *Text that is italicized indicates either the text is referenced, or was italicized to simply make the flow and presentation of the information easier to visually digest. It is easily determined whether the text was referenced or italicized for formatting purposes given the specific circumstance. The italicized text is displayed using Times New Roman 12 point font. Examples of each case are as follows:*

   Case 1: Italicized text to make presentation clearer

   Vulnerability/Risk Item: Solaris 2.6 OS (Operating System) vulnerabilities

   Case 2: Italicized text indicates material used from another source

   The flag values (taken directly from the Nmap man pages) are as follows [3]:

   -sT *: TCP connect() scan*
   -sR *: RPC scan*
   -p 1-65535 *: <port ranges>*
   -O *: remote host identification via TCP/IP fingerprinting*
   -I *: TCP reverse ident scanning*
   -R *: Tells Nmap to ALWAYS do reverse DNS resolution on the target IP addresses.*
   -v *: turn on verbose mode*

IP Addresses Used in the Audit

The following IP address (sanitized) were used in the audit report:

a.b.c.9 – An unallocated IP address in the DMZ subnet that is not allowed use of any firewall proxies or plugs. This IP simulates an attacker from the Internet.

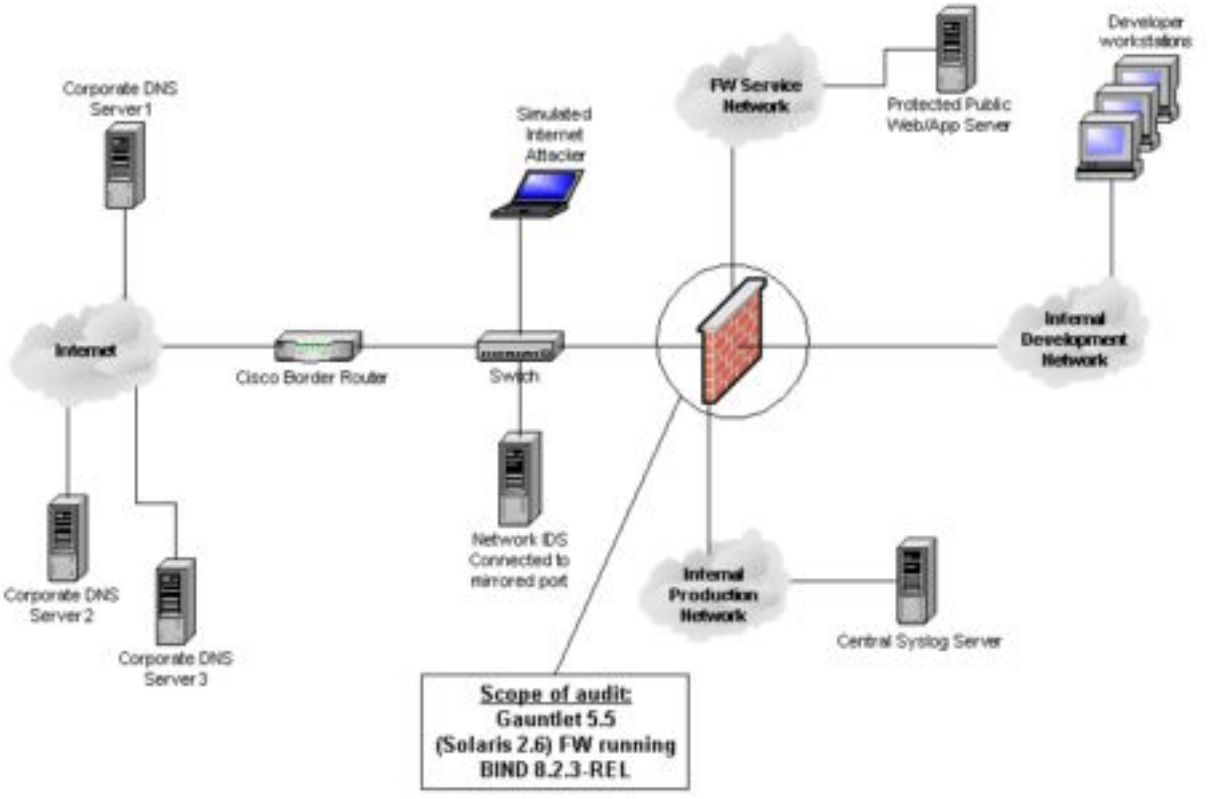
a.b.c.6 – The primary external interface for the firewall's internal development network. Other external firewall interfaces include the production and firewall service network interfaces. Except for auditing of the firewall traffic rules and how they apply to the various interfaces (which is explicitly identified when applicable), all network-based scanning and auditing was conducted against the primary external firewall (hme0) interface.

Executive Summary

Jeff Holland, GCUX/GCIA/GCIH/GSEC and GIAC Enterprises Security Consultant, has prepared this report for the online fortune cookie-sayings maker GIAC Enterprises (giac.f-cookies.com), a subsidiary of the online fortune cookie maker f-cookies.com. This report will address an audit of the GIAC Enterprises exterior Gauntlet 5.5 firewall running on Solaris 2.6 with the BIND 8.2.3-REL implementation of DNS.

Concern about the firewall was expressed by the GIAC security administrators due to the vulnerable nature of recent BIND 8 versions, as well as a newer version of Gauntlet (version 6.0) for Solaris 8 being available that could offer enhanced security. The primary reason for this audit, besides the addressing the aforementioned concerns, is to assess the current firewall software configuration, how "hardened" the OS is when compared against well-known and established benchmarks, and identify security vulnerabilities of the OS and firewall software. An additional benefit of the audit will include independent verification of the most important recommended security upgrades, and their associated labor hours.

Prior to performing this audit, interviews with the security staff were conducted to better be able to assess the firewall and provide defensive recommendations that complement the business case and network topology of GIAC Enterprises. In addition to access to the firewall itself, a simplified network configuration was provided to the auditor so that a more complete and thorough audit could be performed. The (simplified) network configuration at the time of the audit is shown below:



The following facts were discovered upon discussions with the GIAC security staff, and a review of the system documentation (namely the security CONOPS (Concept of Operations) and SSP (System Security Plan)):

- Due to budgetary limitations while designing and building the GIAC Enterprises network, a single (non load-balanced) Gauntlet 5.5 firewall was built.

- To avoid having to purchase a separate DNS server, the most recent version of BIND (8.2.3-REL at the time) was installed locally on the firewall. The public DNS servers of the parent corporation (f-cookies.com) were updated with the zone maps of the GIAC Enterprises sub-domain, giac.f-cookies.com.

- The GIAC Enterprises funding was effectively exhausted in late 2001, and the network has been operating on a very limited budget. This has not allowed proper review and updating of the network configuration and security specific software. However, limited budget has been made to support reviewing of the firewall and IDS logs.

GIAC Enterprises management has stated they would like to use this audit report obtain appropriate funding (both material and labor) from f-cookies.com to upgrade their firewall software and/or its configuration, if such an upgrade were necessary and independently supported by this audit report.

Overall, it is the auditor's opinion that the current security state of the firewall is slightly below average given how most Gauntlet firewalls are built today, and how DNS BIND is typically configured. It is also the opinion of the auditor that the following table of recommendations (which are fully discussed in the following sections and summarized in the Critical Issues and Recommendations section), will greatly enhance the security of the GIAC Enterprises firewall, and provided defense in-depth for the networks behind the firewall:

Summary Table of Defensive Recommendations

Update BIND to version 8.3.3 or 9.2.1	Enable BSM (Basic Security Module) kernel level auditing, and create /var/adm/loginlog
Update the Solaris OS and Gauntlet patches	Harden the OS with a hardening tool such as YASSP, and follow the other recommendations that require manual intervention on the administrator's behalf
Disable Telnet and FTP access from the internal network to the Internet	Comment out the identd daemon in the /etc/inetd.conf file to block reverse ident scanning attacks
Chroot BIND by following the directions here	Harden the BIND /etc/named.conf file by following the recommendation here
Disable CDE and RPC services, and run the espm firewall GUI from an internal protected host	Consider upgrading to Gauntlet 6.0 to take advantage of the newer features described here

Description of System and Audit Methodology

System Description:

The GIAC Enterprises firewall is a stateful inspection, application proxy firewall configured to "deny what is not explicitly allowed". That is, only the specific protocols/services that are needed to perform day-to-day business are enabled, and access is controlled both inbound and outbound via IP address/IP block and/or protocol. For instance, FTP is only allowed outbound from the internal network for purposes of automated anti-virus updates. FTP is not allowed from the Internet to the firewall or to the firewall service or internal networks. Furthermore, access to the internal development and production networks is limited to authorized static IP addresses or IP blocks.

An additional role of the firewall is to be the authoritative source for GIAC Enterprises sub-domain information using the BIND (Berkeley Internet Name Domain) software. To provide redundancy in terms of name resolution, the giac.f-cookies.com zone maps have been transferred to the corporate name servers.

The GIAC Enterprises firewall hardware [1] and software specifications [2] are as follows:

Hardware platform and Software OS and Version Information:

Hardware	Software
Model: Sun Ultra 60 Workstation	**OS/Build:** Solaris 2.6 5/98 s297s_hw3smccServer_09 SPARC
Processor(s): Two 450 MHz UltraSPARC-II	**Firewall:** Gauntlet Firewall 5.5 (UNIX)
External Cache (per processor): 4MB L2	**BIND:** 8.2.3-REL
Memory: 1GB RAM	**Perl:** Perl 5.005_03
Disk: Two 18GB UltraSCSI Disk Drives	**OS Patches:** See the patchlist.scr output
Graphics Card: Sun Creator3D Series 3	**Gauntlet Patches:** See the Gauntlet patch log
DVD/CD-ROM: One 10X DVD-ROM Drive	**Netscape Communicator:** 4.76
Floppy: One 1.44MB floppy drive	**Misc. utilities/software:** tcsh (version 6.07), make (version 3.79.1), Java Runtime Loader (version 1.1.6, installed by Gauntlet in /usr/local/etc/jre/bin)

Firewall role:

The role of the firewall is provide a major layer of defense against unauthorized access of the internal networks by users "outside" GIAC Enterprises network, to prevent internal users (or malicious or trojaned software) from accessing certain IP addresses and/or IP blocks, and to prevent the use of certain protocols (i.e. X-Windows to the Internet) or sending traffic on ports that is not authorized (i.e. IRC traffic outbound). The firewall also serves to isolate the development network from the production network, and to isolate the firewall service network for public web/FTP/etc server hosting.

Risks or concerns associated with the firewall:

The following risks and concerns apply to the GIAC Gauntlet 5.5 firewall:

1. The firewall is the primary defensive device for the network, and therefore it is critical to maintain the patch level for the OS, as well as the Gauntlet Firewall patches.

2. There is a new version of Gauntlet (version 6.0) that is now available. What new security features might this version have that GIAC Enterprises could benefit from?

3. The Gauntlet product has recently been sold by NAI to SecureComputing. The future of the Gauntlet product is discussed here.

4. The firewall operating system is not as hardened/secured as the auditor would recommend, which confirms some of the concerns of the GIAC Enterprises security administrators.

5. The version of BIND is outdated, and more importantly, subject to a buffer overflow vulnerability in the resolver libraries. ISC.org recommends upgrading to BIND version 8.3.3 or 9.2.1 at the time of this audit.

6. BIND is running as root, and is not chroot'ed. This is a very insecure way of running a name server, and immediate action is required to mitigate the risk this poses to GIAC Enterprises' firewall and the internal network.

7. Telnet and FTP access from the internal network to the Internet is allowed.

Audit method overview:

The audit of the Gauntlet firewall was conducted using the following tools, methods and resources. A detailed analysis of the technical checks is addressed in the Detailed Analysis section.

Tools	Methods	Resources
Nmap 2.54BETA22	Port scanning	SANS GCUX courseware
Nessus version 1.2.0	Network vulnerability scanning	Internet searches
TARA version 2.0.9	Host-based vulnerability security	DNS BIND O'Reilly book
Selected Solaris system binaries (ps, grep, rpcinfo, dig, telnet, ftp, etc.)	Configuration comparison against known security recommendations	Auditor's professional experience, and that of other security professionals (referenced where applicable)
	Command line/host auditing	GIAC Enterprises security personnel
	Physical inspection	Physical inspection of the firewall and it's location

The general audit methodology used was as follows:

1. Inspect the physical location of the firewall. Look for possible ways to subvert the physical protection (lack of a secured location, cipher codes and/or passwords written down and not protected in a safe or locked drawer, power conduit not being protected or shielded, etc.). Also inspect the environmental conditions (air conditioning/cooling, fire control, presence of a UPS (Uninterruptible Power Supply), mitigation preparation for ESD (Electro Static Discharge), etc.). Assess if a physical DoS is realistically possible by disabling or subverting one or more of these environmental protections.

2. Conduct a network scan of the firewall using network-based scanning tools. The testing was conducted from a laptop plugged into the switch in front of the firewall that simulated an Internet attacker (see the network diagram).

3. Conduct a network audit and a host audit of the firewall at the system console (including, but not limited to, OS and software patch level identification, configuration of OS and software, identification of known software vulnerabilities, administrative practice, access control, and backup/file integrity procedures).

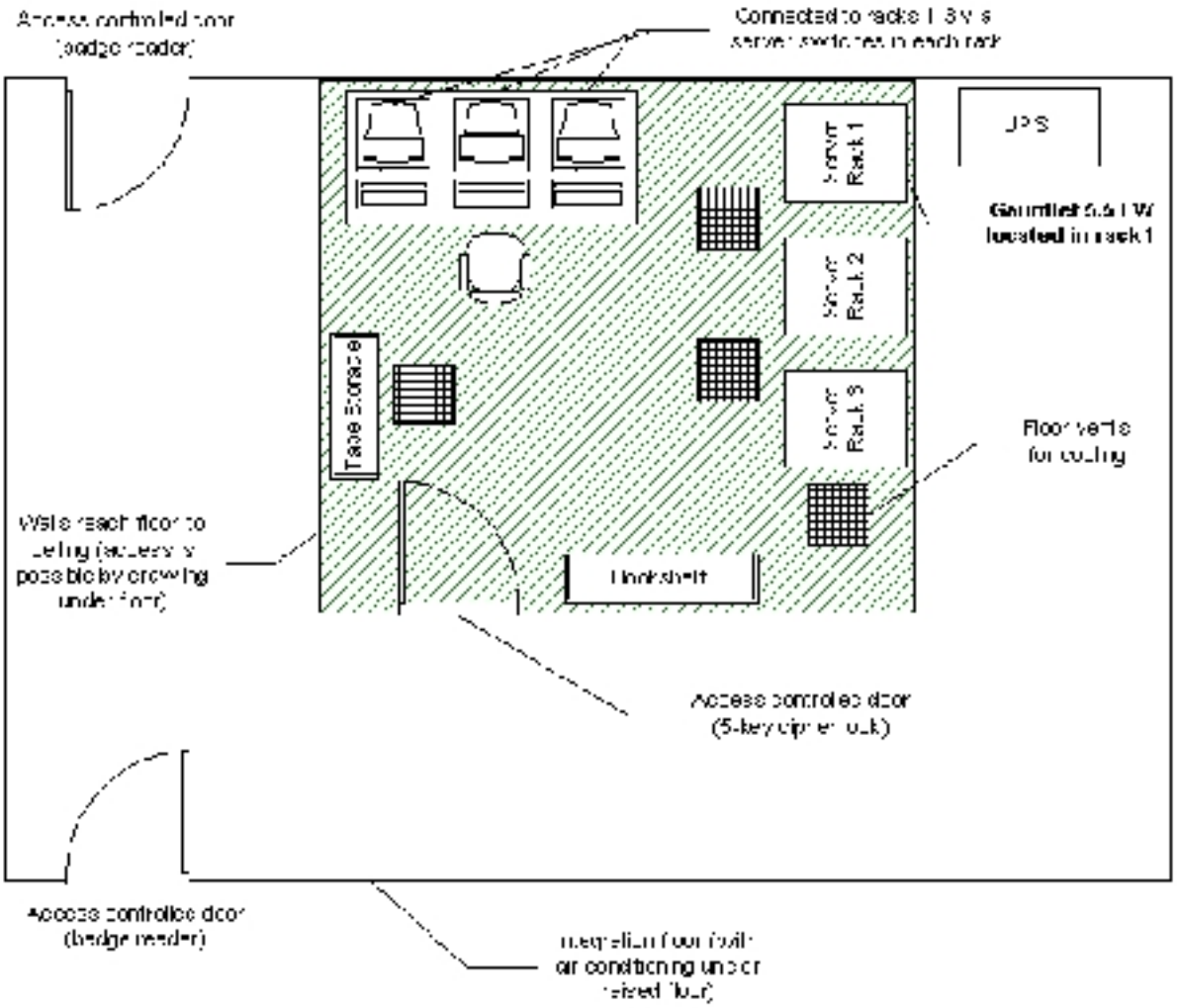
4. Analyze the results of the network and host-based audit and provide ample technical detail to support the findings.

5. Identify critical issues and vulnerabilities, and recommend a course of action based on the issues and vulnerabilities.

Detailed Analysis

Physical Security of the Firewall:

The physical security of the GIAC Enterprises firewall is depicted in the diagram below:



The physical security of the firewall can only be subverted by being on the access control list for the integration floor (which is controlled by corporate security), and then either knowing the cipher code for the server room door, or crawling under the raised floor into the server room. Note that corporate security, the GIAC Enterprises program manager, and the security/system administrators are the only parties in possession of the server room cipher code.

Passwords were written down on paper in the server room, and not secured in a locked storage container. Power to the machines was protected by shielded conduit (under the floor), and supplied from the UPS. The UPS itself is inside the integration room floor, and thus protected from unauthorized access by the ACL on the outer doors. Sufficient air is being supplied to the server room (approximately 70 degree F), and the floor is tiled to prevent static discharge. An

overhead water sprinkler is present in the room, which protects against fire, but could very well ruin the server equipment if it was activated. A smoke alarm, intercom speaker and battery-powered emergency light are also present in the server room.

Vulnerability/Risk Item: Physical security of the GIAC Enterprises firewall

Audit Result: The physical security, with the exception of passwords being written down on paper and stored unsecured in the server room, was satisfactory. Environmental protections could be enhanced by the presence of a chemical fire extinguisher.

Significance of Finding(s): Accidental or careless handling of the hardcopy passwords could allow a root level access on the firewall or other machine by an insider or consultant/vendor. Lack of a chemical fire extinguisher could lead to a partial loss of server equipment to fire and possibly water damage.

Defensive Recommendation:

1. Store passwords in a locked filing cabinet or small safe inside the server room. Keep an additional copy in a locked storage location off-site (ie. another building).
2. Consider replacing the water sprinkler with a safer chemical substitute, and at least purchase a computer friendly portable fire extinguisher.
3. Also consider motion sensors under the raised floor if the data in the server room is deemed sensitive enough.

References:

1. http://www.pmengineer.com/CDA/ArticleInformation/features/BNP__Features__Item/0,2732,9728,00.html
2. http://www.reliablefire.com/portablesfolder/computerrmextinguishers.html

Network and host-based audit of the firewall:

Vulnerability/Risk Item: Solaris 2.6 OS (Operating System) vulnerabilities

Audit Result: From a search of the CERT vulnerability advisories page, Solaris 2.6 has the following known vulnerabilities:

Buffer Overflow in CDE ToolTalk
http://www.cert.org/advisories/CA-2002-26.html

Integer Overflow In XDR Library
http://www.cert.org/advisories/CA-2002-25.html

Multiple Vulnerabilities in CDE ToolTalk
http://www.cert.org/advisories/CA-2002-20.html

Buffer Overflow in Multiple DNS Resolver Libraries
http://www.cert.org/advisories/CA-2002-19.html

Heap Overflow in Cachefs Daemon (cachefsd)
http://www.cert.org/advisories/CA-2002-11.html

Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)
http://www.cert.org/advisories/CA-2002-03.html

Exploitation of Vulnerability in CDE Subprocess Control Service
http://www.cert.org/advisories/CA-2002-01.html

Buffer Overflow in CDE Subprocess Control Service
http://www.cert.org/advisories/CA-2001-31.html

Buffer Overflow in telnetd
http://www.cert.org/advisories/CA-2001-21.html

Buffer Overflow In Sun Solaris in.lpd Print Daemon
http://www.cert.org/advisories/CA-2001-15.html

Sadmind/IIS Worm
http://www.cert.org/advisories/CA-2001-11.html
http://www.cert.org/advisories/CA-1999-16.html

Exploitation of snmpXdmid
http://www.cert.org/advisories/CA-2001-05.html

Vulnerability in statd exposes vulnerability in automountd
http://www.cert.org/advisories/CA-99-05-statd-automountd.html

Significance of Finding(s):

Buffer Overflow in CDE ToolTalk: The Tooltalk database server process is not running on the GIAC firewall. Note that the /etc/inetd.conf file did not have the rpc.ttdbserverd daemon defined due to Gauntlet's wrapping and hardening of the inetd.conf file upon installation. In addition, a `ps -ef` command shows that only rpcbind, and not the rpc.ttdbserverd, daemon is running:

```
root@giac6.giac.f-cookies.com:/>ps -ef
    UID   PID  PPID  C    STIME TTY      TIME CMD
      …<snip>…
    root   144     1  0   Apr 17 ?        0:00 /usr/sbin/rpcbind
      …<snip>…
```

Integer Overflow In XDR Library: Note that per the Sun Alert Notification, the following defensive recommendations are made by Sun [21]:

"***A)*** *To disable the dmispd(1M) daemon, perform the following steps as root:*

Stop the running dmispd(1M) daemon:
 # /etc/init.d/init.dmi stop
Disable the daemon from starting on reboot:
 # mv /etc/rc3.d/S77dmi /etc/rc3.d/DISABLED_S77dmi

B) *To disable the rpc.cmsd(1m) daemon, perform the following steps as root:*

Comment out the following line in the /etc/inetd.conf file by adding a '#' at the beginning:
#100068/2-5 dgram rpc/udp wait root /usr/dt/bin/rpc.cmsd rpc.cmsd
Tell the inetd(1M) process to reread the newly modified /etc/inetd.conf file by sending it a hangup signal, SIGHUP:
 # ps -ef | grep inetd
 # kill -HUP <pid of inetd from above ps output>

This will disable rpc.cmsd(1m)."

