Global Information Assurance Certification Paper

SECURITY AUDIT – UNIX SYSTEMS
GIAC ENTERPRISES

Practical Assignment for SANS NETSEC 2001
San Diego, October 15-22, 2001

Prepared by
Russell Morrison

Submitted December 2001
To fulfill partial Requirements for GIAC GCUX
Practical Assignment Version 1.8

This document analyzes the security infrastructure of a fictitious e-business company called GIAC Enterprises that sells online fortune cookie sayings. In following, any similarities between the information contained herein and an actual company or computing environment are unintended and purely coincidental.

EXECUTIVE SUMMARY

This report summarizes the findings of a security audit that was authorized by GIAC Enterprises and its Information Systems staff and was conducted against target servers located within a specific segment of the GIAC computer network. The security audit was conducted during the week of December 17, 2001.

The GIAC computer networks can be divided into three segments, with the internal corporate network, the DMZ, and the internet. The audit was focused on only Unix-based servers that reside within the DMZ segment of the GIAC network. The DMZ segment is crucial to the GIAC business as this is where the GIAC Web and Email servers operate. There are a total of four GIAC servers within the DMZ segment. The overall intent of the security audit was to determine if the GIAC servers located within the DMZ are well secured and capable of withstanding possible malicious attacks from the internet.

In following, the audit team undertook a manual review of information at each server console along with a suite of vulnerability scans run remotely from both the internal network side of the DMZ and the internet side of the DMZ. Each Unix-based GIAC server was then documented for vulnerabilities and this information was reviewed against vendor supplied information plus third party information sources to determine any available and most appropriate patches for any identified vulnerabilities.

The results of the audit indicate that the GIAC Unix-based systems are generally secure due exclusively to the external corporate firewall. Of the four servers within the DMZ, only the external corporate firewall machine is truly secure. The three other machines have a number is issues that should be addressed. Some of these vulnerabilities require immediate attention to ensure the GIAC networks are not compromised. Others may be delayed somewhat for a recommended maximum period of 60 days.

There are a total of fifteen vulnerabilities or repairs that need immediate attention and a total of thirteen that can be addressed within the next 60 days. The recommended updates and or necessary repairs for each have been documented in this report. In addition, the location of vendor updates has been detailed in Appendix 1. Each of the updates or repairs is straight forward and can be undertaken by the existing GIAC Information Systems staff. However, since the existing GIAC staff tends to be very busy, it may be prudent for GIAC to consider bringing in outside assistance to at least complete the immediate repairs.

Overall, once the recommended repairs and changes detailed in this report have been implemented, the GIAC networks should be secure from known internet attacks based on the current configurations. If the configurations change significantly it may be worthwhile for GIAC to consider undertaking another audit to determine if the changes have opened up any additional vulnerabilities.

TABLE OF CONTENTS

1.0 INTRODUCTION

1.1 Corporate Profile

GIAC Enterprises ("GIAC" or "the company") is a small e-business company. The company has developed a small unique niche market in selling fortune cookie sayings on the internet. The market seems to be experiencing exponential growth and as a result there are a number of "Brick and Mortar" fortune cookie competitors that are very interested in the techniques and strategies that GIAC uses to develop its "catchy" sayings. As well, GIAC is interested in expanding their online presence to gather up and retain more of the online fortune cookie saying business.

1.2 Corporate Information Systems Policy

GIAC has a written Information Systems Policy that is provided to each employee upon hire which documents all acceptable activities on the corporate information systems. In addition, the Information System staff is generally quite diligent in ensuring that the information systems meet a basic set of needs using tested software applications (e.g., Office Suite, Email, Web, Printing for the desktop machines). This policy allows for predictable activity on the internal network.

In addition, "unauthorized" software is promptly removed from internal machines unless its presence can be justified by the user and/or that user's manager. This strategy allows the Information Systems staff to more easily spot "rogue" traffic when monitoring internal network and deal with it as required in a timely manner. Overall, this approach seems to have worked well for the Information Systems despite the rapid growth the company has experienced over the past few years. One issue that is arising is how the newer Unix-based systems will work within the existing Policy.

2.0 INFRASTRUCTURE BACKGROUND

GIAC made some significant changes to its Information Systems Infrastructure approximately 15 monthes ago. At the time, in spring 2000, they had a single host based firewall protecting their internal network from a broadband connection to the internet. All GIAC server systems at that time were operating Microsoft Windows NT Server Operating Systems and the firewall product was a Microsoft Windows NT Server hosting Microsoft Internet Information Server (IIS) and Microsoft Proxy Server 2.0. The GIAC email and e-business web pages were hosted on a Microsoft Windows NT 4.0 server running Lotus Notes 4.6.7 located inside of the Proxy Server using the IIS Web Publishing feature. As well, GIAC hosted a Microsoft based DNS server on it external firewall to service "localized" requests.

In late spring 2000, GIAC experienced a number of "system security" incidents that raised concerns about the integrity of their network. These incidents included several buffer overflow attacks initiated from the internet that essentially destroyed the TCP/IP stack on the Microsoft based firewall and required a complete re-install each time. The concern at the time was the state of the internet connection at the time of firewall failure. Did the firewall connection fail open or closed? As a sideline issue, GIAC had a number of ongoing problems trying to properly configure Lotus Notes to adequately support their growing e-business needs and to effectively stop email spammers from abusing their Lotus Notes email server.

In June 2000, a decision was made to switch away from the existing Microsoft and Lotus based products on the publicly accessible servers to a variety of UNIX based hosts using well tested open source applications for email and web e-business servers. In addition, GIAC installed an additional layer of security to its network by installing a second firewall to isolate all publicly accessible servers away from its "internal" network.

As a result of these changes, GIAC currently has what may be classified as two layers of security between the internet and the internal network (see Figure following). There are two stand alone firewall products, each running a different operating system (both variations of Unix), different firewall software, plus several other Unix-based servers providing both internal and external (i.e., publicly accessible) services. By introducing a second firewall, GIAC had established a "demilitarized zone" (DMZ) in its network. The end result is the DMZ includes all publicly accessible Email, Web e-business servers. As a sideline to these changes, GIAC also switched its Internet Service Provider (ISP) to one that would provide a Service Level Agreement as part of its broadband connection.

GIAC also made some changes to its DNS services by outsourcing all of its publicly accessible DNS listings to its ISP. GIAC continues to maintain a small Unix-based DNS server located in its DMZ that supports all GIAC servers and the internal network.

The external DMZ firewall connects directly into a Cisco 2600 series router supplied by the ISP which connects to the broadband connection and onwards to the ISP network.

The ISP maintains the external connection from the Cisco router out and monitors its condition as per the Service Level Agreement that GIAC negotiated in fall 2000.

The GIAC Information Systems staff has also noted they would like to consider installing a full time monitor (i.e., Intrusion Detection System) within the DMZ to get a better feel for the types of traffic moving around the outside of the GIAC network.

In summary, GIAC has replaced its publicly accessible Microsoft Servers with several Unix-based servers operating open source applications. Since that switch, GIAC has apparently not had a problem with security with its public servers.

3.0 SECURITY AUDIT

3.1 Reasons for the Audit

As noted, GIAC has made a number of significant changes to its information Systems infrastructure over the past 15 monthes. GIAC prior to that time operated only Microsoft based servers and its information system staff was trained to support those Microsoft products. GIAC hired an outside consultant to install and "securely configure" most of the Unix-based servers. The Information System staff did configure one of the Unix-based firewalls. In addition, since the introduction of the Unix-based systems, the information system staff have undertaken training to support the new Unix-based systems. However, the Information Systems Manager has an ongoing concern that they may be missing something. This concern is apparently "growing" since the systems have not been patched or upgraded since their installation last year.

In following, GIAC has initiated this security audit to assess all of its Unix-based systems within its DMZ and recommend changes where necessary to fix known or potential vulnerabilities. There are a total of four servers in the GIAC DMZ with two currently configured to be publicly/externally accessible. The remaining two servers (DNS and internal DMZ firewall) are not currently configured for public/external access.

The decision was made to audit all of the GIAC systems within the DMZ because one compromised system could potentially be used to compromise an adjacent system. Therefore, the audit should also determine any potential "cross-DMZ" issues.

3.2 Final Report Requirements

The GIAC Information Systems staff commissioned this security audit as a one time event generating a stand alone report that would clearly document the "state" of the GIAC Unix-based systems at one moment in time. In addition, the final audit report (this document) was to provide sufficient detail such that the GIAC staff could clearly decide if they were able to undertake the patches, repairs, or changes themselves or whether they should outsource the work to an outside expert/consultant. The report was to also provide the location to obtain each patch and/or directions to complete a patch or repair plus a timeline as to whether the repair or patch should be applied immediately or can be delayed to some later time period. The actual security audit was to last no more than 3 days commencing the week of December 17, 2001 (to minimize disruption to GIAC and its customers) and the final audit report would be due within five working days of the completion of the audit. In addition, any change in this scope or additional follow up work by this audit team resulting from this audit would be under separate contract to GIAC and would be negotiated after the security audit has been completed.

3.3 Audit Methods

The audit was conducted during the week of December 17, 2001 and consisted of a detailed review of all installed packages and configurations (from the server console) as well as a suite of vulnerability scans run against each of the four systems located in the GIAC DMZ. The audit team chose to run some simple console commands such as "netstat –atun", "ps –aux", rpm –q-a, and "lsof" to get a feel for what applications/processes were "running", listening, or even just installed. The audit team also reviewed each of the various configuration files located in /etc, plus other application specific locations such as /home/httpd, or /var/qmail. In the process of moving through the file systems on the four servers, they also reviewed the file and directory permissions within various locations including /bin, /sbin, /usr/bin, /usr/sbin, and /etc.

However, it is commonly known that many UNIX root kits will compromise many of these commands (or the kernel) to hide running processes. Therefore, the audit team also undertook "remote" vulnerability scans using the most current stable release of Nessus (Version 1.09) and also a variety of scans using the current stable release of the popular NMap tool (Version 2.54 Beta30).

As noted below, the Nessus scans had to be run with all "dangerous" tests disabled so as to not "destroy" or "cripple" the servers. The full results of the Nessus scans are provided in Appendix 2. The NMap scans were run using the NMap graphical front end which usually provided helpful suggestions if the scan was not providing any useable information (e.g., when scanning the OpenBSD machine, it suggested turning off all pings (i.e. –P0)). In general, all NMap scans were run using the default settings of SYN connect. Operating System identification was also turned on along with verbose and appended output. The full results of the NMap scans are provided in Appendix 3.

One other issue is both firewalls have two network cards (NICS) and it was determined that a scan should be run from both sides of each firewall to more accurately determine the allowable traffic into and out of each network. The Figure following and also Section 4.0 list the various IP addresses associated with each segment of the network.

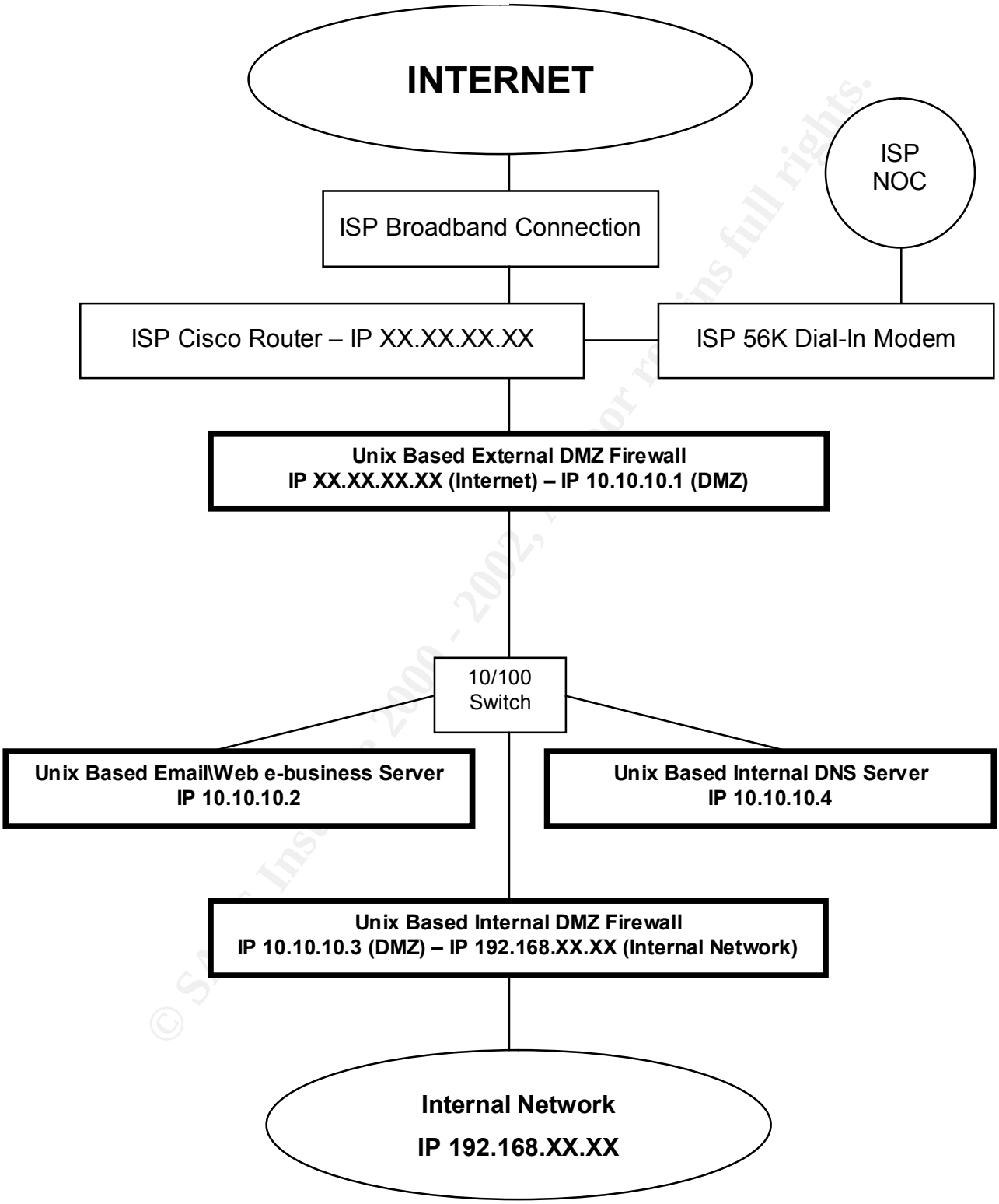
A full list of rpm's installed on each of the Red Hat servers is included in Appendices 4 and 5. These lists are relative to actual original installation as the rpm databases were not updated after that installation.

