GIAC Enterprises

Security Audit of External Contractor's System

GCUX Practical version 1.6d

Mark Weiser
Principal Auditor

Contents

Executive Summary

GIAC Enterprises (GIAC) is a new Internet Startup company that expects to earn $200 million per year in online fortune cookie sayings. During their rapid growth, Jim Bigg, the recent MBA graduate and founder of GIAC chose to outsource several computer processes and administrative services to outside companies, rather than hire or develop additional areas of expertise within the organization. Rising security concerns throughout Internet fortune cookie vendors have stimulated GIAC to audit the systems of these outside vendors. This report details one such audit of a mail and web server, run by an external contractor.

Knowing that Universities have operated e-mail systems since well before the commercialization of the Internet, and being aware of the apparent server expertise of his alma mater, Oscar's University (OU), Mr. Bigg contracted with one of the University's faculty, Professor Mick Wise, to run his web and e-mail server. The faculty member had used Linux for a few years, was already hosting a website on a RedHat 7.0 server, had a good graduate student to run the system, and was able to talk the university into this use of their infrastructure for a portion of the fee paid by GIAC.

Prior to this audit, there was no reason to believe that the server or any services provided to GIAC were either insecure or had been breached. This report, however, details several security problems and identifies one definite security breach, in which an unauthorized person was able to gain root access to the server. The primary applications for which the university was contracted appear to function properly adequately. The system on which these services run, including those applications, however, has not been properly patched, has many unused and potentially vulnerable services running, and has poor administrative controls.

These issues are critical and, because root access has definitely been breached, it is recommended that a new server be installed and properly secured. After a careful analysis and sanitizing of user files on the current system, they could be transferred to the newly secured system. User accounts and passwords, however, should be re-constructed manually to ensure that the root breach has not compromised any of these other user accounts. The original system should then be rebuilt with an identical load to act as a test platform and hot backup.

There is no specific evidence that web or email files have been altered or that contracted services have been interrupted at any time. The level of breach indicated by this audit suggests that such modifications or interruptions could take place at any time. Because web and email services are critical to your business, GIAC is strongly encouraged to either move these services to an environment in which security is emphasized, or include some minimal security requirements in continuing contracts with OU.

Detailed analysis

This section provides details results of the audit. Strengths and weaknesses of the system are highlighted in each category. For each weaknesses found, recommendations to eliminate or mediate the associated risks are presented. The system reviewed is a 200 Mhz Intel Pentium-based Gateway PC running Red Hat Linux 7.0. The current version is RedHat 7.1, so many of the recommendation presented here as patches would be incorporated with a single upgrade to RH7.1. Because of a root-level breach the audit uncovered, our overall recommendation is to re-install the OS from scratch as soon as possible. At that time, it is recommended that the most current version be used and all relevant patches to your system for that OS level be applied.

Operating System Vulnerabilities

This system is running Red Hat version 7.0, although version 7.1 is available. The most current OS is still a 7.x version, however, 7.1 is the first to employ Linux kernel 2.4.x. Because the kernel affects every application that runs on the system, this upgrade is potentially more critical than would normally be assumed with an incremental upgrade.

Available Patches Not Applied

System administrators have indicated that no security patches have been applied since the system was installed. A review of the paper logbook that is casually maintained for major system changes, reveals that, at the time of original installation, there were no bug fixes or security patches listed by RedHat, because this system was implemented less than a week after the release of RH7.0. There are currently 56 Redhat 7.0 Security Advisories Posted[1] and 19 bug fixes[2]. Some of the bug fixes and security advisories are redundant and others do not apply to the major applications that should be running on this system to support the needs of GIAC.

A review of all 75 listed errata and advisories reveal at least the following vulnerabilities in the Operating System itself. Additional listed third party vulnerabilities are discussed in a later section.

- Updated Mount package: “the mount command, as well as other ext2 commands, don't handle labels that are exactly 16 characters long. They properly deal with labels 15 characters and less. If your /etc/fstab contained long volume labels, your system would be unbootable, as mount would fail on these partitions. This release fixes all known problems with volume labels.”[3]
- Update Systat package: “the package which provides the sar and iostat

facilities, provides an invalid crontab entry in Red Hat Linux 7.0. This causes the I/O summaries to never get updated."[4]

- Updated xinetd package "xinetd as shipped with Red Hat Linux 7 does not handle the linuxconf web interface correctly. Internal services (echo, daytime, time, and chargen) have been added for easier configuration with chkconfig or ntsysv. In addition, an xinetd-specific way of doing access control (only_from) has been fixed. "[5]
- Updated tmpwatch "The tmpwatch program periodically cleans up files in temporary directories by removing all files older than a certain age. In Red Hat Linux 6.1, 6.2, and 7.0, it used fork() to recursively process subdirectories. If a malicious user created many layers of subdirectories (thousands) in a temporary directory monitored by tmpwatch, the system process table would fill up, requiring a reboot. Additionally, tmpwatch in 6.2 and 7.0 contains an option, "--fuser", that attempts to user the fuser command to check if a file is in use before removal. However, it executed fuser with the system() call in an insecure fashion. A malicious user could construct an environment such that this provided them a local root shell. Tmpwatch now uses execle() to run fuser. "[6]
- Updated Iputils "Several problems in ping are fixed, including: Root privileges are dropped after acquiring a raw socket; an 8-byte overflow of a static buffer outpack is prevented; an overflow of a static buffer buf is prevented. A non-exploitable root only segfault is fixed as well." [7]
- Updated modutils package "The previous packages of modutils released to address a local root compromise contained an error in new safe guards that caused them to not properly be enabled when run as root from the kmod process. These new safe guards check the arguments passed to modules. The new 2.3.21 modutils package fixes this error and correctly checks the arguments when running from kmod, limiting kernel module arguments to those specified in /etc/conf.modules (on Red Hat Linux 6.2) or /etc/modules.conf (on Red Hat Linux 7). This release supersedes the previous modutils errata packages"[8]
- Updated openssh packages "The init script supplied with a previous openssh update used the daemon() shell function to start the sshd daemon. This function will not start the server if a process of the same name is already executing. As a result, attempts to start the sshd server will always fail if any users are logged in remotely. The PAM configuration file included in the previous update did not include a reference to the pam_limits module, which enforces user resource limits"[9]
- Linux kernel 2.2.19 "A local denial of service attack and root compromise of the kernel have been corrected, drivers have been updated, and NFS version 3 has been integrated."[10]
- Updated man package "A heap overrun exists in the man packages shipped with Red Hat Linux 5.x, 6.x and 7.0. Since man is setgid man, users could gain gid man privileges."[11]