Again, because the GIAC firewall does not run the rpc.cmsd daemon from /etc/inetd.conf, this is not an issue. As for the dmispd daemon, note that the S77dmi daemon was disabled by Gauntlet in /etc/rc3.d, and that the daemon is **not** run from the Gauntlet firewall proxy rc directory (/usr/local/etc/mgmt/rc) from the soft-linked S20gauntlet startup script in /etc/rc3.d (see the listings and contents of /etc/init.d/gauntlet file below).

```
root@giac6.giac.f-cookies.com:/etc/rc3.d>ls -al
total 28
drwxrwxr-x   2 root     sys          512 Apr 23  2001 ./
drwxrwxr-x  31 root     sys         3584 Jun 26 11:14 ../
-rwxr--r--   5 root     sys         1738 Jul 15  1997
disabled.S15nfs.server.PRE5.5*
-rwxr-xr-x   3 root     sys          677 Jul 15  1997
disabled.S76snmpdx.PRE5.5*
-rwxr-xr-x   3 root     sys          951 Jul 15  1997 disabled.S77dmi.PRE5.5*
-rw-r--r--   1 root     sys         1708 Jul 15  1997 README
lrwxrwxrwx   1 root     other         18 Apr  3  2001 S20gauntlet ->
../init.d/gauntlet*
-rwxr-xr-x   1 root     other        453 Apr 13  2001
S99_Gauntlet_interface_fix*
-rwxr-xr-x   1 root     other        493 Apr 13  2001
s99_Gauntlet_interface_fix*

root@giac6.giac.f-cookies.com:/etc/rc3.d>cat ../init.d/gauntlet
#!/bin/sh
#
# Gauntlet(TM) Internet Firewall
# TAG=SOLARIS
#
# DON'T EDIT THIS FILE. USE THE NEW PROXY STARTUP MECHANISM.
```

```
# pjc 5/2/96
# $Header:
/projects/gauntlet/nspdev/V5.5/projects/build/gather/../../gauntlet/system-
products/solaris/root/./etc/init.d/RCS/gauntlet,v 1.12 1999/07/28 21:22:56
skane Exp $
#
RC=/usr/local/etc/mgmt/rc

if [ -d /usr/local/etc ]; then
dmesg >/usr/local/etc/dmesg.boot
fi

if [ -f /usr/local/etc/mgmt/gauntlet.conf ]; then
    echo "Starting firewall daemons.."

        if [ -d $RC ]; then
                cp /usr/local/etc/mgmt/gauntlet.conf
/usr/local/etc/mgmt/gauntlet.saved
                for i in $RC/S* ; do $i stop ; $i start ; done
                exit 0
        fi

else
    echo "Do not start proxies until firewall has been configured"
    exit 0
fi

echo "No configuration database found"

root@giac6.giac.f-cookies.com:/usr/local/etc/mgmt/rc>ls
D330ck-gw*          s115cyberpatrol*   s220info-gw*       s311rammp*
S391afwtimer*
H110http*           s120gopher*        s240rsh*           s312nsmmp*
s400netacl-tn*
H900custom*         s140ftp*           s250lpr*           s313vdolmmp*
s401netacl-rl*
kill-procs*         s150telnet*        s260syb-gw*        s320strmwrks-gw*
s402netacl-ftp*
S050proxymgr-all*   s160rlogin*        S271ikmpd*         s330ck-gw*
s900custom*
s100mail*           s170finger*        s280sql-gw*        s360snmpd*
template*
S105ipnat*          s180auth*          s290snmp-gw*       s380mssql-gw*
s105ipnat*          s200whois*         s300gui*           S390afw*
s110http*           s210pop3*          s310mmp*           s390afw*
```

Multiple Vulnerabilities in CDE ToolTalk: This advisory is very similar to the Buffer Overflow in CDE ToolTalk advisory (CA-2002-26), and thus the GIAC firewall is not subject to this vulnerability. Per the recommendation of Sun, apply the latest cluster patch to insure this vulnerability cannot be exploited in the future should this service be enabled.

Buffer Overflow in Multiple DNS Resolver Libraries: This advisory does not apply to the GIAC firewall either since ISC's BIND software is being run on the GIAC firewall. However, per the Sun recommendation, the latest cluster patch should be downloaded and installed should for any reason the Solaris DNS resolver library (libresolv.so) be utilized for any reason in the future. As

pointed out in the Risk from third-party software section, the GIAC firewall is running ISC's BIND 8.2.3-REL, and per the CA-2002-19 CERT advisory, this version's DNS resolver library (libbind) is indeed vulnerable.

Heap Overflow in Cachefs Daemon (cachefsd): Note that per the Sun Alert Notification, the following defensive recommendations are made by Sun [22]:

"*Comment out cachefsd in /etc/inetd.conf as shown below:*

For Solaris 2.6, 7 and 8:

#100235/1 tli rpc/tcp wait root /usr/lib/fs/cachefs/cachefsd cachefsd

Solaris 2.5.1:

#100235/1 stream rpc/tcp wait root /usr/lib/fs/cachefs/cachefsd cachefsd

Once the line is commented out either:

- reboot, or

- send a HUP signal to inetd(1M) and kill existing cachefsd processes, for example, on Solaris 2.5.1 and 2.6 do the following:

$ kill -HUP <PID of inetd>

$ kill <PIDs of any cachefsd processes>

Solaris 7 and 8 do the following:

$ pkill -HUP inetd

$ pkill cachefsd"

Once again, because the GIAC firewall does not run the rpc.cmsd daemon from /etc/inetd.conf, this vulnerability is not an issue.

Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP): This advisory pertains to SNMP version 1 request and trap handling vulnerabilities. According to the advisory, "*the main agent of SEA, snmpdx(1M), is affected on Solaris 2.6*", which is the requesting handling vulnerability. Further details are available here: http://www.kb.cert.org/vuls/id/854306. There are many recommended defenses against this vulnerability. They include ingress and egress filtering of SNMP traffic, applying a vendor patch, disabling the SNMP service, and changing the default community strings [23]. Since the SNMP daemon is not enabled in the /etc/inetd.conf file, the daemon was not shown to be listening in the Nmap port scan output, and the SNMP proxy is disabled in the /usr/local/etc/mgmt/gauntlet.conf file (the file read by the Gauntlet admin GUI) as shown below, the GIAC firewall is not affected by this vulnerability. It should also be noted that there were no forward filter rules or plug proxies for SNMP ports 161 and 162 TCP/UDP enabled on the firewall either.

SNMP proxy portion of the gauntlet.conf file (yellow bolded portions indicate the SNMP proxy is not enabled):

```
…<snip>…
def_proxy_12_realname=snmpd
def_proxy_12_num_parms=8
```

```
def_proxy_12_parm_1_name=system-contact
def_proxy_12_parm_1_value=
def_proxy_12_parm_2_name=system-name
def_proxy_12_parm_2_value=xxxxx.giac.f-cookies.com
def_proxy_12_parm_3_name=system-location
def_proxy_12_parm_3_value=
def_proxy_12_parm_4_name=snmp-manager
def_proxy_12_parm_4_value=
def_proxy_12_parm_5_name=bind-port
def_proxy_12_parm_5_value=1610
def_proxy_12_parm_6_name=proxy-type
def_proxy_12_parm_6_value=snmpd
def_proxy_12_parm_7_name=proxy-exec
def_proxy_12_parm_7_value=./snmpd
def_proxy_12_parm_8_name=state
def_proxy_12_parm_8_value=off
def_proxy_13_name=snmp-gw
def_proxy_13_realname=snmp-gw
def_proxy_13_num_parms=12
def_proxy_13_parm_1_name=numagents
def_proxy_13_parm_1_value=
def_proxy_13_parm_2_name=trap-port
def_proxy_13_parm_2_value=162
def_proxy_13_parm_3_name=managed-port
def_proxy_13_parm_3_value=161
def_proxy_13_parm_4_name=directory
def_proxy_13_parm_4_value=
def_proxy_13_parm_5_name=groupid
def_proxy_13_parm_5_value=0
def_proxy_13_parm_6_name=userid
def_proxy_13_parm_6_value=0
def_proxy_13_parm_7_name=manager
def_proxy_13_parm_7_value=
def_proxy_13_parm_8_name=timeout
def_proxy_13_parm_8_value=10
def_proxy_13_parm_9_name=bind-port
def_proxy_13_parm_9_value=snmp
def_proxy_13_parm_10_name=proxy-type
def_proxy_13_parm_10_value=snmp-gw
def_proxy_13_parm_11_name=proxy-exec
def_proxy_13_parm_11_value=./snmp-gw
def_proxy_13_parm_12_name=state
def_proxy_13_parm_12_value=off
…<snip>…
```

Exploitation of Vulnerability in CDE Subprocess Control Service: According to the CERT advisory (http://www.cert.org/advisories/CA-2002-01.html), "*On systems running CDE, dtspcd is spawned by the Internet services daemon (typically inetd or xinetd) in response to a CDE client request. dtspcd is typically configured to run on port 6112/tcp with root privileges.*" [41].

Since the dtspcd daemon is not enabled in the /etc/inetd.conf file, the GIAC firewall is not subject to this vulnerability.

Buffer Overflow in CDE Subprocess Control Service: This is the original dtspcd vulnerability notice. CA-2002-01 is an updated advisory based upon this one.

Buffer Overflow in telnetd: While Sun stated that they did not believe that this vulnerability applied to their OS, they did release a patch since the exploit used a buffer overflow to crash the system or be leveraged to gain access [24]. It is recommended that the latest cluster patch be applied. Also, the GIAC firewall does allow outbound telnet connections (using the stateful telnet proxy). It is also recommended (and it discussed in more detail later in the report) that telnet be disabled, and SSH be implemented if remote file transfer is required.

Buffer Overflow In Sun Solaris in.lpd Print Daemon: The GIAC firewall does not start the print service from /etc/inetd.conf, and therefore is not vulnerable to this buffer overflow. As pointed out in the advisory by Sun, the following change should be made to the /etc/system file:

*"Enable the **noexec_user_stack** tunable (although this does not provide 100 percent protection against exploitation of this vulnerability, it makes the likelihood of a successful exploit much smaller). Add the following lines to the /etc/system file and reboot:*

set noexec_user_stack = 1
set noexec_user_stack_log = 1" [25]

Sadmind/IIS Worm: Solaris 2.6, if not patched, is subject to the Sadmind vulnerability. This vulnerability was initially announced in 1999, and then later the Sadmind/ISS worm used the same vulnerability to exploit Solaris systems for attacking IIS web servers. Since the Sadmind service is not started from /etc/inetd.conf, the GIAC firewall is not subject to this vulnerability. Proper patching is also advised for defense-in-depth.

Exploitation of snmpXdmid: While snmpXdmid is installed and turned on by default, referring to the rc3.d directory listing of the GIAC firewall, this daemon does not have a startup script. In addition, a process listing of the dmi service shows the daemon is not running:

```
root@giac6.giac.f-cookies.com:/>ps -ef | grep dmi
    root 22482 22458  0 11:26:03 pts/3    0:00 grep dmi
```

Therefore, the GIAC firewall is not vulnerable to this buffer overflow exploit.

Vulnerability in statd exposes vulnerability in automountd: This vulnerability is described by CERT as such:

"The vulnerability in rpc.statd may allow a remote intruder to call arbitrary rpc services with the privileges of the rpc.statd process, typically root. The vulnerability in automountd may allow a local intruder to execute arbitrary commands with the privileges of the automountd service.

By combining attacks exploiting these two vulnerabilities, a remote intruder is able to execute arbitrary commands with the privileges of the automountd service." [26]

While Solaris 2.6 is not vulnerable to the automountd vulnerability, it is vulnerable to the rpc.statd vulnerability. Sun recommends applying patch 106592-02 for Solaris 2.6 [26]. Since this advisory was release in 1999, Sun has rolled this patch into it's cluster patch long ago. The GIAC firewall was patched with the latest cluster patch in April of 2001, therefore it is not vulnerable to the rcp.statd attack.

Defensive Recommendation: To address the Solaris 2.6 OS vulnerabilities described above, it is recommended that all security relevant patches be applied, as well as the other recommended patches. As pointed out in the Solaris 2.6 OS patch installation/management section, this can be done with the Patch Check tool or by downloading the latest patch cluster and applying it.

Also, as pointed out above (and in the OS Hardening section), make the following change to the /etc/system file:

> *Add the following lines to the /etc/system file and reboot:*
>
> *set noexec_user_stack = 1*
> *set noexec_user_stack_log = 1"* [25]

References:

1. http://www.cert.org/advisories
2. http://sunsolve.sun.com/pub-cgi/show.pl?target=patchk
3. http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access

Vulnerability/Risk Item: Gauntlet 5.5 Firewall vulnerabilities

Audit Result: Gauntlet 5.5 has two serious software vulnerabilities found by Jim Stickley of Garrison Technologies. The first is a two-part vulnerability in the Cyber Patrol software packaged with Gauntlet, and installed by default. According to an article by Kevin Poulsen of Securityfocus [5]:

"In integrating Cyber Patrol, NAI programmers created a custom server that checks web address against the Cyber Patrol database, then approves or disapproves each connection going out through the firewall depending on whether it's permitted by a particular company's policy.

That server contains a buffer overflow bug, and, further, mistakenly accepts connections from the outside world…"

The critical thing to note is that the software is turned on by default for the first 30 days. If the software is not registered, the software is then "turned off" and the firewall is no longer vulnerable [5].

The second vulnerability occurs in the widely used csmap SMTP proxy. In another article by Kevin Poulsen of Securityfocus, he explains that [6]:

"In normal operation, csmap accepts mail connections from the Internet, then forwards only valid traffic to the internal mail server.

By adding reams of text at a particular point in the mail transaction, an attacker can overflow the memory dedicated to storing an email address. Properly crafted computer instructions appended to the text will then be executed by the machine, giving hackers a way in."

Note that the STMP vulnerability also affects Gauntlet 6.0. While this vulnerability does not give the attacker root access upon exploitation, the attacker may be able to leverage off of the access gained and obtain root [6].

Significance of Finding(s): The Cyber Patrol vulnerability allows an attacker to gain root access remotely, if the firewall is vulnerable [5]. The firewall is vulnerable if it was built less than thirty days ago or the Cyber Patrol software was registered and the Cyber Patrol patch was not installed. It is important to note that the GIAC Enterprises firewall had the Cyber Patrol patch installed when the machine was built.

The csmap SMTP vulnerability is especially important for the GIAC Enterprises firewall, as the SMTP proxy is used to proxy inbound and outbound mail to the internal mail server. Fortunately, the patch for this vulnerability was also installed when the machine was built. See the section on Gauntlet firewall patches for more information.

Defensive Recommendation: It is advised that you download all the Gauntlet 5.5 patches from http://www.securecomputing.com/index.cfm?sKey=986 as soon as possible and burn them to CD. This will ensure you have the necessary patches when firewalls must be rebuilt, or additional machines are required. Be sure to repeat this process each time a new patch is released. Printing the contents of this web page is also recommended, as there is a very useful history of the updates to the patches.

References:

1. http://online.securityfocus.com/news/40
2. http://online.securityfocus.com/news/248
3. http://www.securecomputing.com/index.cfm?sKey=986
4. http://www.cert.org/advisories/CA-2001-25.html

Vulnerability/Risk Item: Solaris 2.6 OS patch installation/management

Audit Result: Solaris patch clusters are distributed on CDROM media with the OS, but are also distributed as tar files from http://sunsolve.Sun.COM/pub-cgi/show.pl?target=patches/patch-access. The patch clusters should always be retrieved from the SunSolve site so that the latest patches are installed for your particular OS version.

Once the patch cluster is downloaded, untar'ed in /var/sadm/patch, and installed, there are several options for retrieving the patch log information.

1. Run the command `/usr/sbin/showrev -p` to verify the current patches revs that are applied [9]. For more information on the particular patch, view the /var/sadm/patch/README.<patch.id> file under each patch subdirectory in /var/sadm/patch.

2. For a quick list of the currently installed patch id's and the services they affect, run the patchlist.scr script included as Appendix C. The output of the script when run on the GIAC firewall is shown in the appendix after the script.

3. The best way to determine the current patch id's, patch revs, which patches are current, and which patches are not installed on your firewall is to the run the Sun Patch Check tool locally on the firewall [10]. According to Sun,

   "*Patch Check determines the patch levels on your system against Sun's Recommended and Security patch list. Additionally, it operates from input files and lists all patches that pertain to packages installed on the system. This tool is similar to the PatchDiag Tool that you may have used in the past, with the added advantage of producing reports in HTML format that allow you to select and receive your desired patches.* [11]".

   The tool can be downloaded here (copy and paste the URL to a browser):
   http://sunsolve.sun.com/pub-cgi/show.pl?target=patchk

Significance of Finding(s): While the Patch Check report contained many important patches that should be installed and others that should be considered, the following security relevant patches should be installed on the firewall as soon as possible (note that the screenshots were take from a report run by the Sun Patch Check tool on the GIAC firewall).

Uninstalled Security Patches

note: This list includes the Security patches that are also Recommended

Patch ID	Ins Rev	Lat Rev	Age	Require ID	Incomp ID	Synopsis
☐ 106303	N/A	03	260	106271-07		SunOS 5.6: /usr/lib/netsvc/yp/rpc.yppasswdd patch
				106257-06		
☐ 106361	N/A	14	83			SunOS 5.6: csh/jsh/ksh/rksh/rsh/sh patch
☐ 106629	N/A	23	489		105181-08	SunOS 5.6: CS6400 kernel update patch
☐ 106882	N/A	02	605			SunOS 5.6: /usr/lib/nfs/nfsd patch
☐ 107298	N/A	03	192			SunOS 5.6: ntpdate and xntpd patch
☐ 107326	N/A	02	213			SunOS 5.6: rlmod and telmod patch
☐ 108333	N/A	02	617			SunOS 5.6: jserver buffer overflow
☐ 109100	N/A	02	163			SunOS 5.6: patch usr/sbin/mkdevmaps
☐ 109719	N/A	01	475			SunOS 5.6: arp should lose set-gid bid
☐ 110883	N/A	01	265			SunOS 5.6: useradd date format fixes
☐ 111039	N/A	02	203			SunOS 5.6: /usr/bin/bdiff and /usr/bin/sdiff patch
☐ 111236	N/A	01	349			SunOS 5.6: Patch for /usr/sbin/in.fingerd
☐ 111240	N/A	01	349			SunOS 5.6: Patch to /usr/bin/finger
☐ 111560	N/A	01	310			SunOS 5.6: dmesg security problem
☐ 111645	N/A	01	262			SunOS 5.6: BCP libmle buffer overflow
☐ 111859	N/A	01	241			SunOS 5.6: Buffer overflow in whodo via $TZ
☐ 112073	N/A	03	83			SunOS 5.6: /usr/bin/mailx patch
☐ 112456	N/A	01	49			SunOS 5.6: pt_chmod should call fdetach

Sun Patch Check tool Screen Shot [11]

Other Related Uninstalled Patches

note: This is determined by the packages that have been installed on the system.

When one patch refers to multiple packages, we list the additional packages in the next lines.

The various 'S', 'R', '*' marks denote unbundled packages that are designated as 'Security' or 'Recommended'.

S = Security
R = Recommended Unbundled
* = Both Security and Recommended Unbundled

Patch ID	Package Name	Lat Rev	Age	Synopsis
☐ 107001 S	SUNWmibii	01	1259	Solstice Enterprise Agent 1.0.1: SNMP DMI
	SUNWsacom			
	SUNWsadm			
	SUNWsasnm			
☐ 107035 S	SUNWmibii	01	1255	Solstice Enterprise Agent 1.0.1: SNMP DMI
	SUNWsacom			
	SUNWsadmi			
	SUNWsasnm			
☐ 107715 S	TSIpg#	18	3	PGX32 2.6: PGX32 Graphics Patch
	TSIpgx*n			
	TSIpgpx			

Sun Patch Check tool Screen Shot [11]

Defensive Recommendation: It is recommended that the firewall be taken off line and patched immediately. At the very least, download the latest patch cluster from http://sunsolve.Sun.COM/pub-cgi/show.pl?target=patches/patch-access. If GIAC Enterprises has a Sun support contract, then it is recommended that you use the Patch Check tool at http://sunsolve.sun.com/pub-cgi/show.pl?target=patchk.

References:

1. http://sunsolve.sun.com/pub-cgi/show.pl?target=patchk
2. http://sunsolve.sun.com/pub-cgi/show.pl?target=registerFrontPage
3. http://sunsolve.Sun.COM/pub-cgi/show.pl?target=patches/patch-access

Vulnerability/Risk Item: Gauntlet 5.5 Firewall patch installation/management

Audit Result: The Gauntlet firewall patch log, located at /usr/local/etc/mgmt/patchlog, contains the patch history for the firewall. The timestamp and contents of the file are shown below:

```
root@giac6.giac.f-cookies.com:/usr/local/etc/mgmt>ls -l patchlog
-rw-r--r--   1 root     other        185 Sep  5  2001 patchlog

root@giac6.giac.f-cookies.com:/usr/local/etc/mgmt>cat patchlog
patch kernel.patch 4 a installed Tue Apr  3 11:07:43 CDT 2001
patch cluster.patch 7 a installed Tue Apr  3 11:08:13 CDT 2001
patch smap.patch 9 a installed Wed Sep  5 12:40:14 CDT 2001
```

The csmp SMTP patch was applied on September 5th 2001. Referring to the list of Gauntlet patches at http://www.securecomputing.com/index.cfm?sKey=986, the patch for the Cyber Patrol patch was applied on April 3rd 2001, as the patch was rolled into the cluster.SOLARIS.patch on 06/23/00.

Significance of Finding(s): While evidence of proper patching is shown in the patch log, do note that some of the patches are out of sync with the vendor maintained patch listing. Administrators should carefully consider updating the current patches, and continue to monitor for future vulnerability notices for Gauntlet 5.5 in the future.

Defensive Recommendation: The firewall and security administrators should subscribe to the Gauntlet mailing list. The following information was taken from http://www.rmsbus.com/gauntlet-user.htm [7]:

"*To subscribe to the Gauntlet firewall mailing list (gauntlet-user) send an e-mail message with no subject to majordomo@listserv.v-one.com. In the body of the message (not the subject line) write: subscribe gauntlet-user*

To: majordomo@listserv.v-one.com
From: you
Subj:

subscribe gauntlet-user "

Use the following Gauntlet mail list archive mirror when questions or problems arise with the firewall. The auditor has found the list members very helpful and responsive: http://marc.theaimsgroup.com/?l=gauntlet-user&r=1&w=2.

Finally, care should be exercised when applying patches, as the order in which they are applied is important. Also, do not install patches for services/proxies that are not being used. The auditor has experienced stability problems with firewalls that had all the patches applied, despite the fact that not all the applicable services were running that the patches applied to.

In particular, the following patch has caused stability issues on at least one Gauntlet 5.5 firewall the auditor has worked with:

> *kernel.SOLARIS.patch*, patch version 6 (*Enables installation on both Gauntlet and GVPN systems*. [8])

Therefore, it is recommended that careful consideration be paid before applying patch revision 6 to the GIAC Enterprises firewall. Configuring a test firewall with the same OS version, software and firewall configuration for testing is advised.

Do note that the *cluster.SOLARIS.patch* has had 9 updates since the patch was installed on the GIAC firewall. It is **highly** recommended that you backup your firewall configuration and logs, and then apply the new patch.

The telnet proxy is enabled on your system (for use from the internal network only), but the *tn.patch* is not applied. The patch is to fix the maximum number of policies that can be applied [8]. It is recommended that this patch be applied, even though the auditor is recommending that the telnet proxy be disabled and SSH be installed if it is necessary perform any secure remote administration of the firewall or file transfers to/from the internal network.

References:

1. http://www.securecomputing.com/index.cfm?sKey=986
2. http://www.rmsbus.com/gauntlet-user.htm
3. http://marc.theaimsgroup.com/?l=gauntlet-user&r=1&w=2

Vulnerability/Risk Item: Solaris 2.6 OS configuration vulnerabilities

Audit Result: The host-based UNIX audit tool TARA (version 2.0.9) was run on the firewall to assess the vulnerabilities of file permissions and services [12]. TARA uses a configuration file called "tigerrc" to determine what to scan for, and creates an output file in the local Tara directory. The customized tigerrc file used to scan the GIAC firewall is shown in Appendix D.