3.4 Logistical Problems Encountered

The audit team found that GIAC does not have a backup system to support its e-business services on the web and as a result, any testing performed on the existing systems had to be "non-destructive" (i.e., could not crash/destroy the systems) and if possible timed to avoid the peak times of use so as to not overload the infrastructure (and also potentially cause it to crash). However, despite these limitations, the team

feels it was able to fully assess all characteristics of the existing systems and elicit any vulnerability.

FIGURE 1: Infrastructure Overview



4.0 BASELINE CONFIGURATIONS

The audit team documented the "baseline" conditions in the network. This information was then used to measure the extent of changes necessary to secure the systems. This Section provides a summary of the existing GIAC configurations. The reader is referred to Section 5.0 for a summary discussion on security vulnerabilities found within the infrastructure and also to Appendix 1 for a complete summary list of vendor patches and Appendix 2 and 3 for the Security Tool Scan results.

4.1 Physical Security

The office building (that houses the GIAC offices on the sixth floor) operates on a computer controlled card lock system that automatically locks down all exterior public doors and all elevator systems after 6:00pm on weekdays and 24 hours per day on weekends and holidays. The GIAC office is open to the public between 8:30am and 5:00pm local time from the building elevator systems. The emergency stairwell doors off of the sixth floor (that houses the GIAC office) have push button Unicode locks to prevent public gaining access to the floor from the stairwells 24 hours per day 7 days per week. The building is monitored by night watchman between 6:00pm and 6:00am each day and any "after hour" visitors to the building are required to sign in at the lobby.

The GIAC office encompasses the entire sixth floor of the building and has one glass door (the GIAC main entrance) plus three other solid wood doors (one is the GIAC server room) facing onto the public elevator lobby. The three wood doors have five digit push button Unicode locks. The glass front door has a conventional key lock. The public elevator space and the interior of the GIAC office have a conventional suspended acoustic tile ceiling system with approximately 4 feet of air space above the ceiling panels. There are security wire cages between the public and private spaces within the suspended ceiling areas that separate the public elevator spaces from the GIAC office.

The GIAC server room is located within a portion of the GIAC office. The server room is locked 24 hours per day 7 days per week. There are two locked doors that gain access into the GIAC server room, one from within the GIAC office and one from the public elevator bank outside of the GIAC office. Both doors operate with five digit push button Unicode locks. Both locks are currently programmed to use the same five digit code for access. The server room has the same suspended ceiling system as the rest of the floor and the wire security cage located between the public elevator space and the server room has been compromised by a previous wiring contractor. The cage is no longer complete and secure. A total of four people in the GIAC office know the access code to the server room. The access code is also known to the building owner maintenance staff.

The ISP broadband wiring connections reside within locked closets throughout the office building and terminate in the locked server room located within the GIAC office. As well, the ISP has a "clean" modem connection (that parallels the broadband connection wiring

throughout the building) that is used to dial into the ISP provided Cisco 2600 series router for connection diagnostics between the ISP Network Operations Centre (NOC) and the Cisco router. This was installed by the ISP for line testing as part of their Service Level Agreement and should ensure there is no line tampering.

All of the GIAC network wiring resides within either the ceiling spaces above the GIAC offices (so not directly accessible to the public) or within the locked GIAC server room. The wiring patch panel, all network switches, all ISP broadband hardware, plus all GIAC servers reside within the locked GIAC server room. The room is cooled using an American Power Conversions (APC) Network Air cooling unit and there are no windows into the room. The power use within this server room is backed up with an array of APC battery backup units. None of the hardware located inside the GIAC server room is locked in place. As well, the server CD and floppy drives are not locked and the server BIOS's are currently set to scan first for bootable floppy and CD media. The server BIOS' are also not secured by password.

4.2 Computer Hardware

The GIAC DMZ servers currently run on the following hardware:

- External DMZ Firewall — Intel-based Pentium 2 – 266mhz, 128 mb ECC Ram, 10 GB HD, two 10/100 NICS;
- Internal DMZ Firewall — Intel-based Pentium – 166mhz, 144mb ECC Ram 1.2 GB HD, two 10/100 NICS;
- Email/Web e-business server — Intel-based Pentium 3 – 450mhz 128 mb ECC Ram, 10 GB HD, one 10/100 NIC;
- Internal DNS server — Intel-based Pentium – 200mhz, 144mb ECC Ram 1.2 GB HD, one 10/100 NIC.

4.3 Operating Systems

The GIAC DMZ servers currently operate the following Unix-based operating systems:

- External DMZ Firewall – OpenBSD Version 2.9;
- Internal DMZ Firewall – FreeSCO Router Version 0.2.7;
- Email/Web e-business server – Red Hat Linux Version 6.2;
- Internal DNS server – Red Hat Linux Version 7.1.

4.4 DMZ Applications

The GIAC DMZ servers currently run the following applications:

- qmail Version 1.03;
- Apache Version 1.3.17;
- djbdns Version 1.05;
- wu-ftp Version 2.6.0-3.

4.5 Allowable Protocols, Ports, and Traffic

4.5.1 Network Addresses

The GIAC firewalls each provide Network Address Translation (NAT). Each internal network segment operates on a different non-routable IP address range. The internal corporate network operates on the 192.168.XX.XX IP range and the DMZ operates on the 10.XX.XX.XX IP range. The intent in using this "dual-NAT" was to further remove the internal network from the DMZ and the internet.

4.5.2 External DMZ Firewall (Internet IP XX.XX.XX.XX, DMZ IP 10.10.10.1)

The external DMZ firewall operates the IPFilter (Version 3.4.16) firewall software which comes with OpenBSD Version 2.9. IPFilter is a stateful Packet Filtering firewall capable of a wide range of configurations with a user defined rule set. GIAC has configured their external firewall to only allow inbound public traffic (i.e., traffic coming from the internet) on the following ports:

- Port 25 – SMTP – Corporate Email;
- Port 80 – HTTP – Web e-business;
- Port 110 – POP3 – Corporate Email.

GIAC has configured this external DMZ firewall to only allow outbound TCP traffic (i.e., traffic traveling to the internet from the GIAC networks) with valid IP addresses (i.e., correct source IP's of the 10.10.10.XX range) along with only specific ICMP traffic (type 8 echo request) and specific UDP traffic (Port 53 DNS). All other traffic is dropped without notification. All connections both inbound and outbound are monitored for state, fragmentation, and SYN flag, and all incomplete or incorrect connections are dropped without notification.

The existing installation of OpenBSD is a default install (including the minimum number of packages as selected by OpenBSD). The hard drive was apparently partitioned based on the instructions that came on the CD sleeve. It consists of a total of six partitions including /, <swap>, /tmp, /usr, /var, and /home.

Following installation, edits were made by GIAC Information Systems staff in several of the key system files (/etc/inetd.conf, /etc/sysctl.conf, /etc/rc.conf) to disable all unneeded services. All services listed in the /etc/inetd.conf file were manually disabled and the Inetd service was turned off completely in the /etc/rc.conf file as an additional measure. New files were created for the IPFilter rule files (/etc/ipf.rules, /etc/ipnat.rules). The motd file was also altered to not give up system information. Apparently some problems were encountered with this file as OpenBSD will by default replace the /etc/motd file with its own default if the modified file does not meet certain characteristics. The OpenBSD Man pages detail what format specifics are required for this file to remain customized.

Essentially, everything that could be was disabled following the OpenBSD installation except for IPFilter and IPNat which were turned on in /etc/rc.conf file. The IPFilter and IPNat services are enabled automatically at boot time. The machine boots into run level 3 by default. By choice, the x-windows packages were not installed (they are not part of the minimal install on OpenBSD), and as a result, the machine will not boot into run level 5 without modifications. Currently, the OpenBSD server is configured to boot immediately to the login prompt so any attempts to switch to run level 1 must be made after the user has logged as root user.

The /etc/passwd file was reviewed following installation to determine which default user accounts could be removed completely or edited such that the default login shell for questionable accounts (those that might be needed) was changed to /dev/null.

In addition, the GIAC Information Systems staff apparently made the following security changes a few monthes ago after reviewing a SANS white paper on securing OpenBSD. They created the file /var/cron/allow and entered “root” into it to only allow root to use the cron service. They created the file /var/at/at.allow and entered “root” into it to only allow root to use the at service. They deleted the “.rhosts” file from the /etc/skel directory to ensure that rhost defaults are not used. They also deleted the period in the PATH statements in both “.cshrc” and “.profile” also located under /etc/skel.

The GIAC Information Systems staff seem most comfortable with the OpenBSD version of Unix as this is the one Unix-based system that they have set up.

The OpenBSD set up uses the default logging established by the Operating System. IPFilter is currently not set up to log to a file but has been set up to output a log to the standard output under specific rule defined circumstances. At this time, this is confined to ICMP probes from the internet. Apparently, the GIAC Information Systems staff have considered changing this to log to a file (or even turning it off) as they have found it extremely disruptive to receive random log messages (to the console) while they are working at that console.

4.5.3 Email/Web e-Business Server (DMZ IP 10.10.10.2)

This server has been configured to only respond to TCP traffic on the following ports:

- FTP (Port 21);
- SMTP (Port 25);
- HTTP (Port 80);
- POP3 (Port 110).

The apache (Port 80) and qmail (Ports 25 and 110) servers are initiated at boot time. The FTP server is initiated through /etc/inetd.conf as needed (using the TCPWrappers configuration) and FTP traffic is only allowed from the inside firewall using the hosts.allow file (i.e., originating from the internal GIAC network with the IP 10.10.10.3 of the inside DMZ firewall). The FTP is only used to update the web server files from the internal network. This ensures that regular users do not have a need to login at the server console to update files. In addition, the FTP tool has been configured to drop the FTP user directly into the apache html directory (/home/httpd/htdocs). The FTP user does have some flexibility to move around the directories but only has file permissions within the apache directories. The Red Hat Version 6.2 server is configured to not respond to general ICMP traffic and all of the basic Linux security features have been enabled including syncookies.

The Red Hat 6.2 installation is essentially a default "workstation" installation (see rpm package listing in Appendix 4) with the exception of edits made (by GIAC Information Systems staff) to the following key system files/directories (/etc/inetd.conf, and /etc/rc.d) to disable unneeded services. Many of the startup scripts under rc3.d (and also rc5.d) were manually disabled including all nfs related services (nfs, portmap, netfs) plus other unneeded services depending on the boot level (apmd, xfs, etc.). The x-windows rpm packages were installed on this system by the consultant who set up the machine but have not been used since the original installation. It would appear that the manual edits made in rc3.d and rc5.d were not carried through to the other rcX.d directories.

The /etc/passwd file has been edited to change the default login shell for all users to /dev/null as it was felt that the users do not need a login shell on a server they should be accessing using POP3 or SMTP. The only accounts in /etc/passwd that have not been altered in any way are the FTP account, the qmail server accounts, the apache account plus a few of the default system accounts including root and nobody. Some questionable user accounts such as uucp, mail, and tftp have been removed.

The default Red Hat logging is enabled in its default location under /var/log.

The machine boots into run level 3 by default and operates with both monitor and keyboard. The lilo loader is currently not password protected and it is possible to type "linux 1" at the prompt to drop into a run level 1 session without a password.

4.5.4 Internal DNS Server (DMZ IP 10.10.10.4)

This internal DNS server is configured to only respond to internal GIAC requests. It relies on the ISP DNS server for backup DNS.