Configuration Vulnerabilities

This section outlines potential vulnerabilities in the configuration of the system itself. Configuration of specific applications is covered in the next section. A review of the startup procedures and system support applications were reviewed during the audit. Prior to reviewing the configuration files of the target system, vulnerability scanning tools were used to determine potential weaknesses that would be apparent to an outside attacker. These included Nessus[12] 1.0.8, Nmap[13] 2.53. All were run from a Pentium III system attached to an non-secure network from outside OU's network. Results of each scan can be found in Appendices 1 and 2. Additionally, Appendix 3 shows the results of the netstat command on the target system.

Services Running

Nessus, Nmap, and netstat reveal many services running on the target system that are unnecessary for GIAC's web and email services. Most other services should not be running at all.

smtp (25&587/tcp): This service is necessary for the email functionality required in the GIAC contract with OU. There are configuration problems that will be covered in a later section.

telnet (23/tcp): Telnet allows remote users to log on to a system, which provides a virtual terminal on the remote computer running the telnet client. "This service is dangerous in the sense that it is not ciphered – that is, everyone can sniff the data that passes between the telnet client and the telnet server" (Appendix A). This service is simply a convenience, allowing administrators to log in from any system and location. It is not, however, required to support the necessary functions of this server. If remote login is necessary, a secure shell service should be used instead. Eliminate this service.

ssh (22/tcp): Secure Shell. Providing a secure shell is recommended for this server, rather than the plaintext telnet now being used. The daemon currently running, however, is not up to date and "is vulnerable to a flaw which allows an attacker to insert arbitrary commands in a ssh stream" (Appendix 1). Upgrade this daemon to the current version to remove this vulnerability.

ftp (21/tcp): File Transfer Protocol is defined by RFC 959[14]. It has a number of known exploits. This server should employ a secure file transfer method, making ftp unnecessary.

www (80/tcp): This service provides access to GIAC's web files and is a critical and necessary feature of this server. Apache 1.3.19 is currently

running. There are configuration problems that will be covered in a later section.

auth (113/tcp): "The 'ident' service provides sensitive information to intruders. It reports which accounts are running each service. This helps attackers to focus on valuable services (those which are owned by root)" (Appendix 1). Running netstat (Appendix 3) shows that there are many services owned by root. Some of these could be run from a less privileged account, but at least by removing auth, it will not be as simple to target root services for attack. Disable this service.

POP-3 (110/tcp): The Post Office Protocol allows a remote system to download mail after authenticating as a user. There are configuration problems that will be covered in a later section.

rsh (514/tcp): Remote shell (rlogin) allows users to login and execute commands on the target server. It is possible for "trusted hosts," or hackers who spoof the IP addresses of trusted hosts, to gain access to this server with no authentication whatsoever. This application has no practical purpose for GIAC. Remove it and use a secure shell product.

rpc (1699/udp): Remote Procedure Call was developed to speed deployment of applications. There are many exploits against RPC, with additional ones frequently being developed by hackers. The business requirement of GIAC do not require RPC, so this service should be eliminated.

netbios-ssn (139/tcp): Samba was developed to interoperate with System Message Block (SMB) communication, which is native to Windows network operating systems. There are configuration problems that will be covered in a later section.

Service Level Configuration

RedHat Linux system employs a series of six run levels. Levels range from "halt" (level 0) to Xwindows (level 5). There is also a level 6 with causes a reboot of the system. As the system moves through the various run levels, "START" and "KILL" files are called from "rc.d" directories. For instance, moving upward through level three would start the network services, whereas moving from level three to level two would stop the network services.

`Inittab` is a configuration file that determines how the system behaves while Booting. Appendix 5 shows the `Inittab` file from the OU system. There are two areas of concern, made apparent by this file:

1. Too many run levels: Although the default run level for the system is properly set at 3, there is no reason to include information about levels 4 and 5 on a network server. X Windows brings an additional set of vulnerabilities that need not even be available to the system. In the system's current state, however, X was not running. Remove the directories /etc/rc4.d and /etc/rc5.d and remove those references from the inittab file.
2. CTRL-ALT-DELETE: The system's current configuration allows any user to reboot the system, as long as they gain terminal access. Because physical security is questionable at OU and root access can be gained through this maneuver, the ca line of the inittab file should be removed or commented to read:
   ```
   # ca::ctrlaltdel:/sbin/shutdown -t3 -r now
   ```

Banners:

Banners can be used to notify users of new policies and procedures, distribute message to all users as they log in, or simply confirm what application is being accessed. As a default, most applications announce details about the program being run, including version and build number. For instance, when anyone telnets to this system, without any system rights, they receive the message:

```
Red Hat Linux release 7.0 (Guinness)
Kernel 2.2.16-22 on an i686
login:
```

At this point, outsiders can concentrate their efforts on attacks that target this operating system. Similar banners on this system gave away information about Sendmail, SSH, FTP, Apache, and POP3.

