# Auditing UNIX Systems
## A Case Study

By Lenny Zeltser
www.zeltser.com

August 2001

This report presents results of a detailed security audit of UNIX systems belonging to a fictitious company. It describes discovered vulnerabilities and proposes a prioritized roadmap for addressing them. Any similarities to an actual company or computing environment are purely coincidental. This paper was submitted to SANS Institute in August 2001 as part of fulfilling the requirements for a GIAC GCUX certification.

# Table of Contents

# Section 1: Executive Summary

## 1.1 Project Goals

The objective of this document is to provide GIAC Enterprises, a ficticious company invented for the purposes of creating this case study, with a security assessment of its publicly accessible computer systems. We were commissioned to perform this audit to allow GIAC Enterprises to prioritize its infrastructure advancement efforts and to define a plan of improving its security practices. Due to time and budget constraints, our study focused on weaknesses in design and implementation of systems accessible from the Internet, with the assumption that other aspects of the infrastructure will be examined in subsequent surveys.

This document presents our findings regarding the security of the organization's UNIX-based servers that provide DNS, Web, and mail services. We explore operating system, third-party and configuration vulnerabilities, outline problems with administrative and system maintenance practices, and describe issues relating to the organization's security policy. Finally, we provide a prioritized list of security concerns and propose methods of addressing discovered problems.

## 1.2 Summary of Findings

Our findings and recommendations concentrate on security aspects of the organization's two critical servers accessible from the Internet. Our biggest concern is that a large number of packages installed on these systems are outdated, and contain known vulnerabilities that could be exploited to remotely obtain unauthorized access to the servers. Besides presenting a risk to critical resources, this suggests that GIAC Enterprises does not place sufficient attention on tasks and costs of maintaining systems to ensure reliability and security of their operations. This is also evident from the lack of thoroughly documented security policies and procedures that should describe operational issues associated with security of the organization's systems.

Treating information security as a process requiring ongoing attention, we would have liked to see more resources devoted to anomaly detection. An anomaly, in this context, constitutes an event, whether malicious or not, that negatively impacts performance or availability of a computing resource. The organization does not presently have means of automatically monitoring the "health" of its critical systems, which may result in a prolonged downtime due to an event that could have been noticed earlier via log or process monitoring. Similarly, intrusion detection systems can be used to monitor critical networks and systems for potentially malicious activity, allowing administrators to respond to events during reconnaissance stages of attacks before they escalade into critical incidents. Additionally, the network infrastructure at the organization's corporate office was not designed to segment the environment into security zones that might dampen an attacker's actions once one of the internal systems was compromised.

We were also concerned with some of the tape backup practices employed by GIAC Enterprises. Specifically, test restores from tape are never performed, which will prevent the organization from discovering a fault in the backup mechanism, resulting in the inability to recover lost data. Additionally, all backup tapes are stored in the corporate office, and are never taken away for off-site storage. This may result in a scenario where a local or regional disaster will prevent the organization from recovering its data and resuming operations within a reasonable timeframe. Our findings and recommendation are described in greater detail in subsequent sections.

# Section 2: Analysis of Findings

## 2.1 Infrastructure Overview

Figure 2-1 below summarizes the current state of network infrastructure at GIAC Enterprises. The firewall is located behind the router, which connects the organization to the Internet. All computing resources hosted at the organization's corporate office are located on the same network behind the firewall; this is a significant concern, since a compromise to a publicly accessible system may spread to other corporate servers and workstations.

The router is Cisco 3660, and the firewall is Cisco PIX 515. Computing resources are interconnected using a Cisco Catalyst 4006 switch. The firewall provides Network Address Translation (NAT), dynamically mapping outbound connections to the Internet to a block of public IP addresses assigned to GIAC Enterprises by its ISP; inbound one-to-one NAT is performed for servers that need to be accessed from the Internet.