The command line output of running TARA is shown below:

```
root@giac6.giac.f-cookies.com:/tara-2.0.9>./tiger
Tiger Analytical Research Assistant (TARA)
   Developed by Texas A&M University, 1994
   Updated by the Advanced Research Corporation, 1999
   Covered by GNU General Public License (GPL)

Using configuration files for SunOS 5.6.
09:59> Beginning security report for giac6.giac.f-cookies.com.
09:59> Starting file systems scans in background...
```

```
09:59> Running Crack (password cracker) in background...
09:59> Checking password files...
09:59> Checking group files...
09:59> Checking user accounts...
09:59> Checking .rhosts files...
09:59> Checking .netrc files...
09:59> Checking ttytab, login, securetty, and ftpusers files...
09:59> Checking PATH settings...
09:59> Checking anonymous ftp setup...
09:59> Checking mail aliases...
09:59> Checking cron entries...
09:59> Checking 'inetd' configuration...
10:00> Checking NFS export entries...
10:00> Checking permissions and ownership of system files...
10:00> Checking for indications of breakin...
10:00> Performing system specific checks...
10:00> Waiting for filesystems scans to complete...
/usr/openwin/demo/xil/example2/brainscan.data.Z: No such file or directory
/usr/openwin/demo/xil/example2/brainscan.header: No such file or directory
/usr/openwin/demo/xil/example2/example2.c: No such file or directory
/usr/openwin/demo/xil/example2/window.c: No such file or directory
/dev/msglog: No such file or directory
/dev/sysmsg: No such file or directory
/dev/poll: No such file or directory
/.netscape/lock: No such file or directory
10:01> Filesystems scans completed...
10:01> Performing check of embedded pathnames...
10:04> Security report completed for giac6.giac.f-cookies.com.
Security report is in `./security.report.giac6.giac.f-cookies.com.020614-
09:59'.
```

The /etc/inet/inetd.conf file was also audited to insure that unnecessary services were not being started upon bootup. The file contents is shown below:

```
root@giac6.giac.f-cookies.com:/>cat /etc/inet/inetd.conf
#
# Internet server configuration database
#
# @(#)inetd.conf 5.4 (Berkeley) 6/30/90
#TAG=OSI
#VER=V3.2
#
# modified to allow daemon mode use of proxies.
#ftp stream tcp nowait root /usr/local/etc/netacl ftpd
#telnet stream tcp nowait root /usr/local/etc/netacl telnetd
#login stream tcp nowait root /usr/local/etc/netacl rlogind
#finger stream tcp nowait nobody /usr/local/etc/netacl fingerd
#authsrv stream tcp nowait root /usr/local/etc/authsrv authsrv
#nntp stream tcp nowait root /usr/local/etc/plug-gw plug-gw nntp
#whois stream tcp nowait root /usr/local/etc/plug-gw plug-gw whois

#tftp dgram udp wait root /usr/sbin/in.tftpd in.tftpd -s /tftpboot
#RFC 931 "ident" service (optional)
auth stream tcp nowait nobody /usr/local/etc/identd identd
```

Significance of Finding(s): TARA output assigns each vulnerability check a rating of "INFO", "WARN" or "FAIL". Since the output TARA creates is quite lengthy, only those vulnerabilities identified as "FAIL" are shown and addressed below:

(The command "`./tigexp -F security.report.giac6.giac.f-cookies.com.020614-09:59 > temp`" was run on the firewall, and the resulting file "temp" was searched for the string "FAIL". The snipped output is shown below.)

```
# Performing check of 'services' and 'inetd'...
# Checking services from /etc/services.
--FAIL-- [inet003f] The port for service bootps is assigned to service bootp.

The indicated port number is assigned to the wrong service.  This
indicates either a misconfiguration in the services database, or a
possible sign of an intrusion.  This should be checked and corrected.
If it is not apparent why it is like this, the system should be checked
for other signs of intrusion.

--FAIL-- [inet003f] The port for service iso-tsap is assigned to service
tsap.

The indicated port number is assigned to the wrong service.  This
indicates either a misconfiguration in the services database, or a
possible sign of an intrusion.  This should be checked and corrected.
If it is not apparent why it is like this, the system should be checked
for other signs of intrusion.

--FAIL-- [inet003f] The port for service x400 is assigned to service webster.

The indicated port number is assigned to the wrong service.  This
indicates either a misconfiguration in the services database, or a
possible sign of an intrusion.  This should be checked and corrected.
If it is not apparent why it is like this, the system should be checked
for other signs of intrusion.

…<snip>…

# Performing check of system file permissions...
…<snip>…
--FAIL-- [perm007f] The owner of /etc/mail/aliases.dir should be root (owned
by uucp).

The /etc/aliases, /etc/aliases.dir and /etc/aliases.pag files should
not be writable by non-root users.  On SunOS 4 systems, these files are
shipped world writable.  The permissions should be 644 on all three
files.  If left writable, program aliases can be added which can allow
unauthorized access.

--FAIL-- [perm001w] /etc/mail/aliases.dir should not have group write.

The owner of the indicated file is not what is considered best for
security reasons.  Unless you have a specific reason for not changing
the ownership, this should be corrected.

--FAIL-- [perm007f] The owner of /etc/mail/aliases.pag should be root (owned
```

```
by uucp).

The /etc/aliases, /etc/aliases.dir and /etc/aliases.pag files should
not be writable by non-root users.  On SunOS 4 systems, these files are
shipped world writable.  The permissions should be 644 on all three
files.  If left writable, program aliases can be added which can allow
unauthorized access.

--FAIL-- [perm001w] /etc/mail/aliases.pag should not have group write.

The owner of the indicated file is not what is considered best for
security reasons.  Unless you have a specific reason for not changing
the ownership, this should be corrected.

…<snip>…

# Checking setuid executables...
…<snip>…
--FAIL-- [fsys001f] File /etc/lp/alerts/printer is a setuid script:
-r-sr-xr-x   1 lp       lp           203 Jul  2  1997 /etc/lp/alerts/printer

The listed file is a setuid script.  On most UNIX machines, it is not
possible to write a secure setuid script, due to a race condition in
the Operating System.  Even on systems where this is corrected, the
difficulties in writing a truly secure setuid script make them very
undesirable.  The setuid bits should be turned off of this file.

If you must run a script under another id, then perhaps the best
solution is to write a wrapper program in C which creates a safe
environment for the script, then exec()'s it.

…<snip>…
```

The reason for the first three alerts is that Gauntlet replaces many of the system configuration files upon installation. In particular, Gauntlet replaces the /etc/inet/services files (which /etc/services soft links to) with its own version of the file and renames the old file "services.PRE5.5". This older version of the services file, data 5/9/91, assigns iso-tsap to the tsap service and x400 to the webster service. TARA also reported bootp being assigned to the bootps service, however this was not observed in the /etc/services file installed by Gauntlet.

Note the following flower box from the /etc/services file on the GIAC Enterprises firewall:

```
#
# Network services, Internet style
#
# @(#)services 5.8 (Berkeley) 5/9/91

# Modified rick@tis.com
#TAG=OSI
#VER=V3.2
```

Tis.com owned the Gauntlet product before its sale to NAI/PGP. Similar assignment of iso-tsap to the tsap services was found in an OpenBSD services file here: http://openbsd.secsup.org/src/etc/services. Another interesting note is that the site

http://www.thenetworkadministrator.com/portnumber.htm assigns the x400 and webster services to the same port/protocol (103/tcp). Given this information, and the fact that Gauntlet replaced the services file, it is assumed an intrusion did not take place as stated as a possibility in the TARA output.

To address the system file permission alerts, the ownership and permission of /etc/mail/aliases.dir and /etc/mail/aliases.pag should be changed to root. The command "`chmod 644 /etc/mail/aliases.dir /etc/mail/aliases.pag`" should be run.

Tara found one setuid script when checking for setuid executables. Since the firewall is not connected to a printer, and no one but root logs on, the script /etc/lp/alerts/printer should have its permissions changed. Run the following command:
"`chmod 0555 script /etc/lp/alerts/printer`" so that the script is no longer setuid executable, but is executable by root [13].

For the identd.conf file, the only service started is the ident (or auth) daemon. Since attackers may query a box running ident for the user id of daemons (aka reverse ident scanning), it is suggested that this service be commented out in the identd.conf file. The service was most likely left after the initial Gauntlet product was installed to support servers that queried the firewall (such as mail servers that received SMTP traffic proxied by Gauntlet from an internal mail server).

Defensive Recommendation:

While it is not a security risk to leave the aliases iso-tsap and x400 to the services tsap and webster, removing the aliases will make the /etc/services file more consistent with newer versions of the /etc/services file distributed with Solaris 7 and 8. This change will also serve to remove the warnings from subsequent TARA scans.

To secure the file permission and suid script warnings, run the following commands described above:

```
chmod 644 /etc/mail/aliases.dir /etc/mail/aliases.pag
chmod 0555 script /etc/lp/alerts/printer
```

An additional defensive recommendation is to run the Center for Internet Security's Solaris Benchmarking Tool. Note that because of licensing issues, the auditor could not run this tool and provide the feedback and score to GIAC Enterprises in a for-profit business relationship. However, GIAC security personnel may download this tool for free and use it to assess and secure their own systems.

Finally, comment out the following line in /etc/inet/inetd.conf:

```
# auth stream tcp nowait nobody /usr/local/etc/identd identd
```

References:

1. http://www-arc.com/tara/index.shtml

2. http://openbsd.secsup.org/src/etc/services
3. http://www.thenetworkadministrator.com/portnumber.htm
4. http://www.cisecurity.org/bench_solaris.html
5. http://www.ja.net/CERT/JANET-CERT/prevention/cisco/cisco_acls.html

Vulnerability/Risk Item: Gauntlet 5.5 Firewall configuration vulnerabilities

Audit Result: Because Gauntlet wraps many of the OS's services (i.e. cron, syslog, inetd, etc.), the network-based audit will be primarily addressed in this section. Note that the firewall was configured to only allow access to the internal network by authorized IP addresses and IP blocks from the Internet. Similarly, authorized machines on the internal network could only access the Internet if their IP was assigned to a service group that permitted this access. This configuration effectively enforces a "deny what is not explicitly allowed" firewall access policy.

The network scans were conducted from a vulnerability assessment laptop (running Mandrake Linux 8.1) plugged into the switch in front of the firewall. The laptop was reconfigured with an IP address that was not trusted as an authorized external user by the firewall, a.b.c.9 (but still allocated to the DMZ subnet), which simulated an attack from an untrusted user on the Internet not attempting to spoof internal IP's. While the border router has ingress filtering configured to disallow spoofing of internal IP's, it was discovered that there are many authorized users who can access the internal development, production and firewall service networks via the SSL protocol and userid/password authentication. Because elaborate spoofing attacks such as ARP cache or DNS cache poisoning would have to be employed by external attackers on the Internet using these trusted IP addresses, it is believed that the probability of such a successful attack is small.

While the audit does not focus on the border router, its configuration is pertinent to the configuration of the firewall. The border router is configured to "allow all traffic that is not expressly denied". The business case for this configuration, which does not provide very good defense-in-depth, is that this allows the IDS sensor and sniffer to capture all the attacks from the Internet. This then allows the security administrators to fully asses the attacks being launched upon the network, and respond accordingly with ACL and configuration updates as needed. Also note that due to the router being located remotely across the campus via fiber, a hub or network tap could not be feasibly placed in front of the router for the IDS's to sniff from. On a positive security note, the router does have ingress/egress filtering and both inbound and outbound extended ACL's configured and implemented.

Nessus scan: The network-based vulnerability scanner Nessus was used to audit the network vulnerabilities of the firewall. While the firewall has 5 interfaces (one single-interface NIC and an additional quad-port NIC), only the primary interface for the internal development network (a.b.c.6) will be addressed by the Nessus report. The results of scanning the other interfaces were the same, and therefore were snipped for brevity.

The Nessus output from the vulnerability scan is available in the Append A – Nessus Report.

Nmap scan: While Nessus uses the Nmap engine in its vulnerability scan, the auditor felt that running an Nmap scan provides vulnerability information in a familiar format for most security administrators, and complements the information provided by Nessus.

The Nmap output from the vulnerability scan is available in the Appendix B – Nmap Output.

Remote "rcpinfo –p" scan: The "rpcinfo –p" command returns information from rpcbind concerning RPC services running on the target host [4]. This is useful information for an attacker, as they now know what services are running on which ports and may use this reconnaissance information to plan future attacks. Note that "giac9" is the hostname for a.b.c.9.

```
[root@giac9 root]# rpcinfo -p a.b.c.6
   program vers proto   port
    100000    4   tcp    111  portmapper
    100000    3   tcp    111  portmapper
    100000    2   tcp    111  portmapper
    100000    4   udp    111  portmapper
    100000    3   udp    111  portmapper
    100000    2   udp    111  portmapper
1342177279    5   tcp  32772
1342177279    1   tcp  32772
```

Remote telnet attempt: Telnet is a very dangerous application to run anywhere on the network, due to the fact that the password and all payload is transported in clear text. To prove that the firewall is configured to deny telnet connections to itself from attackers, the following command was executed.

```
[root@giac9 root]# telnet a.b.c.6
Trying a.b.c.6...
Connected to a.b.c.6 (a.b.c.6).
Escape character is '^]'.
unknown/ a.b.c.9 is not authorized to use the telnet proxy
Connection closed by foreign host.
```

Remote telnet attempt to port 25: A telnet attempt to port 25 was also executed to show that a mail banner (whether obfuscated or not) could not be retrieved.

```
[root@giac9 root]# telnet a.b.c.6 25
Trying a.b.c.6...
Connected to a.b.c.6 (a.b.c.6).
Escape character is '^]'.
Connection closed by foreign host.
```

Remote ftp attempt: FTP, like telnet, is a very dangerous service to run on the network due to the password being sent in the clear. To show that FTP connections from the Internet or DMZ to the firewall are denied, the following command was executed.

```
[root@giac9 root]# ftp a.b.c.6
Connected to a.b.c.6.
421 Service not available, remote server has closed connection
      ftp>
```

Significance of Finding(s):

Nessus scan: According to the Nessus scan, the most dangerous "hole" was that port 80 (HTTP) was listening. Since the web server is located behind the firewall, and traffic is proxied via the firewall and checked against a list of authorized external IP's, the risk of this vulnerability is minimal. What Nessus did identify as a vulnerability is the dll (dynamic link library) /_vti_bin/_vti_aut/dvwssr.dll is installed on the webserver. This is a serious vulnerability on the IIS webserver, and should be removed.

Nessus found the following ports listening on the firewall:

general/tcp (Security notes found)
ftp (21/tcp) (Security notes found)
telnet (23/tcp) (Security warnings found)
smtp (25/tcp) (Security notes found)
domain (53/tcp) (Security warnings found)
domain (53/udp)
http (80/tcp) (**Security hole found**)
sunrpc (111/tcp) (Security warnings found)
sunrpc (111/udp) (Security warnings found)
ident (113/tcp) (Security notes found)
xdmcp (177/udp) (Security warnings found)
https (443/tcp) (Security notes found)
isakmp (500/udp)
syslog (514/udp)
unknown (6000/tcp) (Security warnings found)
unknown (32771/tcp) (Security notes found)
unknown (32772/tcp) (Security warnings found)
unknown (32776/udp)
unknown (8004/tcp)
general/icmp (Security warnings found)
general/udp (Security notes found)

The ftp and telnet protocols are only listening for internally initiated connections from the internal subnet, and only from specifically defined IP's on the internal subnet. The ftp protocol is allowed for virus updates on internal Windows hosts. Telnet should be disabled and SSH should be deployed on the internal subnet for administrative use (if necessary). Note that Nessus had the following recommendation: "*Solution : Comment out the 'telnet' line in /etc/inetd.conf*." Per the inetd.conf file in the shown in the Tara section, the telnet service is disabled. What is listening on the firewall is the Gauntlet telnet proxy, `tn-gw`.

SMTP is listening since the firewall proxies mail to the internal mail server. This is perfectly reasonable, and an additional check of the firewall's mail-relaying configuration (in the Gauntlet espm GUI) shows that spammers may not relay mail.

BIND is listening on ports 53 tcp and udp. Port 53 tcp is for zone transfers, or queries where the answer section of the response is truncated when the response is too large for udp to accommodate. Since BIND has been configured to only allow zone transfers from authorized corporate DNS servers, this is an acceptable risk. To confirm this, the following command was issued from an external IP address (a.b.c.9) in the DMZ that was configured to be an un-trusted user on the firewall (as would be an attacker from the Internet):

```
[root@giac9 root]# dig @a.b.c.6 axfr giac.f-cookies.com
; <<>> DiG 9.2.0rc3 <<>> @a.b.c.6 axfr giac.f-cookies.com
;; global options:  printcmd
; Transfer failed.
```

Port 53 udp is the port on which queries are issued and answered, and is normal for a network that is running DNS. Also note that BIND version requests are done using UDP. Per the Nessus report details, the GIAC firewall was configured to have a BIND version of "Cray C90". This was accomplished by adding the following line to the options block of the /etc/named.conf file:

```
version "Cray C90";
```

What should be addressed is the BIND version and the machine on which BIND is running. See the Risk from third-party software section below.

The rpbind service was listening on port 111 (tcp and udp), and ports 32771-2 (tcp) and 32776 (udp). These are the well-known RPC ports (111), and the "sometimes RPC", or ghostmapper, ports 32771,32772 and 37776. RPC's have well known vulnerabilities in certain versions, such as CA-1998-11 and CA-2002-10. It is recommended that RPC services be turned off, but keep in mind that the firewall will no longer be able to run X-windows, which the CDE (Solaris Common Desktop Environment) requires to operate. To still be able to run the Gauntlet admin GUI, a remote internal firewall administration machine with X-windows running should be configured with the GUI. Installing the GUI on this machine and configuring the firewall for remote admin from the internal network will mitigate the risk that running RPC's on the firewall poses.

As stated in the defensive recommendations section of the Solaris 2.6 OS configuration vulnerabilities section, comment out the line that enables the ident/auth service in the /etc/inet/inetd.conf file.

Per the Nessus recommendations for the xdmcp service, disable this service so that the port is not longer listening.

Nessus found the HTTPS service, port 443 tcp, was listening. Given that authorized users can connect to the backend web/application server using SSL, this is an acceptable risk. A server-side 128-bit SSL certificate on the internal web/application servers also helps mitigate the risk to external users by authenticating the server's identity.

The isakmp port is listening on the firewall to support the Gauntlet VPN software. This poses no significant risk if the VPN is configured correctly. Note that currently the Gauntlet VPN is not currently configured, even though the software is installed.

Syslog is listening on port 514 udp. Note that the firewall logs messages to the /var/log/messages file (the log file for Gauntlet connection and securityalert messages), as well as to the internal log server. The firewall will accept syslog messages from external users per the configuration of the /etc/syslog.conf file, but the router does not accept connections from external users on port 514 udp via the extended ACL on the external eth0 interface.

Port 6000 is X-windows, and should be disabled on the firewall. Port 8004 is used by the Gauntlet GUI daemon, espmd. A "ps –ef" on port 8004 is shown below:

```
root@giac6.giac.f-cookies.com:/>ps -ef | grep 8004
    root   948     1  0   Jun 05 ?        0:00 ./mgmt/espmd -as espmd -
service SV8004X -daemon 8004
    root 22631  1382  0 08:09:20 pts/5    0:00 grep 8004
    root 22606   948  0 08:04:04 ?        0:00 ./mgmt/espmd -as espmd -
service SV8004X -daemon 8004
```

The general/icmp warnings state that a ICMP subnet mask and timestamp request are possible from the DMZ by an attacker. This poses a risk since attackers could use the subnet mask to determine the broadcast address of the subnet, and possibly deduce the other broadcast addresses of a variably subnet'ed IP block. Once the attacker has this information, they could use it to Smurf the network if IP directed-broadcasts are allowed. Since the border router does not allow any ICMP packets past its interior interface (including IP directed-broadcasts), the risk is mitigated. However, the firewall should be configured to not allow an ICMP subnet mask request to provide defense-in-depth.

The general/udp warnings refer to a traceroute from the attacking machine to the firewall. Again, the border router blocks all traceroutes to the interior network.

Nmap scan: The Nmap scan did not find anything new that the Nessus scan did not find, but note that Nmap did not find that port 32776 udp was open at the time of the Nmap scan. Port 32776 is the well-known port for the rpc.spray service [14]. This can be explained, as Nessus and Nmap were not run concurrently in terms of time. Nmap was run at a later date during the audit.

Remote "rcpinfo –p" scan: The "rpcinfo –p" queries the rpcbind daemon, and confirms that the portmapper is running on port 111, as well as an RPC service listening on port 32772.

Remote telnet attempt: As noted in the Nessus and Nmap output, the Gauntlet telnet proxy was listening, but only for internally initiated connections (and only then from authorized IP addresses).
Remote telnet attempt to port 25: Similarly, a telnet to port 25 to determine the mail banner was not successful.

Remote ftp attempt: Finally, an ftp attempt to the firewall was tried to show that all ftp attempts from external IP's is denied.

Defensive Recommendation:

- Per CVE : CVE-2000-0260, remove the /_vti_bin/_vti_aut/dvwssr.dll file on the backend webserver.
- Disable all RPC services on the firewall and run the Gauntlet GUI from an internal Solaris machine equipped with CDE.
- Disable the xdmcp service.
- Review the VPN configuration.
- Disable the X-windows service.
- Disable the espmd daemon on the firewall, and install it on a separate management box on the interior network.
- Configure the firewall to respond to ICMP subnet mask requests.

References:

1. http://cgi.nessus.org/cve.php3?cve=CVE-2000-0260

Vulnerability/Risk Item: Solaris 2.6 OS hardening

Audit Result:

OS Hardening Packages: Since Gauntlet disables most of the services normally started in the /etc/inet/inetd.conf file (except for the ident/auth service) by default, some administrators do not harden the Solaris OS. This was found to be true of the GIAC firewall. However, it is highly recommended that a Solaris hardening package such as YASSP or JASS be used to harden the firewall in addition to what Gauntlet does by default.

Note that YASSP uses the Solaris fix-modes program to secure Solaris file permissions, and also performs many of the recommendations to follow with its SECclean script (see http://www.yassp.org/internal.html for more information). If YASSP is installed on the firewall, some of the following recommendations would not need to be applied (such as editing the netconfig file to add selected ndd settings). However, defense-in-depth is attained by installing a hardening package and then hardening other operating system files by hand. In addition, this also serves to educate the administrator on what the hardening package does and does not do.

Recommended Network Parameter Changes in /etc/init.d/netconfig: The firewall may be further secured by tuning networking parameters. To do this, the parameters may be set after the /etc/rc2.d/S69inet script is run, in a new file called /etc/init.d/netconfig that is soft linked to /etc/rc2.d/S69netconfig [36].