Although the presence of banners does not by itself make a system insecure, because there are widely known hacks against specific versions of specific software, information about the system and packages should not be announced by the system. Many system administrators prefer to provide banners with bogus information, although some feel that this practice, when detected, may make a system a "target" for hackers. We recommend turning banners off, where that is possible.

Core Dumps:

When a system process terminates abnormally, the contents of memory are often written to a file referred to as a core dump. The information can then be used to try to debug the process that failed. It contains a picture of the state of

the system, and may include usernames, passwords, contents of secured and possibly encrypted files, and other security-related information.

A production server with the minimum services running to meet its purpose should not require core dumps. Modify the `/etc/profile` file to not allow core dumps.

Risks from Installed Third-Party Software

Sendmail: Our vulnerability scans indicated that the system is allowing email relaying without authentication. Sendmail 8.9 or later is running on the system. As a default, this version would not allow relaying at all. Because GIAC is using this system for mail service on SMTP and POP, relaying is required, however, it can be limited to the domain from which GIAC personnel may access. Sendmail has not been configured for promiscuously relay – a practice that encourages anonymous spamming. A review of the access file (Appendix 4) shows that, although only specific sites are allowed to relay, there are too many of them. For example, all users on America Online, three major universities, and several Internet Service Providers are allowed to relay mail across this server. Better control of access will both limit the amount of processing time being consumed by unauthorized users and also make some hacking exploits difficult or impossible. Another solution would be to employ POP authentication, thereby requiring a user to first authenticate with a proper username and password prior to being able to transmit email.[15]

Additionally, redirection is allowed in the current configuration, allowing even those not authorized to directly use the system to relay messages through it by appending the intended recipient's e-mail address with the domain of the target server. This can be fixed with a modification to the sendmail.cf file.

POP-3 is used by GIAC to retrieve mail from the OU server. This transmits in the clear, so we recommend use of Phil Zimmerman's Pretty Good Privacy® (PGP®)[16] when transmitting email that is at all sensitive. This easy-to-use product will encrypt email that can only be read by the intended recipient, who must also be using PGP.

FTP: This service is currently configured to allow anonymous connections. Unless there is a specific reason that you want people to be able to connect through this protocol to transfer files without logging in, anonymous logins should be disabled. The banner for the product also provides detailed information on the version (wu-2.6.1). This type of information does not increase functionality, but does give potential hackers more information with which to breach the system. Although these problems can be addressed, there is no need to run this service at all. A secured file transfer method should be employed to post new files on the web server, making this program unnecessary.

Apache[17]. Version 1.3.19 is the current HTTP daemon running. 1.3.20 is the current version, however, there is no security-based reason to upgrade to the current version at this time. Vulnerability scans indicated a major security flaw in the configuration that would allow anyone to upload programs and execute them on the server. The program version found, however, if for a Windows server and will not execute on Linux. There are some other unnecessary CGI applications

that have been left from the default installation that should be removed. These, however, do not appear to pose any known security risk.

SAMBA: "Samba is an open source software suite that provides seamless file and print services to SMB/CIFS clients."[18] Installed version is 2.2.0, whereas the current available version is 2.2.1a. No substantial security risk exists with the installed version, however, there are some minor bug fixes in the upgrade. The GIAC server is configured to announce a Netbios name to the local network via broadcast and to register share information with a WINS server. With NT and Windows2000 client systems, Samba computers can be accessed by IP address or host name, eliminating the requirement to broadcast server information. No GIAC personnel are using mapped drives to access the server, however, so there is no reason to have this application installed.

SAMBA: New samba package "The Samba configuration used in Red Hat Linux logs operations into [remotenetbiosname].log. By sending an invalid netbiosname, Samba could be fooled to write its log in unintended and inappropriate locations. This can be especially dangerous if combined with a symlink created by a local user."[19]

Mail: Updated pine and imap packages "By adding specific headers to messages, the pine mail reader and the imap server could be made to exit with an error message when users attempted to manipulate mail folders containing those messages"

PINE: Updated pine packages "Previous versions of the pine email client, and the pico editor have had various temporary file creation issues that allow any user with local system access, to cause files owned by anyone including root to potentially be overwritten if the right set of conditions are met."[20]

Administrative Practices

This area of the audit revealed a dismal lack of any consistent practices in administering the system. For the most part, it appears that this system is simply administered by addressing problems **after** they occur. There is no regular internal auditing of the computer, no regular backup schedule or routine, no review of logs or even running processes. Interviews with administrators revealed that they are aware of system problems when GIAC notifies them that someone is not able to properly access mail or the web site. At that time, the system is typically restarted by OU administrators, without locating the source of the problem.

Until this point, there has been no catastrophic loss of data, however, that will happen, if these practices continue. Our audit uncovered a root-level breach that occurred over two months ago. This could have been detected with either a simple administrative script that runs as a daily cron job, or by periodically checking some of the system files.

This area must be addressed immediately. Because of the detected root breach, the system should be rebuilt, however, new administrative procedures should be put in to place prior to that time and employed from installation time onward.

Log Files:

Logging established is the default provided during RedHat installation. The logging system is reasonable, although it is worthless if never checked. Based on the lack of log files prior to a specific date, a known creation date of a valid user's account, and the log rotation schedule, we were able to approximate the last time a hacker manipulated (deleted) the log files. A simple script to check the existence of the system log file daily would have alerted the system administrator to a problem.