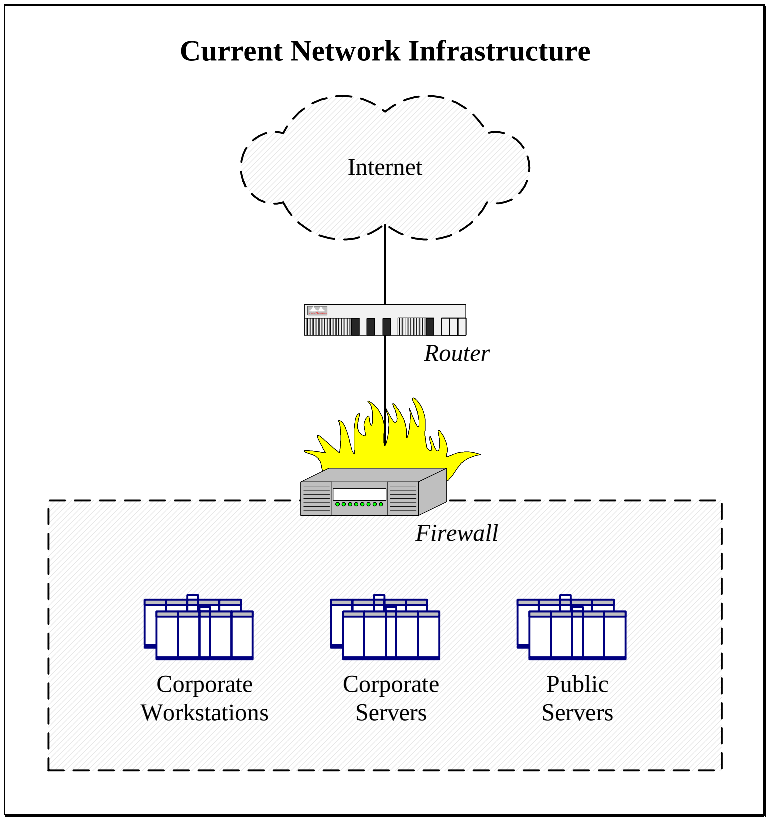

*Figure 2-1*

For the purpose of our assessment, we grouped these resources into systems required for the organization's internal needs: corporate workstations and servers, as well as into publicly accessible servers that provide Domain Name System (DNS), Web, and mail services. Our analysis concentrates on servers accessible from the Internet: these are implemented as two Dell PowerEdge 6450 servers running Red Hat Linux 7.0. DNS services are provided by a system known as *bluewiz*, while Web and mail services are hosted on a single system known as *redrum*, as shown in Figure 2-2 below.

| Server Specifications | Server Functions and Related Notes |
|---|---|
| Name: *bluewiz*<br>OS: Red Hat Linux 7.0<br>IP: 192.168.1.123 | This server provides DNS services to client systems located on the Internet, providing Internet users with information regarding the organization's domain name records. |
| Name: *redrum*<br>OS: Red Hat Linux 7.0<br>IP: 192.168.1.124 | This server provides Web services to Internet users via the HTTP and HTTPS protocols for the purpose of hosting the organization's corporate site. Additionally, the server provides electronic mail services via SMTP and IMAP protocols. |

*Figure 2-2*

## 2.2 OS Vulnerabilities

Both systems that we examined were running custom installations of Red Hat Linux 7.0 as the underlying operating system (OS). A large number of security-related updates to the OS issued by Red Hat were not installed on the organization's servers. Detailed information regarding relevant Red Hat Linux 7.0 security advisories is available at the Red Hat support site.[1] Figure 2-3 below lists applicable advisories that impact the operating environment of the analyzed servers.

| Advisory Identification | Patch Specifications |
|---|---|
| xinetd (RHSA-2001-092) | Vulnerability found in xinetd's string handling could lead to a system compromise. (Note that xinetd is installed on examined systems, but is not running.)<br>http://www.redhat.com/support/errata/RHSA-2001-092.html |
| man (RHSA-2001-069) | A buffer overflow problem in the man package could allow a user to gain privileges assigned to the setgid man command.<br>http://www.redhat.com/support/errata/RHSA-2001-069.html |
| kernel 2.2.19 (RHSA-2001-047) | This update corrects a local denial of service and root-level compromise vulnerability in the kernel.<br>http://www.redhat.com/support/errata/RHSA-2001-047.html |
| openssh (RHSA-2001-041) | This update corrects sshd start-up and PAM issues.<br>http://www.redhat.com/support/errata/RHSA-2001-041.html |
| rpm (RHSA-2001-016) | This update corrects compatibility issues in the rpm package.<br>http://www.redhat.com/support/errata/RHSA-2001-016.html |