The underlying Red Hat 7.1 installation is basically a default "workstation" installation (see Appendix 5 for a complete listing of installed rpm packages) with the exception of edits made (by GIAC Information Systems staff) to key system files/directories (/etc/rc.d) to disable unneeded services. Many of the startup scripts under rc3.d (and also rc5.d) were disabled including all nfs related services (nfs, portmap, netfs) plus other unneeded services depending on the boot level (apmd, xfs). The /etc/inetd and /etc/xinetd services were either not installed or were removed by the consultant that set up the system. It would appear that the manual edits made in rc3.d and rc5.d were not carried through to the other rcX.d directories. The machine boots into run level 3 by default and operates without monitor and keyboard. The lilo loader is currently not password protected and it is possible to type "linux 1" at the prompt to drop into a run level 1 session without a password.

The /etc/passwd file has been edited to change the default login shell for all questionable users to /dev/null. The only accounts in /etc/passwd that have not been altered in any way are the DNS specific account plus a few of the default system accounts including root and nobody. Some questionable user accounts such as uucp, mail, and tftp have been removed.

The default Red Hat logging is enabled and uses the default location under /var/log.

4.5.5 Internal DMZ Firewall (DMZ IP 10.10.10.3, Internal IP 192.168.XX.XX)

This "firewall" is based on the FreeSCO Version 0.2.7 router software and as such is extremely limited in scope and capabilities. Its premise is that the software is trimmed down sufficiently to fit on and boot from a floppy disk and its main role is as a router and not a firewall. It can not accept user created "firewalling" rules and does not have the ability to be configured to drop specific traffic. It is limited to a choice of one of three routing related rules which include wide open traffic, trusted networks traffic, or untrusted networks traffic. Defining the types of traffic that fall within those categories is not an option on the configuration menu. It is currently set for untrusted networks traffic. This "router" also appears to run an older version of BIND (seems to be a Version 8.2.X) as a caching DNS server. GIAC does not use this feature and limited attempts (by the GIAC Information Systems staff) to disable the DNS feature have apparently been unsuccessful. There is a capability in the router advanced "setup" menu to "disable the DNS" which the GIAC staff have apparently tried to use.

The consultant that set up the system had apparently had good success with the software under controlled network situations (i.e., not requiring extensive security). It appears to be a default installation of the software but at GIAC's request has been

installed onto a small hard disk to improve boot speed. All sessions across the internal DMZ firewall are initiated from the internal network. There are no services on the internal GIAC network that need to be accessed from the DMZ or the internet.

By its very nature of having a small footprint (to fit on a boot floppy), the FreeSCO router has limited logging. It will accommodate 200 kilobytes cumulative total of all logging files for syslog, dns, etc. The defaults are 50 kilobytes for syslog and 5kilobytes for dns errors. The server is currently configured with the logging defaults.

The machine boots into run level 3 by default as booting into run level 5 is not an option on the trimmed down software. Currently, the machine is configured to boot immediately to the login prompt so any attempts to switch to a different run level or to enter the router setup must be made after the user has logged as root user.

4.6 Installed DMZ Applications

This lists only those services that are running or can be run (through inetd) on the various DMZ servers.

4.6.1 Email (Ports 25, 110)

GIAC is currently using qmail for its email server which supports both SMTP and POP3 traffic. This was chosen over the more common Sendmail due to its improved security and resource efficiency. The Version of qmail is 1.03 which is the most current and is a default installation (in /var/qmail) other than domain/user specific information. Qmail by design operate as a series of very small applications, each with a defined role and permissions. Only one of the applications actually runs as root and that one is used to place email in the queue. Also by design, several of the applications are written to not trust the other applications which enhances overall security and limits the potential damage if one of the applications is compromised.

Inbound SMTP traffic is restricted to traffic from the ISP as GIAC is using an ISP value added service called “Email Store and Forward” which means all internet sourced SMTP traffic for the GIAC MX domain is temporarily stored on the ISP email servers and then forwarded on to the GIAC qmail server. This allows for guaranteed email delivery for all GIAC clients regardless of whether the GIAC qmail server is operating. In addition, the Email Store and Forward service will retain the email traffic for up to 3 days if necessary. Outbound SMTP traffic from the GIAC server is delivered directly to the target email servers as per usual internet SMTP traffic.

POP3 traffic is primarily confined to requests originating from the internal network out to the email server in the DMZ which limits the exposure of clear text passwords inherent in POP3 traffic. There is some limited random POP3 traffic originating from the internet side from individuals accessing it from their home machines or some temporary remote location (i.e., hotel room). The POP3 service is set up using a default qmail installation.

The qmail server is set up by default to log into its own log files under /var/log/qmail and has been set up with the qmail default rotation.

There have not been any noticeable problems with the qmail server since it was set up.

4.6.2 DNS (Port 53)

GIAC uses a small DNS server software called djbdns Version 1.05 instead of the more common BIND. The DNS server was developed by Dan Bernstein who also developed qmail (see above). This was chosen over BIND due to its improved security and resource efficiency. This server supports both the internal GIAC network and all DMZ server DNS requests. It was placed in the DMZ (instead of the internal GIAC network) to ensure that all traffic across the internal DMZ firewall remains in one direction only (outbound from the internal network). The software is a default installation (service/tinydns; /service/dnscachex; /var/yp; /var/db; /var/lib; /var/cache; /var/arpwatch) other than the DNS zone specific information that was added.

The djbdns DNS server relies on a series of small applications (similar to qmail above) to support a variety of different DNS related actions. Each action is broken down into a small piece that the server passes off to other applications to complete. This seems to be a characteristic of software written by Dan Bernstein and apparently improves resource efficiency and overall server security instead of having one large monolithic server process. The applications are written to not trust most of the other applications so if any one is compromised, the potential damage is extremely limited.

The dns server is set up by default to log all information into the default linux logs in /var/log/messages. The server uses the default linux values for log rotation.

There have not been any noticeable problems with the dns server since it was set up.

4.6.3 Web (Port 80)

GIAC uses the Apache Web server for its web and e-business online presence. It was chosen for its proven reliability, resource efficiency, and potential add-on modules that will support SSL and other e-business requirements (for future business considerations). The Apache installation is a default installation (into /home/httpd) other than domain specific information and is Version 1.3.17. The apache web files are located in /home/httpd/htdocs and are updated/changed from the internal GIAC network using the FTP tool discussed elsewhere. The apache logs are stored in the default location in /var/log/httpd and have been set up for rotation using logrotate every day with a log retention of 30 days. This change was made a few monthes ago after the GIAC Information Systems staff realized that the single activity log file characteristic to apache was becoming extraordinarily large with all of the worm probes from the internet looking for IIS servers. They adjusted the settings to split the activity log up into small

manageable pieces that could then be moved off onto floppy disks for review elsewhere as necessary.

There have not been any noticeable problems with the apache web server since it was set up.

4.6.4 FTP (Port 21)

This is installed on the Email/Web server and is only used to update web pages from the internal corporate network. The FTP software is the WU-FTP Version 2.6.0-3. TCPWrappers has been configured through Inetd.conf to initiate the FTP server as long as the hosts.deny and hosts.allow files permit. The hosts.allow file will only permit a connection from the internal DMZ firewall IP of 10.10.10.3. The hosts.deny file has been correctly set up with the ALL:ALL value to limited others accessing the FTP service. The FTP service uses the default FTP logging under /var/log/xferlog and rotates as per the linux syslog defaults.

There have not been any noticeable problems with the FTP service since it was set up.

4.7 Administrative Issues

4.7.1 Staffing

GIAC currently has one full time information systems staff member (the Manager of Information Systems). GIAC also has one part time staff member (a contract person) with limited skills primarily related to Microsoft Windows environments. The Manager of Information Systems also has a number of other roles in this small company including assisting in the strategy and development of new fortune cookie sayings. As a result, he tends to be very busy.

4.7.2 External Support

GIAC relies on one or two skilled consultants to support the GIAC network as required. One of the consultants is the original installer of several of the GIAC Unix-based systems. Both consultants are generally available with 24 hours notice but some limited level of support could likely be obtained from one of the two within a shorter period if an emergency situation arose.

4.8 Worm/Malware Protection

GIAC currently does not scan for Virus' or Worms within its Unix-based systems. It is considering the installation of another Unix-based system to host a virus gateway for all inbound and outbound SMTP traffic on it DMZ.

4.9 Contingency Plans

4.9.1 Backups

GIAC does not currently perform any backups of its Unix-based systems.

4.9.2 Catastrophic Failure

GIAC does not have plans in place for recovery from a catastrophic failure (e.g., fire) of its Unix-based systems.

4.10 Passwords

The GIAC Unix-based servers are all setup to require login with passwords once they have booted. Only two of the four Unix-based servers share a password, the external DMZ firewall and the internal DNS server. The remaining two machines have unique passwords. In addition, the passwords in each case are completely random character, digit, symbol combinations at least 12 long.

5.0 SECURITY VULNERABILITIES

The following Section summarizes the applicable vulnerabilities based on vendor security notices and the results of vulnerability scans. The reader is referred to Appendix 1 for a summary list of vendor patches and Appendix 2 and 3 for a detailed listing of the security scan results.

5.1 Operating System Vulnerabilities

5.1.1 External DMZ firewall - OpenBSD Version 2.9

Version 2.9 of OpenBSD has nine security issues noted by the vendor at http://www.openbsd.org/security.html#29 and a total of seventeen issues (including all security, reliability, and documentation fixes) noted at http://www.openbsd.org/errata29.html . Of those nine security issues, none of them would allow a remote user to gain root privileges as the GIAC server either does not run the services that have been compromised (e.g., lpd, sendmail, uucp, ssh, nfs, X11). In fact, none of these are started by default in a basic OpenBSD installation.

The vulnerability scans were performed on both the inside (DMZ) and outside (Internet) network interfaces. The inside interface with an IP of 10.10.10.1 only turned up one Security Note with Nessus that related to the general traceroute information between the Nessus scanner (which was positioned on the internal GIAC network at the time) and the OpenBSD server. The Nessus scan on the outside interface (Internet IP XX.XX.XX.XX) (see Appendix 2) came up with three Security Notes and one Security Hole. Of those four issues, three (two Notes and the one Hole) related to the internal Email/Web server (see discussion below) as the IPFilter tool was re-directing permissible port traffic as part of its network address translation. The one issue relevant to the OpenBSD server was the same Security Note found on the inside interface which was the traceroute information between the Nessus Scanner (which was connected to a temporarily introduced switch positioned between the DMZ firewall and the ISP router) and the OpenBSD server.

The NMap scan on the inside and outside interfaces of the OpenBSD server turned up very little information (see Appendix 3). The inside interface (IP 10.10.10.1) did not give up any information to the NMap scanner and was sufficiently hardened to prevent an accurate operating system guess. The outside interface (XX.XX.XX.XX) showed three open ports which relate to the permissible ports being hosted on the Email/Web server inside of the DMZ and the operating system guess was based on those open ports. As a result, the NMap scanner correctly identified the operating system on the Email/Web server located in the DMZ but did not guess the operating system on the OpenBSD server.

OpenBSD in general is a well developed server operating system with a proactive stance on security and is very popular for firewall situations. As such it has very few vulnerabilities in its default installation. The GIAC external firewall does not run any

services (which is the best scenario for a firewall) so there are no services to compromise or crash. This is definitely the preferred configuration for an external corporate firewall. Overall, the OpenBSD server is well hardened and the IPFilter firewall rules would appear to be aggressive enough so that absolutely no information of any sort is given out to well designed scanning tools such as NMap. In its current state, this server is well configured.

It is recommended that the GIAC Information Staff should monitor the security information provided by OpenBSD (http://www.openbsd.org/security.html#29) and determine if any future security issues arise that need to be addressed by installing the necessary patches. At this time, the server is missing some patches but as noted above they are not relevant to the existing configuration and will not improve the security of the server as it is used today.

It should be noted that OpenBSD has switched away from the use of IPFilter as its default bundled firewall tool. OpenBSD is now bundled with a fairly new tool that has undergone less testing. Therefore, if GIAC staff should decide to upgrade their external DMZ firewall to a newer version of OpenBSD, it is recommended that they carefully review the status of the newer packet filter tool. OpenBSD is currently available in Version 3.0 as of December 01, 2001.

The IPFilter tool is still under development and there is a great deal of support from the user community for OpenBSD installation so it is still possible to obtain a newer version of IPFilter to install on either the existing OpenBSD Version 2.9 or on a newer version of OpenBSD. It is currently not clear how long this support will continue but will likely depend on how closely OpenBSD continues to follow the *BSD code base. IPFilter is hosted at this location (http://coombs.anu.edu.au/~avalon/ip-filter.html). It is also recommended that the GIAC Information System staff join the IPFilter list server and monitor the status of IPFilter.

5.1.2 Internal DMZ Firewall - FreeSCO Router Version 0.2.7

As noted above, the FreeSCO router is not intended as a full featured firewall and as such is extremely limited in its capabilities. The web page that supports the FreeSCO tool (www.freesco.org) is aimed more at development of new features and as such does not have a specific security listing. A search for ‘errata” turned up some limited information but this also was aimed primarily at development of new features. The Nessus and NMap scans were performed against both the inside (internal GIAC network) and outside (DMZ) interfaces.