Note that the S69inet script is soft linked to /etc/init.d/inetinit:

```
root@giac6.giac.f-cookies.com:/etc/rc2.d>ls -al S69inet
lrwxrwxrwx   1 root     other         20 Apr  3  2001 S69inet ->
/etc/init.d/inetinit*
```

Furthermore, Gauntlet has replaced the /etc/init.d/inetinit script with a modified version:

```
root@giac6.giac.f-cookies.com:/etc/init.d>ls -al inetinit*
-rwxr-x---   1 root     other        146 Jul 30  1999 inetinit*
-rwxr--r--   1 root     other       5645 Apr  3  2001 inetinit.PRE5.5*
```

The contents of the new/etc/init.d/inetinit file are as follows:

```
root@giac6.giac.f-cookies.com:/etc/init.d>cat inetinit
#
# Copyright (c) 1996-1999 Network Associates, Inc.
# All righs reserved
#
# Gauntlet Firewall Software network startup script
sh /etc/netstart
```

Note that /etc/netstart tunes the following parameters:

```
root@giac6.giac.f-cookies.com:/etc>cat netstart
      …<snip>…
# Turn on IP forwarding so firewall can route packets
ndd -set /dev/ip ip_forwarding 1

# Change inactivity timeout interval to 1 second
ndd -set /dev/tcp tcp_close_wait_interval 60000
      …<snip>…
```

Purge Unnecessary rc2.d Boot Files: A list of the present /etc/rc2.d boot files (or startup scripts) are shown below:

```
root@giac6.giac.f-cookies.com:/>ls -al /etc/rc2.d
total 164
drwxrwxr-x   2 root     sys         1536 Jun 22  2001 ./
drwxrwxr-x  31 root     sys         3584 Sep  5 16:39 ../
-rwxr--r--   1 root     sys         5645 Jul 15  1997
disabled.S69inet.PRE5.5*
-rwxr--r--   1 root     sys         2891 Jul 15  1997 disabled.S71rpc.PRE5.5*
-rwxr--r--   1 root     sys         4386 Jul 15  1997
disabled.S72inetsvc.PRE5.5*
-rwxr--r--   4 root     sys         1236 Jul 15  1997
disabled.S73nfs.client.PRE5.5*
-rwxr--r--   4 root     sys          602 Jul 15  1997
disabled.S74autofs.PRE5.5*
-rwxr--r--   4 root     sys          568 Jul 15  1997
disabled.S76nscd.PRE5.5*
-rwxr--r--   3 root     sys         2452 Jul 15  1997
disabled.S85power.PRE5.5*
-rwxr--r--   4 root     sys          976 Aug 22  2000
disabled.S88sendmail.PRE5.5*
lrwxrwxrwx   1 root     root          13 Apr  2  2001 K20spc ->
../init.d/spc*
-rwxr--r--   5 root     sys         1738 Jul 15  1997 K60nfs.server*
-rwxr-xr-x   3 root     sys          677 Jul 15  1997 K76snmpdx*
```

```
-rwxr-xr-x   3 root     sys          951 Jul 15  1997 K77dmi*
-rw-r--r--   1 root     sys         1369 Jul 15  1997 README
-rwxr--r--   3 root     sys          619 Jul 15  1997 S01MOUNTFSYS*
-rwxr--r--   2 root     sys         2272 Jul 15  1997 S05RMTMPFILES*
-rwxr--r--   2 root     sys          822 Jul 15  1997 S20sysetup*
-rwxr--r--   2 root     sys          548 Jul 15  1997 S21perf*
-rwxr-xr-x   2 root     other       1644 Jul  2  1997 S30sysid.net*
-rwxr--r--   4 root     sys         1474 Jan 15  1998 S47asppp*
lrwxrwxrwx   1 root     other         20 Apr  3  2001 S69inet ->
/etc/init.d/inetinit*
-rwxr--r--   2 root     sys          212 Jul 15  1997 S70uucp*
lrwxrwxrwx   1 root     other         15 Jun 22  2001 S71rpc ->
/etc/init.d/rpc*
-rwxr--r--   1 root     other       2891 May 23  2001 s71rpc*
-rwxr-xr-x   2 root     other       1498 Jul  2  1997 S71sysid.sys*
-rwxr-xr-x   2 root     other       1558 Jul  2  1997 S72autoinstall*
lrwxrwxrwx   1 root     other         19 Apr  3  2001 S72inetsvc ->
/etc/init.d/inetsvc*
-rwxr-xr-x   3 root     other        663 Apr 11  2001 S73bind*
-rwxr--r--   2 root     sys          579 Jul 15  1997 S73cachefs.daemon*
-rwxr--r--   4 root     sys          621 Jul 15  1997 S74syslog*
-rwxr--r--   4 root     sys         1266 Jul 15  1997 S74xntpd*
-rwxr--r--   4 root     sys          513 Jul 15  1997 S75cron*
-rwxr--r--   4 root     sys          403 Jul 15  1997 S80lp*
-rwxr--r--   2 root     sys          218 Jul 15  1997 S80PRESERVE*
lrwxrwxrwx   1 root     root          13 Apr  2  2001 S80spc ->
../init.d/spc*
-rwxr--r--   4 root     sys          492 Jul 15  1997 S88utmpd*
lrwxrwxrwx   1 root     root          31 Apr  2  2001 S89bdconfig ->
../init.d/buttons_n_dials-setup*
-rwxr-xr-x   2 root     sys         1707 Apr 27  1998 S91afbinit*
-rwxr--r--   2 root     sys         1400 May 20  1997 S91agaconfig*
-rwxr-xr-x   2 root     sys         2433 Nov 25  1996 S91leoconfig*
-r-xr-xr-x   2 root     sys         1159 Jun 27  1997 S92rtvc-config*
-rwxr--r--   3 root     sys          524 Jul 15  1997 S92volmgt*
-rwxr--r--   2 root     sys          373 Jul 15  1997 S93cacheos.finish*
-rwxr--r--   4 root     sys          460 Jul 15  1997 S99audit*
-r-xr-xr-x   4 root     other       2613 Apr  4  2001 S99dtlogin*
```

Purge Unnecessary NFS and Crontab Files: The following NFS and Crontab files exist on the GIAC firewall:

```
root@giac6.giac.f-cookies.com:/etc>ls -al auto_*
-rw-r--r--   1 root     bin           50 Apr  2  2001 auto_home
-rw-r--r--   1 root     bin          113 Apr  2  2001 auto_master

root@giac6.giac.f-cookies.com:/etc/dfs>ls -al dfstab
total 14
drwxrwxr-x   2 root     sys          512 Apr  2  2001 ./
drwxrwxr-x  31 root     sys         3584 Sep  7 11:18 ../
-rw-r--r--   1 root     sys          393 Apr  2  2001 dfstab

root@giac6.giac.f-cookies.com:/var/spool/cron/crontabs>ls -al
total 26
drwxr-xr-x   2 root     sys          512 Jun 26 11:14 ./
drwxr-xr-x   4 root     sys          512 Apr  2  2001 ../
```

```
-rw-r--r--   1 root     sys          190 Apr  2  2001 adm
-r--r--r--   1 root     root         750 Apr  2  2001 lp
-r--------   1 root     root        4661 Jun 26 11:14 root
-rw-r--r--   1 root     sys          308 Apr  2  2001 sys
-r--------   1 root     uucp        2819 Jun 26 11:14 uucp
```

Note that since root is the only authorized user account on the firewall (besides accounts created on the firewall such as "nobody"), limiting crontab usage with cron.allow and cron.deny files is not necessary.

PROM Settings: The PROM security-mode setting is set to none by default, which is the current setting on the GIAC firewall [36]. The PROM oem-banner is also empty by default on the GIAC firewall [36].

Recommended Changes to /etc/system:

Stack protection is not enabled, and core dump files are not restricted on the firewall.

Significance of Finding(s):

OS Hardening Packages: Given that a hardening tool was not run on the firewall, and the TARA scan found several serious vulnerabilities, the OS was not sufficiently hardened.

Recommended Network Parameter Changes in /etc/init.d/netconfig: Note that the firewall must be able to route packets, so the following setting in /etc/netstart is appropriate:

```
# Turn on IP forwarding so firewall can route packets
ndd -set /dev/ip ip_forwarding 1
```

However, many other network parameter settings can be applied to the firewall that will help secure it, as will be shown in the defensive recommendations section below.

Purge Unnecessary rc2.d Boot Files: Per [36], the following boot files should be strongly considered for removal so that "sys-unconfig" cannot be run (in the case of the auto configuration files), and since RPC and NFS services have been known to have multiple vulnerabilities [40]. Similarly, the Expreserve service is known to be vulnerable, per http://www.cert.org/advisories/CA-1996-19.html:

Auto Configuration Files:

```
-rwxr-xr-x   2 root     other       1644 Jul  2  1997 S30sysid.net*
-rwxr-xr-x   2 root     other       1498 Jul  2  1997 S71sysid.sys*
-rwxr-xr-x   2 root     other       1558 Jul  2  1997 S72autoinstall*
```

RPC/NFS Files:

[Note: The boot file `s71rpc` will not execute do to the "s" being lower case. It is not clear why this boot file has a lower case "s", but this is a common trick that administrators use to force a

boot file not to execute. Although it does not execute, it is recommended that it be removed anyway so that a well intentioned new administrator does not change it to be a capital "S".]

```
lrwxrwxrwx   1 root     other         15 Jun 22  2001 S71rpc ->
/etc/init.d/rpc*
-rwxr--r--   1 root     other       2891 May 23  2001 s71rpc*
-rwxr--r--   2 root     sys          579 Jul 15  1997 S73cachefs.daemon*
```

Removed Expreserve service that allows recovery of data from a vi session [38]:

```
-rwxr--r--   2 root     sys          218 Jul 15  1997 S80PRESERVE*
```

Note that Gauntlet upon installation disabled the following boot files by default:

```
-rwxr--r--   1 root     sys         2891 Jul 15  1997 disabled.S71rpc.PRE5.5*
-rwxr--r--   1 root     sys         4386 Jul 15  1997
disabled.S72inetsvc.PRE5.5*
-rwxr--r--   4 root     sys         1236 Jul 15  1997
disabled.S73nfs.client.PRE5.5*
-rwxr--r--   4 root     sys          602 Jul 15  1997
disabled.S74autofs.PRE5.5*
-rwxr--r--   4 root     sys          568 Jul 15  1997
disabled.S76nscd.PRE5.5*
-rwxr--r--   3 root     sys         2452 Jul 15  1997
disabled.S85power.PRE5.5*
-rwxr--r--   4 root     sys          976 Aug 22  2000
disabled.S88sendmail.PRE5.5*
```

Purge Unnecessary NFS and Crontab Files: Since the firewall does not have any NFS mounted directories, the adm crontab file is empty, and the firewall is not connected to a printer, the NFS auto_* and adm and lp crontab files are not required on the firewall [36].

PROM Settings: The security-mode PROM setting should be set to "command" so that the administrator is prompted for a password when any `eeprom`, command is issued besides a normal reboot, including a boot to single user mode or a boot to reconfigure (boot -s and boot -r) [36]. This also allows the firewall to reboot without the operator having to be present to type in the password (as is the case when the setting is "full") [36].

In addition, the oem-banner should be set so that a banner message is displayed when the system is started up. Note that this banner will "*override the standard Sun banner*", and have the effect of hiding the IP address, MAC and RAM allocation upon startup [36].

Recommended Changes to /etc/system: Note that from the "diff" command performed below, Gauntlet modified and replaced the /etc/system file:

```
root@giac6.giac.f-cookies.com:/etc>diff system system.PRE5.5
82d81
< moddir: /platform/sun4u/kernel /gauntlet /kernel /usr/kernel
```

From the /etc/system file, the following comment is made:

** moddir:*
***
** Set the search path for modules. This has a format similar to the*
** csh path variable. If the module isn't found in the first directory*
** it tries the second and so on. The default is /kernel /usr/kernel*
***
** Example:*
** moddir: /kernel /usr/kernel /other/modules*

Thus, Gauntlet has set the search path for modules to:
`/platform/sun4u/kernel /gauntlet /kernel /usr/kernel`.

Defensive Recommendation:

OS Hardening Packages: It is highly recommended that YASSP or JASS be run on the firewall. Note that a YASSP'ified (or otherwise hardened Gauntlet firewall) is not supported by the Gauntlet technical support personnel. In response to a post by the auditor to the Gauntlet mailing list (show below [15]),

> "*YASSP replaces some /etc/init.d files with its own "canned" /etc/init.d files. One of the files that gets replaced is the one that starts the Gauntlet drivers. Gauntlet initializes its drivers using this sequence:*
>
> *- execute /etc/rc2.d/S69inet, which is a link to /etc/init.d/inetinit*
> *- /etc/init.d/inetinit calls /etc/netstart*
> *- /etc/netstart initializes the Gauntlet drivers*
>
> *When Gauntlet is installed, it creates /etc/netstart and replaces /etc/init.d/inetinit with its own version, which calls /etc/netstart. When YASSP is installed it replaces /etc/init.d/inetinit with its own script. The YASSP script does not call the Gauntlet /etc/netstart script. If YASSP is installed after Gauntlet, Gauntlet will not come up because the /etc/init.d/inetinit script no longer calls /etc/netstart.*
>
> *This is the fix (after installing YASSP over Gauntlet 6.0, 64-bit version):*
>
> *# cp /etc/init.d/inetinit /etc/init.d/inetinit.YASSP_version*
> *# cp /etc/init.d/inetinit.SUN_Before_YASSP /etc/init.d/inetinit (The .SUN_Before_YASSP extension is what YASSP adds to the files it replaces)*
>
> *Thanks to Scott Oksanen for his notes on this.*
>
> *-Jeff"*

one of Gauntlet's best tech support personnel (Meenoo Shivdasani) had this to say:

> *"> This is the fix (after installing YASSP over Gauntlet 6.0,*

> 64-bit version):
>
> # cp /etc/init.d/inetinit /etc/init.d/inetinit.YASSP_version
> # cp /etc/init.d/inetinit.SUN_Before_YASSP /etc/init.d/inetinit (The
> .SUN_Before_YASSP extension is what YASSP adds to the files
> it replaces)

These two files are not the only files that YASSP installs. YASSP also makes ndd tweaks that can be incompatible with the proper functioning of the firewall.

Additionally, a Gauntlet installation that has been YASSP'ified, either prior to the installation of Gauntlet or post-installation is not a supported configuration.

M" [16].

Meenoo is absolutely correct, YASSP does perform an array of ndd commands in its hardening process. However, the auditor has used YASSP'ified Gauntlet firewalls in a production setting and found them to be quite stable if the installation notes are followed above. The fact that the firewalls needs additional hardening after installing Gauntlet is disturbing, not to mention the fact that Gauntlet tech support will not support trouble tickets on hardened firewalls. Regardless, it is the auditor's recommendation that your Gauntlet firewall be hardened with a tool such as YASSP or JASS.

Recommended Network Parameter Changes in /etc/init.d/netconfig: Per [36], create the /etc/init.d/netconfig and /etc/rc2.d/S69netconfig file. The /etc/rc2.d/S69netconfig file is soft linked to /etc/init.d/netconfig, and serves to execute the netconfig script immediately after S69inet when the startup scripts in /etc/rc2.d are run on bootup. Note that these parameters may be rendered ineffective by the firewall configuration. For example, if the firewall does not allow responses to any ICMP packets (ie. ICMP directed broadcast echo request) from the Internet (or internal network). However, the settings will provide defense-in-depth should the firewall configuration change, either by accident or malicious intent.

Consider adding the following parameter settings to the newly created /etc/init.d/netconfig file [36]. Keep in mind these settings may or may not have an adverse affect up on the firewall. Backup your Gauntlet configuration before making these changes and rebooting.

Limit SYN Flood Attacks:

```
ndd -set /dev/tcp tcp_conn_req_max_q0 8192
ndd -set /dev/tcp tcp_ip_abort_cinterval 60000
```

Limit Smurf Amplifier and Mapping Attacks:

```
ndd -set /dev/ip ip_respond_to_timestamp 0
ndd -set /dev/ip ip_respond_to_timestamp_broadcast 0
ndd -set /dev/ip ip_respond_to_address_mask_broadcast 0
ndd -set /dev/ip ip_forward_directed_broadcasts 0
```

Limit ARP Timeoutes to Help Block ARP Poisoning Attacks:

```
ndd -set /dev/arp arp_cleanup_interval 60000
ndd -set /dev/ip_ire_flush_interval 60000
```

Block ICMP Redirects:

```
ndd -set /dev/ip ip_ignore_redirect 1
ndd -set /dev/ip ip_send_redirectes 0
```

Limit Source Routed Packets:

```
ndd -set /dev/ip ip_forward_src_routed 0
```

Block ICMP Directed Broadcasts Responses:

```
ndd -set /dev/ip ip_respond_to_echo_broadcast 0
```

Finally, perform the following commands on the /etc/rc2.d/S69netconfig and /etc/init.d/netconfig files [36]:

```
touch /etc/rc2.d/S69netconfig
chmod 744 /etc/rc2.d/S69netconfig
chown root:root /etc/init.d/netconfig
chmod 744 /etc/init.d/netconfig
ln -s /etc/init.d/netconfig /etc/rc2.d/S69netconfig
```

Purge Unnecessary rc2.d Boot Files: Remove the following boot files:

Auto Configuration Files:

```
-rwxr-xr-x   2 root     other       1644 Jul  2  1997 S30sysid.net*
-rwxr-xr-x   2 root     other       1498 Jul  2  1997 S71sysid.sys*
-rwxr-xr-x   2 root     other       1558 Jul  2  1997 S72autoinstall*
```

RPC/NFS Files:

```
lrwxrwxrwx   1 root     other         15 Jun 22  2001 S71rpc ->
/etc/init.d/rpc*
-rwxr--r--   1 root     other       2891 May 23  2001 s71rpc*
-rwxr--r--   2 root     sys          579 Jul 15  1997 S73cachefs.daemon*
```

Removed Expreserve service that allows recovery of data from a vi session (but has been known to be vulnerable) [38]:

```
-rwxr--r--   2 root     sys          218 Jul 15  1997 S80PRESERVE*
```

Purge Unnecessary NFS and Crontab Files: Perform the following commands to remove the unnecessary files [36]:

```
rm /etc/auto_home
rm /etc/auto_master
rm /etc/dfs/dfstab
rm /var/spool/adm
rm /var/spool/lp
```

PROM Settings: Configure the PROM security-mode and oem-banner settings with the following commands:

```
eeprom security-mode=command
eeprom oem-banner="<banner message goes here>"
eeprom oem-banner\?=true
```

Recommended Changes to /etc/system: Edit the /etc/system file so that stack protection is enabled (which prevents "*stack-smashing attacks*", or buffer overflows), and so that core files are not created (since this is a firewall and not a software developer's workstation) [36].

To do this, add the following to the /etc/system file:

```
set noexec_user_stack = 1
set noexec_user_stack_log = 1
set sys:coredumpsize = 0
```

Note that a common recommendation is to limit the number of file descriptors a process can have in the /etc/system file [36]. However, given that this is a firewall, many log files are created and processes are created. Thus, limiting the number of file descriptors could impact the operability of the firewall. Therefore, carefully consider setting the *rlim_fd_max* and *rlim_fd_min* parameters.

References:

1. http://www.yassp.org
2. http://wwws.sun.com/software/security/jass
3. http://marc.theaimsgroup.com/?l=gauntlet-user&m=99859896010055&w=2
4. http://marc.theaimsgroup.com/?l=gauntlet-user&m=99860411027272&w=2

Vulnerability/Risk Item: Risk from third-party software

Audit Result: There are no known vulnerabilities in Perl 5.005_03, make 3.79.1 or tcsh 6.07. There is a know vulnerability in the Redhat tcsh-6.07.09-1 package, but this obviously does not apply to a Solaris-based firewall.

The JRE (Java Runtime Loader) version 1.1.6 software installed by Gauntlet does have a security vulnerability that "*can fail to securely confine the activity of an untrusted Java class. In particular, an untrusted Java class might be able to call into a disallowed area.*" [17]. See the "L-032: Class Loading Vulnerability in Sun Java (TM) Runtime Environment" vulnerability located here: http://www.ciac.org/ciac/bulletins/l-032.shtml.

The ISC version of BIND 8.2.3-REL (which the GIAC firewall is running) has a known buffer overflow in the DNS resolver library, libbind. The CERT advisory is located here: http://www.cert.org/advisories/CA-2002-19.html. This is a serious vulnerability as an attacker could run arbitrary code or cause a DoS condition on the machine running BIND. A complete list of BIND vulnerabilities, and which versions they apply to, is located here: http://www.isc.org/products/BIND/bind-security.html.

A critical risk posed by the BIND software is that it is running as root, and is not chroot'ed.

```
root@giac6.giac.f-cookies.com:/>ps -ef | grep named
    root   164     1  0   Apr 17 ?        0:04 /usr/local/sbin/named -f
/etc/dns/named.conf
```

It is highly recommended that while the firewall is offline and BIND is being updated, that you also consider configuring split DNS on the firewall with the named daemons chroot'ed. David Lugo has written a paper on how to do just that, located here: http://www.etherboy.com/dns/chrootdns.html.

Be sure to add the "`query source port * 53`" directive to the options block of named.conf since BIND will be chroot'd. Another option is that you run a separate DNS server on the firewall service network, and use the Gauntlet DNS proxy for queries and responses to the protected DNS server. Given that the DNS server would be protected by the firewall, isolated to a service network, and BIND would be chroot'ed, this would be the more secure option. Given the limited budget of the GIAC network, however, it would be less costly to run a chroot'ed split DNS architecture on the firewall.

Significance of Finding(s): The fact that the JRE and BIND software have vulnerabilities that could allow an attacker to run arbitrary code, it is critical that these packages be updated as soon as possible. Since the firewall is running a vulnerable version of BIND, the integrity of the firewall and entire network could be jeopardized.

Defensive Recommendation: Upgrade to the newest JRE at http://wwws.sun.com/software/solaris/jre/index.html. Note that the JRE is used to run the firewall GUI, so if the GUI software is removed from the firewall and installed elsewhere, the need for the JRE upgrade may be unnecessary. However, in the case the need exists or arises for an Java application, it is wise to update the JRE version to mitigate the risk this vulnerability poses.

It is recommended that the firewall be disconnected from the network and updated with the newest version of BIND (currently 8.3.3 or 9.2.1), available at http://www.isc.org/products/BIND.

Finally, add the allow-query directive to the named.conf file's option block to limit DNS queries only to authorized servers [19]:

```
allow-query {external.dns.server.ip.1;
             external.dns.server.ip.2;
             internal.network1.address/subnetmask;
             internal.network2.address/subnetmask;
             …
             internal.networkx.address/subnetmask;
};
```

References:

1. http://www.ciac.org/ciac/bulletins/l-032.shtml
2. http://www.cert.org/advisories/CA-2002-19.html
3. http://wwws.sun.com/software/solaris/jre/index.html

4. http://www.isc.org/products/BIND

Vulnerability/Risk Item: Firewall administrative practices

Audit Result: The following topics address various firewall administrative practices on the GIAC Enterprises firewall.

Logging: The firewall is configured to syslog all messages written to /var/log/messages (Gauntlet writes to /var/log/messages instead of /var/adm/messages) to the central log server (note that the /etc/hosts file has "loghost" defined as the internal syslog server's IP address). In addition, the firewall also mails the contents of the /var/log/messages file (known as the "system check") and the Gauntlet "daily" reports to the firewall administrator for review. The current syslog.conf file is shown below:

```
#ident "@(#)syslog.conf 1.3 93/12/09 SMI" /* SunOS 5.0 */
#
# Copyright (c) 1991-1993, by Sun Microsystems, Inc.
#
# syslog configuration file.
#
# This file is processed by m4 so be careful to quote (`') names
# that match m4 reserved words. Also, within ifdef's, arguments
# containing commas must be quoted.
# Note: Have to exclude user from most lines so that user.alert
# and user.emerg are not included, because old sendmails
# will generate them for debugging information. If you
# have no 4.2BSD based systems doing network logging, you
# can remove all the special cases for "user" logging.
#
*.err;kern.debug;daemon.notice;auth.notice;user.none /var/log/messages
*.err;kern.debug;daemon.notice;auth.notice;user.none @loghost
#kern.debug @loghost
*.alert;kern.err;daemon.err;user.none operator
*.alert;user.none root
*.emerg;user.none *
# if a non-loghost machine chooses to have authentication messages
# sent to the loghost machine, un-comment out the following line:
auth.debug ifdef(`LOGHOST', /var/log/authlog, @loghost)
mail.debug ifdef(`LOGHOST', /var/log/messages, @loghost)
mail.debug ifdef(`LOGHOST', /var/log/messages, 127.0.0.1)
#
# non-loghost machines will use the following lines to cause "user"
# log messages to be logged locally.
#
ifdef(`LOGHOST', ,
user.err /dev/console
user.err /var/log/messages
user.alert `root, operator'
user.emerg *
)
```

Based on the syslog.conf file, the following syslog facility/severity combinations are sent to the internal syslog server (since the firewall is not the log server, and its host name is not loghost).

This functionality is defined in the syntax

```
auth.debug ifdef(`LOGHOST', /var/log/authlog, @loghost)
```

which says "if the local host is the loghost (or central syslog server), then log the message to /var/log/authlog, otherwise log it to the machine whose IP address is defined by the hostname `loghost` in /etc/hosts" [20]. Since this machine is the firewall, auth.debug messages will be logged to the central syslog server (see the network_diagram for a view of the network architecture).

Syslog Facility/Severity Setting	Meaning
*.err	Log all messages with any facility and the "err" severity
kern.debug	Log all messages with the "kern" facility and the "debug" severity
daemon.notice	Log all messages with the "daemon" facility and the "notice" severity
auth.notice	Log all messages with the "auth" facility and the "notice" severity
auth.debug	Log all messages with the "auth" facility and the "debug" severity
mail.debug	Log all messages with the "mail" facility and the "debug" severity

Because the facility/severity setting of "user.none" is also defined for all messages sent to the loghost, messages that have the facility "user" (with any severity setting) are **not** logged to the syslog server.

Gauntlet also compresses a day's worth of logs (using gzip) and stores the file in the /var/log directory on local disk. These files can be uncompressed on the firewall and searched if desired, or can be used to supplement any logs not recorded by the log server is the syslog daemon died or packets were dropped (since syslog use UDP).

Finally, sufficient disk space should be allocated to the /var partition to insure adequate space is available for logging. The GIAC Enterprises firewall was found to have adequate disk space:

```
root@giac6.giac.f-cookies.com:/var>df -k .
Filesystem            kbytes    used   avail capacity  Mounted on
/dev/dsk/c0t0d0s3    18783017  712390 17882797     4%    /var
```

Integrity Checks: Based on discussions with the firewall administrator, an integrity database was created just after the firewall was installed and configured. The database was saved to floppy and stored in the server room on the designated backup tape shelf. Integrity checks, and updated databases, are not performed on a normal schedule.

Password Policy and Storage: The specific password policy for the GIAC network, for security reasons, will not be divulged in this report. However, it was found that a "strong" password policy was in use, and that the firewall password was unique to the firewall (ie. this password was not used anywhere else in the network).

