Security Audit of GIAC Enterprises' Community Web and Mailing List Server

by
Brian McEntire

Table of Contents

Executive Summary

The Consumer Affairs department of GIAC Enterprises recently engaged in a complete audit of their public information server. The department runs a web server with several auxiliary services to promote positive communications and brand awareness among customers. Management sought to ensure that the server met high security standards. Their online community initiative has grown rapidly, resulting in increased importance to the rest of the company. Management expressed a desire to improve security with a minimum of capital expenditures.

Interviews were conducted with the system administrators and the manager responsible for the server. These meetings defined the parameters for the audit, the role of the server, and provided insight into existing system administration practices. During the course of the audit, the server's configuration, patches, and installed applications were thoroughly examined. A remote scan of the server was performed to identify and highlight openings on the system that might be exploited by criminals to interrupt service or gain deeper access into GIAC Enterprises' computers and networks.

The most important recommendations for improving security on the server are to place the server behind a new or existing firewall and upgrade all third party applications to the most recently released versions. The server has several ports open to the Internet that present security risks. Access to those ports can be restricted without impacting the server's intended functions. Four of the applications used on the server to fulfill its functions, including the web server and mailing list software, are out of date and have widely publicized security vulnerabilities. These risks should be mitigated as soon as possible. Detailed recommendations are given in the Critical Issues and Recommendations section of this audit report.

Another significant factor that impacts the reliability, security, and serviceability of the audited system is the age of the hardware it is based on and the age of the operating system it runs. The primary suggestion for addressing these risks is to locate newer, low cost hardware and upgrade the operating system. However, in light of the popularity of open source software being used in other projects within the company, the department may want to switch from the HP-UX platform to a Linux based platform.

Overall, the audit found many aspects of the server to be well secured and determined that good system administration practices are being followed. However, the audit also found areas in which the server's security and administrative processes can be significantly improved. Detailed recommendations are provided for each issue identified for improvement.

Description of the System and Audit Methodology

Description of Audited System and Associated Software Applications

GIAC Enterprises runs a web server and mailing list server to promote positive communications with their customers and build a dedicated community among consumers of GIAC Enterprises' line of humorous fortune cookie sayings. GIAC Enterprises asked that this audit focus primarily on this community web and mailing list server component of their e-commerce empire. They have previously audited their order taking, billing, and back office assets.

GIAC Enterprises has stated that their online community effort is essential to enhancing their brand recognition. However, given tight margins in the highly competitive fortune cookie saying industry, the company must maintain a lean budget for this effort. While they are dedicated to this initiative, they do not rely on it for day to day operations. GIAC Enterprises prefers to use existing or low cost computing assets as the foundation for their online community effort. Furthermore, they have a strong preference for using free, open source software, in favor of more expensive, proprietary software, whenever feasible.

Currently, the company runs an Apache Web server, Majordomo mailing list server, and Discus discussion forum software on an HP K100 server that was donated to the project by another department when they upgraded their computer systems.

Technical Details of the Audited Server

Hostname	Crunchy
IP Address	10.0.0.2
Manufacturer	Hewlett Packard
Model	HP 9000/809 model K100
Processor	PA7200 RISC 1.1d, 100 MHz
Memory	256 MB RAM
Storage	6GB total, 3 x 2GB internal SCSI drives
Operating System	HP-UX 10.20

Applications and Tools Installed on the Audited Server

Application	Installed Version
Sendmail	8.9.3
Apache	1.3.26
Majordomo	1.94.4
Discus	3.01
WU-FTPD	2.6.0
Analog	4.13

Specific Concerns Related to this System and its Role

Given this system's role as a web, mailing list, and discussion forum server, there are several specific concerns associated with the system. The server is directly connected to the Internet through GIAC Enterprises' ISP; there is no firewall between the system and the general Internet. Services running on the system must allow incoming connections that originate outside of the enterprise LAN because the system is intended for a wide, public audience. Still, there are many ports that need not be exposed to external traffic in order for this system to fulfill its role. Attention must be given to closing or protecting these non-public ports.

Because the system runs services that allow external connections, abundant care must be given to hardening the computer against external threats. The hardening process includes closing all unneeded points of access and maintaining the very latest patch levels. This system runs services that have historically been widely exploited by attackers. Sendmail, in particular, has been a widely targeted service. The "SANS / FBI Top 20 List" states that "Sendmail's widespread use on the Internet has historically made it a prime target of attackers, resulting in numerous exploits over the years." During the course of this audit, Sendmail, BIND, and other potential vulnerabilities from the Top 20 List will be examined for relevance to this server and recommendations will be made to manage risks.

Audit Methodology

The Audit was conducted in two stages. The first stage was a meeting with the system administrators and manager responsible for ensuring the computer's healthy day to day operation. The manager of this group has recently been tasked with ensuring that the computer meets the company's information security guidelines based on consensus best security practices. This group described the system's role and its current configuration very thoroughly during the meeting. I used this meeting to gather information about the department's current processes for patch installation, configuration management, and other system administration practices.

For the second stage of the audit, a mid-level systems administrator was assigned to oversee every step of my work auditing the system. GIAC Enterprises offered to give me full root access to the system to assist my auditing efforts, provided that all work requiring root access was done on the premises and with appropriate oversight. I was given a regular user account on the host and a and home directory where I could store the intermediate results of my auditing. My assigned user name was auditor. My assigned home directory was /home/auditor.

During the second stage of the audit, I inventoried the computer hardware, software, services, and running processes using commands built into the operating system. Commands utilized for this stage included:

- uname –a, to determine the version of the operating system
- swlist, to list HP-UX patches installed with the swinstall command
- SAM – HP's graphical user interface for system administration, to determine the CPU architecture and amount of physical RAM
- vgdisplay -v, to examine volume groups and to determine which internal disks were used by the system
- diskinfo, to query the hardware for the specific disk model numbers and the physical characteristics of the internal disk devices
- lsof –i, to list processes listening for TCP and UDP network connections

Detailed explanations of how the commands were used and the resulting information gathered will be given in the Detailed Analysis section of this report. Additionally, during this stage of the audit, with permission from the system and LAN administrators, security office, and senior management, I used the open source NMap software application, running on my auditing laptop, to probe the server from across the LAN. This allowed me to gather information to aid in reporting what the system currently looks like to any attacker or probing entity on the public Internet. Generally, the audit found some aspects of the server to be very well secured and maintained but also found significant areas in which the server's security and the processes used to maintain the server can be improved.

Detailed Analysis

Operating System Vulnerabilities and Patch Installation

The HP-UX 10.20 operating system is several years old. It was first released in August 1996 according to HP's notice titled "HP-UX on PA-Risc 10.20 Discontinuance and Obsolescence update." Because it is a mature operating system, many patches are available that address security vulnerabilities discovered during the years since the operating system was originally released. It is vitally important to apply all applicable security patches from the operating system vendor on systems directly accessible from the Internet.

HP makes their complete list of HP-UX security patches available to the public each day in a report titled "HP-UX Patch Security Matrix." This report, which can be retrieved with either a web browser or FTP client, contains all applicable security patches for all versions of the HP-UX operating system and all models of HP workstation and server hardware.

This audit focuses on an HP 9000 series 800 server running HP-UX 10.20. Please refer to appendix A.1 for a complete list of applicable security patches for this platform.

I gathered a list of the currently applied patches on the host using the following swlist command run as root. Before running the command, I set /usr/sbin and /usr/bin as the first entries in my environment PATH variable.

```
swlist -l fileset -a state | grep configured | grep 'PH[KL|NE|CO|SS]' >
/home/auditor/patchlist.out
```

This combination of commands uses the HP-UX 10.20 swlist command to examine the registry of software previously installed on the host with swinstall commands. All HP released patches are installed with swinstall so swlist returns a complete listing of operating system patches installed on the system. The rest of the command filters the swlist output to ensure quality of the results. The first grep statement ensures that only patches in a "configured" state, that is patches that are properly and completely applied, are listed. The second grep statement uses regular expressions to list only patches supplied by HP so no other software packages will be listed in the output. Finally, there is a redirection to a file in my home directory named patchlist.out.

Patches not fully applied to the system, because of an error downloading the patch or various problems that can occur during the patch application process, show up in the swlist output with a state other than "configured." The other possible states are "transient", "corrupt", "available", and "installed." I ran the following command to make sure that all patches applied were completely configured:

```
swlist -l fileset -a state |grep 'PH[KL|NE|CO|SS]'|grep -v -e configured -e '^#'
```

That command examines only patches. HP-UX operating system patches fall into one of four types – PHCO, PHKL, PHNE, and PHSS. The grep commands filter out comment lines that begin with a hash mark and filter out lines that contain the word “configured.” The command yielded no output – confirmation that all patches applied to this system are completely configured.

It is possible, although it can be a potentially error prone process, to manually compare the patch list output to the complete list of HP-UX security patches for this platform (listed in Appendix A.1.) Instead, I ran the shell script given in Appendix B. That script filters out all applied patches from the complete list of potential patches, highlighting only patches which may need to be applied.