There are many repeat login failures noted in the log, with several attempts by current users to become root. These should be red flags for the system administrators to investigate prior to a successful root breach. The SU elevation attempts may indicate that a user-level account has been breached and an outsider is attempting to elevate to root.

Manual reviews of log files is an arduous process. There are several automated log analysis packages that are available. Several of them are even free. They can be configured to send messages to an administrator whenever there is something of interest that should be further investigated. Of course, a root breach could manipulate these packages as well, however, an administrator need then only monitor the log analysis package's correct

functioning.

Off-site Logging: It would be beneficial to have logs stored off the main server. Because this is the only server maintained for this project, an additional syslog server is probably not feasible. In lieu of this, however, a system that frequently compresses and sends the files to another system would allow a better analysis should a breach occur.

User Accounts and Passwords:

Account Setup:

When an authorized user requires an account, one of two system administrators establishes that account. Most commonly, the users last name is used as a login name. There is no procedure for setting a password. Often the password is initially set to the same as the login name to make it simpler for novice users to access the account. Account information is then sent to the user via an email to a different mail server account (if available), or a different GIAC employee, who passes the access information on to the new user.

The email access information contains information about connecting by telnet to the system and changing the password to one of the user's choice. Unencrypted email transmission of system access information is, in itself a severe security violation. Because most GIAC user accounts are simply used for POP and SMTP email and users are not comfortable with Unix systems, many leave their assigned password unchanged. Attempts to access several user accounts, using the username as the password, yielded several successful logins. Because the username is the beginning of the email address, anyone receiving an email from one of these accounts has divulged both their username and password.

Password Restrictions:

No password policy has been established. The default RedHat policy of a six-character password has not been changed, however, because many user accounts were established by an administrator logged in as root, that limit was not enforced for the many passwords that have not changed. Users are also not required to use any non-alphanumeric characters. This policy set makes it substantially easier to break the passwords that cannot be guessed.

We recommend that users change their passwords on the first login and

periodically thereafter (60-120 days recommended). Each password should be eight characters in length and should include at least two non-alphabetic characters. If distribution of the password through email is critical, it should be encrypted prior to sending.

The root password is memorized by the system administrators and consists of upper-case, lower-case, non-alphanumeric, and numeric characters. It is eight characters long. This password appears to be reasonably secure.

Password Vulnerability:

The audit team was able to successfully guess a few passwords, because of known patterns of initial assignment and being aware that many users do not change the initial password. In addition, we ran John the Ripper[21] against the `passwd` and `shadow` files. Of the 52 user accounts tested, 8 passwords were cracked in less than two minutes, either because they used the username or a common dictionary word as the password.

Improper Accounts:

There were a total of three accounts on the system with userID 0 (superuser privileges: `root`, `ftpsuper`, and `kork2`. `ftpsuper` was apparently created by the system administrator to make it simpler for him to upload files to any directory. By default, FTP will not allow connection as root. Creating a user account with userID 0, allows remote access as root, with complete system rights. This is a **very poor** practice. Changing to a secure form of file transfer, however, will eliminate FTP entirely, making this type of account less necessary as a convenience.

`kork2` similarly had the root userID. No administrator has any recollection or record of creating this account. Additionally, there is a non-root account, `kork`. Its sequence within the `/etc/passwd` file indicates approximately when these accounts were likely to have been created. These accounts are clearly unauthorized and we have determined that they were set up during a successful hacking session.

Security Patches up to Date:

System administrators have confirmed that no operating system security patches have been applied since the system was built, nor have any application patches been applied since each was installed and tested. There are currently 56 Redhat 7.0 Security Advisories Posted[22] and 19 bug fixes[23]. Most of these are applicable to the default load that currently is on the system. Many of the target applications, however, should be entirely removed from the system, making the patches moot. The remaining vulnerabilities were detailed in the system and applications vulnerabilities sections.

Keeping up with changes has been made simple on RedHat. Redhat distributes a product called up2date. "Using this tool will allow you to always have the most up-to-date Red Hat Linux system with all security patches, bug fixes, and software package enhancements."[24] It works by comparing locally installed packages with those available from the RedHat download site, automating the update process.

Sensitive Data Storage and Encryption:

Because the purpose of this server is to provide web and email services, there is not much in the way of sensitive data. Some email, however, may contain sensitive information and is on the server while awaiting transmission by POP or SMTP. We recommend putting this security burden on the clients by employing PGP security with the email client. This was described earlier in the report.

Network Data Transmission and Encryption:

As mentioned earlier, we recommend application-level encryption of email. Because the web is not used for online transactions, but as a method to distribute information, http need not include encryption of transmitted information. It is important, however, that logins to the server from the account that has write access to the web area be protected. A secure shell product should be implemented. During the reinstallation of Linux that is recommended, OpenSSH can be included, or the current version may be acquired and installed separately. Other accounts that do not have write access are not as critical, however, they will not have any reason to do file transfers other than email access.

Encryption is largely intended to prevent eavesdropping of packets as the traverse the network. GIAC's server at OU is connected to the network via a 100 Mbit switch, making sniffing of packets difficult. Other segments that

may be between a valid user and the GIAC server, however, may not be connected by a switch, making encryption helpful.

Access Restricted to Required Users:

Ideally, only required users are granted accounts on any computer and are only given the minimum access that they need to perform necessary tasks. A review of GIAC users against the passwd file indicates many accounts that are not necessary. It appears that several accounts exist that have nothing to do with GIAC. These have been set up for other OU users as alternate mail accounts. Although there is no evidence of a breach via these accounts, limiting user-level access helps to limit inappropriate access that could result in a breach of root.

As part of the administrative policies, we recommend that only active administrators and users that are approved by GIAC be granted accounts on this system or any replacement system.