The Nessus scan on the inside interface (IP 192.168.XX.XX) generated one Security Note and three Security Warnings (see Appendix 2). The Security Note relates to the traceroute information between the Nessus scanner and the FreeSCO router. The other Security Warnings relate to the router responding to ICMP timestamp requests, an older version of BIND is running on the router, and the router uses non-random IPID’s for its

IP sequencing which could open the host up to attackers guessing the next IP packet ID. Of the three Warnings, only one is considered serious, the BIND version which as noted above GIAC does not use but apparently has not been able to disable.

The Nessus scan on the DMZ interface (IP 10.10.10.3) generated the same Security Note about traceroute information plus two Security Warnings including the one noted above about ICMP timestamp requests and the one about non-random IPID's. The router is configured to only allow DNS queries from a specific (i.e., inside) interface and as a result the BIND vulnerability should not be an issue from the DMZ side.

The NMap scan on the inside interface turned up the DNS server on Port 53 and correctly identified the operating system as Linux Version 2.0.34-38 and stated the IPID sequencing as incremental. The NMap scan on the outside interface also turned up the DNS server which Nessus was not able to find as noted above. NMap noted the DNS server service was "filtered". NMap also was not able to accurately guess the operating system from the DMZ side.

In summary, it would appear the FreeSCO router does a relatively effective job of limiting access to the one serious vulnerability it has which is the older version of BIND. This is commendable for such a trimmed down operating system. However, the fact that NMap was able to see the DNS server service as filtered means that it is visible to some extent from the DMZ and may lead to a full system compromise from another system within the DMZ.

In following, it is recommended that GIAC consider replacing this installation with a more secure "firewall" that allows specific rules and that will not be hosting other services such as a DNS server that might lead to a compromise. A minimal installation of OpenBSD similar to that of the external DMZ firewall (with the IPFilter rules adjusted accordingly to address the different IP ranges and to drop all connection attempts from the DMZ) may suit that purpose admirably.

This switch to a "full firewall" on the internal side of the DMZ does not require immediate attention but considering the current number of BIND vulnerabilities and the number of internet worms that are actively searching the internet for BIND, it should be enacted within the next 30-60 days particularly if any changes are made to the external DMZ firewall which might lead to additional access to DMZ machines.

Red Hat Linux Version 6.2

As of December 2001, Red Hat had released 79 Security Errata and 19 Bug Fix or Enhancement patches for Version 6.2. There is some overlap amongst the Errata, Bug Fix, and Enhancement notifications as they tend to be released on different list servers. Of the Security Errata, only 20 relate to the packages currently in use on the GIAC server and of those 20, several were general updates of the kernel or other common system tools such as mouse support or libraries that will generally fix a variety of bugs or

smaller security issues. Only 6 Security Errata could potentially be exploitable on the existing GIAC server. Two of the six relate to applications installed (apache and wu-ftp) and the remaining four relate to either kernel or tool updates that solve a security issue (inetd update, glibc vulnerability, syslog vulnerability, and glibc update). There are also a large number of general fixes that update many features such as the Red Hat Package Manager (rpm) tool, the Bash shell, plus others.

It is always recommended that existing applications should be updated for known security vulnerabilities. However, it is not necessary to install all patches. Many of the patches made available may not be applicable to the existing installation so it requires a thorough review of the patches.

The apache vulnerability (RHSA-2001:126-27) does not apply to the current GIAC configuration as it relates to specific apache module settings in the apache configuration files that are currently disabled in the GIAC setup. However, it may be a good idea to update the version of apache to the most current to prevent this from ever being a problem as GIAC moves forward with their e-business. This update should be undertaken within the next 30-60 days.

The wu-ftp vulnerability (RHSA-2001:157-06) does apply to the GIAC configuration as it is a buffer overflow issue which is always a serious concern. At this time, the FTP server is not accessible to the internet which has presumably protected the server so far. However, this update should be applied immediately in case internet access is gained to non-public portions of the DMZ through changes to the external DMZ firewall or through compromise of another machine within the DMZ.

The glibc vulnerability (RHSA-2001:002-03) deals with incorrect permissions such that a non-privileged user can preload libraries into SUID programs even if not permitted to do so. On the GIAC server, this is a small vulnerability as all user shells have effectively been disabled in /etc/passwd. However, it may be possible for a non-privileged user to compromise another system account that may have SUID privileges. Therefore, as GIAC moves forward in their e-business, there may be changes enacted on the server that introduce software that would open up this vulnerability. In following, it is recommended that GIAC undertake this update to the most current version of glibc for Red Hat 6.2. These libraries are noted in RHSA-2001:160-09 (released on December 14, 2001). This should be undertaken within the next 30-60 days.

The syslog vulnerability (RHSA-2000:061-02) deals with various problems with syslog and klog daemons. These are local exploits and as such are less of an issue to GIAC as their console is located in a locked server room. This is a theoretical exploit that Red Hat consider serious enough to release a patch for prior to any known exploits. Therefore, it is recommended that GIAC undertake this update to remove this possible problem. This should be undertaken within the next 30-60 days.

The inetd update (RHSA-2001:006-03) solves a problem with incorrect closure on internal server services that could potentially starve the server of resources. GIAC does not have any internal services (e.g., daytime) activated but they do use the inetd service

for controlling the wu-ftp tool so they should consider installing this update to solve potential problems down the road as they move forward with their e-business. This should be undertaken within the next 30-60 days.

The Nessus scan on the Email/Web e-business server interface (IP 10.10.10.2) was performed from the internal GIAC network and generated two Security Holes, four Security Notes, and one Security Warning (see Appendix 2). The Security Holes relate to the qmail server and the wu-ftp server. The qmail issue seems to be a "false positive" related to sending mail directly to programs. The wu-ftp hole relates to known buffer overflows in the earlier versions of the FTP daemon. These will be discussed further under Application Vulnerabilities.

The Security Notes relate to the apache web server which gives out banner information, the POP3 server also giving out banner information, the traceroute information that could be elicited between the Nessus scanner and the target server, and that the operating system version was correctly determined as Linux 2.1.xx or 2.2.xx.

The Security Warning relates to ICMP timestamp requests and replies and the server responding to those requests.

The NMap scans turned up a listing of all four open ports based on the four services running (FTP, SMTP, HTTP, and POP3) (see Appendix 3). NMap was also able to very accurately (and very quickly) determine operating system type and the exact version of Linux (2.2.13).

Once the vulnerabilities noted above have been patched, it will still be possible for tools like Nessus or NMap to elicit the information they can. To hide the applications and underlying operating system somewhat, it may be possible to set up some simple IPChains firewall rules that will drop some of the information that Nessus and NMap use to make decisions. It is also possible to edit some of the default banners to remove some of the really obvious information. It is recommended that GIAC consider altering the basic Linux banner information to confuse an attacker. These can be found in the /etc/issue and /etc/issue.net files.

However, all this will do is potentially confuse or slow down an attacker by giving them potentially false information. The actual applications can not be disabled as GIAC needs them to operate its business. In following, the best solution would be to update the underlying operating system and the key applications for known vulnerabilities as discussed above. It is also recommended that GIAC Information System staff monitor the Red Hat Security listings at http://www.redhat.com/support/errata/rh62-errata-general.html .

In summary, the Red Hat Version 6.2 server is somewhat hardened and with the protection of the external OpenBSD server fulfills its role well. However, if the OpenBSD server was to change and allow increased access from the internet or if another server within the DMZ was to become compromised, the Red Hat Version 6.2 server would be completely exposed and could be easily "rooted" using the known wu-ftp vulnerabilities.

Therefore, it is recommended that GIAC undertake to update the critical security hole identified above immediately.

Red Hat Linux Version 7.1

As of December 2001, Red Hat had released 36 Security Advisories http://www.redhat.com/support/errata/rh71-errata-security.html, 16 Bug Fixes http://www.redhat.com/support/errata/rh71-errata-bugfixes.html, and 52 General Advisories http://www.redhat.com/support/errata/rh71-errata.html for Version 7.1. There is quite a bit of overlap amongst the General Advisories and the Bug Fixes and some limited overlap with the Security Advisories. Of the Security Advisories, only 5 relate to the packages currently in use on the GIAC DNS server.

One Security Advisory (RHSA-2001-144) relates to the IPTables firewall and is a general update to resolve some rule loading issues and sideline issues such as FTP traffic. This is not an immediate concern for GIAC but any updates to firewall tools are usually a good idea so GIAC should consider undertaking this patch within the next 30-60 days.

Another Security Advisory (RHSA-2001-142) deals with a syncookie vulnerability in the kernel. The syncookie is a linux security tool to combat denial of service attacks and as such should operate properly. Therefore, if there are problems with it and a security fix has been released it is a good idea to install the patch. It is recommended that GIAC Information System staff undertake this fix immediately.

The next Security Advisory that may concern GIAC deals with glibc updates, one development library (RHSA-2001-160) and one common library (RHBA-2001-121). These fixes solve a number of problems so are recommended updates. None of the problems is expected to be critical for GIAC based on the existing applications and use for the Red Hat Version 7.1 server so it is recommended that the GIAC Information System staff undertake the updates in the next 30-60 days.

There is Security Advisory (RHSA-2001:072-14) dealing with man packages due to problems with GID security. This is not expected to be a critical problem for the GIAC server as this is a local console exploit and the GIAC server console (which this server does not immediately have as it does not have a monitor or keyboard) is located inside of a locked server room. However, this is a man to root exploit so it should be considered for an update. It is recommended that the GIAC Information Systems staff undertake this patch within the next 30-60 days.

The next Security Advisory (RHSA-2001:058-04) deals with mount permissions on Swap. This is a time limited security problem during the actual operating system installation or system updates and deals with permission problems on files within the swap space. It may be possible for an attacker to gain access to files on the swap partition during the installation and read the contents of those files which may contain

passwords. Therefore, it is recommended that GIAC Information System staff undertake this update prior to updating any packages on this server.

Of the Bug Fixes, only two directly relate to the GIAC configuration, one is the glibc common update and was discussed above and the other (RHBA-2001-153) deals with the login program failing to set the controlling terminal. This problem has two parts and is not directly applicable to the GIAC server configuration unless they were to change their default shell away from Bash to tcsh. However, to avoid this potential problem, it is recommended that this update be applied within the next 30-60 days.

The Nessus scan on this server interface (IP 10.10.10.4) was run from inside the GIAC internal network. It generated two Security Warnings and two Security Notes plus it listed two extra open ports that should be disabled. The first Security Warning warns about the DNS name server allowing third party recursive queries which is an issue if the DNS server is exposed to the internet. This will be discussed in more detail below under Application Vulnerabilities.

The second Security Warning deals with the ICMP timestamp request and reply and recommends the server be configured to not accept timestamp requests nor reply to timestamp queries.

The Security Notes deal with the traceroute information that was elicited between the Nessus scanner and the target server and the fact that Nessus was able to accurately identify the server operating system.

The Nessus scanner also turned up two additional ports, Port 111 (sunrpc) and Port 1024 (unknown TCP) that were listening. It was not able to elicit any information from either so did not issues any warnings or notes. Both of these should be disabled immediately on the server.

The NMap scan on the server interface generated a listing of three open ports (Port 53, Port 111, and Port 1024) and also very quickly and accurately identified the server operating system (Linux 2.40-2.4.9) (see Appendix 3). It is possible to edit some of the default banners to remove some of the really obvious information. It is recommended that GIAC consider altering the basic Linux banner information to confuse an attacker. These can be found in the /etc/issue and /etc/issue.net files.

As noted above, once the vulnerabilities noted above have been patched, it will still be possible for tools like Nessus and NMap to elicit the information they can. The one feature on the GIAC DMZ that saves this server from possible abuse is the presence of the OpenBSD external firewall. It is possible to hide the DNS application and underlying operating system somewhat by setting up some simple IPTables firewall rules that will drop some of the information that Nessus and NMap use to make decisions. However, the best solution is to update the underlying operating system and the key applications for any known vulnerabilities as discussed above. It is also recommended that GIAC Information System staff monitor the Red Hat Security listings at www.redhat.com/support/errata on a regular basis.

In summary, the Red Hat Version 7.1 server is basically a default installation with the protection of the external OpenBSD server. In that situation, it is able to fulfill its role as internal DNS server. However, if the OpenBSD server was to change and allow increased access from the internet or if another server within the DMZ was to become compromised, the Red Hat Version server would be completely exposed and could be compromised (e.g., rpc vulnerabilities) or abused with DNS cache poisoning. Therefore, it is recommended that GIAC undertake to update the security issues identified above within the timeframes specified.

5.2 Application Vulnerabilities

5.2.1 Apache Version 1.3.17

There is only one known vulnerability listed by both Red Hat and the Apache Software Foundation (www.apache.org) for the apache 1.3 series in the version range between 1.3.14 and 1.3.19. This is discussed above under the Red Hat Version 6.2 vulnerabilities and specifically in Red Hat Security Errata (RHSA-2001:126-27). As noted above, this is currently not an issue for the GIAC configuration as they do not use the module features noted. As noted above, it is recommended that the GIAC Information Staff undertake the Red Hat patch noted above or upgrade their apache server to the most current version (version 1.3.22) within the next 30-60 days. The Red Hat update for apache is located here: ftp://updates.redhat.com/6.2/en/os/i386/apache-1.3.22-0.6.i386.rpm

If GIAC should decide to only undertake the patch and then at some later date decide to add on additional features to their apache server to host additional e-business services, it is recommended that the GIAC Information System staff update their version of apache to the most current at that time. The Version 2.0 series of apache has a number of new features and is currently under testing and may be considered stable at that time.