Some of the candidate patches listed by that script may not need to be applied because they patch a specific OS subsystem that is not used on this host. With a pared down list of potentially applicable patches in hand, I met with department system administrators to determine which patches were applicable to this platform. The only recommended security that was applicable to the server but had not yet been applied was patch PHCO_27564. That is a sort() cumulative patch that fixes a local privilege escalation vulnerability. The full results of the patch comparison are given in Appendix A.2.

A final concern for this operating system is Hewlett-Packard’s planned obsolescence of this version of the HP-UX operating within a short period of time. Per the “HP-UX on PA-Risc 10.20 Discontinuance and Obsolescence update” notice cited earlier, HP plans to cease support for the HP-UX 10.20 as of June 30, 2003. There are two security implications associated with the impending obsolescence.

HP will no longer release patches for the operating system. It a virtual certainty that security related bugs still remain in the operating system and some will be uncovered after June 30, 2003. However, HP will not release software fixes to patch vulnerabilities in HP-UX 10.20 after that date. If a vulnerability applies to a subsystem or service that is a necessary part of this computer, and if the threat cannot be mitigated, the only options will be to either shutdown that component of the server or risk running the vulnerable service and suffering a computer security compromise.

The other issue related to obsolescence is the lack of available technical support. HP technical support contracts for HP-UX 10.20 assistance can no longer be purchased. Although the operating system is stable and GIAC Enterprises administrators have several years of experience maintaining it, there is a significant risk associated with serving the online community presence from a computer with no vendor support. Any failures that cannot be solved by GIAC Enterprise's system administrators may result in extended unavailability of the web presence. Such problems may require consultants or third party support avenues in order to attain a solution. If the decision is made to stay with HP-UX 10.20 beyond June 2003, an effort should be made to arrange 3rd party support as soon as possible so that support contracts are established and available in the event they are needed.

Patch Management

During interviews conducted with GIAC Enterprises' system administrators, current patch management practices were explained. Systems administrators apply vendor recommended patches to this system on a six month cycle unless GCIRT recommends applying a specific patch immediately. GCIRT is GIAC Enterprises' Computer Incident Response Team. They are responsible for ensuring security across the entire enterprise's computer and network infrastructure. GCIRT is the authority that responds to computer compromises in the organization and coordinates forensics, system clean-up, and prosecution of legal cases in the event of a computer security breach. Occasionally, GCIRT will classify a newly discovered security vulnerability as critical and ask the entire organization to patch their systems within 72 hours. GCIRT may also mandate immediate action if a vulnerability is seen exploited on multiple computer systems within the organization. GCIRT is tasked with tracking the security threat environment, major security announcements, and making timely recommendations upon which GIAC Enterprises' departments must take action.

Computers should always be backed up prior to applying new patches since the possibility exists that a corrupted download or interrupted patch installation may put a system into an inconsistent or inoperable state. GIAC system administrators confirmed that they always make a bootable system image backup immediately prior to installing new patches. They use the HP make_tape_recovery command with options to backup the entire root volume. This is a sound practice since the host uses only the root volume and the root volume is small enough to fit, in its entirety, on a single DAT tape. The following command is used to make a bootable backup image of the host:

```
/opt/ignite/bin/make_tape_recovery –A –a /dev/rmt/0m
```

The administrators document their routing patching and their intra-cycle patching activities in the department's issue tracking system. The department uses the Bugzilla issue tracking system. They find that solution very robust and they like the price tag – free, because it is open source software and they support it themselves. Each time administrators apply patches to the system, they open a new Bugzilla case and document the new patches installed on the system. They also include patch descriptions and any GCIRT directives in each case. Their documentation processes are commendable. The issue tracking system provides a sound mechanism to document system changes which eases configuration management. Administrators commented that, occasionally, GCIRT will mandate a new patch and the administrators can quickly certify that they have already installed the patch with a simple query to the issue tracking system.

Configuration Vulnerabilities

Passwords

The audited computer runs HP-UX 10.20 in untrusted mode. This presents a configuration vulnerability with respect to account passwords. Most modern UNIX operating systems use shadow passwords. Shadow passwords move the encrypted password string out of the world readable /etc/passwd file and into a shadow file, usually /etc/shadow. When running in trusted mode, the HP-UX 10.20 operating system maintains the shadow password database in the /tcb/files/auth/ directory and below.

Shadow passwords provide an improvement in system security by moving the encrypted password strings to a file that is only readable by root. On an untrusted HP-UX system with encrypted passwords stored in a user readable /etc/passwd file, any user with telnet or FTP access to the host can copy that file off to another computer and run a password cracking program, such as John The Ripper (http://www.openwall.com/john/), against the password file. John The Ripper can quickly identify any weak passwords in the /etc/passwd file, potentially exposing the root password or allowing privilege escalation in which an authorized user with restricted privileges gains access to an account with higher permissions and access to more sensitive files and areas of the system.

Telnet

During the audit interview, I discovered that systems administrators use telnet to access the computer across the network. This is not surprising since telnet clients have long been used to connect to computers via local networks and even across the Internet from great geographic distances. However, this is a major security vulnerability because telnet sessions can be easily hijacked. The SANS Reading Room has a good article that gives a detailed, technical description of telnet session hijacking. The article, titled “Analysis of a Telnet Session Hijack via Spoofed MAC Addresses and Session Resynchronization,” can be found at http://www.sans.org/rr/threats/hijack.php. The synopsis of the article is that tools are readily available that allow hackers to gain control of established telnet sessions. This allows an attacker to gain control of any telnet sessions connected to the computer at the time of the attack. The attacker may gain access to a regular user account and then exploit a local privilege escalation attack to gain higher or super user privileges on the computer. The attacker may also gain access to a telnet session being used by a remote root user. In that case, the attacker has complete access to all parts of the system. They could install back door accounts, malicious software, or access private information such as customer comments or contact information.

Risks From Installed Third-Party Software

In the course of auditing the system, it was determined that none of the third party software applications used to provide the online community had been upgraded to current versions and patch levels. All but one of the third-party software applications exposed the server to security risks because their versions were out of date.

Application	**Installed Version**	**Latest Version**
Apache	1.3.26	1.3.27
Majordomo	1.94.4	1.94.5
Discus	3.01	4.00.3
WU-FTPD	2.6.0	2.6.2
Analog	4.13	5.32

The versions of the installed applications were gathered with the following commands (output shown immediately beneath each command):

```
$ /opt/apache/bin/httpd -v
Server version: Apache/1.3.26 (Unix)
Server built:   Jul  2 2002 10:23:07
```

```
$ grep majordomo_version /opt/majordomo/majordomo_version.pl
$majordomo_version = "1.94.4";
```

```
$ grep DISCUS_VERSION /opt/apache/cgi-bin/discus/board-setup.cgi
$DISCUS_VERSION = '3.01';
```

[FTP version determined simply by connecting via FTP client to the site]

```
220 kingfisher FTP server (Version wu-2.6.0) ready
```

[Analog version determined simply by connecting to the web stats page]

```
This analysis was produced by analog_4.13.
```

Keeping third party applications up to date is a very important part of maintaining the security of publicly accessible computer systems. Newer versions of applications frequently fix security vulnerabilities discovered in older releases. This is the case with several of the installed third party applications.

The Apache software provides the web server running on this computer. Apache version 1.3.27 fixes three know vulnerabilities in Apache 1.3.26. Those vulnerabilities include a fix for a cross-site scripting vulnerability, a denial of service attack, and a buffer overflow that could lead to a denial of service or execution of arbitrary code on the server. These significant vulnerabilities could lead to a service outage or even a root compromise of the computer. The vulnerabilities are identified in MITRE Corporation's Common Vulnerabilities and Exposures Dictionary available on the web at http://cve.mitre.org/cve/index.html. See CAN-2002-0839, CAN-2002-0840, and CAN-2002-0843 for more information about the vulnerabilities in Apache version 1.3.26.

The Majordomo software provides a mailing list server. The software automates the management of message distribution via mailing lists. Majordomo is the component that enables people to subscribe to the GIAC Enterprises "Outrageous Fortunes" mailing list to suggest fortune cookie slogans and discuss interesting fortune cookie happenings. Majordomo version 1.94.5 fixes a local privilege escalation vulnerability in that affected versions 1.94.4 and earlier. See CAN-2000-0035 for additional details.

The installed version of the Discus website discussion forum software is several versions out of date. There has been a major version upgrade and several maintenance releases since the release currently installed. The CVE dictionary does not list any security vulnerabilities for Discus and Discus's website does not indicate there are any vulnerabilities in the older version. Still, the newer version fixes bugs in the older versions and offers speed improvements. The speed improvements will help keep the load on the server low and improve visitors' experiences on the web site by serving pages faster.