Backup Policies and Disaster Recovery:

Backups:

There is no specific policy to limit potential catastrophic data loss. Because no mission-critical information (other than email) is stored on the system, the administrators have not given this much attention. They periodically backup the home directories and the web document area. None of the configuration files are backed up, potentially making recovery from a system failure much more time-consuming than necessary. This is done by manually creating a compressed tar file of these directories. No scripts have been created to ensure that the same files are even backed up each time the process is done.

Although the system has a tape system, files are backed up to a directory on the same system. Appendix 6 shows the file structure of the target system. There are two physical drives in the system. The backup files are kept on the same file system as the web files (/back and /export, respectively). One type of catastrophic data loss is a drive crash. In the case of a crash of the second physical disk, all web files and their backups would be lost. Backups should always be separated from the original files. Preferably, this would be on a different system or alternate media, such as tape or removable drive.

At the time of the audit, it had been six weeks since the last backup of home directories and almost five months since a backup of the web directory. This time should be reduced dramatically. The web content does not change

frequently, so a backup of that material could be done weekly, with a special backup performed when a major content change is made. Home directories should really be backed up at least daily. Ideally, this should be automated, with a full backup of the entire system being done each week and an incremental backup done each day. The following schedule is an example of a good backup policy, that always maintains two copies of data, and usually maintains a third copy:

Sun	Tue	Wed	Thu	Fri	Sat
Full1	Inc1	Inc1	Inc1	Inc1	Inc1
Full2	Inc2	Inc2	Inc2	Inc2	Inc2
Full1	Inc1	Inc1	Inc1	Inc1	Inc1

The above schedule presumes that the backups will run in the early morning hours when system load is known to be the lightest. Tapes are changed each Saturday and Monday. Each Saturday, tapes sets should be changed, with the former set being taken off-site. Periodically, each tape set should be tested to insure that data is actually retrievable from the media. Once the above process is established, it is mostly an automated process, with the exception of the tape changes.

Recovery Planning:

The administrators have not real disaster plan, however, they do have a notion of how they would approach a rebuild of the entire system. Their feeling is that, because the backups are physically separated from the root partition, if a crash occurs, they would be able to rebuild the root and link to the second drive. This is true, should a failure be of the first drive. If the second drive fails, however, all web data and backups will be lost, making recovery impossible – all web files would need to be recovered from client-side copies at best and re-written entirely at worst. In either case, the recovery will be a time-consuming process.

A second server would also be a very good idea. Although it would be best to have an identical system that could act as a backup and test bed for new software, even a low-end system with sufficient storage would suffice to replace the primary server when recovering from an outage.

The bottom line is that a recovery plan should be developed, so that administrators and GIAC personnel know the responsibilities of all involved in returning the system to service in as expedient a manner as possible.

<u>Other Issues</u>:

Breach Identified: A quick review of /etc/passwd revealed a root-level account that is not authorized. We also located a directory in which several files had been left by the attacker. Appendix 7 lists all the files found in the `/dev/.kork` directory. Most are simple to follow perl scripts.

`Stream.c` is somewhat more complex than the basic script and indicates that this system may have been used as a platform for initiating malicious activity against other systems. It is an improved version of the popular `mstream.c`[25], a distributed denial of service (DDoS) attack tool, based on the source code of `stream2.c`, a classic point-to-point DoS attack tool.

The perl scripts are mostly utilities for making system manipulation easier and faster from a remote connection.

Once a root-level breach has been achieved, it is typically wise to rebuild the system from the OS up. It is difficult to determine whether or not additional backdoors have been placed that would allow the hacker to gain entry through another channel.

Automated watch of critical files: Implement a program, such as Tripwire that will monitor critical system files for changes. This works by creating a hash signature for each critical file. Periodically (as scheduled), a new hash is created and compared to the original. If any monitored file has changed, an administrator is notified.

Prioritized Security Vulnerabilities and Issues

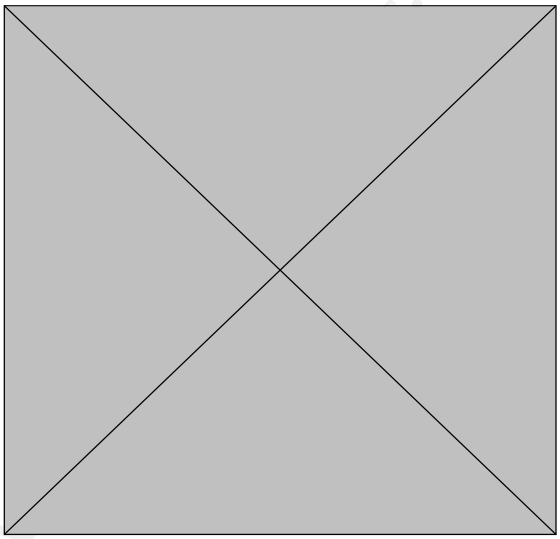
The following are among the issues have been identified on the audited system. A root breach that has occurred (highest priority issue) indicates that the system needs to be rebuilt. As such, many of the security vulnerabilities that were identified in earlier section are not listed here.