| | |
|---|---|
| vixie (RHSA-2001-014) | The new vixie-cron package fixes a buffer overflow vulnerability that could allow users to gain elevated privileges.<br>http://www.redhat.com/support/errata/RHSA-2001-014.html |
| glibc (RHSA-2001-001) | Several bugs in the GNU C library allow unprivileged users to access restricted files and preload libraries into setuid programs.<br>http://www.redhat.com/support/errata/RHSA-2001-001.html |
| slocate (RHSA-2000-128) | This update corrects a problem that could allow users to overwrite slocate's internal structures and obtain access to the entire slocate database, which would allow them to learn locations of files they normally would not be able to locate.<br>http://www.redhat.com/support/errata/RHSA-2000-128.html |
| ed (RHSA-2000-123) | The ed utility uses files in /tmp in an insecure fashion, which could allow users to modify restricted files.<br>http://www.redhat.com/support/errata/RHSA-2000-123.html |
| PAM (RHSA-2000-120) | This update to the PAM package fixes a number of security bugs, including a possible buffer overflow vulnerability.<br>http://www.redhat.com/support/errata/RHSA-2000-120.html |
| gnorpm (RHSA-2000-072) | The gnorpm utility contains a vulnerability that may allow a local user to trick the root user into writing to arbitrary files.<br>http://www.redhat.com/support/errata/RHSA-2000-072.html |
| modutils (RHSA-2000-108) | Vulnerability in the modutils package could allow a local user to obtain root-level access to the system.<br>http://www.redhat.com/support/errata/RHSA-2000-108.html |
| ncurses (RHSA-2000-115) | Local users may exploit a vulnerability in ncurses to gain privileges assigned to a setuid application utilizing ncurses.<br>http://www.redhat.com/support/errata/RHSA-2000-115.html |
| iputils (RHSA-2000-087) | This update fixes a number of security-related problems with the implementation of the ping utility.<br>http://www.redhat.com/support/errata/RHSA-2000-087.html |
| tmpwatch (RHSA-2000-080) | The tmpwatch program has a local denial of service and a root exploit, associated with its use of the fork() system call.<br>http://www.redhat.com/support/errata/RHSA-2000-080.html |

*Figure 2-3*

In Figure 2-3 above we listed only patches to OS components that were installed on the analyzed servers; advisories related to third-party applications are discussed further in the document. Additionally, in Section 4: Recommendations we describe specific procedures for patching up the systems in the most efficient manner.

## 2.3 Third-Party Software

When performing our assessment, we examined third-party software installed on the *bluewiz* and *redrum* servers. Figure 2-4 below lists software components that are required for fulfilling business needs associated with these systems. Our analysis showed that these applications have not been patched to address known vulnerabilities. Critical nature of several discovered vulnerabilities could allow a remote attacker to gain access to internal systems.

| Installed Software | Software Description | Patch Specifications |
|---|---|---|
| Bind 8.2.2 | Provides DNS functionality on the *bluewiz* server. | A number of significant security vulnerabilities have been discovered and fixed since release 8.2.2 of BIND.<br>http://www.isc.org/products/BIND/bind-security.html |
| UW imapd 2000c | Provides mail-related IMAP functionality on the *redrum* server. | Various buffer overflow vulnerabilities were fixed by the latest release of imapd.<br>http://www.redhat.com/support/errata/RHSA-2001-094.html |
| Sendmail 8.11.1 | Provides mail transport functionality on the *redrum* server. | Sendmail may be susceptible to possible race condition, which may elevate privileges of a local *redrum* user.<br>http://www.securityfocus.com/vdb/bottom.html?vid=2794 |
| Procmail 3.1.4 | Assists with mail processing tasks on the *redrum* server. | There is a problem with signal handling in procmail that may allow a local *redrum* user to obtain elevated access on the server.<br>http://www.securityfocus.com/vdb/bottom.html?vid=3071 |
| Apache 1.3.14<br>mod_ssl 2.7.1 | Provides Web functionality via HTTP, and possibly HTTPS later, on the *redrum* server. | A vulnerability in Apache may allow attackers to view directory contents despite the presence of the “index.html” file.<br>http://www.securityfocus.com/vdb/bottom.html?vid=3009 |
| OpenSSL 0.9.5a | Not currently used, but may at some point assist in providing Web functionality via HTTPS on the *redrum* server. | A flaw in the OpenSSL pseudo-random number generator could, theoretically, allow an attacker compromise the integrity of the encrypted data stream.<br>http://www.securityfocus.com/vdb/bottom.html?vid=3004 |