By default, the /etc/default/passwd file was set to have a minimum length password of 6:

```
root@giac6.giac.f-cookies.com:/var>cat /etc/default/passwd
#ident  "@(#)passwd.dfl 1.3     92/07/14 SMI"
MAXWEEKS=
MINWEEKS=
PASSLENGTH=6
```

More information on configuring the /etc/default/passwd file can be found here: http://www.qnx.com/developer/docs/qnx_4.25_docs/qnx4/utils/p/passwd.html.

Finally, the firewall root password is known by the system/security administrators and the GIAC Enterprises software development manager. It is written down, and stored in the mangers locked desk drawer, but was also found to be written down on a sheet of paper stored inside the firewall/network server room.

Firewall GUI Access: The GIAC firewall has the Gauntlet Java GUI loaded on the firewall locally. This requires X to be running on the firewall, which means CDE and RPC services are running at the same time. By administrating the firewall remotely with the GUI, from an internal host, the firewall could be hardened further by disabling CDE/OpenWindows and subsequently RPC services.

Firewall Configuration Changes: Firewall configuration changes are made only upon the approval of the security administrator, and with the full knowledge of the project manager. Requests for potentially harmful services (ie. inbound telnet access) are discussed and decided upon by both the security administrator and the project manager.

If a configuration change is to be made, the current configuration is saved to floppy and labeled and stored in both the server room, and at the offsite storage location (in this case a separate building's locked integration room floor's dedicated cabinet). If the new configuration causes any adverse affects, the change is backed out. In the case of the firewall crashing and having to be rebuilt (or a disk failure), the latest configuration is available on floppy for quick rebuilding of the firewall.

Screen Lock: The screen lock is set to 30 minutes via the Solaris CDE screen lock setting. Since the firewall resides in a locked server room, which is further protected behind an ACL controlled door, the screen lock configuration simply adds a layer of defense-in-depth should the server room door be left open or an unauthorized person gain access.

Console Login: The GIAC firewall is configured to only allow root to login via the console with the root password. This is set in the /etc/default/login file, whose relevant portion is shown below:

```
#ident  "@(#)login.dfl  1.8     96/10/18 SMI"   /* SVr4.0 1.1.1.1       */

# Set the TZ environment variable of the shell.
#
#TIMEZONE=EST5EDT

# ULIMIT sets the file size limit for the login.  Units are disk blocks.
# The default of zero means no limit.
#
#ULIMIT=0

# If CONSOLE is set, root can only login on that device.
# Comment this line out to allow remote login by root.
#
CONSOLE=/dev/console

# PASSREQ determines if login requires a password.
#
PASSREQ=YES
```
…<snip>…

There was no /etc/issue file found on the firewall. Since the contents of this file is not shown at the login prompt when CDE is running, this file would not have been shown at the user login. It would, had FTP and telnet connections been allowed to the firewall, been displayed at the user login. Since it is being recommended that CDE and OpenWindows be disabled, the banner in /etc/issue will be displayed at the user login.

Significance of Finding(s):

Logging: Except for the /var/adm/loginlog file not existing to capture failed login messages, the logging configuration of the Gauntlet firewall was found to be sufficient.

Integrity Checks: Integrity checks are not performed on a regular schedule, and an integrity check and database re-baseline has not been done since the initial firewall installation. Given the budgetary constraints of the project, it is understandable how this task may fall by the wayside. However, running an integrity check and creating a new database is not a time intensive or difficult task. It is highly recommended that a scheduled file integrity-checking task be created and followed by the firewall administrator.

Password Policy and Storage: The password policy was found to be adequate, but room for improvement exists. The minimum length should be increased to 8 in the /etc/default/passwd file, and at least two character types should be required (ie. letters and punctuation). Storage of passwords should continue to be stored in the locked administrators desk, but the plaintext passwords written down on paper could be easily removed or lost from the firewall/network server room. This poses a significant risk, as they paper contains all the passwords to all the security relevant devices.

Also, the root password has not been changed on the firewall since it was built.

Firewall GUI Access: As pointed out in the Solaris 2.6 Operating System Vulnerabilities section, running CDE and RPC services poses a danger not only from previous vulnerabilities, but from potential vulnerabilities that have yet to be discovered. Running the Gauntlet firewall from the command line is a much safer configuration. In addition, by administering the firewall from the internal network, the Java JRE that Gauntlet installs by default can be removed from the firewall.

Firewall Configuration Changes: Having only a single firewall without an active-standby, or even a hot spare, creates a single point of failure should the firewall crash in an unrecoverable manner. Having the current configuration saved to floppy is essential so that the firewall can be rebuilt and network connectivity restored in a timely manner.

Also, if IP blocks are entered as a network entity (ie. 192.168.1.*), different network groups (ie. development vs production) for the internal network cannot choose specific hosts when an internal subnet uses variable subnetting (ie. internal network and production variably subnet a class C IP block). Each individual host must be entered into the GUI one at a time (note that this has been fixed in Gauntlet version 6.0). Having the firewall configuration on floppy prevents the time consuming task of re-entering all these IP addresses.

Therefore, it is critical for configuration changes to be saved to floppy to minimize downtime in the event of an unrecoverable system or disk crash.

Screen Lock: The screen lock is appropriately set to 30 minutes.

Console Login: The lack of a warning banner at the user login prompt is a serious issue. Lack of this banner can hinder prosecution of an attacker should they be taken to court. It is also a good reminder, for both administrators and any other authorized users of the firewall, to be made aware of the privacy and security policy of the organization via a login banner.

Defensive Recommendation:

Logging: Consider running BSM (Basic Security Module) logging on the firewall. BSM is kernel level auditing for Solaris, whose details are beyond the scope of this paper. However, there are some excellent papers on BSM located here (note that viewing the SANS papers first requires registering for a free user account):

- http://rr.sans.org/sun/COTS.php (contains a methodology for syslogging BSM data that has been run through the *praudit* binary, and uses Perl and the Perl module Net::Syslog.)
- http://rr.sans.org/sun/C2_audit.php
- http://online.securityfocus.com/infocus/1362
- http://www.shmoo.com/mail/ids/aug99/msg00016.html (this message post contains an interesting shell script for normalizing selected BSM data).

Some final notes on BSM include that it is advised to carefully consider your local disk and log server disk (or RAID) space allocations before running the "ex" BSM fileclass on the user "root". Doing so will create literally gigabytes worth of log data on even a moderately used and

administered firewall (since all exec calls will be logged). Also be aware that enabling BSM disables the "stop-a" key sequence that allows the user to get to the boot prompt. Given that the firewall is well protected physically, consider turning this back on. To do this, comment out the line "*set abort enable = 0"* in the /etc/system file. [34]

Finally, create the file /var/adm/loginlog to capture failed login attempts. Perform the following commands to do this [36]:

```
touch /var/adm/loginlog
chown root /var/adm/loginlog
chgrp sys /var/adm/loginlog
chmod 600 /var/adm/loginlog
```

Integrity Checks: It is recommended that an integrity check be performed on the firewall, and the differences be compared with the integrity database. Once it is determined that no files have been changed that should not have (for example, the /etc/passwd and /etc/shadow files), a new integrity database should be created. In addition, a new policy is advised where each time a firewall configuration is made, an integrity check and new database should be created and stored to a floppy.

To create an integrity database, perform the following steps (taken from the Gauntlet 5.5 Users Guide) [27]:

*"1. From within the Gauntlet Firewall Manager, open the **Maintenance** folder.*
*2. Click the **Integrity Check** option.*
*3. Make sure Online Database is selected, then click **Create New**.*
A Confirmation screen displays, telling you that the creation of the integrity database may take up to 30 minutes.

*4. Click **OK**.*
The firewall creates the integrity database on your system at: /usr/local/etc/checksums/gauntlet.sum"

To update an integrity database, perform the following steps (taken from the Gauntlet 5.5 Users Guide) [27]:

*"1. On the Integrity Check screen, click **Online Database**.*
*2. Click **Update**.*
A Confirmation screen displays.

*3. Click **OK**.*
The firewall updates the integrity database".

To check the integrity of files on the firewall against the integrity database stored to floppy, perform the following steps (taken from the Gauntlet 5.5 Users Guide) [27]:

"1. Put the floppy disk with the integrity database into the disk drive.

*2. On the Integrity Check screen, click **Floppy Disk**.*
*3. Click **Check**.*
A Confirmation screen displays.

*4. Click **OK**.*
The firewall creates a new integrity database and compares the new integrity database against the old database on the floppy."

Password Policy and Storage: While the room is locked with a cipher door, and is further located behind ACL controlled doors, it is recommended that the passwords be further protected by a small safe or locked cabinet inside the server room. An alternative would be to PGP encrypt the passwords and save them to a floppy and store them within a safe or locked filing cabinet within the firewall/network server room. In the event an administrator forgot a password, they could decrypt the passwords file with their private key and pass phrase. Note that if this method is followed, the file should NOT be saved in plaintext to the computer's local disk once decrypted.

In the /etc/default/passwd file, add the STRICTPASSWORD variable to force the use of two character types in passwords [29]. The password policy should also be updated to state that root passwords be changed every 60 days, especially on the firewall.

Finally, consider using PAM (Pluggable Authentication Module) to enforce strong password creation, which is built into Solaris 2.6. More information is available here: http://wwws.sun.com/software/solaris/pam/.

Firewall GUI Access: Install the Gauntlet GUI on an internal machine (perhaps on a host in a firewall service network), and remotely administer the firewall. Subsequently, disable CDE and RPC's by not running X-Windows on the firewall itself. Note that YASSP has an option in its /etc/yassp.conf file to disable CDE, and does so by default

Firewall Configuration Changes: Firewall configuration changes should be written down in a log book that is stored in the server room. This is not only good for documentation purposes, but allows the backup firewall administrator to see what has been changed in the past on the firewall should they ever be called upon.

Screen Lock: Disable CDE/OpenWindows and do not rely upon a X-Windows generated screen lock. Disable CDE with the following command [28]:
`mv /etc/rc2.d/S99dtlogin /etc/rc2.d/s99dtlogin.disabled`. Instead, consider a curses based screen lock, such as Slock (http://sources.isc.org/utils/terminal/slock-1.1.txt).

Console Login: First, obtain your company's approved login banner from the appropriate person, whether that is a manager or the legal department. If no such banner exists, have legal draft one and approve it for use on the network. One example of a login banner is shown below (taken from http://www.dougmoran.com/Guide/login-banner-titan.htm):

"This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel.

In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials." [30]

Finally, once the /etc/issue file is created and updated with the approved banner, cat the contents to the /etc/motd file, which is by default blank. This is the message that is displayed to users after they login. [33]

```
cat /etc/issue > /etc/motd
```

References:

1. http://www.enteract.com/~lspitz/example.html
2. http://www.sunspot.noao.edu/cgi-bin-local/man-cgi?syslog.conf+4
3. http://www.sunspot.noao.edu/cgi-bin-local/man-cgi?m4+1
4. https://www.securecomputing.com/pdf/55admin.pdf
5. https://www.securecomputing.com/pdf/55ug.pdf
6. http://www.qnx.com/developer/docs/qnx_4.25_docs/qnx4/utils/p/passwd.html
7. http://wwws.sun.com/software/solaris/pam/
8. http://www.dougmoran.com/Guide/login-banner-titan.htm
9. http://www.perl.com/CPAN-local/modules/by-module/Net/Net-Syslog-0.03.tar.gz

Vulnerability/Risk Item: Identification and protection of sensitive data on the firewall

Audit Result: Sensitive data on the firewall includes the following:

1. DNS zone map(s)
2. DNS Bind version number
3. Passwords
4. Firewall Configuration file (/usr/local/etc/mgmt/gauntlet.conf)
5. External IP addresses and/or blocks that are allowed access to the internal network via protocols defined in various network groups
6. Firewall log messages, which include logs written to the following files:
    - /var/log/messages
    - /var/adm/loginlog
    - /var/adm/sulog
    - /var/adm/wtmp
    - /var/adm/utmp

The protection of this data is as follows:

1. DNS zone maps are protected from unauthorized transfers by attackers using the "allow-transfer" directive in the zone definitions of the named.conf file. For example, consider the following zone from the named.conf file:

```
zone "giac.f-cookies.com" in {
        type master;
        file "db.giac";
        allow-transfer { x.y.v.25; x.y.w.25; x.y.z.25; a.b.c.67 };
        };
```

   This allows the external corporate name servers, x.y.v.25, x.y.w.25 and x.y.z.25 to transfer the GIAC zone map over the Internet (unencrypted), and the internal name server a.b.c.67 to transfer the zone map as well.

2. DNS Bind version requests are obfuscated by setting the version string in the options block of the named.conf file. For example, consider the following options block from the named.conf file:

```
options {
                directory "/etc/dns";
                pid-file  "/etc/dns/named.pid";
                forwarders      {
                        x.y.v.25;
                        x.y.w.25;
                        x.y.z.25;
                };
                fake-iquery yes;
                query-source address * port 53;
                version "Cray C90";
                notify yes
        };
```

   This will force any reply to a DNS Bind version request to contain the string "Cray C90". See the result of the Bind version request from the Nessus scan for confirmation of this.

3. Passwords are encrypted, and stored using the standard /etc/passwd and /etc/shadow files. No other password or authentication software (such as PAM) is in use on the firewall.

4. The /usr/local/etc/mgmt subdirectory, and the /usr/local/etc/mgmt/gauntlet.conf file, are both readable by the owner, group and world (which are the default permissions after Gauntlet is installed).

```
root@giac6.giac.f-cookies.com:/usr/local/etc>ls -ld mgmt
drwxr-xr-x   7 root     other       4608 Jun 26 11:14 mgmt/

root@giac6.giac.f-cookies.com:/usr/local/etc>ls -l ./mgmt/gauntlet.conf
-rw-r--r--   1 root     root      120706 Jun 26 11:14
./mgmt/gauntlet.conf
```

   Note that the only user account on the firewall is the root user.

5. External IP addresses or blocks, which are allowed access to the internal network via protocols defined in specific network groups, should be protected from attackers. If an attacker were to know an authorized IP that was allowed access to the internal network, they could launch a moderately elaborate man-in-the-middle attack coupled with DNS cache poisoning to gain access. Since these IP's are defined in the gauntlet.conf file, and the firewall only allows access by root from the console, these IP's are relatively safe from access by an attacker (baring something like a buffer overflow attack that gains the attacker root level access).

6. The messages that get written to /var/log/messages are also syslog'd off to the internal log server, as described in the logging section of the Administrative Practices. The sulog, wtmp and utmp files in /var/adm are not remotely logged off to the log server, nor are they stored to tape or floppy. In addition, the logs files are not encrypted or digitally signed on the local firewall disk.

Significance of Finding(s): The security protection of zone transfers was found to be acceptable. Obfuscating BIND version requests is a good security measure so attackers cannot identify vulnerabilities in certain versions of BIND and launch a more focused and lethal attack. The use of /etc/passwd and /etc/shadow files is appropriate given the limited physical access to the firewall, and that fact that root must login from the console. The permission settings of the gauntlet.conf file, and the /usr/local/etc/mgmt directory, could be locked down a little tighter so that read access is only given to root, but again root is the only user account on the firewall. Locking down the permissions of these files could adversely affect the operation of the firewall as well.

The contents of the sulog, wtmp and utmp files could be syslog'd to the central syslog server for secure storage to tape, and for central analysis along with all other host and IDS logs.

Defensive Recommendation: The following defensive recommendations should be considered to address the protection of sensitive GIAC Enterprises data:

1. Consider configuring and using PAM on the GIAC firewall. This would allow the use of various PAM modules, such as cracklib, to enforce password strength [31]. Note that the use of PAM often requires custom code development and integration to incorporate it.
2. Change the permissions on the /usr/local/etc/mgmt directory and /usr/local/etc/mgmt/gauntlet.conf file. This will protect the file from viewing from non-root accounts, should one ever be created.

```
chmod 711 /usr/local/etc/mgmt
chmod 600 /usr/local/etc/mgmt/gauntlet.conf
```

3. To syslog the contents of the /var/adm/loginlog (which needs to be created as previously discussed), /var/adm/sulog, /var/adm/wtmp, and /var/adm/utmp files, refer to the techniques and software described in the paper by Kent Stout, located here: http://rr.sans.org/sun/COTS.php. Keep in mind that this would require installing the Net::Syslog module, but this should not pose a security risk to the GIAC firewall. Also, the utmp and wtmp files (which were replaced by utmpx and wtmpx in later versions of

Solaris) are database files that cannot be read directly. To syslog the contents of these files to the central syslog server, first use a command such as "who" to read the contents of the database [32]. Then redirect the contents to a file that the syslog Perl daemon (as described in http://rr.sans.org/sun/COTS.php) can syslog off to the central syslog server. The following command accomplishes this file creation:

```
who /var/adm/utmp > /var/adm/utmp_output_<date>
```

There are file rotation and cron issues with the utmp and wtmp output that will obviously need to be addressed should this recommendation be followed.

References:

1. http://rr.sans.org/sun/COTS.php
2. http://search.cpan.org/author/LHOWARD/Net-Syslog-0.03/Syslog.pm
3. http://wwws.sun.com/software/solaris/pam/
4. http://campuscgi.princeton.edu/man?utmp
5. http://campuscgi.princeton.edu/man?wtmp

Vulnerability/Risk Item: Protection of sensitive data in transit over the network

Audit Result: Sensitive data that traverses the GIAC firewall is either encrypted via SSL (in the case of encrypted web access of files or web-mail on the inside network), or is sent outside the internal network PGP encrypted (in the case of external user id's and passwords). Note that FTP and Telnet access is allowed from the internal development network for anti-virus updates and software developer ease of use.

Corporate policy specifically prohibits the dissemination of any propriety data, or data of a sensitive nature. While this is not a proactive security defense, there is a well-established and mandatory security awareness training program which incorporates information security and ethics.

Significance of Finding(s): The use of FTP and Telnet on the internal network is a cause for concern. Malicious internal users could exploit the trust given to them, or an attacker could exploit these protocols should they gain physical or network access on the internal network.

Defensive Recommendation: It is highly recommended that FTP and Telnet access be disabled for the internal network. Instead, allow outbound SSH access if file transfers are absolutely necessary, and incorporate a centrally managed anti-virus signature update policy from a protected host.

References:

1. http://www.pgp.com/index.php
2. http://www.gnupg.org/
3. http://www.openssh.com/

Vulnerability/Risk Item: Access controls (general access, least privilege, separation of duties)

Audit Result: As described previously, logins are limited to the console only. No remote access, with either SSH, telnet or the Gauntlet esmp GUI is enabled. There are no "general user" accounts on the firewall. All administration is done with the root account. As previously mentioned, it is advised that the firewall be administered remotely from the internal network with the firewall GUI. Files that have excessive permissions were identified using the TARA host-based vulnerability scanner. See the OS Configuration Vulnerabilities section for more detail. Separation of duties was not accomplished on the GIAC firewall, as the security administrator built, configured and maintains the firewall. There is a backup firewall administrator, but duties are not separated in any formal manner.

Significance of Finding(s): While remote access is convenient if a problem occurs in the off-hours, GIAC Enterprises is an 8:00am – 6:00pm operation. The firewall administrator, or his backup, is available onsite Monday thru Friday if needed (and by pager if an emergency arises). Therefore, SSH access for remote administration of the firewall is not necessary at this time. A handful of file permissions should be changed per the Tara report and the inspection of the /usr/local/etc/mgmt directory. If YASSP is installed, as recommended, a variety of file permission and security changes will be made that will support least privilege. Finally, separation of duties would make sense if there were other administrators who should not be granted root access but did have firewall administration duties (for example, duties that could be performed using the espm GUI remotely). However, this situation does not exist, and therefore separation of duties beyond what is currently defined is deemed unnecessary.

Defensive Recommendation: Install the espm Java GUI on an internal client, preferably in a firewall service network. Install YASSP to further harden the operating system of the remote administration machine.

References: N/A

Vulnerability/Risk Item: Backup, disaster and incident handling policy

Audit Result:

Backup Policy: Backups of the GIAC firewall consist of backing up the Gauntlet configuration file, /usr/local/etc/mgmt/gauntlet.conf, to a floppy. Security relevant changes would include adding a new plug proxy, adding a new service group, or adding/removing an IP block/address. In the event the firewall needed to be completely rebuilt (ie. the operating system reloaded), the firewall could be returned to its prior operating state after OS patches and Gauntlet were loaded by copying the saved gauntlet.conf file over existing one in the /usr/local/etc/mgmt subdirectory.

To mitigate the risk of a primary hard drive failure, there is a script run from cron that mirrors the primary drive to the secondary hard drive every week. If the primary disk failed, the firewall could then be booted from the secondary disk. It is not procedure in the backup policy to backup the contents of the primary drive to tape.

Disaster Preparedness: Backups of the gauntlet.conf file are kept in the server room on a shelf, and another copy is stored in a different building on the corporate campus behind an ACL's controlled door. Both locations contain smoke alarms, and sprinklers. The secondary tape backup location is located on the 1st floor of a second floor building, and is relatively safe from tornadoes and floods. Both locations are also equipped with fire extinguishers, emergency lighting, and telephones. In the case of a power failure, there is a UPS located adjacent to the server room.

Incident Handling Policy: There is an incident handling policy in place that supports the proper identification, containment and eradication of any malicious agent or intrusion. The firewall administrator is also a certified SANS GCIH incident handler, and is well prepared and knowledgeable of what to do in the event of an intrusion. There is also corporate policy on incident handling, with a primary point of contact should such an event take place.

Upon inspection of the SSP (System Security Plan) and Security ConOps (Concept of Operations) documents, the incident handling policy, procedures and points of contact were found to be clearly documented.

Significance of Finding(s):

Backup Policy: The backup policy was found to be adequate given the relatively static condition of the firewall configuration, and the fact that production operations past 6:00pm local time are not guaranteed. If the firewall drives did need to be "swapped", or the firewall rebuilt from the vendor OS media and the saved Gauntlet configuration reloaded, it could be done in less than 4 hours. It was noted that there is a Veritas NetBackup server in use on the internal network, which could be used to backup the firewall. This would require purchasing and installing a NetBackup client on the firewall, and unfortunately creating a forward filter rule that permits an IP-to-IP connection over a wide range of ports. At the time the NetBackup server was purchased (April of 2001), NetBackup (Version 3.4) did not support the use a static ephemeral port (or even a narrow range of ports) for it's backup clients. It instead relies upon a very wide range of ports, which the firewall administrator found to range anywhere between reserved and large ephemeral port numbers. In particular, forward filter rules between internal hosts and the NetBackup server were configured for the port range 150 – 65535 TCP.

Disaster Preparedness: Disaster preparedness was found to be adequate.

Incident Handling Policy: The incident handling policy was well documented, and reflects the knowledge the administrator took away from the SANS GCIH training. The SSP and CONOPS were also well documented with respect to the IH policy, and provided very clear instruction on who to contact, and how, given an incident.

In at least one documented case, the incident handling procedure was put into place and identified a compromised host on the internal network that was trying to connect to the Internet on the IRC port 6667 TCP. The incident handling procedure was followed, the proper security

administrators and corporate security officers were contacted, and the malicious agent was identified and removed.

Defensive Recommendation:

Backup Policy: Consider installing a Veritas NetBackup client on the firewall and creating the necessary forward filter rule from the internal qfe0 interface to allow the NetBackup client to backup up the disk to the NetBackup server. Also, investigate the latest version of NetBackup (Version 4.5) to determine if the client supports a more narrow, or fixed, range of ports for the backups to occur on. NetBackup information can be found here: http://www.veritas.com/products/listing/ProductListingByFamily.jhtml?categoryId=110

An additional Sun Ultra 60 should be purchased so that there is a fully configured "hot spare" firewall that can be used to minimize downtime while the primary firewall is rebuilt.

Disaster Preparedness: Consider having the ceiling water sprinklers replaced with a foam or other chemical fire agent that is not destructive to computer equipment. See the Physical Security of the Firewall section for a discussion of fire suppression.

Incident Handling Policy: Incident handling procedures and policies should be periodically reviewed and updated. The current policy and procedures were found to have been over 1 year old. Consider reviewing and possibly revising the procedures and documents, giving special attention to any points of contact whose information may have changed, or who have left the organization.