Some of the default ownership and permissions allowed by apache are too lax. There are several locations within your apache directory tree that permissions should be very carefully defined. By default, apache will access any directory that it has permissions on which may open up your file system to review by attackers. Therefore, it is recommended that the user and group permissions be carefully reviewed and GIAC should consider including some access control statements within the apache.conf file. Some of this information is available here http://httpd.apache.org/docs/howto/auth.html .

It is also recommended that the banner information in apache be changed or disabled so that security scans are not able to elicit version information.

5.2.2 qmail Version 1.03

There are no specific vulnerabilities listed for the qmail email server other than unnecessary banner information. As noted above, the Nessus scan indicated a Security Hole relating to the qmail server. This seems to be a "false positive" related to sending mail directly to programs. Qmail will not complain to the Nessus test but will either drop the mail silently or forward it on to the system administrator email account for notification. Therefore, this is not a security concern. qmail retains all of its configuration files in the /var/qmail/control directory including default host name, default domain name, and host name used in the initial SMTP HELO command. It is recommended that the GIAC Information Systems staff undertake to modify these control files as necessary to mask their domain, host, and version information. There is more information available at http://web.infoave.net/~dsill/lwq.html which is a well written article called "Life with qmail" written by Dave Sill. There is also a qmail Frequently asked questions forum at this location (http://cr.yp.to/qmail/faq.html) and an announcement mailing list (noted on this web page at http://cr.yp.to/lists.html#qmail) for qmail announcements and it is recommended the GIAC Information System staff should join this list to stay current with qmail issues.

5.2.3 djbdns Version 1.05

There were two vulnerabilities listed for the djbdns DNS server, one being the capability for third party recursive lookups and the other being the unnecessary banner information provided by the DNS server.

It is not clear on the djbdns web page (www.djbdns.org) nor in the installed man pages whether it is possible to disable the DNS server banner information. There is an announcement mailing list noted on this page (http://cr.yp.to/lists.html#dns) for djbdns announcements. It is recommended the GIAC Information System staff should join. There is a frequently asked questions page:
(http://www.faqts.com/knowledge_base/index.phtml/fid/699/).

The other vulnerability relates to allowing third party recursive queries which is a security concern if the DNS server is exposed to the internet as it can lead to DNS cache poisoning. However, if it is an internal DNS name server this should not an issue. It is recommended that the DNS server be configured to restrict third party recursive queries and only allow identified servers to use its services. In following, the GIAC Information Systems staff should undertake to configure the already operating dnscache program to only allow queries from a specific IP range (10.10.10.XX) This will limit queries to only the GIAC servers and internal network because the external DMZ firewall drops all internet DNS queries outside the DMZ network. This should be undertaken immediately. See http://cr.yp.to/djbdns/faq/cachex.html for more information.

5.2.4 WU-FTP Version 2.6.0-3

As noted earlier under the Red Hat Version 6.2 discussion, the version of wu-ftp running on the Email/Web e-business server is vulnerable to a remote buffer overflow exploit. This requires an immediate upgrade to a current version to ensure this is not a useable exploit should an attacker gain access into the DMZ. The Red Hat web site has the most current version of wu-ftp located at ftp://updates.redhat.com/6.2/en/os/i386/wu-ftp-2.6.1-0.6x.21.i386.rpm .

5.3 Other Vulnerabilities

Three other security vulnerabilities that were noted during the baseline audit are the compromised wire security cage between the GIAC server room and the public elevator bank, the duplicate passwords on two of the DMZ servers, and the fact that the two Red Hat servers are essentially default installations.

The elevator bank area is locked to the public during off hours and not accessible by stairway unless the stairway door has been lodged open during the daytime (public access hours). If this was to occur, this would expose the GIAC server room to compromise since the wire security cage contains many large holes and once access has been gained to the server room, the doors can be opened from the inside and equipment can be very easily removed and taken down the stairway. GIAC should approach the building owner to have the security cage repaired immediately.

The use of duplicate passwords is a concern from the standpoint of a cross-DMZ compromise. Each server within the DMZ should have a unique random password that is not written down on a note near the console nor stored in written form in the server room. They should be kept locked in a cabinet away from the server room. This is an immediate concern and should be addressed as soon as possible. In addition, GIAC Information Systems staff should develop a regular plan to change all of the server passwords within the DMZ on a regular basis. It is recommended that they be changed every 3-6 monthes.

The default installation of linux servers generally come with many unneeded packages and also file and directory permissions that are too permissive. This has spawned the development of many “hardening” tools such as the bastille linux script and others. Many of these scripts will remove many of the default permissions and if directed may remove several packages. It is recommended that the GIAC Information Systems staff either obtain one of the hardening scripts and use it to secure the Red Hat servers or manually work their way through the list of installed rpm packages and remove most as very few are actually used based on the current server roles. The Bastille script supports both Red Hat 6.2 and Red Hat 7.1 and is available at this location (www.bastille-linux.org).

One other default vulnerability on Red Hat servers that should be disabled is the use of Ctl-Alt-Del keys to reboot the server. While this is very convenient, it bypasses the requirement for root to issue the shutdown command. The GIAC servers are located in a locked server room but it is recommended that these keys be disabled so that only root will be able to shut down the server after logging in. These can be disabled by looking for the ctrlaltdel tag in the file /etc/inittab and then changing that line to:

#no C-A-D: ca: :ctrlaltdel :/sbin/shutdown –t5 –rfn now

5.4 Event Logging

Another issue of concern is the extent of monitoring that goes on with the GIAC DMZ servers. The GIAC Information Systems staff is very busy with their small and growing company so finding time to monitor system and application logs on each server is difficult and extremely sporadic. This is a concern as a compromise could occur and the staff would be unaware of it until something broke or noticeably changed. GIAC relies on its e-business presence so it should spend an appropriate amount of time to monitor its servers to ensure that its online presence remains untarnished and its fortune cookie sayings are always available online.

Therefore, it is recommended that the GIAC staff setup a centralized syslog server in the DMZ (potentially using their old Internal DMZ firewall if they upgrade it), and have all of the various logs from all DMZ servers gather at a single point. This can be completed by adding a duplicate line in the /etc/syslog.conf file for the log types to be forwarded (or a complete copy of all log types if desired) but change the tail end of each logging line from "/var/log/filename" to "@<sysloghostname>". It is also recommended that only the syslog service be running on the syslog server host to minimize any opportunities for an attacker to compromise the syslog server host. TCPWrappers could also be used for the syslog service on the syslog host machine so that the hosts.allow file would define the DMZ systems that can send log files.

Once the logs have reached the syslog server, the logs could be sorted and reviewed using any number of "log alert" programs and once specific events are caught, notification would be automatically sent to specific GIAC staff. The CPU and memory requirements for a syslog server are minimal but require an extensive amount of drive space for the various log files that are rotated. The installation of a centralized syslog server should be undertaken immediately.

As part of the installation of the centralized syslog server, GIAC should consider the installation of a time server to synchronize the various time clocks on all of the DMZ servers. Intel based hardware clocks are notoriously inaccurate so a time server would help to correct that problem. It is recommended that GIAC setup a time server within the DMZ that can ensure that all clocks are synchronized especially the proposed syslog server. This should be undertaken during the same timeframe as the installation of the centralized syslog server.

5.5 File Integrity Databases

The existing GIAC DMZ servers have been installed for approximately 15 monthes and have being operating presumably without incident since. However, there is no way to accurately determine if changes have occurred on the systems as the rpm databases have not been updated since the initial installation and are incorrect since they do not include even the key applications running on the systems (e.g., apache, qmail, and djbdns). A tool such as tripwire would help to track changes after the system is installed and hardened.

It is recommended that tripwire be installed on all newly introduced or re-installed DMZ systems. Tripwire for Linux was released in October 2000 and versions for *BSD Unix have been available for some time. The linux and *BSD versions are both available at: (http://www.tripwire.org/downloads/index.php). It is recommended that GIAC Information Systems staff undertake to install tripwire on all of their DMZ systems immediately after installing the suggested patches and updates noted in this report. Installing tripwire on a system after it has been operating in a public domain for some period is not always recommended but the servers appear to be operating correctly based on the tests run for this audit so a tripwire installation at this point will help to establish a baseline with the current configuration. The tripwire database should then be stored on removable media. If the tape backups discussed below are undertaken and copies are stored offsite, then those backups can serve as the offsite tripwire database.

5.6 Tape Archives

The audit team was also concerned that the GIAC DMZ servers had not been backed up. This is presumably due to the lack of available equipment for backups. It is a prudent practice to backup a fully installed and hardened system prior to making it public. If the system should ever fail or be compromised, the backup can be used to completely restore the system to its original state in a very short time period. Considering that GIAC does not have any backup server systems in case their Email/Web server should fail, a tape archive or CD/DVD of the original installation would server as a suitable recovery mechanism and would generally allow the system to be back up within an hour (assuming the server hardware has not failed).

It is therefore recommended that GIAC undertake regular tape backups (or CD/DVD backups) of their DMZ systems and store some copies of the backup's onsite in the server room (for immediate access) and some copies offsite (for catastrophic failure). A regular plan of backups and which copies stay and which go offsite should be developed. Relying on a backup of a system after it has been operating in a public domain for some period is also not recommended but the servers appear to be operating correctly based on the test run during this audit and a backup will help to

maintain a baseline with the current configuration that during a restore will at least get back to the current state. It is recommended that GIAC Information Systems staff undertake regular backups of the various DMZ servers particularly the Email/Web server which is so critical to its online presence. It is also recommended that they test restore the backups on a regular basis to ensure the backup archives are valid.

5.7 Information Updates

The audit team has recommended that the GIAC Information Systems staff subscribe to various mailing lists for Red Hat, OpenBSD, Apache, qmail, and djbdns. It is also recommended they go to the following security sites and sign up for the available security newsletters:

http://www.sans.org/newlook/digests/
www.securityfocus.com
www.incidents.org

5.8 Planning for Security Updates

Moving forward from this audit, it is recommended that the GIAC Information Systems staff develop a regular program of reviewing security patches that are released and determining which patches should be installed. Generally reviewing the information provided by the vendor with the security patch will explain why the patch is required and detail the versions that require patches. Based on that information the GIAC staff should be able to determine the relevance of the patch to their situation and the urgency of applying those patches.

6.0 RECOMMENDATIONS

6.1 Immediate Concerns

There are several identified concerns that the GIAC Information Systems staff should immediately secure. They include the following:

- Upgrade to the most current version of wu-ftp on the Red Hat 6.2 server;
- Syncookie update to the Red Hat 7.1 server;
- Disable Ports 111 and 1024 on Red Hat 7.1 server;
- Re-configure the Internal DNS server to only allow specific clients;
- Repair the wire security cage above the GIAC server room;
- Change server passwords so each is unique;
- Introduce passwords to each server BIOS;
- Change server BIOS to boot from hard disk first;
- Introduce passwords and no wait time to LILO on each Red Hat server;
- Check all rcX.d directories on Red Hat servers to disable unneeded services;
- Install a central syslog server in DMZ with log monitoring software;
- Install a time server that each DMZ server will synchronize to;
- Run a hardening script against the linux servers to make them more secure;
- Install tripwire on each DMZ server;
- Undertake regular backups of each server and maintain copies offsite.

The Red Hat System and Application updates can be undertaken quite easily by GIAC Information Systems staff using the Red Hat Package Manager. The staff can download the patches (see Appendix 1 for a URL to the vendor patches) and place them in a specific directory on the local server drive (e.g., /root). From within that directory where the patch or upgrade files reside, the following command can be issued:

Rpm –Fvh [filename]

The filename would be one of the upgrades or patches in that directory. The rpm tool will then "freshen" the installed copy to the newer version with the patch or upgrade. It is also recommended that once the updates have been completed, the rpm files be either moved off the server onto backup media or be deleted to ensure they are not compromised and potentially reused during some later update.

The wire security cage repair should be implemented as soon as possible. The GIAC Information Systems staff should approach the building manager with a request and if necessary a plan for the repair to make it suitably secure.

The extraneous Ports identified on the Red Hat 7.1 server should be disabled and GIAC staff should be able to undertake this at the same time they complete their edits on the various /etc/rc.d/rcX.d directories. Once these have been completed, they should reboot

the server and run "netstat –atun" to determine if the Ports are still listening for connections.

The various passwords that need to be changed and or introduced will just require some time on the part of the GIAC Information Systems staff to sit at the console and work their way through the changes. The BIOS and login passwords are straight forward changes. The LILO password requires a change to the /etc/lilo.conf file. Enter the following two lines:

restricted
password=secret

within the top couple lines of the /etc/lilo.conf file. Then edit (if it's there already) or enter the following line within the /etc/lilo.conf file to remove the lilo prompt wait time:

timeout=0

and then run the lilo command to store the new lilo.conf file in the Master Boot Record.

The reconfiguration of the DNS server is outlined above in the discussion under Application Vulnerabilities.