*Figure 2-4*

As mentioned in Figure 2-4 above, the version of UW imapd running on *redrum* server could be exploited by authenticated clients to obtain interactive access to the host. Furthermore, vulnerabilities present in installed versions of sendmail and procmail, when combined with the imapd exploit, could allow an authenticated remote user to obtain root-level access to *redrum* server. Vulnerabilities present in Apache and related SSL libraries on *redrum* are not critical, although they could leak sensitive information to a determined attacker.

We are also concerned that the version of BIND running on the *bluewiz* server is vulnerable to a number of denial of service (DoS) attacks. Additionally, one of the bugs may allow an attacker to obtain privileges of the user *named* that the Web server process is running as; this could be used as a launching pad for further attacking *bluewiz* server as well as other systems behind the corporate firewall. Specifics for BIND bugs are listed at the Internet Software Consortium site.[2] The impact of each relevant BIND vulnerability is presented in Figure 2-5 below.

| Bug Name | Vulnerability Description | Impact on GIAC Enterprises |
|---|---|---|
| zxfr | Remote DoS via a transfer of compressed zone files. | This is not critical, since the DNS server is configured to accept zone transfers only from the ISP’s DNS server. |
| sigdiv0 | Remote DoS via signature verification of signed zone transfers. | This is not critical, since the DNS server is configured to accept zone transfers only from the ISP’s DNS server. |
| srv | Remote DoS due to the handling of the compression pointer table. | This may result in DNS service downtime if exploited by an attacker. |
| nxt | Remote privilege elevation due to unsafe processing of NXT records. | This could allow an attacker to execute arbitrary code with the privileges of user *named* that BIND runs as on *bluewiz*. |
| sig | Remote DoS due to improper handling of SIG records. | This may result in DNS service downtime if exploited by an attacker. |
| naptr | Remote DoS due to improper validation of zone data for the NAPTR record. | This is not critical, since the DNS server is configured to accept zone transfers only from the ISP’s DNS server. |
| maxdname | Remote DoS and possible unexpected behavior via a buffer overflow attack. | This may result in DNS service downtime, and possible privilege elevation if exploited by an attacker. |
| infoleak | Remote information loss via a malicious inverse query. | This may result in the attacker reading environment variables from *bluewiz*. |
| tsig | Remote privilege elevation via a buffer overflow when handling TSIG signed queries. | This could allow an attacker to execute arbitrary code with the privileges of user *named* that BIND runs as on *bluewiz*. |

*Figure 2-5*

## 2.4 Configuration Vulnerabilities

When examining configurations of systems in question, we were pleased to see that packages installed on the servers were primarily limited to applications and utilities that were necessary for the servers to function. A notable exception to this was knfsd and portmap packages, which were installed on both *bluewiz* and *redrum*, but were not running; we suggest removing them since these servers do not need to provide NFS or RPC functionality. We also recommend removing the xinetd package, since none of the xinetd-based services are being used.

Additionally, both servers that we analyzed were running the XFree86 and GNOME packages. The X Window System, in combination with GNOME provides graphical user interface (GUI) for various interactive applications. While GUI utilities often streamline system administration, we suggest considering removing these packages from the systems to minimize the number of applications that could be exploited by a determined attacker. Based on our conversations with the system administration staff at GIAC Enterprises, we believe that they will feel comfortable administering the systems from the command line after an initial learning period.

Both servers also had the Netscape Communicator package installed. There are a number of vulnerabilities associated with browsing the Internet from a critical server. At the same time, the Web browser may be useful for system administrators when viewing HTML-based documentation or accessing Intranet servers. Pending further assessment of the administrators' needs, we suggest not performing any tasks associated with the use of the Web browser from production servers, and removing the Netscape Communicator package from *bluewiz* and *redrum*.