References:

1. http://www.pmengineer.com/CDA/ArticleInformation/features/BNP__Features__Item/0,2732,9728,00.html
2. http://www.reliablefire.com/portablesfolder/computerrmextinguishers.html
3. http://www.veritas.com/products/listing/ProductListingByFamily.jhtml?categoryId=110

Vulnerability/Risk Item: Other miscellaneous security issues

Audit Result:

Firewall Root Path: The root user's path should not contain ".", as this would put the user at risk to a trojaned binary. Consider if a box was rooted, and the attacker created a program in the "/" directory called "netstat". If "." was in the root users path, before the location of the real netstat binary, the attackers trojaned version of netstat would be run first.

```
root@giac6.giac.f-cookies.com:/>echo $PATH
/usr/ccs/bin:/usr/openwin/bin:/usr/local/bin:/usr/local/etc:/bin:/usr/bin:/us
r/sbin:/usr/ucb:/etc:/usr/local/etc/mgmt:/usr/local/etc/infodb/tools:/downloa
ds/proctool/bin/5.6_sparc32
```

Firewall Root umask: The default umask setting for the root user in their .cshrc file is 022. This allows users in the root group and others to read and execute files created by root [33].

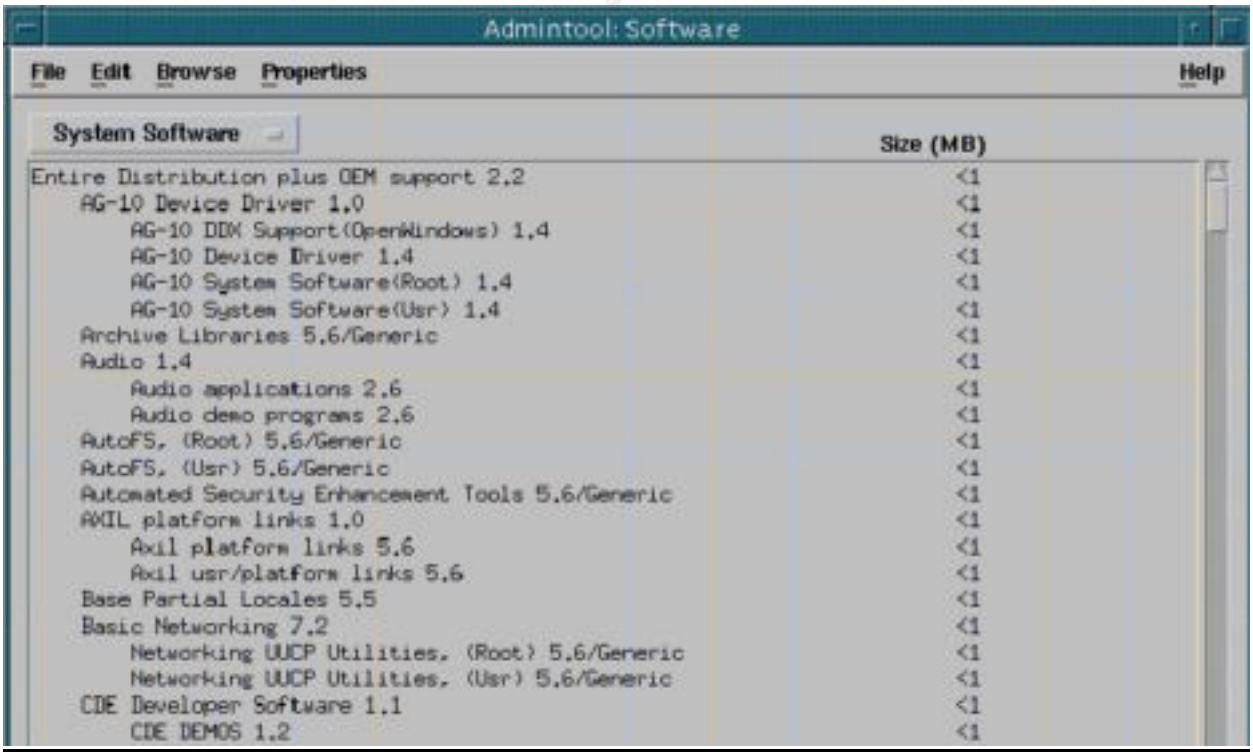
```
root@giac6.giac.f-cookies.com:/>grep umask /.*
/.cshrc:umask 022
/.login:umask 2
```

NTP (Network Time Protocol): NTP is not being used within the GIAC network to keep time.

Anti-Virus: Anti-virus is not being run on the GIAC firewall. In fact, anti-virus is not being run on any of the Solaris or Linux boxes in the network. Anti-virus is being run on all Windows hosts, however.

Upgrading to Gauntlet 6.0: Gauntlet 6.0 has been available for some time now. Since the GIAC Enterprises firewall is still under license, a free upgrade version of Gauntlet 6.0 is available from the vendor.

Solaris Package Support: According to the Gauntlet 5.5 Getting Starting Guide (http://www.securecomputing.com/pdf/55gsg.pdf), the Solaris OS should have been installed with "*Developer System Support (do **not** select End User System Support or Core System Support*)" [42]. As can be seen in the screenshot of the Solaris Admintool below, Solaris 2.6 was installed with the "Entire Distribution plus OEM support" option. This option installs all available packages and various third party software packages on the machine for the particular version of Solaris that was installed.



Sun Admintool Screenshot [44]

Significance of Finding(s):

Firewall Root Path: The root path does not contain ".", which is the recommended setting. Note that if "." were to be needed in the root users path, it should be added at the end. However, the recommended root path would not contain ".".

Firewall Root umask: The umask setting in the root user's .cshrc file not as secure as it should be. When new files are created by root, users not in the root user's group are allowed to read and execute these files.

In addition, the umask for files created by system daemons should also be set to a more secure permissions state so that files cannot be written to by users other than root (such as log files created by the syslog daemon). [36]

NTP (Network Time Protocol): Since NTP is not being used to keep the time of machines current, there will be some amount of time drift on various machines (including the firewall) on the GIAC Enterprises network. This is a cause for concern since log messages will not be synched up with respect to time across the network. This makes correlation of logs more difficult, and could impede prosecution of intruders in court if the log times were not properly synched.

Anti-Virus: While there are malicious agents that affect *nix distributions, like the Adore and Sadmind worms, they are much more rare than those that affect Windows. Most of the malicious agents that affect *nix distributions can be defended against with proper patch updates. There are anti-virus packages available for Solaris and Linux hosts, such as Kaspersky's Corporate Suite.

Upgrading to Gauntlet 6.0: Gauntlet 6.0 has many new security enhancements, some of which include enhanced logging over what syslog normally supplies, a UDP proxy for those UDP protocols that are not broadcast dependent (such as DNS and Syslog), single rule review for all forward filter, VPN and proxy rules, and Single Sign On (SSO) authentication for internal users [37].

Solaris Package Support: Installing Solaris with full OEM support on the firewall can create security vulnerabilities, as some third party software is installed, along with other Solaris packages that may not be necessary for the operation of Gauntlet.

Defensive Recommendation:

Firewall Root Path: Consider checking the path periodically to make sure that a new or backup firewall administrator (or attacker) did not add "." to the path for convenience's sake. This could be accomplished from a simple bourne shell script that is run from cron every *x* number of days and mails root the current path. Such a script might look like this:

```
#!/bin/sh
#######################################################################
#If path information has been saved previously to the file /path_info,
#delete it, echo the contents of $PATH to the /path_info file, and change
#the permissions to be read only by root.
```

```
#Then, mail the contents of the /path_info file to the root user.
##########################################################################

cd /
rm ./path_info

# echo path information to /path_info file and mail to root user
echo "From: Firewall\nTo: Firewall Admin (root)" > ./path_info
echo "Subject: Firewall Path Info\n" >> ./path_info
echo " " >> ./path_info
echo $PATH >> ./path_info
chmod 400 ./path_info
/bin/mail root@giac.f-cookies.com < ./path_info
```

Firewall Root umask: Change the umask setting to 027 in the root user's .cshrc file. This will allow users in root's group to read and execute any new files created by root, but no one else may do so.

Run the following script (based upon the script from [36]) to set the umask to 027 for files created by system daemons:

```
echo `umask 027` > /etc/init.d/umask.sh
chmod 744 /etc/init.d/umask.sh
for dir in /etc/rc?.d
do
      ln -s ../init.d/umask $dir/S00umask.sh
done
```

NTP (Network Time Protocol): Configure the network for the use of NTP. An internal time server may be used, but there are numerous publicly available time servers that may be used. The GIAC Gauntlet firewall also contains an NTP proxy for keeping time current on the internal network. A list of public time servers can be found here:

http://www.eecis.udel.edu/~mills/ntp/clock1.htm

Keep in mind the recent CERT Note (VU#970472) on an NTP daemon buffer overflow vulnerability. This vulnerability affects Solaris 2.6, among other OS's. The following patch fixes the vulnerability in Solaris 2.6: `Sun OS 5.6 107298-03`. This patch is available in the most recent Sun patch cluster.

Anti-Virus: Consider purchasing and installing an anti-virus suite that protects all hosts and gateways in the GAIC Enterprises network, such as Kaspersky's Corporate Suite.

Upgrading to Gauntlet 6.0: Consider upgrading to Gauntlet 6.0 to take advantage of the newer security features.

Solaris Package Support: Packages could be removed using the `pkgrm` command, but this will require a very careful investigation of what packages were needed and what dependencies existed before removing them. A useful reference is a list of packages needed for running FW-1 4.0 with core Solaris support only (see http://www.enteract.com/~lspitz/core6.txt). In this paper,

certain packages are identified that could be removed from a FW-1 4.0 firewall, such as the following [43]:

"If you want to add compiling capabilities (not recommended)
system SUNWsprot Solaris Bundled tools
system SUNWhea SunOS Header Files
system SUNWtoo Programming Tools
system SUNWarc Archive Libraries
system SUNWbtool CCS tools bundled with SunOS"

These packages are most likely not needed on a FW-1 (or a Gauntlet 5.5) firewall, as there should be no code development being done that requires compiling. Shell scripts do not require a compiler, and Perl is an interpreted language.

Another option would be to rebuild the existing Gauntlet 5.5 firewall, or upgrade to Gauntlet 6.0 and choose the recommended package support level. However, is it is recommended that unless GIAC Enterprises chooses to upgrade to Gauntlet 6.0, that unnecessary packages be identified and removed by the firewall administrator.

References:

1. http://www.cs.bu.edu/help/unix/customizing_your_.cshrc_file.html
2. http://www.eecis.udel.edu/~mills/ntp/clock1.htm
3. http://www.enteract.com/~lspitz/core6.txt

Critical Issues and Recommendations

Critical issues were identified, and defensive recommendations made, throughout the report for ease of reference and to keep the associated information close at hand for the administrator while incorporating the recommendations. To summarize the ten most critical issues and defensive recommendations, the following table is presented. The categories are as follows:

Issue – The critical issue or vulnerability at hand. A link to the location of the audit results in this report is provided.

Severity – Severity will be based upon how critical the issue is with respect to the security of the firewall, and rated on a 10-point scale (based upon the auditor's experience and opinion). For example, a buffer overflow vulnerability that could allow an attacker to gain root would rate a 10, whereas upgrading a software package's version (such as Gauntlet) would rate much lower.

Recommendation – The defensive recommendation to mitigate or eliminate the risk posed by the issue.

Estimated Time – The time estimated to fully implement the defensive recommendation and bring the system back online. An experienced security or system administrator is assumed to make the change, and is the experience baseline for the estimated time.

Item #	Issue	Severity	Recommendation	Est. Time
1	The version of BIND (8.2.3-REL) on the firewall is subject to a buffer overflow vulnerability (see CA-2002-19). See: BIND Audit Results	10	Update BIND to the latest version (8.3.3 or 9.2.1). This recommendation should be addressed first, as an attacker could gain root access on the firewall due to CA-2002-19.	2 hours
2	The Gauntlet 5.5 patches are not up to date. See: Gauntlet Firewall Patch Audit Results	10	Many of the Gauntlet patches are specific to performance enhancement, or other non-critical issues (compared to a vulnerability that allows an attacker to gain root). However, it is highly advised that the current Gauntlet patches be updated, as the *cluster.SOLARIS.patch* is many revisions behind. Due to Gauntlet being subject to several root-level vulnerabilities in the past, it his highly recommended that the patches be updated as the second most critical issue.	1 hour
3	Telnet and FTP connection are allowed outbound from the internal network for virus updates and for software developer's ease of use. See: Telnet and FTP Audit Results	10	Disable FTP and Telnet access to the Internet. If FTP access is required, only allow anonymous FTP. Permitting the use of these protocols could allow a malicious agent on the internal network to make unauthorized connections and/or allow the internal user's passwords to be sniffed. For the aforementioned reasons, this recommendation should be followed third.	< 1 hour
4	BIND is not chroot'd, and is running as "root".	10	Chroot BIND, either on the firewall or a separate DNS server, and do not run the	5 hours

	See: Chroot Audit Results		named daemon as root. This recommendation, and the following ones, should be followed in order based up on their relative ordering and severity.	
5	Running CDE requires running RPC services. Both of these services have numerous vulnerabilities. See: CDE and RPC Audit Results	9	Disable CDE on the firewall and run the firewall admin GUI from a host on the internal network (or a firewall service network).	3 hours
6	The Solaris 2.6 OS patches are not up to date. See: Solaris OS Patch Audit Results	8	Install the latest Solaris 2.6 patch cluster, and use the Patch Check tool to manage patch updates in the future.	1 hour
7	Kernel level auditing is not being performed on the firewall. See: BSM Audit Results	8	Enable kernel level auditing with BSM. This would allow logins/logoffs, exec calls, and other kernel actions to be audited and syslog'd to a central syslog server (keep in mind this will require custom logging daemons to be created as previously discussed).	10 hours
8	The OS is not hardened beyond what Gauntlet provides after the initial installation of the firewall software. See: OS Hardening Audit Results	7	Harden the Solaris 2.6 OS with a hardening tool such as YASSP, as well as making hardening changes by hand. While the Gauntlet firewall that is installed by default is somewhat well secured, additional hardening will provide defense-in-depth.	10 hours
9	The ident/auth daemon is started from the /etc/inetd.conf file. See: Identd/Auth Daemon Audit Results	6	Remove the identd/auth daemon from the /etc/identd.conf file so that attackers may not perform reverse ident scanning against the identd/auth daemon on the firewall.	< 1 hour
10	The GIAC Enterprises firewall	4	Upgrade the firewall to	30 hours

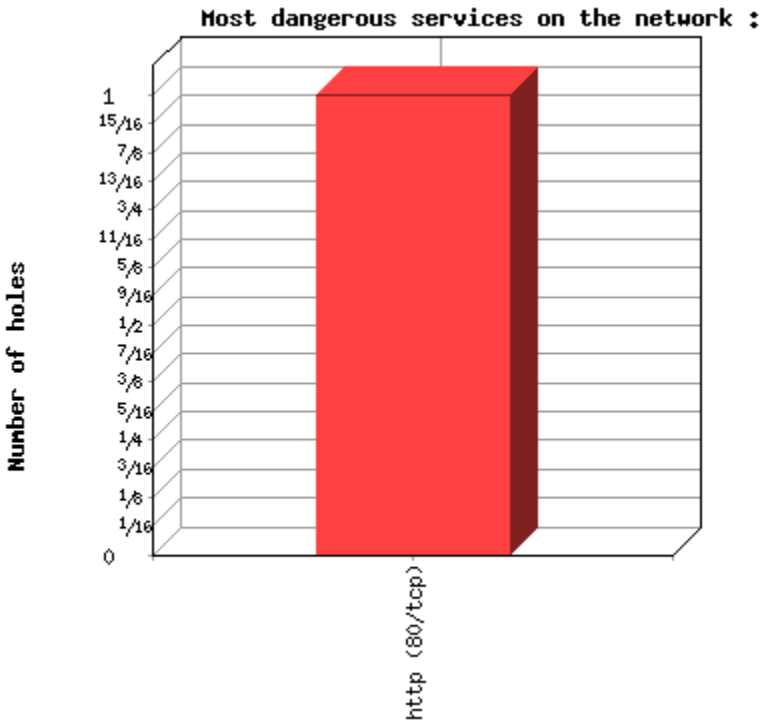
	software (Gauntlet 5.5) is outdated. See: Gauntlet 6.0 Audit Results		Gauntlet 6.0 to take advantage of the many new features. Keep in mind that this will require rebuilding the entire firewall, including patches, hardening and rebuilding the configuration.	

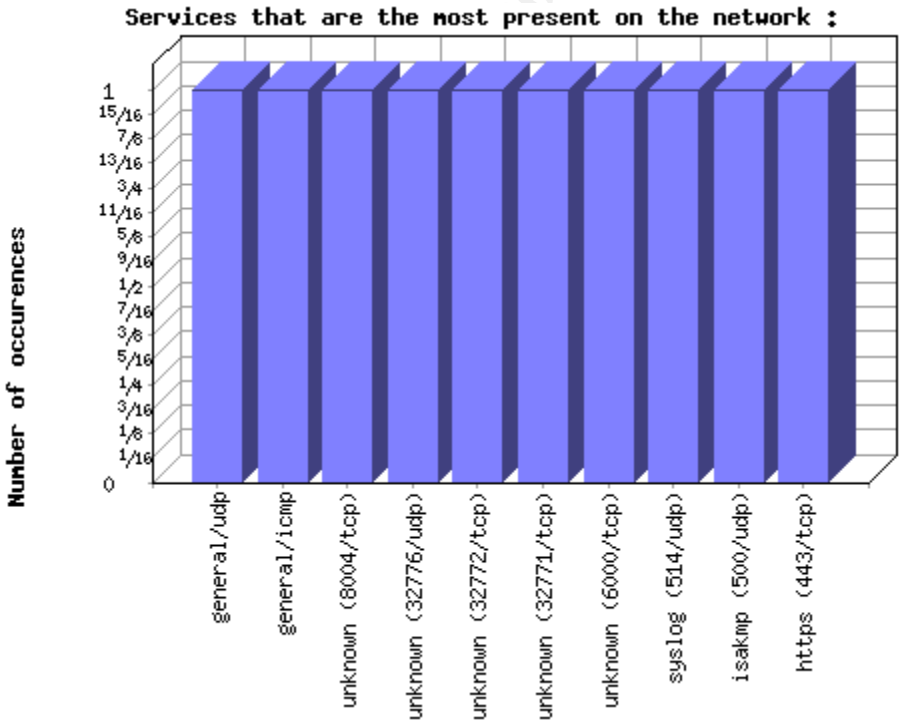
Further defensive recommendations include:

1. Hardening BIND's /etc/named.conf file. See the defensive recommendations here.
2. Install a Veritas Backup client on the firewall. See the defensive recommendations here.
3. Create /var/adm/loginlog. See the defensive recommendations here.
4. After disabling CDE, install a screen lock utility. Also create a console login message. See the defensive recommendations here.
5. Incorporate the recommendations to protect the sensitive data local to the firewall that were identified. See the defensive recommendations here.
6. If remote file transfer or administration of the firewall is deemed necessary, install and configure SSH on the GIAC firewall.
7. Consider running anti-virus software on *nix hosts. One such product is Kaspersky's Corporate Suite.
8. Identify and remove unnecessary Solaris packages installed with the full OEM support option. See the defensive recommendation here.

Appendix A – Nessus Report

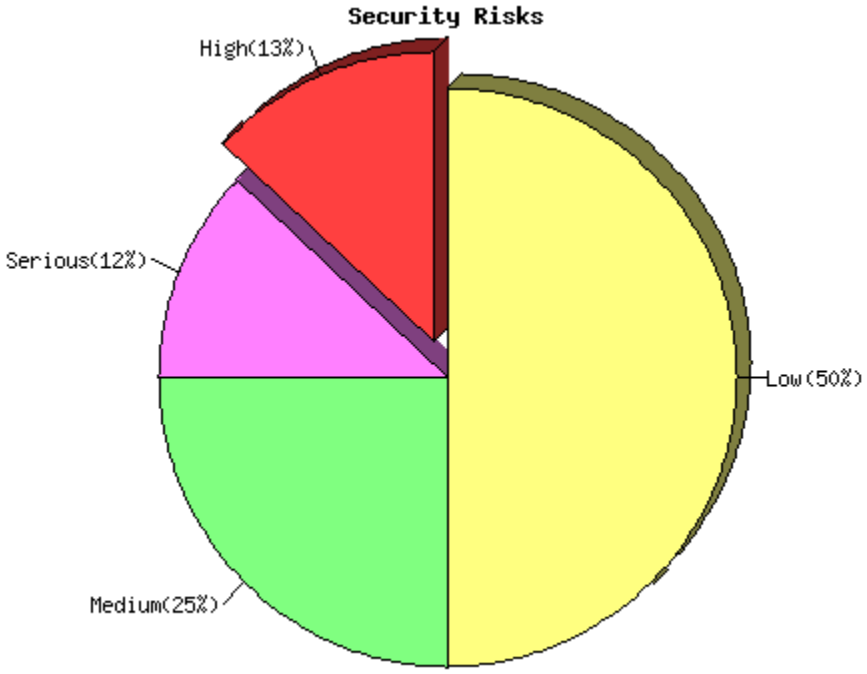
Output from the Nessus scan:





a.b.c.6

Repartition of the level of the security problems:



List of open ports :

- o general/tcp (Security notes found)
- o ftp (21/tcp) (Security notes found)
- o telnet (23/tcp) (Security warnings found)
- o smtp (25/tcp) (Security notes found)
- o domain (53/tcp) (Security warnings found)
- o domain (53/udp)
- o http (80/tcp) (**Security hole found**)
- o sunrpc (111/tcp) (Security warnings found)
- o sunrpc (111/udp) (Security warnings found)
- o ident (113/tcp) (Security notes found)
- o xdmcp (177/udp) (Security warnings found)
- o https (443/tcp) (Security notes found)
- o isakmp (500/udp)
- o syslog (514/udp)
- o unknown (6000/tcp) (Security warnings found)
- o unknown (32771/tcp) (Security notes found)
- o unknown (32772/tcp) (Security warnings found)

o unknown (32776/udp)
o unknown (8004/tcp)
o general/icmp (Security warnings found)
o general/udp (Security notes found)

Information found on port general/tcp

"Default scan" set. nmap will ignore the user specified port range and scan only the 1024 first ports and those declared in nmap-services

Information found on port general/tcp

Nmap found that this host is running Solaris 2.6 - 2.7

Information found on port general/tcp

The plugin PC_anywhere_tcp.nasl was too slow to finish - the server killed it

Information found on port ftp (21/tcp)

This service is owned by user firewall-user

Warning found on port telnet (23/tcp)

The Telnet service is running. This service is dangerous in the sense that it is not ciphered – that is, everyone can sniff the data that passes between the telnet client and the telnet server. This includes logins and passwords.

You should disable this service and use OpenSSH instead.
(www.openssh.com)

Solution : Comment out the 'telnet' line in /etc/inetd.conf.

Risk factor : Low
CVE : CAN-1999-0619

Information found on port telnet (23/tcp)

This service is owned by user firewall-user

Information found on port telnet (23/tcp)

Remote telnet banner :
unknown/a.b.c.9 is not authorized to use the telnet proxy

Information found on port smtp (25/tcp)

This service is owned by user firewall-user

Information found on port smtp (25/tcp)

Remote SMTP server banner :
0
0

Warning found on port domain (53/tcp)

The remote name server allows recursive queries to be performed by the host running nessusd.

If this is your internal nameserver, then forget this warning.

If you are probing a remote nameserver, then it allows anyone to use it to resolve third parties names (such as www.nessus.org). This allows hackers to do cache poisoning attacks against this nameserver.

Solution : Restrict recursive queries to the hosts that should use this nameserver (such as those of the LAN connected to it). If you are using bind 8, you can do this by using the instruction 'allow-recursion' in the 'options' section of your named.conf

If you are using another name server, consult its documentation.

Risk factor : Serious

Warning found on port domain (53/tcp)

The remote name server allows DNS zone transfers to be performed. This information is of great use to an attacker who may use it to gain information about the topology of your network and spot new targets.

Solution: Restrict DNS zone transfers to only the servers that absolutely need it.