WU-FTPD is an open source replacement for ftpd servers included in vendor operating system releases. WU-FTPD was developed to improve security and FTP server performance at high traffic FTP sites. The application provides the file transfer capability of GIAC's online community. The 2.6.0 version of WU-FTPD installed on the server is out of date and is open to many critical security exploits including vulnerabilities allowing remote code execution. Two serious vulnerabilities that could result in remote execution of arbitrary commands are discussed in CERT Advisory CA-2001-33 which is available on the web at http://www.cert.org/advisories/CA-2001-33.html. See the CVE dictionary for details on several other issues related to the 2.6.0 version of WU-FTPD: CVE-2000-0573, CVE-2001-0138, CVE-2001-0187, CVE-2001-0550, CAN-1999-0076, CAN-1999-0156, CAN-1999-066, CAN-1999-0911, CAN-2001-0935.

Analog is an open source web site statistics analysis application. It is used to analyze web server logs and deliver reports about the number of visitors to the site over time, pages accessed most frequently, pages that contain errors, etc. This is very useful software for a webmaster but many corporations do not want their web server statistics made widely available to the public. Analog version

4.13, installed on this server, is vulnerable to a buffer overflow that allows remote attackers to execute arbitrary commands. CAN-2001-0935 has more details.

Systems administrators indicated that no routine schedule currently exists for patching or upgrading third party software. They do not subscribe to security announcement lists. They do not routinely check to determine if new versions of the installed third party applications are available or whether security issues related to the software have been announced.

Administrative Practices

This system's administrators use a robust, query able issue tracking system to track all patching and software installation tasks for the system. The issue tracking system provides a good revision tracking mechanism for monitoring configuration changes made to the system. Use of the issue tracking system for these purposes and related documentation purposes is commendable and should continue.

The administrators maintain several facilities for monitoring the health of the server which notify them at regular intervals if there are any problems with the server. They set up syslogd to log not only to the local system, but also to a remote log host that is behind the corporate firewall. This ensures that even if the server is compromised, the log host behind the firewall should have accurate records of the attackers activity. They worked with the administrator of the log host system to install the LogSentry application created by Psionic. (At the time of writing this report, the LogSentry software was no longer available on the web. The software might not be actively maintained.) Administrators configured that application to e-mail them once an hour if there are any active hacker alerts or critical messages in the syslog messages sent from the server.

The administrators also monitor the health of the server and several other hosts on the network in real time using the Big Brother system and network monitoring application available from BB4 Technologies at http://bb4.com/. They keep a close eye on several aspects of the server health including CPU load, disk space, swap space, and whether the httpd server is functional. Administrators configured the Big Brother application to send them e-mail if any monitored subsystems enter into a warning state and send a message to their pagers if any of the monitored subsystems enter a failed state.

All administrators must log in to the system with their own, unprivileged accounts. They share the root password and access to the root account. The system is configured not to accept remote logins as root. Instead, users must switch to root with the su command. This provides a level of protection against brute force attacks on the root account and provides a record, via syslogd, indicating which user switch to root and at what time.

Identification and Protection of Sensitive Data on the Host

This server is used to promote GIAC Enterprises online community and is dedicated for the department's brand recognition enhancement program. The server provides discussion forums, several fortune cookie related mailing lists, and product information pages. However, this server is not used for any of GIAC Enterprises back office functions, nor order processing, nor business to business services. The server is strictly dedicated to promoting the company's brand and providing a vibrant community for its customers. Given these parameters, relatively little sensitive information is kept on the server.

Only the systems administrators have accounts on the server. Public visitors to the site do not need accounts to access the web site, discussion forums, or mailing lists. The FTP file transfer functionality provided by the server is for anonymous FTP downloads only. The decision to keep FTP as outgoing only was made jointly by administrators and managers since there had been little interest by visitors to upload files and the administrators knew that allowing anonymous uploads could open the site to partial denial of service attacks if someone intentionally, or unintentionally, consumed all the space in the incoming directory.

Still, there are areas of the server that need to be protected so that if the system is compromised, damage to the system can be limited or the attacker's journey through the system may be slowed. The /etc/passwd file was checked to make sure it was only writable by root. Because the system is untrusted, it cannot use shadow passwords which would give better protection of the accounts. The web server's configuration files are owned, readable, and writable only by the special purpose www user. Regular users do not need access to those configuration files. Web server configuration files are located in /opt/apache/conf. All log files written by processes running as root are owned, readable, and writeable only by root. Log files for the web server and other processes running as a non-root users are owned, readable, and writeable only by the user associated with that process. These precautions ensure that if an attacker does gain access to a non-privileged account on the system they cannot peer into system logs to gain insight into the workings of the system or examine logs to extract any information.

Protection of Sensitive Data Transmitted Over the Network

This server does not transmit any sensitive data to end users on the Internet. Therefore, it is not necessary to use SSL or other methods of secure web site access. Also, all e-mail sent to the mailing list is for public discussion, there is no need to use public key cryptography to encrypt messages. These communications are explicitly for public consumption and none of the transmitted data is sensitive.

However, the system administrators need to modify the way they access the server. They currently use insecure methods to connect to the server and they do transmit sensitive data, such as passwords, over the corporate network. Administrators use telnet and FTP to remotely manage the server. Telnet sessions should not be used because the sessions can be hijacked by a malicious attacker. Administrators indicated they connect to the server via FTP, using their own user accounts and passwords, to transfer files when they need to place new software or configuration files on the server. FTP is an extremely insecure method of accessing password protected user accounts because the FTP client transmits the user's password the FTP server in clear text form and in a single packet. It is trivial for an attacker who is able to place a packet sniffer on the network to watch data traversing the network and capture the passwords of the administrators. Such an attacker could be external to the corporation and could have compromised another server on the company network or could be a disgruntled employee with access to a computer on the same network segment as the server. Once the passwords are captured, the attacker can gain access to a regular user account on the server and can look for local vulnerabilities or local privilege escalation opportunities to gain root access to the server.

Access Controls

The server implements TCP Wrappers to restrict telnet access to the server to connections originating from the corporate network. This is a good precaution, but again, telnet should be avoided since it is trivial to hijack connected sessions. Administrators do not use TCP Wrappers to restrict access to FTP, mail, or the web server since all of those functions are intended to be publicly accessible. Appendix C contains the output from a remote NMap scan of the server. The scan revealed that the server is partially hardened. Only the ports needed for serving the online community are open, with a few exceptions: the system is running a DNS named daemon that is accessible from outside the corporate network and several system maintenance, backup, and software depot daemons currently accept connections from across the Internet. When I asked the systems administrators about that DNS component they were surprised to find out it was running on the server and thought it must be a relic of the server's previous role in another department.

The NMap scan shows the telnet port as being open because NMap can connect to the port. However, telnet connections originating outside the corporate network do not result in a successful connection because the telnet service is protected with TCP Wrappers. When external telnet connections are attempted, the connection is closed before the server presents a login sequence. The NMap command line used to probe remote access is given below. Note that all ports from 1 to 65000 were scanned because ports above 1024 can also be exploited to gain access to the system. The default NMap behavior only scans privileged ports, the –p parameter specifies a larger port range:

```
nmap –sS –p 1-65000 –O 10.0.0.2 –oN nmap-crunchy.log
```

NMap found several ports listening for which it could not find a port number to service name mapping in /etc/services. NMap labeled these services as “unknown.” To determine what processes were running and listening on those ports, I ran an lsof command to list processes and their associated ports. The output from that command is given in Appendix D. The command executed was:

```
/opt/lsof/bin/lsof –i | grep LISTEN
```

TCP Wrappers access controls are governed by the /etc/hosts.allow and /etc/hosts.deny files. The contents of those files are:

```
$ cat /etc/hosts.allow
telnet: 10.0.
ftpd: ALL

$ cat /etc/hosts.deny
ALL: ALL
```

TCP Wrappers, as implemented on this server, will only affect TCP based services started by the inetd super server. Inetd starts network daemons as incoming connections are made. High traffic services, such as the httpd web daemon incur too much overhead if they must be started by inetd for each incoming connection. The httpd web server daemon is run in standalone mode. Httpd is started at boot time and it runs constantly, spawning additional instances as web traffic increases. Sendmaild, the mailer daemon responsible for receiving and delivering e-mail to the lists in conjunction with Majordomo, is another daemon that runs constantly since it must always listen for incoming mail. Sendmaild is started at boot time. Therefore, the only desired services on this machine that can be protected by TCP Wrappers are telnet and FTP daemons. The contents of the server’s inetd.conf configuration file are:

```
ftp        stream tcp nowait root /opt/tcp_wrappers/bin/tcpd
        /opt/wu_ftpd/bin/ftpd -l -i -a -u022 -d
telnet      stream tcp nowait root /opt/tcp_wrappers/bin/tcpd
        /usr/lbin/telnetd -b /etc/issue
```

This inetd.conf configuration is the correct configuration for this server. No other network daemons will be spawned by inetd since only telnet and FTP are listed in the configuration file.

Another important aspect of access control is privilege separation and separation of duties. The server has good access controls in the file system: only root can access and modify the configuration of the core operating system. Only root can apply patches and installing core operating system software. Also, no user except root can access operating system log files.

The administrators each have their own user accounts which they must use to log into the system before they can switch to the root user. This provides the ability to track when administrators are connected to the system and when they switch to the root account.