Priority	Vulnerability / Issue	Risk Level	Recommended Action	Correction Hours
1	Root breach	Critical	Rebuild OS on different system with sufficient specification, using Linux version 7.1. Use custom install with no applications. This eliminate many of the other problems.	4
2	Eliminate Unnecessary Apps and Services	Medium	Review rc#.d structure and netstat to see what services are started. Modify rc#.d directory scripts to prevent apps from restarting. Remove unnecessary apps	4
3	Security and Bug Patches to OS	High	Review the known bugs and security warnings for version 7.1 and apply applicable patches	3
4	Reinstall Web and E-mail Apps and Patches	Low	Use current releases and minimize access to mail products. Be sure to eliminate CGI availability through web daemon.	3
5	Implement Secure Shell	Medium	Implement current secure transfer for all file transfer	6
6	Backup Policy	Medium	Implement administrative procedures and schedules for backup of the system. Use suggested schedule provided previously	4
7	User accounts	Medium	Eliminate unnecessary user and system accounts from /etc/passwd	2
8	Up2date	Low	Implement a program to automate update process to OS and application	3

9	Virus	Low	Low risk for this system, but can be an additional line of defense for email users. Install anti-virus software.	4
10	Log Auditing Procedures	Mediu m	Establish procedures and software for monitoring log files and notifying administrators of anomalies	6
11	Network and System Audit	Low	Establish regular periodic audits of the system, similar to this audit. In addition, check network for promiscuous cards (sniffers).	8
12	Banners	Low	Remove banners from applications	2
13	Backup System	Low	Establish a hot backup system with identical load to the primary server.	40

Appendix 1
Nessus Results

List of open ports :



- *smtp (25/tcp) (Security warnings found)*
- *telnet (23/tcp) (Security warnings found)*
- *ssh (22/tcp) (Security hole found)*
- *ftp (21/tcp) (Security warnings found)*
- *www (80/tcp) (Security hole found)*
- *finger (79/tcp)*
- *auth (113/tcp) (Security warnings found)*
- *sunrpc (111/tcp)*
- *pop3 (110/tcp) (Security notes found)*
- *netbios-ssn (139/tcp)*
- *shell (514/tcp) (Security warnings found)*
- *login (513/tcp) (Security warnings found)*
- *unknown (587/tcp) (Security warnings found)*
- *general/udp (Security notes found)*
- *general/tcp (Security notes found)*
- *unknown (1699/udp) (Security warnings found)*
- *general/icmp (Security warnings found)*

Warning found on port smtp (25/tcp)

The remote SMTP server
answers to the EXPN and/or VRFY commands.

The EXPN command can be used to find
the delivery address of mail aliases, or
even the full name of the recipients, and
the VRFY command may be used to check the
validity of an account.

Your mailer should not allow remote users to
use any of these commands, because it gives
them too much informations.

Solution : if you are using sendmail, add the
option
O PrivacyOptions=goaway
in /etc/sendmail.cf.

Risk factor : Low
CVE : CAN-1999-0531

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

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

Information found on port smtp (25/tcp)

Remote SMTP server banner :
mstm.okstate.edu ESMTP Sendmail 8.11.0/8.11.0
Sat, 28 Jul 2001 18:17:17 -0500
214-2.0.0 This is sendmail version 8.11.0214-2.0.0 Topics:

214-2.0.0 HELO EHLO MAIL RCPT DATA
214-2.0.0 RSET NOOP QUIT HELP VRFY
214-2.0.0 EXPN VERB ETRN DSN AUTH
214-2.0.0 STARTTLS
214-2.0.0 For more info use "HELP <topic>".
214-2.0.0 To report bugs in the implementation send email to
214-2.0.0 sendmail-bugs@sendmail.org.
214-2.0.0 For local information send email to Postmaster at your site.
214 2.0.0 End of HELP info

Warning found on port telnet (23/tcp)

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

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

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

Risk factor : Low
CVE : CAN-1999-0619

Information found on port telnet (23/tcp)

Remote telnet banner :

Red Hat Linux release 7.0 (Guinness)
Kernel 2.2.16-22 on an i686
login:

Vulnerability found on port ssh (22/tcp)

You are running a version of SSH which is
older than version 1.2.32,
or a version of OpenSSH which is older than
2.3.0.

This version is vulnerable to a flaw which
allows an attacker to insert arbitrary commands
in a ssh stream.

Solution :
Upgrade to version 1.2.32 of SSH which solves this problem,
or to version 2.3.0 of OpenSSH

More information:
http://www.core-sdi.com/english/ssh/

Risk factor : High
CVE : CAN-2001-0144

Information found on port ssh (22/tcp)

Remote SSH version : ssh-1.99-openssh_2.1.1

Warning found on port ftp (21/tcp)

The FTP service allows anonymous logins. If you do not
want to share data with anyone you do not know, then you should deactivate
the anonymous account, since it can only cause troubles.
Under most Unix system, doing :
echo ftp >> /etc/ftpusers
will correct this.

Risk factor : Low
CVE : CAN-1999-0497

Information found on port ftp (21/tcp)

Remote FTP server banner :
mstm.okstate.edu ftp server (version wu-2.6.1(1) wed aug 9 05:54:50 edt 2000)
ready.

Vulnerability found on port www (80/tcp)

The 'uploader.exe' CGI is installed. This CGI has
a well known security flaw that lets anyone upload arbitrary

CGI on the server, and then execute them.

Solution : remove it from /cgi-win.

Risk factor : Serious
CVE : CVE-1999-0177

Information found on port www (80/tcp)

The remote web server type is :
Apache/1.3.19 (Unix)

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

Warning found on port auth (113/tcp)

The 'ident' service provides sensitives informations
to the intruders : it mainly says which accounts are running which
services. This helps attackers to focus on valuable services [those
owned by root]. If you don't use this service, disable it.

Risk factor : Low.

Solution : comment out the 'auth' line in /etc/inetd.conf
CVE : CAN-1999-0629

Information found on port pop3 (110/tcp)

The remote POP server banner is :
+OK POP3 mstm.okstate.edu v7.64 server ready

Warning found on port shell (514/tcp)

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

You should disable this service and use ssh instead.