The installation of the syslog and time servers is recommended for data tracking and data integrity and will help to simplify monitoring of the various logs form all of the servers by centralizing the information. Having an accurate time record for the logs is critical if a GIAC server is compromised and GIAC (and potentially law enforcement officials) are trying to rebuild a picture of the events that took place and determine if other servers have also been compromised.

It is recommended that GIAC run one of the hardening scripts against their Linux servers since they are essentially default installs. There are too many unnecessary files installed that could be used by an attacker should a system become compromised. The default directory permissions are also too lax so a packaged script will to help change that. Alternatively, GIAC staff could manually go through the various rpm packages installed and remove them one at a time and then manually alter directory permissions to make their systems more secure. Obviously, the script is easier but either will work.

Installing Tripwire and undertaking regular tape archives is necessary for fault tolerance. If a GIAC server fails or is compromised, having to completely rebuild an entire server could take a day or more. Having an accurate idea of the exact files on a system (using Tripwire) and having valid backups will expedite a recovery of the server. GIAC will be able to track the files that have been compromised and if necessary perform a partial or complete restore of those files from the backups.

It is therefore recommended that GIAC develop a tape archive system involving regular backups from each Unix-based server. Some servers should be backed up more frequently than others but all should be backed up regularly. The critical public servers

such as the Email/Web server should be backed up at least once per week. The other servers can be backed up every few weeks. However, initially, two full backups should be made of each server and one copy of each backup should be kept offsite (away from the GIAC office building) and one copy should be kept onsite in the GIAC office but not in the server room. As noted, these backup copies will help expedite a recovery during a server failure or compromise and also during a catastrophic failure such as a fire within the GIAC office building.

6.2 Other Concerns

There were also several updates that could be delayed to a certain extent as they are not of immediate concern but could become an issue as GIAC continues to grow and make changes to its network of Unix-based servers. Therefore, it is highly recommended that these updates be undertaken within 30-60 days. These include:

- Replace the internal DMZ firewall/router with a full firewall;
- Upgrading the IPTables firewall on the Red Hat 7.1 server to the current version;
- Man page updates for the Red Hat 7.1 server;
- Glibc updates for both the Red Hat 6.2 and 7.1 servers;
- Syslogklog updates to the Red Hat 6.2 server;
- Inetd update on the Red Hat 6.2 server;
- Upgrade apache version to latest version;
- Set up IPChains firewall rules on Red Hat 6.2 Server;
- Set up IPTables firewall rules on Red Hat 7.1 server;
- Consider cable locking each server to the wall or floor;
- Set up long term plan to regularly change passwords on DMZ servers;
- Adjust banner information on applications to obscure version information;
- Consider the installation of an intrusion detection system.

As noted above, the Red Hat upgrades or patches (including the upgrade of apache) can be performed using the

rpm –Fvh [filename]

command noted above.

The installation of the OpenBSD firewall should be fairly straight forward as it was the GIAC Information Systems staff that configured the original External DMZ firewall. It is recommended that a newer piece of hardware be considered for the upgraded firewall as the existing Pentium 166mhz machine is getting dated. This older machine could be reconfigured with larger hard drives and used for the proposed centralized syslog server.

It is recommended that GIAC consider configure minimal firewalls using IPChains (on the Red Hat 6.2 server) and IPTables (on the Red Hat 7.1 server) to drop certain types

of unwanted probes or traffic against these servers. This should include ICMP probes plus all non-relevant UDP traffic. The rules should be set up only allow TCP traffic to specific ports and from specific IP addresses. An example would be the Red Hat 6.2 server should only be submitting DNS queries to the Red Hat 7.1 server. Therefore, the only UDP traffic traveling between those servers should be restricted to port 53 traffic. By carefully crafting the rules, the Red Hat servers could be well secured. There are documents located here that explain setting up linux firewalls:

http://www.linuxdoc.org/LDP/nag2/x-087-2-firewall.howto.html .

The adjustment to banner information can be undertaken by GIAC Information Systems staff as time is available as this doesn't really fix anything but rather obscures information that others may be collecting. There are detailed instructions provided on changing some of the banners under Section 5.0 of this report.

It is also recommended that GIAC consider some sort of full time network monitoring. The centralized syslog server noted above will GIAC the ability to control and monitor its server logs in a central location and if configured to receive alerts to important past events. A full time network monitor (i.e., intrusion detection system) will allow GIAC to monitor its servers in near real time and receive alerts while questionable activities are underway. Considering the critical nature of the GIAC web server and their online presence, catching attackers early rather than later is recommended. There is quite a range of options for network monitoring. In following, this consultant can provide more information on this upon request.

In conclusion, the GIAC DMZ network is well secured based on its current configuration and the hardened version of OpenBSD protecting its exterior from the internet. With a few adjustments, some updates, some further hardening, and creation of some file integrity and tape backups, and the replacement of one machine, the DMZ will be well secured and is expected to server the GIAC e-business needs well into the future.

Should GIAC wish to have this consultant perform these updates and changes, please advise. This report is respectfully submitted on this 21st of December, 2001.

7.0 REFERENCES

1) Anonymous, Maximum Linux Security, SAMS Publishing, 2000

2) Brotzman, L. and Ranch, D.. Securing Linux Step-by-Step. Version 1.0. SANS Institute, 2000.

3) Brotzman, L. and Pomeranz, H. Track 6 - 6.5 Linux/Solaris Practicum. SANS Institute. 2001

4) Frederick, K. OpenBSD 2.8 Security Checklist GCUX Paper SANS Institute. 2000

5) Gray, M.. Build a Secure Web Server Using Red Hat Linux Version 6.2 Step-by-Step. GCUX Paper SANS Institute. 2001

6) McClure, S., Scambray, J., and Kurtz, G., Hacking Exposed – Network Security Secrets and Solutions, Osborne/McGraw Hill. California. 1999

7) Parzen, P. GIAC Enterprises Internal Report on Security Audit of Unix Host Security April 3, 2001 GCUX Paper SANS Institute. 2001

8) Pomeranz, H. Solaris Security Step-by-Step. SANS Institute. 2001

9) Schaller, J. Intranet Web Server Security GCUX Paper SANS Institute. 2000

10) Sheer, P. LINUX Rute Users Tutorial and Exposition Version 0.9.1. http://rute.sourceforge.net/ 2001

11) Sill, D. Life with qmail. http://web.infoave.net/~dsill/lwq.html 2001

12) Skoudis, E., Counter Hack – A Step-by-Step Guide to Computer Attacks and Effective Defenses, Prentice Hall, New Jersey, 2002

13) Sonnenreich, W. and Yates, T. Building Linux and OpenBSD Firewalls. John Wiley and Sons. New York. 2000

14) Toxen, B., Real World Linux Security – Intrusion Prevention, Detection, and Recovery, Prentice Hall, New Jersey, 2001

15) Wells, N. Guide to Linux Installation and Administration. Course Technology-Thomson Learning. Cambridge. 2000

16) Zeltser, L. Consultant's Report from Auditing Unix GCUX Paper SANS Institute. 2001

17) Zwicky, E., Cooper, S., and Chapman, D., Building Internet Firewalls 2nd Edition. O'Reilly and Associates. California. 2000

APPENDIX 1: SUMMARY LIST VENDOR SECURITY

Red Hat Linux Version 6.2 Security Patches

http://www.redhat.com/support/errata/rh62-errata-general.html

Red Hat Linux Version 7.1 Security Patches

http://www.redhat.com/support/errata/rh71-errata-security.html

Red Hat Linux Version 7.1 Bug Fixes

http://www.redhat.com/support/errata/rh71-errata-bugfixes.html

Red Hat Linux Version 7.1 General Advisories

http://www.redhat.com/support/errata/rh71-errata.html

OpenBSD Version 2.9 Security Patches

http://www.openbsd.org/security.html#29

Apache Software Foundation software and documentation

http://www.apache.org

Apache Version 1.3 Series Security Vulnerabilities

http://www.apacheweek.com/features/security-13

IPFilter Software and Documentation

http://www.obfuscation.org/ipf/ipf-howto.html

qmail manual – life with qmail

http://web.infoave.net/~dsill/lwq.html
http://www.qmail.org

djbdns software and documentation

http://www.djbdns.org

FreeSCO software and documentation

http://www.freesco.org

APPENDIX 2: NESSUS RESULTS

Nessus Scan Report

Number of hosts which were alive during the test : 1
Number of security holes found : 0
Number of security warnings found : 0
Number of security notes found : 1

List of the tested hosts :

- 10.10.10.1 **(Security notes found)**

[Back to the top]

10.10.10.1 :

List of open ports :

- *general/udp (Security notes found)*

[back to the list of ports]

Information found on port general/udp

For your information, here is the traceroute to 10.10.10.1 :
192.168.XX.XX
?

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

Nessus Scan Report

Number of hosts which were alive during the test : 1
Number of security holes found : 4
Number of security warnings found : 3
Number of security notes found : 6

List of the tested hosts :

- 10.10.10.2**(Security holes found)**

[Back to the top]

10.10.10.2 :

List of open ports :

- *smtp (25/tcp) (Security hole found)*
- *ftp (21/tcp) (Security hole found)*
- *http (80/tcp) (Security notes found)*
- *pop3 (110/tcp) (Security notes found)*
- *general/udp (Security notes found)*
- *general/tcp (Security notes found)*
- *general/icmp (Security warnings found)*

[back to the list of ports]

Vulnerability found on port smtp (25/tcp)

The remote SMTP server did not complain when issued the command :
MAIL FROM: root@this_host
RCPT TO: |testing

This probably means that it is possible to send mail directly to programs, which is a serious threat, since this allows anyone to execute arbitrary command on this host.

NOTE : ** This security hole might be a false positive, since
some MTAs will not complain to this test, and instead will
just drop the message silently **

Solution : upgrade your MTA or change it.

Risk factor : High
CVE : CAN-1999-0163

[back to the list of ports]

Vulnerability found on port smtp (25/tcp)

The remote SMTP server did not complain when issued the
command :
MAIL FROM: root@this_host
RCPT TO: /tmp/nessus_test

This probably means that it is possible to send mail directly
to files, which is a serious threat, since this allows
anyone to overwrite any file on the remote server.

NOTE : ** This security hole might be a false positive, since
some MTAs will not complain to this test and will
just drop the message silently. Check for the presence
of file 'nessus_test' in /tmp ! **

Solution : upgrade your MTA or change it.

Risk factor : High
CVE : CVE-1999-0096

[back to the list of ports]

Vulnerability found on port smtp (25/tcp)

The remote SMTP server did not complain when issued the
command :
MAIL FROM: |testing

This probably means that it is possible to send mail
that will be bounced to a program, which is
a serious threat, since this allows anyone to execute
arbitrary command on this host.

NOTE : ** This security hole might be a false positive, since
some MTAs will not complain to this test, but instead
just drop the message silently **

Solution : upgrade your MTA or change it.

Risk factor : High
CVE : CAN-1999-0203

[back to the list of ports]

Warning found on port smtp (25/tcp)

The remote SMTP server is vulnerable to a redirection
attack. That is, if a mail is sent to :

user@hostname1@victim

Then the remote SMTP server (victim) will happily send the
mail to :
user@hostname1

Using this flaw, an attacker may route a message
through your firewall, in order to exploit other
SMTP servers that can not be reached from the
outside.

*** THIS WARNING MAY BE A FALSE POSITIVE, SINCE
SOME SMTP SERVERS LIKE POSTFIX WILL NOT
COMPLAIN BUT DROP THIS MESSAGE ***

Solution : if you are using sendmail, then at the top
of ruleset 98, in /etc/sendmail.cf, insert :
R$*@$*@$* $#error $@ 5.7.1 $: '551 Sorry, no redirections.'

Risk factor : Low

[back to the list of ports]

Warning found on port smtp (25/tcp)

The remote SMTP server allows the relaying. This means that
it allows spammers to use your mail server to send their mails to
the world, thus wasting your network bandwidth.

Risk factor : Low/Medium

Solution : configure your SMTP server so that it can't be used as a relay any more.
CVE : CAN-1999-0512

[back to the list of ports]

Information found on port smtp (25/tcp)

Remote SMTP server banner :
www.giac.com ESMTP
214 qmail home page: http://pobox.com/~djb/qmail.html

[back to the list of ports]

Vulnerability found on port ftp (21/tcp)

You are running a version of wu-ftpd which is older or as old as version 2.6.0.
These versions do not sanitize the user input properly and allow an intruder to execute arbitrary code through the command SITE EXEC.

*** Note that Nessus could not log into this server
*** so it could not determine whether the option SITE
*** EXEC was activated or not, so this message may be
*** a false positive

Solution : upgrade to wu-ftpd 2.6.1
Risk factor : High
CVE : CVE-2000-0573

[back to the list of ports]

Information found on port ftp (21/tcp)

Remote FTP server banner :
www.giac.com ftp server (version wu-2.6.0(1) mon feb 28 10:30:36 est 2000) ready.

[back to the list of ports]

Information found on port http (80/tcp)

The remote web server type is :
Apache/1.3.17 (Unix)

We recommend that you configure your web server to return bogus versions, so that it makes the cracker job more difficult

[back to the list of ports]

Information found on port pop3 (110/tcp)

The remote POP server banner is :
+OK <17546.1008620836@www.giac.com>

[back to the list of ports]

Information found on port general/udp

For your information, here is the traceroute to 10.10.10.2 :
192.168.XX.XX
10.10.10.2

[back to the list of ports]

Information found on port general/tcp

QueSO has found out that the remote host OS is
* Linux 2.1.xx or 2.2.xx

CVE : CAN-1999-0454

[back to the list of ports]

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 authentifications protocols.