Finally, the administrators followed good security practices by isolating third party server processes from each other and from the operating system. Administrators created a separate, unprivileged user account to run the Apache web server. They run the FTP server in a chroot jail. The web server has been configured to drop privileges and run as user www once the daemon has been started by root. The daemon must originally be spawned by root since it uses the privileged TCP port 80. All ports numbered below 1024 are privileged. Only processes started by root may bind to privileged ports. The benefits of dropping privileges and running the web server as an unprivileged user as the same benefits as running the FTP server in a chroot jail. If one of the services is compromised, possibly through a vulnerability that has not yet been exposed, the damage that the attacker can do can be contained. If the attacker is able to take over the web server process running as www and execute arbitrary commands, they will not be able to modify any parts of the operating system which are only accessible to root. Further, they will not be able to access files owned by other accounts on the system because all accounts limit their files to only be readable by themselves. The same is true if an attacker is able to take control of the FTP server process. It is run in a chroot jail, which means the server sets the working directory of the process to appear to the process as though it is the root directory of the server. An attacker who gains control of the ftp server cannot traverse upwards through the file system because the process has its working directory as the top of the file system tree. These measures help prevent an attacker from accessing files in other parts of the operating system and prevent them from making changes to the operating system.

Backup Policies and Disaster Preparedness

Administrators explained that the server is protected by a robust backup system. The department runs nightly backups of all hosts on the network, including this server. Incremental backups are performed each night of the week, and a full backup is performed each weekend. The full backup is done on the weekend because it takes much longer to run and the weekends typically see lower usage of GIAC Enterprises' system and network resources. This two level backup process ensures that there is always a full backup that is less than one week old.

Because incremental backups are made every night, administrators can always restore files deleted or lost due to a disk failure to the state they were in on the previous business day.

The department uses the Legato backup application on a server located behind the corporate firewall. Administrators pointed out that this is one area where they were not willing to use an open source solution because none of the open source alternatives offered support for large tape libraries and graphical user interfaces that junior administrators could use. The critical nature of data protection justified the cost of a full featured, proprietary backup application. The backup system uses a large capacity (3 TB) automated tape library system. The total disk space in use by all computers in the department is less than 400 GB and more than 95% of the data does not get modified from day to day. Administrators explained that their backup routine allows a four week window during which any lost files can be recovered. Their backup policy expires backups after the fourth week so that tapes can be reused. Their system includes significant extra capacity so that the nightly backup system will not need to be modified until much more disk storage is consumed. When the amount of slack in their backup system falls to less than 10%, they will add an additional automated tape library device. The backup policy for this server is well matched to its functional role in the department. The frequency of backups and length of time that backups are kept are appropriate given the non-mission-critical role of this server and given that it does not do online transaction practicing.

Disaster preparedness is closely related to backup policies because many businesses implement disaster recovery policies that include the use of routine backups. Organizations must have plans and procedures in place to guarantee continuity of important operations in the event of a natural disaster, fire, or any other catastrophic damage to their site. Basic measures for implementing disaster preparedness usually include storing full backups, or all critical data, at offsite facilities. It is important to document system configurations thoroughly and keep that information with offsite backups so that data can be restored and the system architecture replicated when the plan is needed to recover from a disaster.

The server, while part of a successful backup policy, is not covered by any disaster preparedness policy. No process is in place to store data backed up from the server at an offsite facility. The system is not well documented on hard copy. Most of the system configuration information is stored only in the onsite issue tracking system. This finding is significant because, while not considered a critical or core piece of GIAC Enterprises' business, the brand building initiative is valuable to the company. It has accumulated a large community of loyal customers. Measures should be taken to protect this asset and ensure this initiative can survive a large property damage event. The issue tracking system is a sound method for managing change, but because that system is not protected by a disaster preparedness policy, a fire, hardware loss, or other incident at the site could force the online community project to start over from scratch.

Other Issues

A final concern with this system is the age of the hardware. Just as the operating system this server depends on is slated for obsolescence in June 2003, the hardware too, is obsolete. The HP9000 K100 server has been officially obsolete since September 1, 1996. Hewlett-Packard offered limited support through June 1, 2002, while parts were still available. HP no longer maintains a parts depot for the components and peripherals required to support this platform. HP will not support the hardware. They do not sell hardware support contracts that cover the HP9000 K100. No component upgrades are available for the K100 through HP.

This is significant because the department has no spare K100 parts and the department does not currently have a third party hardware support contract to protect the K100 server. Any hardware failure, such as an internal disk or power supply failure, will take this system offline for an extended period of time. Hardware failures have to be expected and anticipated. Many modern hard disk drives have an expected service life of five years. The Seagate Cheetah 36ES SCSI disk drive is one example of a modern drive that specifies a five year expected service life in its Technical Specifications. My experience with older Seagate disk drives used in older HP servers, especially in servers that perform heavy disk input and output, is that the drives frequently fail within 3 years. Given the age of this server, and the fact that replacement parts have been unavailable for an extended period of time, component failure and lack of hardware support pose a significant risk that should be mitigated.

Critical Issues and Recommendations

The audit of GIAC Enterprises online community server has uncovered security issues and vulnerabilities that should be addressed to improve the safety and availability of the server. The server provides a valuable Internet presence to GIAC Enterprises' customers. Project leaders indicated that the brand initiative, which depends on this server, is meeting its targets faster than expected. It is important to manage and mitigate the risks that threaten this server in order to keep that project on track and to continue pleasing GIAC's customers.

In the sections that follow, the top ten most significant vulnerabilities and issues uncovered by the audit are explained. Each explanation includes details that describe why the issues are critical and makes recommendations for fixing or mitigating the risks. Given the budget constraints associated with this project, suggestions are focused on high value, low cost solutions whenever such solutions are available and feasible. Following the Critical Issues section, some additional, lower priority recommendations are provided.

Recommendations And Explanations For Top Ten Vulnerabilities

Vulnerabilities and risks discussed in this section are the most significant issues impacting the security of this server. These items should be addressed as soon as possible in order to ensure the security and proper function of the server. When appropriate, the estimated level of effort or time required to implement the recommendation is provided.

1. Upgrade Vulnerable Third Party Applications

Critical vulnerabilities were identified in several third party software applications used on this server in support of its mission. These vulnerabilities included allowing remote attackers to execute arbitrary code on the server and exposure to denial of service attacks. Remote code execution vulnerabilities are among the most critical type because they allow an attacker to gain unauthorized access to your computer from anywhere on the Internet. Once the attacker has gained access to the computer, they can sabotage the server to deny visitors access to the online community resources. An attacker who has compromised the server can use it as a base to launch attacks on other computing resources sharing the corporate network.

The vulnerable third party applications found on the server were the Apache web server, Majordomo mailing list server, Washington University FTP server (WU-FTPD), and the Analog web server log analysis application. Each of these applications should be upgraded to the latest versions as soon as possible.

Please note: there are large differences between the Apache 1.3.x series and Apache 2.0.x series web servers. Because GIAC administrators are familiar with the Apache 1.3.x series servers, I recommend upgrading to the latest 1.3.x series Apache server. That measure offers a simple upgrade path and provides all of the security improvements from the latest Apache releases. All identified third party applications are open source and free upgrades are available from their authors. Download the source code for the applications from their respective web sites:

- Apache web server – http://httpd.apache.org/
- Majordomo mailing list server – http://www.greatcircle.com/majordomo/
- Washington University FTP server – http://www.wu-ftpd.org/
- Analog log analysis application – http://analog.cx/

Downloading, installing, and testing all of these upgrades can be accomplished within 3 business days. Be sure to backup the server before making these major changes to its configuration. Make sure to adequately test each application after it is upgraded to ensure it works as expected. These applications are independent of each other and can be upgraded in any order.

Administrators should join a comprehensive security announcement mailing list such as the weekly SANS Security Alert Consensus mailing list that includes CERT, NIPC, and vendor bulletins. They should periodically check for new versions of third party software installed on this server. The measures will assist the technical staff in keeping abreast of associated, new security threats and will enable them take corrective action.

2. Place a Firewall Between the Server and the Internet

This server should be protected by a firewall that allows incoming connections only to the ports intended for public access. The firewall should allow access to port 80 (http), ports 20 and 21 (ftp), and port 25 (smtp / mail). All other ports should be blocked.

The server was found to be partially hardened through the elimination of many unneeded network services and TCP Wrappers access controls placed on telnet and FTP access. Still, several potentially vulnerable ports are completely open to connections from the Internet. These potentially vulnerable processes and their associated ports are:

Process	**Port**
named	53
diagmond	1025
diagmond	1086
psmond	1788

swagentd	2121
nsrexecd	7938
nsrexecd	7937
diaglogd	1025
memlogd	1025
memlogd	1086

According to its administrators, this server is not intended to offer DNS services to any computers. The multitude of diagnostic and monitoring daemons used by the operating system on this server should not be reachable across the company network and should definitely not be reachable by entities on the public Internet. Finally, the nsrexecd daemon used by the Legato backup client on this host should not be reachable or allow connections from hosts on the Internet. There are currently no known vulnerabilities related to these open ports on a completely patched HP-UX 10.20 operating system. However, any open port is a ripe target for an attacker trying to gain access to the server or trying to deny service to valid users of the site.