Risk factor : Medium

Information found on port domain (53/tcp)

This service is owned by user firewall-user

Information found on port domain (53/tcp)

```
The remote bind version is : Cray C90
```

Vulnerability found on port http (80/tcp)

The dll '/_vti_bin/_vti_aut/dvwssr.dll' seems to be present.

This dll contains a bug which allows anyone with authoring web permissions on this system to alter the files of other users.

In addition to this, this file is subject to a buffer overflow which allows anyone to execute arbitrary commands on the server and/or disable it

Solution : delete /_vti_bin/_vti_aut/dvwssr.dll
Risk factor : High
See also : http://www.wiretrip.net/rfp/p/doc.asp?id=45&iface=1
CVE : CVE-2000-0260

Information found on port http (80/tcp)

This service is owned by user firewall-user

Warning found on port sunrpc (111/tcp)

The RPC service rpcbind V2-4 is running on this port. If you do not use it, disable it, as it is a potential security risk

Information found on port sunrpc (111/tcp)

This service is owned by user firewall-user

Warning found on port sunrpc (111/udp)

The RPC service rpcbind V2-4 is running on this port. If you do not use it, disable it, as it is a potential security risk

Information found on port ident (113/tcp)

This service is owned by user firewall-user

Warning found on port xdmcp (177/udp)

The plugin sends a XDMCP QUERY request to see if the remote host is running XDM (or similar display manager) with XDMCP protocol enabled.

This protocol was used to provide X display connections for old X terminals. XDMCP is completely insecure, since the traffic and passwords are not encrypted.

Risk factor : Medium
Solution : Disable XDMCP

Information found on port https (443/tcp)

This service is owned by user firewall-user

Warning found on port unknown (6000/tcp)

This X server does *not* accept clients to connect to it however it is recommended that you filter incoming connections to this port as attacker may send garbage data and slow down your X session or even kill the server. Here is the message we received :

Client is not authorized to connect to Server

Solution : filter incoming connections to ports 6000-6009
Risk factor : Low
CVE : CVE-1999-0526

Information found on port unknown (6000/tcp)

This service is owned by user firewall-user

Information found on port unknown (32771/tcp)

This service is owned by user firewall-user

Warning found on port unknown (32772/tcp)

The RPC service ttsession V5 is running on this port. If you do not use it, disable it, as it is a potential security risk

Warning found on port general/icmp

The remote host answered to an ICMP_MASKREQ query and sent us its netmask (255.255.255.X)

An attacker can use this information to understand how your network is set up and how the routing is done. This may help him to bypass your filters.

Solution : reconfigure the remote host so that it does not answer to those requests.
Set up filters that deny ICMP packets of type 17.

Risk factor : Low
CVE : CAN-1999-0524

Warning found on port general/icmp

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine.

This may help him to defeat all your time based authentication protocols.

Solution : filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk factor : Low
CVE : CAN-1999-0524

Information found on port general/udp

For your information, here is the traceroute to a.b.c.6 :
a.b.c.6

This file was generated by Nessus, the open-sourced security scanner.

Appendix B – Nmap Output

Output from the Nmap scan:

The output below was taken from the "Nmap Front End v0.2.54BETA22" GUI when run with the following command: `nmap -sT -sR -p 1-65535 -O -I -R -v a.b.c.6`. The flag values (taken directly from the Nmap man pages) are as follows [3]:

***-sT** : TCP connect() scan*
***-sR** : RPC scan*
***-p 1-65535** : <port ranges>*
***-O** : remote host identification via TCP/IP fingerprinting*
***-I** : TCP reverse ident scanning*
***-R** : Tells Nmap to ALWAYS do reverse DNS resolution on the target IP addresses.*
***-v** : turn on verbose mode*

```
Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )
 Host  (a.b.c.6) appears to be up ... good.
Initiating Connect() Scan against  (a.b.c.6)
Adding TCP port 23 (state open).
 Adding TCP port 113 (state open).
 Adding TCP port 111 (state open).
 Adding TCP port 32771 (state open).
 Adding TCP port 53 (state open).
 Adding TCP port 6000 (state open).
 Adding TCP port 32772 (state open).
 Adding TCP port 8004 (state open).
 Adding TCP port 443 (state open).
 Adding TCP port 21 (state open).
 Adding TCP port 80 (state open).
 Adding TCP port 25 (state open).
  The Connect() Scan took 13 seconds to scan 65535 ports.
Initiating RPCGrind Scan against  (a.b.c.6)
The RPCGrind Scan took 4 seconds to scan 65535 ports.
For OSScan assuming that port 21 is open and port 1 is closed and neither are
firewalled
Interesting ports on  (a.b.c.6):
(The 65523 ports scanned but not shown below are in state: closed)
Port       State       Service (RPC)           Owner
21/tcp     open        ftp                     firewall-user
23/tcp     open        telnet                  firewall-user
25/tcp     open        smtp                    firewall-user
53/tcp     open        domain                  firewall-user
80/tcp     open        http                    firewall-user
111/tcp    open        sunrpc (rpcbind V2-4)   firewall-user
113/tcp    open        auth                    firewall-user
443/tcp    open        https                   firewall-user
6000/tcp   open        X11                     firewall-user
8004/tcp   open        unknown                 firewall-user
32771/tcp  open        sometimes-rpc5          firewall-user
32772/tcp  open        sometimes-rpc7 (ttsession V5)firewall-user
```

```
Remote operating system guess: Solaris 2.6 - 2.7
Uptime 3.076 days (since Wed Apr 17 12:11:05 2002)
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=13143 (Worthy challenge)

IPID Sequence Generation: Incremental

Nmap run completed -- 1 IP address (1 host up) scanned in 21 seconds
```

Appendix C – Sun Patch List Script and Output of its Execution on the Firewall

patchlist.scr script:

```
#!/bin/csh
##############################################################################
# Name:         patchlist.scr
#
# Author(s):    Jeff Holland (original script concept by Marc Criss)
#
# Description:  Script to summarize Solaris cluster patch information and create
#               a documented history of patch status in the /var/sadm/patches directory.
#
# Install:      Put this script in /usr/local/bin and change permissions
#               to rwx for root only (i.e. chmod 700 /usr/local/bin/patch_list_scr).
#               Source your /.cshrc file so the script is found in your path.
#
# Usage:        Run the patch_list_scr script from any directory after applying any
#               new patches. Use the diff or xdiff utilities to view differences after patch updates.
#               Use the following commands to diff and remove fields with a time stamp:
#
#               cd /var/sadm/patch
#               diff <file1> <file2> | egrep -v "Date output:" | egrep -v "File:"
#
# Output:       View the output in the /var/sadm/patch directory. The ouput file is
#               time stamped with the date the script was run. Files are chmod'd read
#               only for the owner (root) to prevent accidental deletion and enforce
#               limited access to this information.
#
# Change Log:
#               - 07/12/01, Version 1.0, Marc Criss
#                 Initial release.
#
#               - 04/23/02, Version 1.1, Jeff Holland
#                 Updated script to contain more patch information and time
#                 stamp the files. Also modified to keep a history of patch
#                 status in /var/adm/patch. Added install, usage and output info to the
#                 flower box.
##############################################################################

cd /var/sadm/patch
set CDT=`date +'%m.%d.%y_%H:%M:%S'`

echo
"*******************************************************************************
" >> ./patch.list.$CDT
```

```
echo "* File: patch.list.$CDT" >> ./patch.list.$CDT
echo "* Date output created:" `date` >> ./patch.list.$CDT
echo "*" `uname -a | awk '{ print " OS: "$1"\n" }'` >> ./patch.list.$CDT
echo "*" `uname -a | awk '{ print "OS Version: "$3"\n" }'` >> ./patch.list.$CDT
echo "*" `uname -a | awk '{ print "OS Build: "$4"\n" }'` >> ./patch.list.$CDT
echo "* See the /var/sadm/patch/<patch_id> subdirectory for patch more information." >>
./patch.list.$CDT
echo "* Obtain updated patches at: www.sunsolve.sun.com" >> ./patch.list.$CDT
echo
"**********************************************************************
" >> ./patch.list.$CDT
echo " " >> ./patch.list.$CDT
echo "==============================" >> ./patch.list.$CDT
echo " "
echo "   Creating file: patch.list.$CDT ... please wait."

foreach patch (`/bin/ls | grep ^10 `)
      set KW=`grep Keywords $patch/README* | cut -d: -f2`
      set SY=`grep Synopsis $patch/README*`
      set DT=`grep Date $patch/README* | cut -d: -f2`

      echo "Patch-ID: $patch" >>./patch.list.$CDT
      echo "Keywords: $KW" >> ./patch.list.$CDT
      echo "$SY" >> ./patch.list.$CDT
      echo "Patch Creation Date: $DT" >> ./patch.list.$CDT
      echo "==============================" >> ./patch.list.$CDT
end

/bin/chmod 400 ./patch.list.$CDT

echo " "
echo " "
echo "   Patch list created. View the output at: /var/sadm/patch/patch.list.$CDT"
echo " "
         echo " "
echo "   A complete patch rev status can be obtained by running the /usr/sbin/showrev -p
command."
echo "   Better yet, use the Sun patchcheck tool to diff your current patch rev's against the up to
date list"
echo "   on the SunSolve site and download new patches on a patch by patch basis (requires a
Sunsolve login acct.)."
echo "   Download the patchcheck tool here: http://sunsolve.sun.com/pub-
cgi/show.pl?target=patchk "
echo " "
```

patchlist.scr script stdout output after running the script on the GIAC Enterprises firewall:

```
root@giac6.giac.f-cookies.com:/usr/local/bin>./patchlist.scr

   Creating file: patch.list.04.26.02_11:10:27 ... please wait.

   Patch list created. View the output at:
   /var/sadm/patch/patch.list.04.26.02_11:10:27

   A complete patch rev status can be obtained by running the
   /usr/sbin/showrev -p command. Better yet, use the Sun patchcheck tool to
   diff your current patch rev's against the up to date list on the SunSolve
   site and download new patches on a patch by patch basis (requires a
   Sunsolve login acct.). Download the patchcheck tool here:
   http://sunsolve.sun.com/pub-cgi/show.pl?target=patchk
```

patchlist.scr script output file contents after running the script on the GIAC Enterprises firewall:

```
giac6.giac.f-cookies.com:/usr/local/bin>cat
/var/sadm/patch/patch.list.04.26.02_11:10:27

********************************************************************************
* File: patch.list.04.26.02_11:10:27
* Date output created: Fri Apr 26 11:10:27 CDT 2002
* OS: SunOS
* OS Version: 5.6
* OS Build: Generic_105181-22
* See the /var/sadm/patch/<patch_id> subdirectory for patch more information.
* Obtain updated patches at: http://sunsolve.sun.com/
********************************************************************************

==============================
Patch-ID: 105181-19
Keywords: security kernel ST_FIX_ALIGN FFB2 ECC VOP_REALVP sockfs klmmod
Synopsis: SunOS 5.6: kernel update patch
Patch Creation Date: 07/Dec/99
==============================
Patch-ID: 105181-22
Keywords: security kernel ST_FIX_ALIGN FFB2 ECC VOP_REALVP sockfs sbus
pci_pci
Synopsis: SunOS 5.6: Kernel update patch
Patch Creation Date: Aug/07/00
==============================
Patch-ID: 105210-32
Keywords: security y2000 watchmalloc libc readdir SIGCHLD pthread_cancel
Synopsis: SunOS 5.6: libaio, libc & watchmalloc patch
Patch Creation Date: Aug/07/00
==============================
Patch-ID: 105216-04
Keywords: security rpcbind indirect daemons CALLIT tmp
Synopsis: SunOS 5.6: /usr/sbin/rpcbind patch
Patch Creation Date: Apr/14/00
==============================
Patch-ID: 105284-37
```

```
Keywords: 2.6 motif drag ScrollBar crash BadValue libxm Netscape keyboard
Synopsis: Motif 1.2.7: Runtime library patch
Patch Creation Date: Aug/07/00
==========================
Patch-ID: 105338-25
Keywords: security charset on-line help spellchecker subtypes sentmail NFS
Synopsis: CDE 1.2: dtmail patch
Patch Creation Date: Dec/27/99
==========================
Patch-ID: 105356-16
Keywords: FC-AL mutex ssd bp_resid multinode MHIOCTKOWN lun vold.conf timeout
Synopsis: SunOS 5.6: /kernel/drv/ssd and /kernel/drv/sd patch
Patch Creation Date: Jul/10/00
==========================
Patch-ID: 105357-04
Keywords: luxadm HBA ses pm-hardware-state needs-suspend-resume
Synopsis: SunOS 5.6: /kernel/drv/ses patch
Patch Creation Date: Jun/30/99
==========================
Patch-ID: 105362-18
Keywords: PGX m64 driver window config
Synopsis: PGX 2.6: M64 Graphics Patch
Patch Creation Date: Jan/06/99
==========================
Patch-ID: 105363-16
Keywords: afb xfb afb.ucode afbconfig afbdaemon afbinit ddx window xgl ogl
Synopsis: Elite3D 2.6: AFB Graphics Patch
Patch Creation Date: Jan/19/1999
==========================
Patch-ID: 105375-24
Keywords: luxadm sf socal FCIO_DIAG_XRAM SCSI PLOGI l_forcelip_al
Synopsis: SunOS 5.6: sf & socal driver patch
Patch Creation Date: Jul/26/00
==========================
Patch-ID: 105379-06
Keywords: security nfssrv ACL UFS read-only cluster nfs3 VOP_FSYNC
Synopsis: SunOS 5.6: /kernel/misc/nfssrv patch
Patch Creation Date: Aug/09/00
==========================
Patch-ID: 105395-06
Keywords: security sendmail NIS lookup core SMTP denial-of-service vacation
Synopsis: SunOS 5.6: /usr/lib/sendmail patch
Patch Creation Date: Jun/15/99
==========================
Patch-ID: 105401-28
Keywords: security rpcinfo libnsl lookup ypbind.pid clients rpc.nisd RPC
buffer
Synopsis: SunOS 5.6: libnsl and NIS+ commands patch
Patch Creation Date: Apr/14/00
==========================
Patch-ID: 105403-03
Keywords: security ypbind ypbind.pid diskless clients lookup rpcbind
Synopsis: SunOS 5.6: ypbind/ypserv patch
Patch Creation Date: Apr/14/00
==========================
Patch-ID: 105464-02
Keywords: y2000 xterm size cde incorrect rows cols switched 4 digit date kill
```

```
Synopsis: OpenWindows 3.6: Multiple xterm fixes
Patch Creation Date: Feb/22/99
==============================
Patch-ID: 105472-07
Keywords: automountd automounter loopback local memory GSSAPI
Synopsis: SunOS 5.6: /usr/lib/autofs/automountd patch
Patch Creation Date: Jan/07/99
==============================
Patch-ID: 105529-09
Keywords: security tcp rlogin TCP ACK FIN packet listen
Synopsis: SunOS 5.6: /kernel/drv/tcp patch
Patch Creation Date: Jun/16/00
==============================
Patch-ID: 105552-03
Keywords: security rpc.nisd_resolv svc_getreqset FD_ISSET
Synopsis: SunOS 5.6: /usr/sbin/rpc.nisd_resolv patch
Patch Creation Date: Apr/14/00
==============================
Patch-ID: 105558-04
Keywords: security dtpad multi-screen file multiple processes spellchecker
Synopsis: CDE 1.2: dtpad patch
Patch Creation Date: Apr/06/99
==============================
Patch-ID: 105562-03
Keywords: security NIS+ server domain chkey keylogin
Synopsis: SunOS 5.6: chkey and keylogin patch
Patch Creation Date: Jul/01/98
==============================
Patch-ID: 105566-08
Keywords: security y2000 dtcm calendar crash remind repeated weekly date
Synopsis: CDE 1.2: calendar manager patch
Patch Creation Date: Feb/22/00
==============================
Patch-ID: 105568-18
Keywords: sigtimedwait libthread SIGTERM SIGALRM SIGLWP pthread_cancel
UNBOUND
Synopsis: SunOS 5.6: /usr/lib/libthread.so.1 patch
Patch Creation Date: Jun/30/00
==============================
Patch-ID: 105570-01
Keywords: sunvideo, rtvc, xil
Synopsis: SunVideo 1.3: SunVideo fixes
Patch Creation Date: Nov/17/97
==============================
Patch-ID: 105580-15
Keywords: glm TRAP panic boot 53c810A DDI_PROP_DONOTPASS
Synopsis: SunOS 5.6: /kernel/drv/glm patch
Patch Creation Date: May/22/00
==============================
Patch-ID: 105591-09
Keywords: libC.so.5 libCrun.so.1 libdemangle.so.1
Synopsis: SunOS 5.6: Shared library patch for C++
Patch Creation Date: May/19/00
==============================
Patch-ID: 105600-19
Keywords: isp panic NFS D_HOTPLUG cb_ops LUN32 ddi_putw() isp_i_alive
Synopsis: SunOS 5.6: /kernel/drv/isp patch
```

```
Patch Creation Date: Jun/22/00
==============================
Patch-ID: 105615-08
Keywords: security mountd permission -osec=krb5
Synopsis: SunOS 5.6: /usr/lib/nfs/mountd patch
Patch Creation Date: Apr/14/00
==============================
Patch-ID: 105621-24
Keywords: security y2000 ITSEC libbsm auditreduce audit_event cron
Synopsis: SunOS 5.6: c2audit, libbsm and cron patch
Patch Creation Date: Jul/21/00
==============================
Patch-ID: 105633-05
Keywords: Xsun mhc AFB Thread fonts Type1 scaled
Synopsis: OpenWindows 3.6: Xsun patch
Patch Creation Date: Mar/05/98
==============================
Patch-ID: 105633-46
Keywords: security Xsun connections X server Xview font cameleo's XRead
Synopsis: OpenWindows 3.6: Xsun patch
Patch Creation Date: Aug/14/00
==============================
Patch-ID: 105642-08
Keywords: prtdiag Ultra-250 UE3500 status keyswitch
Synopsis: SunOS 5.6: prtdiag patch
Patch Creation Date: Apr/12/00
==============================
Patch-ID: 105654-03
Keywords: driver aliases classes name_to_major uata dad atapicd simba
Synopsis: SunOS 5.6: driver_aliases/driver_classes/name_to_major patch
Patch Creation Date: 05/Jan/98
==============================
Patch-ID: 105665-03
Keywords: security loginlog invalid username RETRIES
Synopsis: SunOS 5.6: /usr/bin/login patch
Patch Creation Date: Sep/09/98
==============================
Patch-ID: 105667-02
Keywords: security rdist buffer overflow
Synopsis: SunOS 5.6: /usr/bin/rdist patch
Patch Creation Date: Oct/16/98
==============================
Patch-ID: 105669-10
Keywords: security SIGBUS coredump hang Action multi screen open set
Synopsis: CDE 1.2: libDtSvc Patch
Patch Creation Date: Jan/07/00
==============================
Patch-ID: 105703-22
Keywords: security help restart SIGHUP Corona killed configured dtl screen
PAM
Synopsis: CDE 1.2: dtlogin patch
Patch Creation Date: Mar/13/00
==============================
Patch-ID: 105720-12
Keywords: nfs SIGALRM SIGCLD ENOENT xdr_getrddirres() DNLC nfs3lookup
Synopsis: SunOS 5.6: /kernel/fs/nfs patch
Patch Creation Date: Mar/10/00
```

```
==============================
Patch-ID: 105722-05
Keywords: security ufsdump 2GB ufsrestore
Synopsis: SunOS 5.6: /usr/lib/fs/ufs/ufsdump and ufsrestore patch
Patch Creation Date: May/24/00
==============================
Patch-ID: 105741-07
Keywords: nibble DMAC ecpp_isr printers prime deadlock ecpp_wsrv ecpp_close
Synopsis: SunOS 5.6: /kernel/drv/ecpp patch
Patch Creation Date: Mar/22/00
==============================
Patch-ID: 105755-08
Keywords: security libresolv multithreaded in.named res_mkquery
Synopsis: SunOS 5.6: libresolv, in.named, named-xfer, nslookup, nstest patch
Patch Creation Date: Apr/19/00
==============================
Patch-ID: 105780-05
Keywords: security fifofs panic VOP_REALVP WebNFS getattr
Synopsis: SunOS 5.6: /kernel/fs/fifofs patch
Patch Creation Date: May/25/00
==============================
Patch-ID: 105786-13
Keywords: security ip tcp_priv_stream routing ip_enable_group_ifs ndd
Synopsis: SunOS 5.6: /kernel/drv/ip patch
Patch Creation Date: Jul/12/00
==============================
Patch-ID: 105795-05
Keywords: hme mutex deadlock QSI 28115 D_HOTPLUG cb_ops hmesendup hmeinit
Synopsis: SunOS 5.6: /kernel/drv/hme patch
Patch Creation Date: Aug/11/98
==============================
Patch-ID: 105800-06
Keywords: security y2000 user manager admintool passwd buffer
Synopsis: SunOS 5.6: /usr/bin/admintool, y2000 patch
Patch Creation Date: Feb/18/00
==============================
Patch-ID: 105802-12
Keywords: security libtt leak tt_open display core hang TT_SESSION enhanced
Synopsis: OpenWindows 3.6: ToolTalk patch
Patch Creation Date: Mar/22/00
==============================
Patch-ID: 105837-03
Keywords: security dtappgather view file
Synopsis: CDE 1.2: dtappgather Patch, including SDE 1.0 installations
Patch Creation Date: Jul/26/99
==============================
Patch-ID: 105924-03
Keywords: se minor_perm devlink.tab iu.ap
Synopsis: SunOS 5.6: devlink.tab/iu.ap/minor_perm & se driver patch
Patch Creation Date: 25/Mar/98
==============================
Patch-ID: 106027-08
Keywords: security PAM passwd 8 characters hang dtsession randomly
Synopsis: CDE 1.2: SDE 1.0: dtsession patch
Patch Creation Date: Feb/14/00
==============================
Patch-ID: 106040-03
```

```
Keywords: Esc 513166, bug 4097754 dtwm dumps core under s998 due to problems
in remote IM
Synopsis: SunOS 5.6: dtwm dumps core under s998 due to problems in remote IM
Patch Creation Date: Feb/23/98
==============================
Patch-ID: 106040-14
Keywords: IM OM htt xlibi18n locale.alias locale.dir compose.dir ximp40
Synopsis: SunOS 5.6: X Input & Output Method patch
Patch Creation Date: Aug/15/00
==============================
Patch-ID: 106112-06
Keywords: security dtfile multi screen NFS access huge sdtvolcheck CPU
Synopsis: CDE 1.2: dtfile patch
Patch Creation Date: Jul/25/00
==============================
Patch-ID: 106123-04
Keywords: security locale smgl2roff SDATA catman getNAME makewhatis
Synopsis: SunOS 5.6: sgml patch
Patch Creation Date: Jan/04/99
==============================
Patch-ID: 106125-10
Keywords: patchadd patchrm CD du
Synopsis: SunOS 5.6: Patch for patchadd and patchrm
Patch Creation Date: Jun/21/00
==============================
Patch-ID: 106172-04
Keywords: fas D_HOTPLUG cb_ops DDI_SUSPEND/RESUME
Synopsis: SunOS 5.6: /kernel/drv/fas patch
Patch Creation Date: Nov/16/98
==============================
Patch-ID: 106193-05
Keywords: security y2000 NIS locale unzip sysid
Synopsis: SunOS 5.6: y2000 sysid unzip patch
Patch Creation Date: Jun/21/00
==============================
Patch-ID: 106222-01
Keywords: security ff.core
Synopsis: OpenWindows 3.6: filemgr (ff.core) fixes
Patch Creation Date: Apr/28/98
==============================
Patch-ID: 106226-01
Keywords: format core disk MTI-9000
Synopsis: SunOS 5.6: /usr/sbin/format patch
Patch Creation Date: Jun/02/98
==============================
Patch-ID: 106235-06
Keywords: security lp.tell in.lpd lpfilter bsd_lpsched.so.1 -y
Synopsis: SunOS 5.6: lp patch
Patch Creation Date: Jul/31/00
==============================
Patch-ID: 106242-02
Keywords: workshop help core japanese ja dithered images
Synopsis: CDE 1.2: libDtHelp.so.1 fixes
Patch Creation Date: Jan/06/99
==============================
Patch-ID: 106257-05
Keywords: security libpam.so.1 passwd protocol login pam_start
```

```
Synopsis: SunOS 5.6: /usr/lib/libpam.so.1 patch
Patch Creation Date: Feb/03/00
==============================
Patch-ID: 106271-06
Keywords: security pam_unix.so.1 csh umask nispasswd Passwd_compat
Synopsis: SunOS 5.6: /usr/lib/security/pam_unix.so.1 patch
Patch Creation Date: Sep/24/99
==============================
Patch-ID: 106301-01
Keywords: security in.ftpd CPU client shutdown
Synopsis: SunOS 5.6: /usr/sbin/in.ftpd patch
Patch Creation Date: May/05/98
==============================
Patch-ID: 106415-03
Keywords: security xdm fingers users utmp wtmp who root console install
Synopsis: OpenWindows 3.6: xdm patch
Patch Creation Date: May/04/99
==============================
Patch-ID: 106437-03
Keywords: security dtprintinfo core "lp -o" SIGSEGV
Synopsis: CDE 1.2: Print Manager Patch
Patch Creation Date: Feb/01/00
==============================
Patch-ID: 106439-06
Keywords: syslogd file descriptors MP pipe -1
Synopsis: SunOS 5.6: /usr/sbin/syslogd patch
Patch Creation Date: Mar/08/00
==============================
Patch-ID: 106448-01
Keywords: security buffer overflow hnamebuf
Synopsis: SunOS 5.6: /usr/sbin/ping patch
Patch Creation Date: Jul/14/98
==============================
Patch-ID: 106468-02
Keywords: security cu 8bit locale
Synopsis: SunOS 5.6: /usr/bin/cu and usr/bin/uustat patch
Patch Creation Date: Mar/30/00
==============================
Patch-ID: 106495-01
Keywords: truss PCRUN hang lwp
Synopsis: SunOS 5.6: truss & truss support library patch
Patch Creation Date: Jun/23/98
==============================
Patch-ID: 106522-04
Keywords: security ftp mget mput fork client
Synopsis: SunOS 5.6: /usr/bin/ftp patch
Patch Creation Date: May/19/00
==============================
Patch-ID: 106569-01
Keywords: security libauth buffer overflow stack
Synopsis: SunOS 5.6: libauth.a & libauth.so.1 patch
Patch Creation Date: Sep/16/98
==============================
Patch-ID: 106592-03
Keywords: security statd fork fd service
Synopsis: SunOS 5.6: /usr/lib/nfs/statd patch
Patch Creation Date: Apr/14/00
```

```
==============================
Patch-ID: 106625-08
Keywords: security libsec ACL df unmount vfs_minfrags i_contents ufs
Synopsis: SunOS 5.6: libsec.a, libsec.so.1 and /kernel/fs/ufs patch
Patch Creation Date: Jun/27/00
==============================
Patch-ID: 106639-05
Keywords: security rpcmod clnt_clts_kinit leak COTS
Synopsis: SunOS 5.6: /kernel/strmod/rpcmod patch
Patch Creation Date: Jun/27/00
==============================
Patch-ID: 106648-01
Keywords: libce security mailtool
Synopsis: OpenWindows 3.6: libce suid/sgid security fix
Patch Creation Date: Sep/02/98
==============================
Patch-ID: 106649-01
Keywords: libdeskset mailtool security filemgr core HOME
Synopsis: OpenWindows 3.6: libdeskset patch
Patch Creation Date: Sep/02/98
==============================
Patch-ID: 106650-04
Keywords: security mailtool attachments home mailrc
Synopsis: OpenWindows 3.6: mailtool attachment security patch
Patch Creation Date: Dec/21/99
==============================
Patch-ID: 106828-01
Keywords: y2000 date wrong
Synopsis: SunOS 5.6: /usr/bin/date patch
Patch Creation Date: Oct/29/98
==============================
Patch-ID: 106834-01
Keywords: security mv ln cp root ownership
Synopsis: SunOS 5.6: cp/ln/mv patch
Patch Creation Date: Jan/21/99
==============================
Patch-ID: 106894-01
Keywords: security uux buffer overflow
Synopsis: SunOS 5.6: /usr/bin/uux patch
Patch Creation Date: Jan/04/99
==============================
Patch-ID: 107336-01
Keywords: security kcms -P printer
Synopsis: OpenWindows 3.6: KCMS configure tool has a security vulnerability
Patch Creation Date: Mar/19/99
==============================
Patch-ID: 107434-01
Keywords: spellchecker libSDtSpell.so.1
Synopsis: CDE 1.2: Spell checking occasionally kills mail
Patch Creation Date: Apr/05/99
==============================
Patch-ID: 107497-01
Keywords: sun4u platform links
Synopsis: SunOS 5.6: sun4u platform links patch
Patch Creation Date: Feb/25/99
==============================
Patch-ID: 107565-02
```

```
Keywords: security tftp passed
Synopsis: SunOS 5.6: /usr/sbin/in.tftpd patch
Patch Creation Date: Oct/15/99
==============================
Patch-ID: 107618-01
Keywords: security permissions vol
Synopsis: SunOS 5.6: Permissions problem in /vol.
Patch Creation Date: Nov/09/99
==============================
Patch-ID: 107733-08
Keywords: security dlerror linker audit libdl mcs 64-bit rtld_db tsorted
cyclic
Synopsis: SunOS 5.6: Linker patch
Patch Creation Date: May/25/00
==============================
Patch-ID: 107758-01
Keywords: security pax modes symlinks
Synopsis: SunOS 5.6: Pax incorrectly change mode of symlink target file
Patch Creation Date: May/26/99
==============================
Patch-ID: 107766-01
Keywords: security ASET cklist 6 months
Synopsis: SunOS 5.6: ASET cklist reports unchanged 6month older files as new
Patch Creation Date: Aug/09/99
==============================
Patch-ID: 107774-01
Keywords: security inetd
Synopsis: SunOS 5.6: inetd denial-of-service attack
Patch Creation Date: Jun/08/99
==============================
Patch-ID: 107991-01
Keywords: security rcp LC_MESSAGES buffer overflow
Synopsis: SunOS 5.6: /usr/sbin/static/rcp patch
Patch Creation Date: Jun/25/99
==============================
Patch-ID: 108199-01
Keywords: security dtspcd
Synopsis: CDE 1.2: dtspcd Patch
Patch Creation Date: Sep/13/99
==============================
Patch-ID: 108201-01
Keywords: security dtaction buffer
Synopsis: CDE 1.2: dtaction Patch
Patch Creation Date: Sep/13/99
==============================
Patch-ID: 108307-02
Keywords: security keyserv fork
Synopsis: SunOS 5.6: keyserv fixes
Patch Creation Date: Apr/14/00
==============================
Patch-ID: 108346-03
Keywords: security rpc.nispasswdd shadow
Synopsis: SunOS 5.6: patch usr/sbin/rpc.nispasswdd
Patch Creation Date: Apr/14/00
==============================
Patch-ID: 108468-02
Keywords: security denial service
```

```
Synopsis: SunOS 5.6: ldterm streams module fixes
Patch Creation Date: May/25/00
==============================
Patch-ID: 108492-01
Keywords: security snoop exploit access root
Synopsis: SunOS 5.6: Snoop may be exploited to gain root access
Patch Creation Date: Dec/07/99
==============================
Patch-ID: 108499-01
Keywords: security ASET gid /tmp med high
Synopsis: SunOS 5.6: ASET sets the gid on /tmp, /var/tmp when setting med
high
Patch Creation Date: Jan/24/00
==============================
Patch-ID: 108660-01
Keywords: security sadmind
Synopsis: SunOS 5.6: Patch for sadmind
Patch Creation Date: Dec/24/99
==============================
Patch-ID: 108804-01
Keywords: security tip overrun
Synopsis: SunOS 5.6: tip has buffer overrun with security implications
Patch Creation Date: Jun/05/00
==============================
Patch-ID: 108890-01
Keywords: security ypxfrd
Synopsis: SunOS 5.6: patch /usr/lib/netsvc/yp/ypxfrd
Patch Creation Date: Apr/14/00
==============================
Patch-ID: 108893-01
Keywords: security Denial Transports
Synopsis: SunOS 5.6: patch /usr/lib/netsvc/yp/rpc.ypupdated
Patch Creation Date: Apr/14/00
==============================
Patch-ID: 108895-01
Keywords: security Denial Transports
Synopsis: SunOS 5.6: patch /usr/sbin/rpc.bootparamd
Patch Creation Date: Apr/14/00
==============================
Patch-ID: 109266-01
Keywords: security mail overflow
Synopsis: SunOS 5.6: security: /bin/mail has buffer overflow
Patch Creation Date: May/09/00
==============================
Patch-ID: 109339-01
Keywords: security nscd
Synopsis: SunOS 5.6: nscd has a potential security problem
Patch Creation Date: May/25/00
==============================
Patch-ID: 109388-01
Keywords: security chkperm buffer
Synopsis: SunOS 5.6: patch /usr/vmsys/bin/chkperm
Patch Creation Date: Jun/02/00
==============================
```