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

Risk factor : Low
CVE : CAN-1999-0524

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

Nessus Scan Report

Number of hosts which were alive during the test : 1
Number of security holes found : 0
Number of security warnings found : 2
Number of security notes found : 1

List of the tested hosts :

- 10.10.10.3 **(Security warnings found)**

[Back to the top]

10.10.10.3 :

List of open ports :

- *general/udp (Security notes found)*
- *general/tcp (Security warnings found)*
- *general/icmp (Security warnings found)*

[back to the list of ports]

Information found on port general/udp

For your information, here is the traceroute to 10.10.10.3 :
10.10.10.3

[back to the list of ports]

Warning found on port general/tcp

The remote host uses non-random IP IDs, that is, it is possible to predict the next value of the ip_id field of the ip packets sent by this host.

An attacker may use this feature to determine if the remote host sent a packet in reply to another request. This may be used for portscanning and other things.

Solution : Contact your vendor for a patch
Risk factor : Low

[back to the list of ports]

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 authentifications protocols.

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

Risk factor : Low
CVE : CAN-1999-0524

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

Nessus Scan Report

Number of hosts which were alive during the test : 1
Number of security holes found : 0
Number of security warnings found : 2
Number of security notes found : 2

List of the tested hosts :

- 10.10.10.4 **(Security warnings found)**

[Back to the top]

10.10.10.4 :

List of open ports :

- *domain (53/tcp) (Security warnings found)*
- *sunrpc (111/tcp)*
- *unknown (1024/tcp)*
- *general/udp (Security notes found)*
- *general/tcp (Security notes found)*
- *general/icmp (Security warnings found)*

[back to the list of ports]

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

[back to the list of ports]

Information found on port general/udp

For your information, here is the traceroute to 10.10.10.4 :
192.168.XX.XX
10.10.10.4

[back to the list of ports]

Information found on port general/tcp

QueSO has found out that the remote host OS is
* Standard: Solaris 2.x, Linux 2.1.???, Linux 2.2, MacOS

CVE : CAN-1999-0454

[back to the list of ports]

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 authentifications protocols.

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

Risk factor : Low
CVE : CAN-1999-0524

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

Nessus Scan Report

Number of hosts which were alive during the test : 1
Number of security holes found : 0
Number of security warnings found : 3
Number of security notes found : 2

List of the tested hosts :

- 192.168.XX.XX **(Security warnings found)**

[Back to the top]

192.168.XX.XX :

List of open ports :

- *general/udp (Security notes found)*
- *general/tcp (Security warnings found)*
- *general/icmp (Security warnings found)*
- *domain (53/tcp) (Security warnings found)*

[back to the list of ports]

Information found on port general/udp

For your information, here is the traceroute to 192.168.XX.XX :
192.168.XX.XX

[back to the list of ports]

Warning found on port general/tcp

The remote host uses non-random IP IDs, that is, it is possible to predict the next value of the ip_id field of the ip packets sent by this host.

An attacker may use this feature to determine if the remote host sent a packet in reply to another request. This may be used for portscanning and other things.

Solution : Contact your vendor for a patch
Risk factor : Low

[back to the list of ports]

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 authentifications protocols.

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

Risk factor : Low
CVE : CAN-1999-0524

[back to the list of ports]

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

[back to the list of ports]

Information found on port domain (53/tcp)

The remote bind version is : 8.2.4-REL

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

Nessus Scan Report

Number of hosts which were alive during the test : 1
Number of security holes found : 3
Number of security warnings found : 0
Number of security notes found : 4

List of the tested hosts :

- XX.XX.XX.XX**(Security holes found)**

[Back to the top]

XX.XX.XX.XX :

List of open ports :

- *general/udp (Security notes found)*
- *smtp (25/tcp) (Security hole found)*
- *http (80/tcp) (Security notes found)*
- *pop3 (110/tcp) (Security notes found)*

[back to the list of ports]

Information found on port general/udp

For your information, here is the traceroute to XX.XX.XX.XX :
?

[back to the list of ports]

Vulnerability found on port smtp (25/tcp)

The remote SMTP server did not complain when issued the command :
MAIL FROM: root@this_host
RCPT TO: |testing

This probably means that it is possible to send mail directly to programs, which is a serious threat, since this allows anyone to execute arbitrary command on this host.

NOTE : ** This security hole might be a false positive, since
some MTAs will not complain to this test, and instead will
just drop the message silently **

Solution : upgrade your MTA or change it.

Risk factor : High
CVE : CAN-1999-0163

[back to the list of ports]

Vulnerability found on port smtp (25/tcp)

The remote SMTP server did not complain when issued the
command :
MAIL FROM: root@this_host
RCPT TO: /tmp/nessus_test

This probably means that it is possible to send mail directly
to files, which is a serious threat, since this allows
anyone to overwrite any file on the remote server.

NOTE : ** This security hole might be a false positive, since
some MTAs will not complain to this test and will
just drop the message silently. Check for the presence
of file 'nessus_test' in /tmp ! **

Solution : upgrade your MTA or change it.

Risk factor : High
CVE : CVE-1999-0096

[back to the list of ports]

Vulnerability found on port smtp (25/tcp)

The remote SMTP server did not complain when issued the
command :
MAIL FROM: |testing

This probably means that it is possible to send mail
that will be bounced to a program, which is
a serious threat, since this allows anyone to execute
arbitrary command on this host.

NOTE : ** This security hole might be a false positive, since
some MTAs will not complain to this test, but instead

just drop the message silently **

Solution : upgrade your MTA or change it.

Risk factor : High
CVE : CAN-1999-0203

[back to the list of ports]

Information found on port smtp (25/tcp)

Remote SMTP server banner :
www.giac.com ESMTP
214 qmail home page: http://pobox.com/~djb/qmail.html

[back to the list of ports]

Information found on port http (80/tcp)

The remote web server type is :
Apache/1.3.17 (Unix)

We recommend that you configure your web server to return
bogus versions, so that it makes the cracker job more difficult

[back to the list of ports]

Information found on port pop3 (110/tcp)

The remote POP server banner is :
+OK <2557.1008702004@www.giac.com>

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

APPENDIX 3: NMAP RESULTS

```
Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap/ )
Host  (10.10.10.4) appears to be up ... good.
Initiating SYN Stealth Scan against  (10.10.10.4)
Adding open port 1024/tcp
Adding open port 53/tcp
Adding open port 111/tcp
The SYN Stealth Scan took 1 second to scan 1549 ports.
For OSScan assuming that port 53 is open and port 1 is closed and neither are
firewalled
Interesting ports on  (10.10.10.4):
(The 1546 ports scanned but not shown below are in state: closed)
Port       State       Service
53/tcp     open        domain
111/tcp    open        sunrpc
1024/tcp   open        kdm

Remote operating system guess: Linux Kernel 2.4.0 - 2.4.9 (X86)
Uptime 59.108 days (since Fri Oct 19 13:55:46 2001)
TCP Sequence Prediction: Class=random positive increments Difficulty=2082115
(Good luck!)
IPID Sequence Generation: All zeros
Nmap run completed -- 1 IP address (1 host up) scanned in 4 seconds
```

```
Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap/ )
Host  (10.10.10.2) appears to be up ... good.
Initiating SYN Stealth Scan against  (10.10.10.2)
Adding open port 21/tcp
Adding open port 25/tcp
Adding open port 110/tcp
Adding open port 80/tcp
The SYN Stealth Scan took 1 second to scan 1549 ports.
For OSScan assuming that port 21 is open and port 1 is closed and neither are
firewalled
Interesting ports on  (10.10.10.2):
(The 1545 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
25/tcp     open        smtp
80/tcp     open        http
110/tcp    open        pop-3

Remote OS guesses: Linux 2.1.19 - 2.2.17, Linux kernel 2.2.13
Uptime 2.952 days (since Fri Dec 14 16:41:51 2001)
TCP Sequence Prediction: Class=random positive increments Difficulty=1381891
(Good luck!)
IPID Sequence Generation: Incremental
Nmap run completed -- 1 IP address (1 host up) scanned in 2 seconds
```

```
Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap/ )
Host  (10.10.10.1) appears to be up ... good.
Initiating SYN Stealth Scan against  (10.10.10.1)
The SYN Stealth Scan took 18 seconds to scan 1549 ports.
Warning:  OS detection will be MUCH less reliable because we did not find at
least 1 open and 1 closed TCP port
All 1549 scanned ports on  (10.10.10.1) are: closed
Too many fingerprints match this host for me to give an accurate OS guess

TCP/IP fingerprint:
SInfo(V=2.54BETA30%P=i686-pc-linux-gnu%D=12/17%Time=3C1E72C1%O=-1%C=1)
T5(Resp=Y%DF=Y%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=N)
T7(Resp=N)
PU(Resp=N)
Nmap run completed -- 1 IP address (1 host up) scanned in 33 seconds

------------------------------------------------------------------------------

Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap/ )
Host (192.168.XX.XX) appears to be up ... good.
Initiating SYN Stealth Scan against (192.168.XX.XX)
Adding open port 53/tcp
The SYN Stealth Scan took 0 seconds to scan 1549 ports.
For OSScan assuming that port 53 is open and port 1 is closed and neither are
firewalled
Interesting ports on (192.168.XX.XX):
(The 1548 ports scanned but not shown below are in state: closed)
Port       State       Service
53/tcp     open       domain

Remote operating system guess: Linux 2.0.34-38
TCP Sequence Prediction: Class=truly random Difficulty=9999999 (Good luck!)
IPID Sequence Generation: Incremental
Nmap run completed -- 1 IP address (1 host up) scanned in 2 seconds

------------------------------------------------------------------------------
```

```
Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap/ )
Host  (10.10.10.3) appears to be up ... good.
Initiating SYN Stealth Scan against  (10.10.10.3)
The SYN Stealth Scan took 1 second to scan 1549 ports.
Warning:  OS detection will be MUCH less reliable because we did not find at
least 1 open and 1 closed TCP port
Interesting ports on  (10.10.10.3):
(The 1548 ports scanned but not shown below are in state: closed)
Port       State       Service
53/tcp     filtered    domain

Too many fingerprints match this host for me to give an accurate OS guess
TCP/IP fingerprint:
SInfo(V=2.54BETA30%P=i686-pc-linux-gnu%D=12/18%Time=3C1FA447%O=-1%C=1)
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=Y%DF=N%W=0%ACK=S%Flags=AR%Ops=)
PU(Resp=Y%DF=N%TOS=C0%IPLEN=164%RIPTL=148%RID=E%RIPCK=E%UCK=E%ULEN=134%DAT=E)
Nmap run completed -- 1 IP address (1 host up) scanned in 5 seconds

------------------------------------------------------------------------------

Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap/ )
Host www.giac.com (XX.XX.XX.XX) appears to be up ... good.
Initiating SYN Stealth Scan against www.giac.com (XX.XX.XX.XX)
Adding open port 110/tcp
Adding open port 25/tcp
Adding open port 80/tcp
The SYN Stealth Scan took 314 seconds to scan 1549 ports.
Warning:  OS detection will be MUCH less reliable because we did not find at
least 1 open and 1 closed TCP port
For OSScan assuming that port 25 is open and port 37941 is closed and neither
are firewalled
Interesting ports on www.giac.com (XX.XX.XX.XX):
(The 1546 ports scanned but not shown below are in state: filtered)
Port       State       Service
25/tcp     open        smtp
80/tcp     open        http
110/tcp    open        pop-3

Remote operating system guess: Linux 2.1.19 - 2.2.17
Uptime 3.882 days (since Fri Dec 14 16:41:58 2001)
TCP Sequence Prediction: Class=random positive increments
Difficulty=1270520 (Good luck!)
IPID Sequence Generation: Incremental
Nmap run completed -- 1 IP address (1 host up) scanned in 319 seconds
```