Another reason that a firewall should be used to protect this host is that, due to its role as a public information server, it is a higher profile target and because it runs services that are intended to allow connections from untrusted networks, it is inherently more vulnerable to bugs in the software it uses to provide those services. For example, WU-FTPD, running on this server, was found to be vulnerable and could allow remote code execution by an attacker. The risk of a larger compromise can be mitigated through the use of a firewall that prevented incoming connections on all but a few ports. A less skilled hacker would not be able open up access to the server because the access controls provided by the firewall would not let traffic pass through to new services that the hacker had started.

Purchasing and implementing a firewall is a more difficult undertaking than most of the recommendations provided by this audit. However, it is a critical recommendation with a significant return on investment. Two alternatives to purchasing a new, dedicated firewall should be considered in light of budget constraints. Other portions of GIAC Enterprises' network are protected by a dedicated firewall. Can this server be moved onto the DMZ segment of GIAC's existing firewall? This option would save money and working with the administrator of the existing firewall could also save the department significant man power resources. The other option, especially given the open source approach favored by the department, is to build a Linux based firewall using IP Tables and place that packet filtering firewall between the server and the rest of the network. This approach offers a low capital cost option if existing, spare hardware can be used for the project. The amount of time required to implement these options ranges from 16 hours up to several weeks depending on administrators' level of skill and familiarity of the subject matter.

3. Eliminate Telnet, Use SSH Instead

Administrators currently use telnet to access and remotely manage the server. This presents a significant security risk because many tools exist, such as Juggernaut, that make session hijacking as simple as running a program and following onscreen instructions. Another vulnerability facing telnet sessions, as well as FTP sessions, is that users' passwords are transmitted in clear text over the network during the login sequence. Any attacker on the same network segment as either the server or the client, or positioned anywhere on the network path between them, can run a packet sniffer and capture TCP packets traversing the network. Packets captured while users were logging in to the server, will contain the user's password in clear text. Armed with a password an attacker can then log in to the computer using a stolen account and may be able to use a local privilege escalation vulnerability to gain root access to the computer.

To protect against these critical weaknesses in telnet and FTP, administrators should install SSH on the server and SSH clients on their workstations and anywhere they require remote access to the server. SSH stands for secure shell. SSH refers to a protocol and a suite of applications which follow the SSH protocol. These applications allow secure remote access and file transfer across untrusted networks by making use of encrypted tunnels for all communications.

OpenSSH, an open source implementation of SSH, is available for a wide variety of computing platforms including HP-UX 10.20. More information and the latest release of OpenSSH are available on the web at http://openssh.net/. Installing and configuring OpenSSH on the server should take less than 4 hours. Putty is an SSH client for Microsoft Windows that can be installed in minutes. Putty is available from http://www.chiark.greenend.org.uk/~sgtatham/putty/.

4. Upgrade the Operating System Software to HP-UX 11

The HP-UX 10.20 operating system running on the server is no longer being distributed by Hewlett Packard and it will become obsolete – no longer supported – on June 30, 2003. At that time, HP will cease fixing security vulnerabilities found in the operating system. If a vulnerability is found in the operating system, there may be no way to mitigate the risk it poses. Some risks may be mitigated by obtaining the source code to the application and building it from source rather than installing a patch provided by HP. This strategy could be used, for example, if a new Sendmail vulnerability is found in the version of Sendmail running on the server. However, not all components of the HP-UX operating system can be easily replaced by third party solutions.

Another risk associated with obsolescence of HP-UX 10.20 is that technical support will no longer be provided by Hewlett Packard. It is important to have a technical support vehicle in place because problems can occur with the operating system that are not easily and immediately curable by department system administrators.

These are important issues to consider. My recommendation is to plan an upgrade of the operating system before June 30, 2003. The department currently has technical support contracts with Hewlett Packard and can rely on skilled help from HP engineers during the upgrade process. HP makes transition kits available all current support contracts and they offer free upgrade media and licensing to HP-UX 11. The downtime required to complete the upgrade should be less than one day, however, please allow several days for planning, backups, and reinstallation of third party software.

5. Upgrade Hardware or Obtain Third Party Hardware Support

Similar to the software issue, the hardware this server is based on is long overdue for an upgrade. The HP 9000 series model K100 has not been fully supported by Hewlett Packard since 1996. HP offered limited support beyond 1996 while replacement parts were available. Hardware support for the K100 is now completely unavailable through HP.

Some action must be taken to ensure continuity of operations in the event of a component failure in the K100 server. Hard drives and power supplies are fallible parts. They can be expected to fail after 3-5 years and components of this server have been in use much longer than that.

One of the more unorthodox methods that could be used to address this problem depends on GIAC Enterprises' purchasing rules and their administrators level of comfort servicing K100 hardware. If these considerations are not obstacles, spare K100 servers could be purchases from a refurbished hardware dealer or at auction. Spare servers might be located in this manner at a cost of less than $50 each. However, this solution may best be considered a temporary solution. Another temporary solution is to locate a third party hardware support vendor who maintains spare K100 parts and is willing to service the machine.

A more permanent solution to this issue is to buy new, or newer refurbished, HP hardware. The department should try to locate hardware that meets the budget for this project but which is also going to remain supported by HP for several more years. This solution requires a larger capital expenditure but offers the best long term solution to the risk associated with existing hardware that is quite dated. A positive side effect of purchasing newer hardware would be the addition of several times more computing power to the online community server and additional storage and memory capacity. These will be real assets to the project as the site continues to grow in popularity and serves more traffic.

6. Implement A Disaster Preparedness Process

The server is covered by a very thorough nightly backup process. However, no disaster recovery process is in place to protect the server in cases of natural disasters or widespread property damage. Implementing a basic level of disaster preparedness is highly recommended.

Two components of basic disaster preparedness are: making backups to be stored at an offsite location and thoroughly documenting the system configuration to be stored with offsite backups. The challenge of maintaining system documentation boils down to making sure documentation is kept up to date as the configuration of the system changes. Given the group's commendable practice of documenting all server configuration changes in the department's issue tracking system, an simple solution to the documentation problem would be to print out all existing cases relevant to the server and store them with offsite backups. As new cases are entered into the issue tracking system, they can be printed and added to the other documentation.

Making backups to be stored at an offsite facility can also be addressed easily for this server because the amount of data stored on the server is relatively small. The server has an internal DAT tape drive that is capable of storing all of the files on the server onto a single tape. Administrators regularly make bootable system image backups of the server before patching. They should add a step and make a simple tar (tape archive) backup of the server before patching. After several days, when administrators are satisfied that all patches installed cleanly and did not negatively impact the system, the new image, tar backup, and hardcopy documentation should be taken offsite.

Professional data storage services are beyond the constraints of the online community initiative. However, because the only sensitive information kept on the server are the user and root account passwords, tapes and accompanying documentation can safely be stored at the residence of any of the administrators responsible for this computer. If the tapes are ever misplaced, simply changing the passwords will be enough to protect the server.

These simple steps can be implemented right away with a minimal level of work. The steps also represent a major improvement towards disaster preparedness for this server.

7. Disable the DNS Server

Administrators were unaware that named, an implementation of the Berkeley Internet Name Domain package (DNS), was running on this server. When I asked about the server they assured me that none of the applications on the server require a local instance of named and that no other computers on the network rely on named running on the server.

The SANS/FBI Top 20 List of vulnerabilities places BIND among the top 10 most critical vulnerabilities exploited on UNIX operating systems. A quote from Unix vulnerability #9 from the list:

> "The ubiquity of BIND has made it a frequent target of attack. While BIND developers have historically been quick to repair vulnerabilities, an inordinate number of outdated or misconfigured servers remain in place and exposed to attack."

BIND/named has been running on this server but it does not provide any benefit and potentially exposes the system to another common vulnerability. The BIND/named component of this server has not received attention because no one was aware it was installed and running.

This vulnerability has a very simple solution – stop the process and change the boot scripts so that named does not start automatically at boot. The command used to stop named is:

```
/sbin/init.d/named stop
```

To prevent named from starting each time the system boots, change the line "NAMED=1" to read "NAMED=0" in the /etc/rc.config.d/namesvrs configuration file.

This change can be made in minutes. Allow some time to monitor the network closely and be ready to respond just in case an overlooked host on the network was counting on named on this server. If any such host is found, reconfigure it to use GIAC Enterprises authorized DNS servers.

8. Reduce Time Between Routine Patch Applications

Administrators indicated that the server is patched for all security and HP Recommended operating system patches once every six months. That interval is too long, even for the mature HP-UX 10.20 operating system. Several considerations merit a faster patching cycle.