Appendix D - TARA "tigerrc" file used to scan the GIAC firewall:

```
##########################################
# GIAC Enterprises customized tigerrc file #
##########################################
#
# 'rc' file for tiger.  This file is preprocessed, and thus
# can *only* contain variable assignments.
#
#
# TAMU version
#
# Note:  This disables many of the checks.  You should not use this.
#        The checks enabled here are the ones we definitely want done
#        but all of them should be done.
#
#-------------------------------------------------------------------------
#
# Select checks to perform.  Specify 'N' (uppercase) for checks
# you don't want performed.
#
Tiger_Check_PASSWD=Y          # Fast
Tiger_Check_GROUP=Y           # Fast
Tiger_Check_ACCOUNTS=Y        # Time varies on # of users
Tiger_Check_RHOSTS=Y          # Time varies on # of users
Tiger_Check_NETRC=Y           # Time varies on # of users
Tiger_Check_ALIASES=Y         # Fast
Tiger_Check_CRON=Y            # Fast
Tiger_Check_ANONFTP=Y         # Fast
Tiger_Check_EXPORTS=Y         # Fast
Tiger_Check_INETD=Y           # Could be faster, not bad though
Tiger_Check_KNOWN=Y           # Fast
Tiger_Check_PERMS=Y           # Could be faster, not bad though
Tiger_Check_SIGNATURES=N      # Several minutes
Tiger_Check_FILESYSTEM=Y      # Time varies on disk space... can be hours
Tiger_Check_PATH=Y            # Fast for just root... varies for all
Tiger_Check_EMBEDDED=Y        # Several minutes
#
# Should messages tagged with INFO be shown?
#
Tiger_Show_INFO_Msgs=Y
#
# In order for this to be effective, you must set 'CRACK' in a
# 'site' config file.
#
Tiger_Run_CRACK=Y               # First time, ages; subsequent fairly quick
#
# Line size (for formatting of output)... default is 79...
# Specifying '0' means unlimited
#
Tiger_Output_Width=79
#
# Same as above, except used when run via 'tigercron'...
# You should set this once and never change it, 'cause if you
# change it, you'll get lots and lots of new stuff according
# to the scripts (the diff's against previous reports will find
```

```
# lots of changes due to the formatting changes).
#
Tiger_CRON_Output_Width=0
#
# If an embedded pathname refers to an executable file, this executable
# will in turn be checked.  This will continue "recursively" until
# either no new executables are found, or a maximum reference depth
# is reached.  Setting this variable to 0 is equivalent to infinity.
# On a Sun 4/490, SunOS 4.1.2, 6GB disk, an infinite depth check
# took about 30 minutes.  Your milage will vary.
#
# On small memory systems, a large search depth can result in out
# of memory situations for 'sort'... :-(...
#
Tiger_Embed_Max_Depth=3
#
# Only search executables for embedded pathnames.  If this is
# set to 'N', then all regular files will be searched.  Otherwise
# only executable files will be searched.
#
Tiger_Embed_Check_Exec_Only=Y
#
# Check all setuid executables found.  This will cause 'tiger'
# to run longer on many systems, as it will have to wait for the
# file system scans to complete before it can begin checking the
# embedded pathnames.
#
Tiger_Embed_Check_SUID=Y
#
# Only report executables which are writable or not owned by root.  If set
# to 'Y' only the executables will be reported.  Any other value will result
# in regular files and directories being reported as well.
#
# Note that currently, device files are never reported.
#
Tiger_Embed_Report_Exec_Only=Y
#
# Who do you allow to own system files.
# List of usernames separated by '|'... no whitespace
#
Tiger_Embedded_OK_Owners='root|bin|uucp'
#Tiger_Embedded_OK_Owners=root
#
# What groups can have write access to system files?
# List of group names separated by '|'... no whitespace.
# No value means no groups should have write access.
#
Tiger_Embedded_OK_Group_Write=
#
# Should all users' PATH variables be checked.  This has the potential
# of being dangerous because of the way it is done.  You might want to
# take a look at check_path and decide for yourself whether the precautions
# are sufficient before enabling this.
#
Tiger_Check_PATHALL=Y           # Check all user PATHs in startup files.
#
# Who can own executables in 'root's PATH?
```

```
# List of usernames separated by '|'... no whitespace
#
Tiger_ROOT_PATH_OK_Owners='root|uucp|bin|sys|daemon'
#Tiger_ROOT_PATH_OK_Owners='root'
#
# What groups can have write access to executables in 'root's PATH?
# List of group names separated by '|'... no whitespace.
# No value means no groups should have write access.
#
Tiger_ROOT_PATH_OK_Group_Write=
#
# Who can own things in other users PATH?
# List of usernames separated by '|'... no whitespace
#
Tiger_PATH_OK_Owners='root|bin|uucp|sys|daemon'
#
# What groups can have write access to executables in non-root user PATH?
# List of group names separated by '|'... no whitespace.
# No value means no groups should have write access.
#
Tiger_PATH_OK_Group_Write=
#
# Should 'tiger' wait for Crack to finish?  If set to 'Y' it will wait
# until it finishes.  If set to 'N', it will collect the output if
# Crack finishes before the rest of the checks.  If it isn't finished
# 'tiger' will simply report where the output will be stored.
#
Tiger_Collect_CRACK=N
#
# Run Crack on local password sources only?  If set to Y, no network
# sources will be used.  If set to 'N', NIS, NIS+, NetInfo, etc
# sources will also be used.
#
Tiger_Crack_Local=Y
#
# Who gets output from 'tigercron'?
#
Tiger_Mail_RCPT=root
#
# List of '/' separated filename globs (NOT pathnames) to look for
# on the filesystems.
#
Tiger_Files_of_Note="..[!.]*/.* */.*      */.[!.]/.log/.FSP*"
#
# File system scan - things to look for
#
Tiger_FSScan_Setuid=Y         # Setuid executables
Tiger_FSScan_Devs=Y           # device files
Tiger_FSScan_SymLinks=Y       # strange symbolic links
Tiger_FSScan_ofNote=Y         # wierd filenames
Tiger_FSScan_WDIR=Y           # world writable directories
Tiger_FSScan_Unowned=Y        # files with undefined owners/group
#
# Should we scan read-only filesystems
#
Tiger_FSScan_ReadOnly=N
#
```

```
# List of dot files commonly found in user home directories.  These
# will be checked by check_accounts for proper access permissions.
#
# Note that .rhosts and .netrc need not appear here, as they will
# be checked by scan_rhosts or scan_netrc.
#
USERDOTFILES=".cshrc .profile .login .mailrc .exrc .emacs .forward .tcshrc
.zshenv .zshrc .zlogin .zprofile .rcrc .bashrc .bash_profile .inputrc
.xinitrc"
#
# Rhost sites which are expected to be in the .rhosts files.
# Anything that doesn't match will be reported.  The patterns
# are simple patterns as used in Bourne Shell 'case' statement.
#
#RHOST_SITES='*.tamu.edu|jupiter'
```

References

[1] Sun Mircrosystems, "Ultra 60 Workstation". URL: http://www.sun.com/desktop/products/ultra60 (April, 15 2002)

[2] Johnson, Bryan, "BigAdmin[sm] System Administration Portal", URL: http://www.sun.com/bigadmin/shellme/, (April, 17 2002)

[3] Fyodor, "Nmap network security scanner man page". URL: http://www.nmap.org/nmap/nmap_manpage.html (April 20, 2002)

[4] "rpcinfo - report RPC information". URL: http://www.unidata.ucar.edu/cgi-bin/man-cgi?rpcinfo+1 (April 20, 2002)

[5] Poulsen, Kevin, "Security Hole found in NAI Firewall" May 22, 2000. URL: http://online.securityfocus.com/news/40 (April 23, 2002)

[6] Poulsen, Kevin, "NAI firewall suffers second serious hole. Experts ask, is anything safe?" September 4, 2001. URL: http://online.securityfocus.com/news/248 (April 23, 2002)

[7] "Gauntlet firewall mailing list", URL: http://www.rmsbus.com/gauntlet-user.htm (April 23, 2002)

[8] SecureComputing.com, "Gauntlet 5.5 Patches" February 26, 2002. URL: http://www.securecomputing.com/index.cfm?sKey=986 (April 23, 2002)

[9] Sunsolve.sun.com, "Solaris 2.6 Recommended Patch Cluster" URL: http://sunsolve.Sun.COM/pub-cgi/retrieve.pl?doctype=patch&doc=2.6_Recommended.README (April 24, 2002)

[10] Robinson, Phillip, "SANS GCUX Practical Assignment" March 23, 2002. URL: http://www.giac.org/practical/Phillip_Robinson_GCUX.doc (April 24, 2002)

[11] Sun.com, "Sun(tm) Patch Check, Version 1.1" URL: http://sunsolve.sun.com/pub-cgi/show.pl?target=patchk (April 26, 2002)

[12] Advanced Research Corporation, "*T*iger *A*nalytical *R*esearch *A*ssistant" August 15, 2002. URL: http://www-arc.com/tara/index.shtml (June 15th, 2002)

[13] Stanford University, "Solaris Fixperms" September 26, 2000. URL: http://www.stanford.edu/group/itss-ccs/security/unix/Solaris/solaris_fixperms.html (July 3rd, 2002)

[14] ISS, "Port 32776 rpc.spray" URL: http://www.iss.net/security_center/advice/Exploits/Ports/32776/default.htm (July 9th, 2002)

[15] Holland, Jeff "Re: [gauntlet-user] Problem installing 64-bit Gauntlet 6.0 on SUNBlade" August 23, 2001. URL: http://marc.theaimsgroup.com/?l=gauntlet-user&m=99859896010055&w=2 (July 10th, 2002)

[16] Shivdasani, Meenoo Jeff "Re: [gauntlet-user] Problem installing 64-bit Gauntlet 6.0 on SUNBlade"August 23, 2001. URL: http://marc.theaimsgroup.com/?l=gauntlet-user&m=99860411027272&w=2 (July 10th, 2002)

[17] U.S. Department of Energy, "L-032: Class Loading Vulnerability in Sun Java (TM) Runtime Environment", January 30, 2001. URL: http://www.ciac.org/ciac/bulletins/l-032.shtml (July 10th, 2002)

[18] Sunsolve.sun.com, "Solaris 2.6 Patch Report Update" URL: http://sunsolve.sun.com/pub-cgi/show.pl?target=patchrpts/2.6&type=0 (July 10th, 2002)

[19] Holland, Jeff "SANS GCIA Practical", August 28, 2001. URL: http://www.giac.org/practical/Jeff_Holland_GCIA.doc (July 18th, 2002)

[20] "syslog.conf - configuration file for syslogd system log daemon" URL: http://www.sunspot.noao.edu/cgi-bin-local/man-cgi?syslog.conf+4,(August 9, 2002)

[21] Sun.com, "Security Vulnerability in the Network Services Library, libnsl(3LIB)" August 19, 2002. URL: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F46122 (August 13, 2002)

[22] Sun.com, "Buffer Overflow in cachefsd in Solaris" May 31, 2002. URL: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F44309 (August 13, 2002)

[23] CERT Coordination Center, "CERT® Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)" August 28, 2002. URL: http://www.cert.org/advisories/CA-2002-03.html (August 13, 2002)

[24] CERT Coordination Center, "CERT® Advisory CA-2001-21 Buffer Overflow in telnetd" April 16, 2002. URL: http://www.cert.org/advisories/CA-2001-21.html (August 13, 2002)

[25] CERT Coordination Center, "CERT® Advisory CA-2001-15 Buffer Overflow In Sun Solaris in.lpd Print Daemon", August 31, 2001. URL: http://www.cert.org/advisories/CA-2001-15.html (August 13, 2002)

[26] CERT Coordination Center, "CERT® Advisory CA-99-05 Vulnerability in statd exposes vulnerability in automountd" June 9, 1999. URL: http://www.cert.org/advisories/CA-99-05-statd-automountd.html (August 13, 2002)

[27] SecureComputing.com, "Gauntlet Firewall for UNIX – User's Guide Version 5.5" URL: http://www.securecomputing.com/pdf/55ug.pdf (August 26, 2002)

[28] Spitzner, Lance "Armoring Solaris" August 19, 2001. URL: http://www.enteract.com/~lspitz/armoring.html (August 26, 2002)

[29] "Password Man Page" URL: http://www.qnx.com/developer/docs/qnx_4.25_docs/qnx4/utils/p/passwd.html (August 26, 2002)

[30] Farmer, Dan, Powell, Brad and Archibald, Matt "Example Login Banner - Titan system", URL: http://www.dougmoran.com/Guide/login-banner-titan.htm (August 26, 2002)

[31] "A reference guide for available modules", URL: http://www.kernel.org/pub/linux/libs/pam/Linux-PAM-html/pam-6.html (August 26, 2002)

[32] Princeton University, "man page – utmp" URL: http://campuscgi.princeton.edu/man?utmp (August 26, 2002)

[33] Caldera.com, "Changing the /etc/motd file", June 22, 2001. URL: http://ou800doc.caldera.com/SM_startup/sstT.etcmotd.html (August 28, 2002)

[34] Sun.com, "AnswerBook2 · SunSHIELD Basic Security Module Guide" URL: http://216.239.53.100/search?q=cache:bimhSORVhbcC:tide.scc.ua.edu:8888/ab2/coll.47.4/SHIELD/%40Ab2PageView/554+bsm+%22stop-a%22+&hl=en&ie=UTF-8 (August 28, 2002)

[35] "Customizing Your `.cshrc' File" URL: http://www.cs.bu.edu/help/unix/customizing_your_.cshrc_file.html (August 30, 2002)

[36] Brotzman, Lee, Pomeranz, Hal, "Track 6 – Securing UNIX Systems – Linux/Solaris Practicum" 2002. (August 30, 2002)

[37] SecureComputing.com, "Release Notes for Gauntlet Firewall Version 6.0" URL: http://www.securecomputing.com/pdf/G6README.TXT (September 7, 2002)

[38] CERT Coordination Center, "CERT® Advisory CA-1996-19 Vulnerability in expreserve" July 5, 1996. URL: http://www.cert.org/advisories/CA-1996-19.html (September 7, 2002)

[39] Northcutt, Stephen, Ettinger, Sheila, "GIAC Intrusion Detection Curriculum Practical Assignment Guidelines: The Traces and Analysis Segment of the Practical – Version 1.1" URL: http://www.giac.org/ID_assignment_guidelines.php#9 (September 8, 2002)

[40] Kurt Koenigsknecht, "SANS GCUX Practical" November 2001, URL: http://www.giac.org/practical/Kurt_Koenigsknecht_GCUX.doc (September 9, 2002)

[41] CERT Coordination Center, "CERT® Advisory CA-2002-01 Exploitation of Vulnerability in CDE Subprocess Control Service" January 14, 2002. URL: http://www.cert.org/advisories/CA-2002-01.html (September 9, 2002)

[42] SecureComputing.com, "Gauntlet 5.5 Getting Started Guide" URL: http://www.securecomputing.com/pdf/55gsg.pdf (September 12, 2002)

[43] Spitzer, Lance "Core Installation of Solaris 2.6 for FW 4.0", URL: http://www.enteract.com/~lspitz/core6.txt (September 12, 2002)

[44] Sun.com, "Solaris 2.6 Admintool" (September 13, 2002)