APPENDIX 4: RED HAT SERVER 6.2 INSTALLATION RPMS

This is a listing of RPM packages that were originally installed on the Email/Web e-business server (Red Hat Server 6.2). This list has not been updated since that original installation. It was generated using the rpm –q –a command.

```
setup-2.1.8-1
filesystem-1.3.5-1
basesystem-6.0-4
ldconfig-1.9.5-16
gpm-1.19.3-0.6.x
shadow-utils-19990827-10
mktemp-1.5-2
termcap-10.2.7-9
libtermcap-2.0.8-20
ed-0.2-19.6x
MAKEDEV-2.5.2-1
SysVinit-2.78-5
XFree86-Mach64-3.3.6-20
anacron-2.1-6
chkconfig-1.1.2-1
m4-1.4-12
pam-0.72-20.6.x
info-4.0-5
fileutils-4.0-21
grep-2.4-3
ash-0.2-20
at-3.1.7-14
authconfig-3.0.3-1
bc-1.05a-5
bdflush-1.5-11
binutils-2.9.5.0.22-6
bzip2-0.9.5d-2
sed-3.02-6
console-tools-19990829-10
e2fsprogs-1.18-5
cpio-2.4.2-16
cracklib-2.7-5
cracklib-dicts-2.7-5
crontabs-1.7-7
textutils-2.0a-2
dev-2.7.18-3
diffutils-2.7-17
iputils-20001010-1.6x
mailx-8.1.1-16
byacc-1.9-12
etcskel-2.3-1
file-3.28-2
findutils-4.1-34
gawk-3.0.4-2
cdecl-2.5-10
gdbm-1.8.0-3
bison-1.28-2
glib-1.2.6-3
gmp-2.0.2-13
autoconf-2.13-5
slocate-2.4-0.6.x
```

```
groff-1.15-8
gzip-1.2.4a-2
hdparm-3.6-4
inetd-0.16-4
initscripts-5.00-1
ipchains-1.3.9-5
tmpwatch-2.6.2-1.6.2
cpp-1.1.2-30
kbdconfig-1.9.2.4-1
man-1.5h1-2.6.x
cproto-4.6-3
kernel-utils-2.2.14-5.0
ElectricFence-2.1-3
ld.so-1.9.5-13
less-346-2
libc-5.3.12-31
libstdc++-2.9.0-30
lilo-0.21-15
pwdb-0.61-0
sysklogd-1.3.31-17
sh-utils-2.0-5
automake-1.4-6

logrotate-3.3.2-1
losetup-2.10f-1
lsof-4.47-2
rmt-0.4b19-5.6x
traceroute-1.4a5-24.6x
telnet-0.16-6
mingetty-0.9.4-11
mkbootdisk-1.2.5-3
mkinitrd-2.4.1-2
nscd-2.1.3-22
mount-2.10f-1
mouseconfig-4.4-1
patch-2.5-10
ncompress-4.2.4-15
net-tools-1.54-4
newt-0.50.8-2
ntsysv-1.1.2-1
passwd-0.64.1-1
ftp-0.16-3
tcsh-6.10-0.6.x
dump-static-0.4b19-5.6x
procmail-3.14-2
procps-2.0.6-5
psmisc-19-2
pump-0.7.8-1
quota-2.00pre3-2
ctags-3.4-1
readline-2.2.1-6
flex-2.5.4a-9
rootfiles-5.2-5
bash-1.14.7-23.6x
sash-3.4-2
gdb-4.18-11
open-1.4-7
```

```
setuptool-1.2-5
shapecfg-2.2.12-2
slang-1.2.2-5
indexhtml-6.2-1
stat-1.5-12
popt-1.5-9.6x
tar-1.13.17-3
tcp_wrappers-7.6-10
tcpdump-3.4-19
telnet-server-0.16-6
time-1.7-9
timeconfig-3.0.3-2
utempter-0.5.2-2
util-linux-2.10f-7
vim-common-5.6-11
vim-minimal-5.6-11
vixie-cron-3.0.1-40
which-2.9-2
zlib-1.1.3-6
dev86-0.15.0-2
egcs-1.1.2-30
wu-ftpd-2.6.0-3
lynx-2.8.3-2
make-3.78.1-4
rpm-3.0.5-9.6x
dump-0.4b19-5.6x
glibc-2.1.3-22
ncurses-5.0-12
perl-5.00503-12
glibc-devel-2.1.3-22
```

APPENDIX 5: RED HAT SERVER 7.1 INSTALLATION RPMS

This is a listing of RPM packages that were originally installed on the Internal DNS server (Red Hat Server 7.1). This list has not been updated since that original installation. It was generated using the rpm –q –a command.

```
RED HAT VERSION 7.1 SERVER
GIAC DNS Server


glibc-common-2.2.2-10
indexhtml-7.1-2
redhat-logos-1.1.2-3
setup-2.4.7-1
basesystem-7.0-2
termcap-11.0.1-8
man-pages-1.35-5
pciutils-devel-2.1.8-19
bdflush-1.5-16
compat-libstdc++-6.2-2.9.0.14
db1-1.85-5
db3-3.1.17-7
e2fsprogs-1.19-4
file-3.33-1
fortune-mod-1.0-13
glib-1.2.9-1
hdparm-3.9-6
iputils-20001110-1
libjpeg-6b-15
libtool-libs-1.3.5-8
mktemp-1.5-8
audiofile-0.1.11-1
esound-0.2.22-1
libstdc++-2.96-81
groff-1.16.1-7
modutils-2.4.2-5
ncurses-5.2-8
cpio-2.4.2-20
at-3.1.8-16
gawk-3.0.6-1
grep-2.4.2-5
dhcpcd-1.3.18pl8-10
less-358-16
make-3.79.1-5
netpbm-9.9-5
bind-utils-9.1.0-10
perl-5.6.0-12
pnm2ppa-1.04-1
logrotate-3.5.4-1
procps-2.0.7-8
pspell-0.11.2-2
psutils-1.17-10
raidtools-0.90-20
readline-4.1-9
console-tools-19990829-34
setserial-2.17-2
dev-3.1.0-14
sharutils-4.2.1-7
```

```
newt-0.50.22-2
ntsysv-1.2.22-1
slocate-2.5-5
sysklogd-1.4-7
tcl-8.3.1-53
tcsh-6.10-5
textutils-2.0.11-7
mkinitrd-3.0.10-1
mkbootdisk-1.4.2-1
switchdesk-3.9.5-1
tmpwatch-2.7.1-1
traceroute-1.4a5-25
vim-common-6.0-0.27
whois-1.0.6-1
cracklib-dicts-2.7-8
authconfig-4.1.6-1
sh-utils-2.0-13
freetype-2.0.1-4
krbafs-1.0.5-1
openldap-2.0.7-14
nss_ldap-149-1
pam_krb5-1.31-1
SysVinit-2.78-15
gtk+-1.2.9-4
libungif-4.1.0-7
tk-8.3.1-53
expect-5.31-53
timetool-2.8-1
tksysv-1.3-2
zlib-1.1.3-22
libmng-1.0.0-2
libtiff-3.5.5-10
libxml-1.8.10-1
imlib-1.9.8.1-2
gdk-pixbuf-0.8.0-7
locale_config-0.2-4
pygtk-libglade-0.6.6-7
python-1.5.2-30
pygnome-1.0.53-7
pythonlib-1.28-1
rpm-4.0.2-8
initscripts-5.83-1
apmd-3.0final-29
ipchains-1.3.10-7
kernel-2.4.2-2
netcfg-2.36-3
pciutils-2.1.8-19
portmap-4.0-35
timeconfig-3.2-1
vixie-cron-3.0.1-62
XFree86-xfs-4.0.3-5
urw-fonts-2.0-12
Mesa-3.4-13
qt-2.3.0-3
XFree86-100dpi-fonts-4.0.3-5
XFree86-tools-4.0.3-5
XFree86-xdm-4.0.3-5
```

```
xtt-fonts-0.19990222-9
ghostscript-5.50-17
ypbind-1.7-6
unzip-5.41-3
dos2unix-3.1-6
unix2dos-2.2-11
expat-1.95.1-1
sgml-common-0.5-5
docbook-dtd31-sgml-1.0-10
docbook-dtd41-sgml-1.0-10
docbook-style-dsssl-1.59-10
docbook-utils-0.6-13
autoconf-2.13-10
binutils-2.10.91.0.2-3
byacc-1.9-18
cdecl-2.5-17
ctags-4.0.3-1
cyrus-sasl-devel-1.5.24-17
db2-devel-2.4.14-5
db3-utils-3.1.17-7
diffstat-1.27-5
expat-devel-1.95.1-1
freetype-devel-2.0.1-4
gdb-5.0rh-5
glib-devel-1.2.9-1
gcc-2.96-81
gmp-devel-3.1.1-3
indent-2.2.6-1
libjpeg-devel-6b-15
libstdc++-devel-2.96-81
libtermcap-devel-2.0.8-26
libtool-1.3.5-8
ltrace-0.3.10-5
Mesa-devel-3.4-13
ncurses-devel-5.2-8
njamd-0.8.0-3
pam-devel-0.74-22
pmake-1.45-1
rcs-5.7-14
rpm-build-4.0.2-8
slang-devel-1.4.2-2
strace-4.2.20010119-3
Xaw3d-devel-1.5-9
gtk+-devel-1.2.9-4
kernel-source-2.4.2-2
iproute-2.2.4-10
shapecfg-2.2.12-5
ghostscript-fonts-5.50-3
redhat-release-7.1-1
filesystem-2.0.7-1
glibc-2.2.2-10
kudzu-devel-0.98.10-1
openssl-devel-0.9.6-3
chkconfig-1.2.22-1
cracklib-2.7-8
db2-2.4.14-5
dosfstools-2.2-8
```

```
eject-2.0.2-7
gdbm-1.8.0-5
gmp-3.1.1-3
ksymoops-2.4.0-3
libtermcap-2.0.8-26
losetup-2.10r-5
mingetty-0.9.4-16
bash-2.04-21
bzip2-1.0.1-3
hotplug-2001_02_14-15
arts-2.1.1-5
MAKEDEV-3.1.0-14
mpage-2.5.1-5
info-4.0-20
diffutils-2.7-21
fileutils-4.0.36-4
findutils-4.1.6-2
gettext-0.10.35-31
gzip-1.3-12
m4-1.4.1-4
man-1.5h1-20
net-tools-1.57-6
nkf-1.92-4
openssl-0.9.6-3
ORBit-0.5.7-3
groff-perl-1.16.1-7
popt-1.6.2-8
psmisc-19-4
aspell-0.32.6-2
pwdb-0.61.1-1
rdate-1.0-7
rootfiles-7.0-4
sed-3.02-9
shadow-utils-20000826-4
nscd-2.2.2-10
slang-1.4.2-2
kbdconfig-1.9.12-1
setuptool-1.7-2
slrn-0.9.6.4-2
syslinux-1.52-1
tar-1.13.19-4
tcp_wrappers-7.6-18
mount-2.10r-5
lilo-21.4.4-13
time-1.7-13
crontabs-1.9-2
utempter-0.5.2-4
vim-minimal-6.0-0.27
which-2.12-1
words-2-16
pam-0.74-22
cyrus-sasl-1.5.24-17
kudzu-0.98.10-1
passwd-0.64.1-4
a2ps-4.13b-13
krb5-libs-1.2.2-4
autofs-3.1.7-14
```

```
openldap-clients-2.0.7-14
XFree86-libs-4.0.3-5
control-panel-3.18-4
rxvt-2.7.5-15
tclx-8.2.0-53
tix-4.1.0.6-53
Xaw3d-1.5-9
gnupg-1.0.4-11
libpng-1.0.9-1
lynx-2.8.4-9
netpbm-progs-9.9-5
gnome-libs-1.2.8-11
libglade-0.14-3
pan-0.9.5-1
pygnome-libglade-0.6.6-7
4Suite-0.10.1-1
pygtk-0.6.6-7
python-xmlrpc-1.4-1
rpm-python-4.0.2-8
tkinter-1.5.2-30
urlview-0.9-2
util-linux-2.10s-12
kernel-headers-2.4.2-2
devfsd-2.4.2-2
iptables-1.2.1a-1
lokkit-0.43-6
pidentd-3.0.12-4
nfs-utils-0.3.1-5
quota-3.00-4
usermode-1.42-1
anacron-2.3-16
chkfontpath-1.9.5-1
XFree86-4.0.3-5
mkxauth-1.7-15
XFree86-75dpi-fonts-4.0.3-5
XFree86-twm-4.0.3-5
xinitrc-3.6-1
xloadimage-4.1-16
xsri-1.0-8
VFlib2-2.25.1-12
gv-3.5.8-11
yp-tools-2.4-7
zip-2.3-8
mtools-3.9.7-4
cpp-2.96-81
gd-1.8.3-7
docbook-dtd30-sgml-1.0-10
docbook-dtd40-sgml-1.0-11
openjade-1.3-13
perl-SGMLSpm-1.03ii-4
sgml-tools-1.0.9-9
automake-1.4-8
bzip2-devel-1.0.1-3
cproto-4.6-7
cvs-1.11-3
db1-devel-1.85-5
db3-devel-3.1.17-7
```

```
dev86-0.15.0-5
e2fsprogs-devel-1.19-4
flex-2.5.4a-13
gd-devel-1.8.3-7
gdbm-devel-1.8.0-5
glibc-devel-2.2.2-10
gcc-g77-2.96-81
krb5-devel-1.2.2-4
libpng-devel-1.0.9-1
gcc-c++-2.96-81
libtiff-devel-3.5.5-10
libungif-devel-4.1.0-7
memprof-0.4.1-3
ncompress-4.2.4-21
netpbm-devel-9.9-5
openldap-devel-2.0.7-14
patch-2.5.4-9
python-devel-1.5.2-30
readline-devel-4.1-9
rpm-devel-4.0.2-8
newt-devel-0.50.22-2
texinfo-4.0-20
XFree86-devel-4.0.3-5
zlib-devel-1.1.3-22
arpwatch-2.1a10-39
ical-2.2-21
lsof-4.51-1
screen-3.9.8-3
stat-2.2-2
xpdf-0.92-3
XFree86-SVGA-3.3.6-35
```

Last Updated: July 23rd, 2017

Upcoming Training

SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**