This audit uncovered a security patch that had not yet been applied – PHCO_27564 the cumulative sort(1) patch. Without this patch applied, the server is vulnerable to a local privilege escalation exploit. Because this server does not possess accounts for any users other than the system administrators, the threat posed by this vulnerability is small but not insignificant. Although the administrators are trusted with root access, if an attacker is able to gain access to one of the administrators regular user accounts, the attacker will be able to exploit the privilege escalation vulnerability to gain root access to the system. That patch should be applied as soon as possible. Applying the patch should take less than one hour and does not require a reboot of the server.

Given this server's role as an interface to the public, it is exposed to a higher risk of compromise due to the services running on it which accept incoming connections. The server should be patched more aggressively to reduce the window of opportunity available to attackers.

Finally, recommendation #4 suggested upgrading the operating system to HP-UX 11. That operating system is stable and has been in wide use for several years. However, it is much younger than HP-UX 10.20 and new patches for that version of the operating system can be expected to be released more frequently. Increasing the frequency of routine patch applications will reduce the risk posed by existing bugs in the operating system.

9. Consider Converting the Operating System to Trusted System Mode

HP-UX 10.20 does not allow shadow passwords when operating in untrusted mode. This is a risk because anyone who gains regular user level access to the system can read the /etc/passwd file and can decrypt any weak account passwords stored in that file, including the password to the root account. Besides shadow passwords, trusted mode also allows the administrators to enforce stricter password construction policies as another method to improve password security on the server.

Converting to a trusted system is simple task, especially on this system with few users and no special programs accessing /etc/passwd. First run /usr/sbin/pwck to check the /etc/passwd file for any errors and correct them. Then run /usr/lbin/tsconvert –c to convert to a trusted system. The process can be reverted with /usr/lbin/tsconvert –r. Administrators can also convert the system to trusted mode using the SAM graphical system administration tool. Using SAM, select Auditing -> System Defaults. The system will ask you if you want to convert, answer Yes.

This procedure can be completed in less than one hour and will immediately improve the password security on the server.

10. Remove the Analog Web Server Analysis Application

During the Audit, the Analog web server analysis application was found to be one of several third party applications that were out of date and contained critical security bugs. Recommendation #1 included a suggestion to upgrade Analog to the latest version to address that specific security risk. The recommendation stands, whether or not Analog is kept on the server or moved to some other host on the network. In either case, the application should be updated to the latest, secure version. However, administrators should consider whether Analog can be moved to another host. This is in keeping with a general concept in computer security – reducing complexity makes a system easier to secure and easier to audit and maintain. Administrators gave no indication that they want to make their web server statistics available to public visitors to the web site and I did not see a link to the statistics while perusing the site.

If there is no need to make the web server statistics available to the public, it would be safer to move that software to another host. The upside to moving the software is that if a new vulnerability is found in the latest version, that will not impact the security of the server.

Additional Recommendations

Implementing the recommendations given in the previous section will ensure the server is well protected from many of the most common threats to security. Following those recommendations will significantly raise the overall security of the server. The following recommendation and comments are not vitally important to improving the security of the system but they are intended to provide additional value to this audit and suggest an alternate course of addressing some of the obstacles confronting the current server configuration.

1. Encourage Use of Sudo for Tasks Requiring Root Access

Sudo is an application that addresses one of the problems with the UNIX security model. Under the UNIX security model, users are either super users (root) with access to all parts of the operating system and all files stored on the host, or they are regular users with access only to their own files and to files with permissions that grant shared group access or access to all. A good illustration of this two level model is demonstrated by considering access to privileged ports. Ports below 1024 can only be bound by processes running as root. If a user needs to run a process on a privileged port, the UNIX security model offers a choice between bad and worse: give the user root access to the system or write a set-UID wrapper for the program the user wishes to execute. Neither option is desirable because the first grants the user access to every aspect of the system and all the data stored there. The latter option is dangerous because set-UID scripts, even those that seem trivial, often have enormous security holes. Sudo neatly addresses these problems.

The sudo utility can be installed on many operating systems, including HP-UX 10.20. Sudo tackles the all or nothing security model of UNIX by allowing finer grained control over who can execute what programs and with what privileges. With sudo, it is easy to allow one user to execute several programs they need to run as root without giving them complete root access. Another user, with different requirements, can be granted access to run a different set of programs to run as root. Users can even be granted access to run programs as a user other than themselves.

Another beneficial feature of sudo is that it logs every command executed and can generate e-mail when a user attempts to run a sudo command that they are not permitted to run. The primary reason to run sudo on the GIAC Enterprises web server is its command logging feature. Logging all commands executed with super user privileges offers another level of configuration tracking. If changes are made and the system becomes unstable, it can be useful to refer back to logs to step through all commands that were run prior to the event.

Sudo is a free software application available from http://www.courtesan.com/sudo/index.html.

2. Linux Alternative to HP Hardware and Operating System

This audit and recommendations focused on the current server, its operating system, and its installed third party applications. The existing server is based entirely upon the HP platform that was donated to the project by another GIAC department. However, it is interesting to note that while conducting the audit, in both official meetings and in casual conversations with GIAC Enterprises employees, I detected a growing, optimistic push toward wider adoption of open source software. Some of GIAC's current projects are considering switching to the Linux operating system and new projects are enthusiastically embracing Linux because of its high performance to cost ratio and low cost of entry.

As an alternative to upgrading to a newer version of the HP-UX operating system and purchasing new HP computing hardware, the department may want to consider using commodity, off-the-shelf PC computing hardware and the Linux operating system as the next platform upon which to base their growing web initiative. Many of the recommendations given in this report still need to be implemented if Linux is chosen as a new platform. Recommendations that still apply include: upgrading all third party applications to the latest available versions, placing a firewall between the server and the public Internet, eliminating telnet and using ssh in its place, adopting a routine to supply basic disaster preparedness, and reducing the interval between routine patch applications. On the other hand, switching to a Linux platform could save money by providing a cheaper option to the recommendation of upgrading the HP hardware. Additionally, many flavors of Linux use shadow passwords and harder to crack MD5 password encryption right out of the box. Linux also includes tools that assist and automate system administration tasks.

Switching to Linux is not a clear cut choice. The decision depends on many other factors including the level of experience that GIAC's system administrators have with the operating system and whether the department plans wider adoption of Linux. Switching may offer cheaper spare parts and will likely offer much more processing power per dollar compared to HP RISC platforms.

References

1. “SANS / FBI Top 20 List.” SANS / FBI The Twenty Most Critical Internet Security Vulnerabilities. The SANS Institute. Updated 3 March 2003. Retrieved 23 March 2003. <http://www.sans.org/top20/>.

2. “REMINDER : HP-UX on PA-Risc 10.20 Discontinuance and Obsolescence update”. HP-UX 10.20 Discontinuance. Hewlett-Packard Company. Updated 21 March 2003. Retrieved 24 March 2003. <http://www.software.hp.com/RELEASES-MEDIA/notices/ITRCenewsletterFEB03.htm>.

3. “HP-UX Patch Security Matrix”. Hewlett-Packard Company. Updated 24 March 2003. Retrieved 24 March 2003. <ftp://ftp.itrc.hp.com/export/patches/hp-ux_patch_matrix>.

4. “John the Ripper password cracker”. John the Ripper Password Cracker. The Openwall Project. Retrieved 29 March 2003. <http://www.openwall.com/john/>.

5. Ed Norris. "Analysis of a Telnet Session Hijack via Spoofed MAC Addresses and Session Resynchronization”. Analysis of a Telnet Session Hijack via Spoofed MAC Addresses and Session Resynchronization. SANS. Updated 20 March 2001. Retrieved 29 March 2003. <http://www.sans.org/rr/threats/hijack.php>.

6. “Common Vulnerabilities and Exposures – The Key to Information Sharing”. Get CVE. The MITRE Corporation. Updated 18 March 2003. Retrieved 29 March 2003. <http://cve.mitre.org/cve/index.html>.

7. “CERT® Advisory CA-2001-33 Multiple Vulnerabilities in WU-FTPD”. CERT Advisory CA-2001-33 Multiple Vulnerabilities in WU-FTPD. CERT Coordination Center. Updated 15 February 2002. Retrieved 29 March 2003. <http://www.cert.org/advisories/CA-2001-33.html>.

8. “Big Brother is Watching”. Big Brother System and Network Monitor. BB4 Technologies. Updated 12 February 2003. Retrieved 29 March 2003. <http://bb4.com/>.

9. “Cheetah 36ES Technical Specifications”. Cheetah 36ES - ST318406LW Detailed Specifications. Seagate Technology LLC. Retrieved 30 March 2003. <http://www.seagate.com/cda/products/discsales/enterprise/tech/0,1084,344,00.html>.

10. "Apache HTTP Server Project". The Apache HTTP Server Project. Apache Software Foundation. Retrieved 31 March 2003. <http://httpd.apache.org/>.

11. "Majordomo". Majordomo. Great Circle Associates, Inc. Updated 27 February 2003. Retrieved 31 March 2003. <http://www.greatcircle.com/majordomo/>.

12. "WU-FTPD Development Group". WU-FTPD Development Group. Updated 18 February 2003. Retrieved 31 March 2003. <http://www.wu-ftpd.org/>.