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

Risk factor : Low
CVE : CAN-1999-0651

Warning found on port login (513/tcp)

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

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

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

Risk factor : Low
CVE : CAN-1999-0651

Warning found on port unknown (587/tcp)

a SMTP server is running on this port.
Here is its banner :
220 mstm.okstate.edu esmtp sendmail 8.11.0/8.11.0
sat, 28 jul 2001 18:12:53 -0500

Warning found on port unknown (587/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

Information found on port unknown (587/tcp)

Remote SMTP server banner :
mstm.okstate.edu ESMTP Sendmail 8.11.0/8.11.0
Sat, 28 Jul 2001 18:17:19 -0500
214-2.0.0 This is sendmail version 8.11.0214-2.0.0 Topics:

214-2.0.0 HELO EHLO MAIL RCPT DATA
214-2.0.0 RSET NOOP QUIT HELP VRFY
214-2.0.0 EXPN VERB ETRN DSN AUTH
214-2.0.0 STARTTLS

214-2.0.0 For more info use "HELP <topic>".
214-2.0.0 To report bugs in the implementation send email to
214-2.0.0 sendmail-bugs@sendmail.org.
214-2.0.0 For local information send email to Postmaster at your site.
214 2.0.0 End of HELP info

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

Warning found on port unknown (1699/udp)

The nlockmgr RPC service is running.
If you do not use this service, then
disable it as it may become a security
threat in the future, if a vulnerability
is discovered.

Risk factor : Low
CVE : CAN-2000-0508

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

Appendix 2
NMAP Results

```
[root@b1 student]# nmap -p 1- -sT -I -O

Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Interesting ports:
(The 65521 ports scanned but not shown below are in state: closed)
Port       State       Service                 Owner
21/tcp     open        ftp                     root
22/tcp     open        ssh                     root
23/tcp     open        telnet                  root
25/tcp     open        smtp                    root
79/tcp     open        finger                  root
80/tcp     open        http                    advise
110/tcp    open        pop-3                   root
111/tcp    open        sunrpc                  bin
113/tcp    open        auth                    nobody
139/tcp    open        netbios-ssn             root
513/tcp    open        login                   root
514/tcp    open        shell                   root
587/tcp    open        submission              root
1214/tcp   filtered    unknown

TCP Sequence Prediction: Class=random positive increments
                         Difficulty=3799106 (Good luck!)
Remote operating system guess: Linux 2.1.122 - 2.2.14

Nmap run completed -- 1 IP address (1 host up) scanned in 23 seconds
```

Appendix 3
Netstat Results

```
 [root@b1 student]# netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 b1.benchb.cxm:domain    *:*                     LISTEN
tcp        0      0 localhost.locald:domain *:*                     LISTEN
tcp        0      0 *:login                 *:*                     LISTEN
tcp        0      0 *:shell                 *:*                     LISTEN
tcp        0      0 *:pop3                  *:*                     LISTEN
tcp        0      0 *:telnet                *:*                     LISTEN
tcp        0      0 *:ftp                   *:*                     LISTEN
tcp        0      0 *:finger                *:*                     LISTEN
tcp        0      0 *:587                   *:*                     LISTEN
tcp        0      0 *:smtp                  *:*                     LISTEN
tcp        0      0 *:printer               *:*                     LISTEN
tcp        0      0 *:ssh                   *:*                     LISTEN
tcp        0      0 *:auth                  *:*                     LISTEN
tcp        0      0 *:1024                  *:*                     LISTEN
tcp        0      0 *:sunrpc                *:*                     LISTEN
udp        0      0 *:1027                  *:*
udp        0      0 b1.benchb.cxm:domain    *:*
udp        0      0 localhost.locald:domain *:*
udp        0      0 *:1025                  *:*
udp        0      0 *:994                   *:*
udp        0      0 *:1024                  *:*
udp        0      0 *:sunrpc                *:*
raw        0      0 *:icmp                  *:*                     7
```

```
raw        0      0 *:tcp                   *:*                     7
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node Path
unix  0      [ ACC ]     STREAM     LISTENING     921    /var/run/ndc
unix  0      [ ACC ]     STREAM     LISTENING     658    /dev/gpmctl
unix  0      [ ]         STREAM     CONNECTED     204    @0000001b
unix  0      [ ACC ]     STREAM     LISTENING     694    /tmp/.font-unix/fs7100
unix  12     [ ]         DGRAM                    375    /dev/log
unix  0      [ ]         DGRAM                    1365
unix  0      [ ]         DGRAM                    1316
unix  0      [ ]         DGRAM                    919
unix  0      [ ]         DGRAM                    812
unix  0      [ ]         DGRAM                    738
unix  0      [ ]         DGRAM                    718
unix  0      [ ]         DGRAM                    669
unix  0      [ ]         DGRAM                    639
unix  0      [ ]         DGRAM                    494
unix  0      [ ]         DGRAM                    456
unix  0      [ ]         DGRAM                    432
unix  0      [ ]         DGRAM                    387
```

Appendix 4
Sendmail Relay File

```
cat access
# Check the /usr/doc/sendmail-8.9.3/README.cf file for a description
# of the format of this file. (search for access_db in that file)
# The /usr/doc/sendmail-8.9.3/README.cf is part of the sendmail-doc
# package.
#
# by default we allow relaying from localhost...
localhost.localdomain          RELAY
localhost                      RELAY
127.0.0.1                      RELAY
ionet.net       RELAY
ou.edu     RELAY
dsl.okcyok.swbell.net   RELAY
juno.com        RELAY
63.146  RELAY
61.0    RELAY
utulsa.edu      RELAY
home.com        RELAY
129.244         RELAY
gci-net.com     RELAY
bpa.arizona.edu RELAY
cmi.arizona.edu RELAY
aol.com RELAY
tamu.edu        RELAY
```