13. Stephen Turner. "Analog". Analog: WWW Logfile Analysis. Updated 23 March 2003. Retrieved 31 March 31, 2003. <http://analog.cx/>.

14. "SANS Newsletter Subscription Service". SANS Institute - Computer Security Education and Information Security Training. The SANS Institute. Retrieved 31 March 2003. <http://server2.sans.org/sansnews>.

15. Juggernaut, A Session Hijacking Tool. SecuriTeam.com (Juggernaut, A Session Hijacking Tool). Beyond Security Ltd. Retrieved 31 March 2003. <http://www.securiteam.com/tools/Juggernaut__a_session_hijacking_tool.html>.

16. "Open SSH". OpenSSH. OpenBSD. Updated 31 March 2003. Retrieved 31 March 2003. <http://openssh.net/>.

17. Simon Tatham. "PuTTY: A Free Win32 Telnet/SSH Client". PuTTY: A Free Win32 Telnet/SSH Client. Updated 13 January 2003. Retrieved 31 March 2003. <http://www.chiark.greenend.org.uk/~sgtatham/putty/>.

18. Todd Miller. "Sudo Main Page". Sudo Main Page. Courtesan Consulting. Updated 30 March 2003. Retrieved 31 March 2003. <http://www.courtesan.com/sudo/index.html >.

Appendix A.1 – Patches for Security Issues (as of 3/24/03)

HP-UX 10.20 series 800 security patches

PHCO_9597 s700_800 10.20 chfn(1) cumulative patch
PHCO_9602 s700_800 10.20 chsh(1) cumulative patch
PHCO_12097 s700_800 10.20 newgrp(1) cumulative patch
PHCO_13734 s700_800 10.20 passwd(1) cumulative patch
PHCO_17555 s700_800 10.20 mediainit sioflop driver support
PHCO_22228 s700_800 10.20 ex(1),vi(1),expreserve(1) cumulative patch
PHCO_22273 s700_800 10.20 bdf(1M) cumulative patch
PHCO_22275 s700_800 10.20 df(1M) cumulative patch
PHCO_22556 s700_800 10.20 top(1) cumulative patch
PHCO_22764 s700_800 10.20 cu(1) cumulative patch
PHCO_22956 s700_800 10.20 auto_parms/set_parms
PHCO_23089 s700_800 10.20 man(1) patch
PHCO_23319 s700_800 10.20 kermit(1) cumulative patch
PHCO_23437 s700_800 10.20 LVM commands cumulative patch
PHCO_23844 s700_800 10.20 fsck_vxfs(1M) cumulative patch
PHCO_25316 s700_800 10.20 Software Distributor cumulative patch
PHCO_25591 s700_800 10.20 login(1) cumulative patch
PHCO_25640 s700_800 10.20 libc cumulative patch
PHCO_26962 s700_800 10.20 cumulative patch for shutdown(1M)
PHCO_27133 s700_800 10.20 lpspool subsystem cumulative patch
PHCO_27422 s700_800 10.20 cumulative cron/at/crontab patch
PHCO_27560 s700_800 10.10-20 ied(1) cumulative patch
PHCO_27564 s700_800 10.20 sort(1) cumulative patch
PHKL_16751 s800 10.20 SIG_IGN/SIGCLD,LVM,JFS,PCI/SCSI cumulative patc
PHKL_16957 s800 10.20 Physical dump devices configuration patch
PHKL_20611 s800 10.20 Correct process hangs on ufs inodes
PHKL_21661 s800 10.20 lo_realvfs panic fix, Cumulative LOFS patch
PHKL_22702 s800 10.20 argv[0] passing, ptrace, core creation
PHKL_24518 s800 10.20 UFS/mmap: hangs, stale data, disk space leak
PHKL_26981 s800 10.20 VxFS (JFS) mount, fsck, vx_real_iget deadlock
PHKL_27833 s800 10.20 VxFS quotas; directory sticky-bit
PHNE_10043 s700_800 10.20 talk(1) patch
PHNE_15287 s700_800 10.20 ppl(1) cumulative patch
PHNE_16308 s700_800 10.20 NetWare 3.12 cumulative patch for B.10.08
PHNE_17948 s700_800 10.20 Domain Management (DESMS and DESMS-NS)
PHNE_18061 s700_800 10.20 arp general patch
PHNE_20747 s700_800 10.20 inetd(1M) cumulative patch
PHNE_20748 s700_800 10.20 remote network commands cumulative patch
PHNE_22496 s700_800 10.20 vacation(1) patch
PHNE_22507 s800 10.20 cumulative ARPA Transport patch
PHNE_23277 s700_800 10.01-[12]0 BIND 4.9.7 components

```
PHNE_23948 s700_800 10.20 ftpd(1M) and ftp(1) cumulative patch
PHNE_24161 s700_800 10.20 kftpd(1M) and kftp(1) cumulative patch
PHNE_24510 s700_800 10.X NTP timeservices upgrade plus utilities
PHNE_24821 s700_800 10.20 telnetd(1M) cumulative patch
PHNE_24822 s700_800 10.20 ktelnetd(1M) cumulative patch
PHNE_25183 s700_800 10.20 sendmail(1M) 8.9.3 cumulative patch
PHNE_25234 s700_800 10.20 NFS/NIS General Release/Performance Patch
PHSS_9669  s700_800 10.20 MPower/Web 1.1 movemail point patch
PHSS_12865 s700_800 10.X OmniBackII A.02.10 patch
PHSS_16478 s700_800 10.X OV OB2.10 DA patch
PHSS_16648 s700_800 10.20 Receiver Services October 1998 Patch
PHSS_17495 s800 10.20 Predictive C.10.2[0,A-I,M-X,a-k] cumul. patch
PHSS_19473 s800 10.20 MC/ServiceGuard A.10.11 cummulative patch
PHSS_20815 s700_800 10.[12]0 MPower 2.03 Jan 2000 Periodic Patch
PHSS_21325 s700_800 10.X OV OB2.55 patch - DA packet
PHSS_21636 s700_800 10.X OV OB2.55 patch - WindowsNT packet
PHSS_21957 s700_800 10.20 X11R5/Motif1.2 DevKit AUG2000 Periodic Patch
PHSS_22404 s800 10.20 MC/LockManager A.10.07.01 cumulative patch
PHSS_22622 s700_800 10.20 HP Visualize Conference patch
PHSS_23103 s700_800 10.X OV OB3.00 patch - CORE packet
PHSS_23265 s800 10.20 OnlineDiag/Support Tool Manager A.21.00 Patch
PHSS_23268 s800 10.20 OnlineDiag/Support Tool Manager A.22.00 Patch
PHSS_23654 s800 10.20, OnlineDiag/Support Tool Manager Patch A.24.00
PHSS_23660 s800 10.20 MC/ServiceGuard and MC/LockManager A.10.06 patc
PHSS_24423 s700_800 10.X OV OB3.10 patch - CORE packet
PHSS_24797 s700_800 10.20 OV NNM6.1 Consolidated Patch 4
PHSS_24863 s700_800 10.20 PRM C.01.07 Cumulative Patch
PHSS_26496 s700_800 10.20 XClients Periodic Patch
PHSS_26777 s700_800 10.X OV NNM4.1x ovutil/ovsnmp fixes for core dump
PHSS_26788 s700_800 10.[12]0 HP Vue 3.0 APR2002 Patch
PHSS_26908 s700_800 10.X OV ECS3.00 Intermediate patch April 2002
PHSS_27191 s700_800 10.X AudioSubsystem Periodic Patch
PHSS_27221 s700_800 10.20 OV NNM6.0x pmd/ovtrapd fixes
PHSS_27332 s700_800 10.20 OV NNM6.2 Consolidated Patch 3
PHSS_27478 s700_800 10.20 OV NNM6.1 NNMDevKit/pmd fixes
PHSS_27589 s700_800 10.X OV OB3.50 patch - CORE packet
PHSS_27695 s700_800 10.X OV DM5.03 Consolidated Patch Sep2002
PHSS_27783 s700_800 10.20 OV NNM6.1 http server fix
PHSS_27857 s700_800 10.20 OV EMANATE14.2 Agent Consolidated Patch
PHSS_27877 s700_800 10.20 CDE Runtime Periodic Patch
PHSS_27878 s700_800 10.20 CDE DevKit Periodic Patch
PHSS_28001 s700_800 10.X OV NNM5.0x netmon dump on invalid sysObjectID
PHSS_28206 s700_800 10.X OV DM6.00 Intermediate Patch Nov2002
PHSS_28364 s700_800 10.20 X/Motif Runtime Periodic Patch
PHSS_28365 s700_800 10.20 X11R6/Motif1.2 DevKit Periodic Patch
PHSS_28468 s700_800 10.20 X11R6 Font Server Patch
```

PHSS_28704 s700_800 10.20 OV NNM6.2 Intermediate Patch, Feb 2003

Appendix A.2 – Comparison of HP Recommended Patches to Currently Installed Patches

The following security patches are not installed on this system:

PHCO_27564 s700_800 10.20 sort(1) cumulative patch
PHNE_16308 s700_800 10.20 NetWare 3.12 cumulative patch for B.10.08
PHNE_17948 s700_800 10.20 Domain Management (DESMS and DESMS-NS)
PHNE_23277 s700_800 10.01-[12]0 BIND 4.9.7 components
PHNE_24161 s700_800 10.20 kftpd(1M) and kftp(1) cumulative patch
PHNE_24822 s700_800 10.20 ktelnetd(1M) cumulative patch
PHSS_12865 s700_800 10.X OmniBackII A.02.10 patch
PHSS_16478 s700_800 10.X OV OB2.10 DA patch
PHSS_19473 s800 10.20 MC/ServiceGuard A.10.11 cummulative patch
PHSS_20815 s700_800 10.[12]0 MPower 2.03 Jan 2000 Periodic Patch
PHSS_21325 s700_800 10.X OV OB2.55 patch - DA packet
PHSS_21636 s700_800 10.X OV OB2.55 patch - WindowsNT packet
PHSS_21957 s700_800 10.20 X11R5/Motif1.2 DevKit AUG2000 Periodic Patch
PHSS_22404 s800 10.20 MC/LockManager A.10.07.01 cumulative patch
PHSS_22622 s700_800 10.20 HP Visualize Conference patch
PHSS_23103 s700_800 10.X OV OB3.00 patch - CORE packet
PHSS_23265 s800 10.20 OnlineDiag/Support Tool Manager A.21.00 Patch
PHSS_23268 s800 10.20 OnlineDiag/Support Tool Manager A.22.00 Patch
PHSS_23654 s800 10.20, OnlineDiag/Support Tool Manager Patch A.24.00
PHSS_23660 s800 10.20 MC/ServiceGuard and MC/LockManager A.10.06 patc
PHSS_24423 s700_800 10.X OV OB3.10 patch - CORE packet
PHSS_24797 s700_800 10.20 OV NNM6.1 Consolidated Patch 4
PHSS_24863 s700_800 10.20 PRM C.01.07 Cumulative Patch
PHSS_26777 s700_800 10.X OV NNM4.1x ovutil/ovsnmp fixes for core dump
PHSS_26788 s700_800 10.[12]0 HP Vue 3.0 APR2002 Patch
PHSS_27221 s700_800 10.20 OV NNM6.0x pmd/ovtrapd fixes
PHSS_27332 s700_800 10.20 OV NNM6.2 Consolidated Patch 3
PHSS_27478 s700_800 10.20 OV NNM6.1 NNMDevKit/pmd fixes
PHSS_27589 s700_800 10.X OV OB3.50 patch - CORE packet
PHSS_27695 s700_800 10.X OV DM5.03 Consolidated Patch Sep2002
PHSS_27783 s700_800 10.20 OV NNM6.1 http server fix
PHSS_27878 s700_800 10.20 CDE DevKit Periodic Patch
PHSS_28001 s700_800 10.X OV NNM5.0x netmon dump on invalid sysObjectID
PHSS_28206 s700_800 10.X OV DM6.00 Intermediate Patch Nov2002
PHSS_28364 s700_800 10.20 X/Motif Runtime Periodic Patch
PHSS_28365 s700_800 10.20 X11R6/Motif1.2 DevKit Periodic Patch
PHSS_28468 s700_800 10.20 X11R6 Font Server Patch
PHSS_28649 s700_800 10.X OV ECS3.00 Consolidated Patch March2003
PHSS_28877 s700_800 10.20 OV NNM6.2 Intermediate Patch, March 2003

PHSS_9669 s700_800 10.20 MPower/Web 1.1 movemail point patch

40 of 88 security patches may need to be installed on this system

* The only reason these patches may not be needed, is in the case that
  the target software for the patch is not installed on this system.

Appendix B – Script to Compare Installed Patches to List of Recommended Patches

```
#!/bin/sh
#
# Brian McEntire - 3/11/02
#
# check_security_patches -
#
# Compares list of installed and configured patches on the system to the
# current list of all needed security patches given in a user created file placed in
# the same directory as this script. The file must be named:
#   hp_security_patch_list
#
# A list of patches, grouped by operating system version and hardware platform
# can be obtained from ftp://ftp.itrc.hp.com/export/patches/hp-ux_patch_matrix
#
# Find the appropriate operating system version and hardware series in that file
# and copy and paste the list of patches, one per line, into hp_security_patch_list
#
# Output:
#
# List of HP recommended patches that should be installed if applicable to the
# core software installed on the system

SWLISTOUT=/tmp/$0.$$-1
SECPATCHOUT=/tmp/$0.$$-2
SECPATCHNEED=/tmp/$0.$$-3
SECPATCHFILE=hp_security_patch_list

# Set full paths to executables: eases portability, better than counting on PATH
AWK = /usr/bin/awk
SORT = /usr/bin/sort
SWLIST = /usr/sbin/swlist
GREP = /usr/bin/grep
CUT = /usr/bin/cut
COMM = /usr/bin/comm.
WC = /usr/bin/wc
RM = /usr/bin/rm

$AWK '{print $1}' $SECPATCHFILE | $SORT > $SECPATCHOUT

$SWLIST -lfileset –astate | $GREP PH | $GREP configured | \
  $AWK -F'.' '{print $1}' | $CUT -c 3- | $SORT > $SWLISTOUT

$COMM -13 $SWLISTOUT $SECPATCHOUT > $SECPATCHNEED
```

```
echo ""
echo The following security patches are not installed on this system:
echo ""

for patch in `cat $SECPATCHNEED`; do
  $GREP $patch $SECPATCHFILE
done

echo ""
echo `$WC -l $SECPATCHNEED | $AWK '{print $1}'` of\
 `$WC -l $SECPATCHFILE | $AWK '{print $1}'`\
  security patches may need to be installed on this system
echo ""
echo \* The only reason some of these patches may not be needed, is if
echo the target software for the patch is not installed on this system.

#Cleanup
for tmpfile in $SWLISTOUT $SECPATCHOUT $SECPATCHNEED; do
  $RM $tmpfile
done
```

Appendix C – Output from Remote NMap Scan of the Server

The following are the nmap command used to scan the server from across the network and the subsequent output of that command.

```
$ Nmap –sS –p 1-65000 –O 10.0.0.2 –oN nmap-crunchy.log

Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )
 Interesting ports on crunchy.name.changed.com (10.0.0.2):
(The 64988 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
23/tcp     open        telnet
25/tcp     open        smtp
53/tcp     open        domain
80/tcp     open        http
1025/tcp   open        listen
1086/tcp   open        unknown
1508/tcp   open        diagmond
1788/tcp   open        unknown
2121/tcp   open        unknown
7937/tcp   open        unknown
7938/tcp   open        unknown

Remote operating system guess: HP-UX 10.20 E 9000/777 or A 712/60 with
tcp_random_seq = 0

Nmap run completed -- 1 IP addresses (1 hosts up) scanned in 35 seconds
```

Appendix D – Output from lsof –i | grep LISTEN

The following command lists processes on the server that are listening for incoming network connections.

```
$  /opt/lsof/bin/lsof -i |grep LISTEN

named      498    root  20u  inet  0x01796100  0t0  TCP  *:domain    (LISTEN)
inetd      507    root  5u   inet  0x01796c00  0t0  TCP  *:telnet    (LISTEN)
diagmond   640    root  0u   inet  0x015c8b00  0t0  TCP  *:1025      (LISTEN)
diagmond   640    root  1u   inet  0x01c00c00  0t0  TCP  *:diagmond  (LISTEN)
psmond     645    root  2u   inet  0x01cb8400  0t0  TCP  *:psmond    (LISTEN)
swagentd   653    root  6u   inet  0x01c57500  0t0  TCP  *:2121      (LISTEN)
nsrexecd   665    root  4u   inet  0x019dc000  0t0  TCP  *:7938      (LISTEN)
nsrexecd   669    root  5u   inet  0x019dcb00  0t0  TCP  *:7937      (LISTEN)
diaglogd   940    root  0u   inet  0x015c8b00  0t0  TCP  *:1025      (LISTEN)
memlogd    941    root  0u   inet  0x015c8b00  0t0  TCP  *:1025      (LISTEN)
memlogd    941    root  1u   inet  0x01c1f600  0t0  TCP  *:1086      (LISTEN)
httpd      1303   root  15u  inet  0x01e21400  0t0  TCP  *:http      (LISTEN)
httpd      1326   www   15u  inet  0x01e21400  0t0  TCP  *:http      (LISTEN)
httpd      1327   www   15u  inet  0x01e21400  0t0  TCP  *:http      (LISTEN)
httpd      1328   www   15u  inet  0x01e21400  0t0  TCP  *:http      (LISTEN)
httpd      1329   www   15u  inet  0x01e21400  0t0  TCP  *:http      (LISTEN)
httpd      1330   www   15u  inet  0x01e21400  0t0  TCP  *:http      (LISTEN)
sendmail:  27273  root  4u   inet  0x017b5500  0t0  TCP  *:smtp      (LISTEN)
```