Appendix 5
INITTAB File

```
cat inittab
#
# inittab       This file describes how the INIT process should set up
#               the system in a certain run-level.
#
# Author:       Miquel van Smoorenburg, <miquels@drinkel.nl.mugnet.org>
#               Modified for RHS Linux by Marc Ewing and Donnie Barnes
#

# Default runlevel. The runlevels used by RHS are:
#   0 - halt (Do NOT set initdefault to this)
#   1 - Single user mode
#   2 - Multiuser, without NFS (The same as 3, if you do not have networking)
#   3 - Full multiuser mode
#   4 - unused
#   5 - X11
#   6 - reboot (Do NOT set initdefault to this)
#
id:3:initdefault:

# System initialization.
si::sysinit:/etc/rc.d/rc.sysinit

l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
```

```
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6

# Things to run in every runlevel.
ud::once:/sbin/update

# Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now

# When our UPS tells us power has failed, assume we have a few minutes
# of power left.  Schedule a shutdown for 2 minutes from now.
# This does, of course, assume you have powerd installed and your
# UPS connected and working correctly.
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"

# If power was restored before the shutdown kicked in, cancel it.
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"


# Run gettys in standard runlevels
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6

# Run xdm in runlevel 5
# xdm is now a separate service
```

```
x:5:respawn:/etc/X11/prefdm -nodaemon
```

Appendix 6
File System structure

```
Filesystem           1k-blocks      Used Available Use% Mounted on
/dev/hda1              9480080   3155920   5842592  36% /
/dev/hdb1             20158340  10068404   9065936  53% /back
/dev/hdb5              3430316   2809216    446844  87% /export
```

Appendix 7
Identified Hacker Utility Files

```
.kork:
total 124
drwx------    3 root     lp          4096 Apr 19 20:58 .
drwxr-xr-x   12 root     root       98304 Jun 13 09:48 ..
drwx------    2 root     lp          4096 Apr 19 21:02 .dos
-rwx------    1 root     lp         15816 Apr 19 20:57 ghost.c

.kork/.dos:
total 48
drwx------    2 root     lp          4096 Apr 19 21:02 .
drwx------    3 root     lp          4096 Apr 19 20:58 ..
-rwx------    1 kork     wise        760 Apr 16 03:47 finx2.pl
-rwx------    1 root     root         812 Apr 14 12:55 floc.pl
-rwx------    1 kork     wise        713 Apr 15 12:03 floc2.pl
-rwx------    1 root     root         756 Apr 15 07:29 glock.pl
-rwx------    1 kork     wise        747 Apr 16 00:01 kork.pl
-rwx------    1 root     root        1469 Apr  1 03:24 porp.pl
-rwx------    1 kork     wise       3240 Apr 14 13:40 project.pl
-rwx------    1 root     lp          5503 Apr 19 21:02 red.tar
-rwx------    1 root     root         740 Apr  1 03:26 twister.pl
```

References:

[1] Red Hat Linux 7.0 Security Advisories. http://www.redhat.com/support/errata/rh7-errata-security.html.
[2] Red Hat Linux 7.0 Bug Fixes. http://www.redhat.com/support/errata/rh7-errata-bugfixes.html001.
[3] Red Hat Linux 7 Bug Fix, http://www.redhat.com/support/errata/RHBA-2000-074.html.
[4] Red Hat Linux 7 Bug Fix, http://www.redhat.com/support/errata/RHBA-2000-083.html.
[5] Red Hat Linux 7 Bug Fix, http://www.redhat.com/support/errata/RHBA-2000-090.html
[6] Red Hat Linux 7.0 Security Advisories, http://www.redhat.com/support/errata/RHSA-2000-080.html
[7] Red Hat Linux 7.0 Security Advisories, http://www.redhat.com/support/errata/RHSA-2000-087.html
[8] Red Hat Linux 7.0 Security Advisories, http://www.redhat.com/support/errata/RHSA-2000-108.html
[9] Red Hat Linux 7.0 Security Advisories, http://www.redhat.com/support/errata/RHSA-2001-041.html
[10] Red Hat Linux 7.0 Security Advisories, http://www.redhat.com/support/errata/RHSA-2001-047.html
[11] Red Hat Linux 7.0 Security Advisories, http://www.redhat.com/support/errata/RHSA-2001-069.html
[12] Nessus. http://nessus.securiteam.com/.
[13] Nmap Network Security Scanner. http://www.insecure.org/nmap/.
[14] Postel, J. and Reynolds, J. File Transfer Protocol. Internet Working Group, RFC 959. Oct. 1985.
[15] Levine, J. POP before SMTP. http://spam.abuse.net/tools/smPbS.html.
[16] MIT. PGP Freeware. http://web.mit.edu/network/pgp.html.
[17] Apache HTTP Server Project. http://httpd.apache.org/.
[18] SAMBA. http://us1.samba.org/samba/samba.html.
[19] Red Hat Linux 7.0 Security Advisories, http://www.redhat.com/support/errata/RHSA-2001-086.html
[20] Red Hat Linux 7.0 Security Advisories, http://www.redhat.com/support/errata/RHSA-2001-042.html
[21] John the Ripper: Password Cracker. http://www.openwall.com/john/.
[22] Red Hat Linux 7.0 Security Advisories. http://www.redhat.com/support/errata/rh7-errata-security.html.
[23] Red Hat Linux 7.0 Bug Fixes. http://www.redhat.com/support/errata/rh7-errata-bugfixes.html001.
[24] http://www.redhat.com/support/manuals/RHNetwork/ref-guide/up2date.html
[25] MStream Distributed Denial of Service Tool.

http://www.nipc.gov/warnings/advisories/2000/00-044.htm