Even though the version of BIND running on the *bluewiz* server was vulnerable to a number of attacks, we were pleased to see that BIND was configured in a manner that minimized impact of a successful compromise. Specifically, the *named* process was running in a properly chroot'ed environment consistent with recommended industry practices.[3] However, a number of files in *named's* "jail" were left world-readable, instead of being accessible only to the *named* user.

BIND configuration properly restricted zone transfers to take place only between *bluewiz* and the organization's ISP; in this configuration, *bluewiz* acts as the maser server, while the ISP's DNS server offers redundancy by acting as a slave server. One option that was notably missing from the server's named.conf file was the *allow-query* tag – we suggest utilizing this command to restrict which clients may query the DNS server for external domain information.

The Apache configuration file */etc/httpd/conf/httpd.conf* on *redrum* server was world-readable. We recommend making this file accessible only to the root user to ensure that configuration specifics of the Web server remain confidential. Additionally, the Apache server is currently configured to allow CGI script execution in any public HTML directory. We suggest removing the globally placed *Options ExecCGI* directive and using the *ScriptAlias* directive to limit which directories can host executable content on the Web server.[4]

## 2.5 Security Patches

As described above, a number of software packages installed on the *bluewiz* and *redrum* servers were not patched against known vulnerabilities. The process of updating these packages can be automated through the use of the Red Hat Update Agent that is already installed on affected systems. Moreover, the Update Agent can be used to determine which of the installed software packages are outdated. For instance, Figure 2-6 below shows an excerpt from the output of the "`up2date --nox --list`" command that we executed on the *redrum* server to list packages that may need to be updated.

**Checking for Patches via the Red Hat Update Agent**

```
# up2date --nox --list

Name                           Version        Rel
-----------------------------------------------------
XFree86-VGA16                  3.3.6          38
gnorpm                         0.95.1         6.7x
libstdc++                      2.96           85
man                            1.5i2          0.7x
mount                          2.10r          5
netscape-common                4.77           1
netscape-communicator          4.77           1
nfs-utils                      0.3.1          7
openssh                        2.5.2p2        1.7.2
openssh-clients                2.5.2p2        1.7.2
openssh-server                 2.5.2p2        1.7.2
openssl                        0.9.6          9
perl                           5.6.0          10a
popt                           1.6.2          7x
procmail                       3.21           0.71
rhn_register                   1.3.2          1
rhn_register-gnome             1.3.2          1
xinetd                         2.3.0          1.71

The following Packages were marked to be skipped by your
configuration:

Name                           Version        Rel  Reason
-------------------------------------------------------------------
kernel                         2.2.19         7.0.8Pkg name/pattern
kernel-doc                     2.2.19         7.0.8Pkg name/pattern
kernel-pcmcia-cs               2.2.19         7.0.8Pkg name/pattern
kernel-source                  2.2.19         7.0.8Pkg name/pattern
kernel-utils                   2.2.19         7.0.8Pkg name/pattern
```

*Figure 2-6*

We do not recommend using the Red Hat Update Agent to update major software packages that are not considered to be a part of the underlying system, specifically Apache, Sendmail, and UW imapd. This is because original distribution sites for these applications often distribute newer versions of the software than what is available from Red Hat. In general, it is a good idea to look for the latest version of the software when deciding whether to obtain the upgrade from Red Hat or from the original site. For instance, the Update Agent would retrieve version 2.5.2p2 of OpenSSH on *redrum*, even though the latest version of OpenSSH as of this writing is 2.9p2.[5]

## 2.6 Administrative Practices

The internal system administration staff at GIAC Enterprises consists of three administrators, one of which specializes in UNIX technologies and is responsible for installing, monitoring, and maintaining UNIX-based services on the corporate network. Given the organization's staff constraints, GIAC Enterprises does not currently provide computing support services for its critical systems on 24-hour basis.

At the time of our analysis, system monitoring was performed manually by the staff, relying primarily on the organization's users to detect and report anomalies. We highly recommend automating monitoring of critical systems, specifically of the *redrum* and *bluewiz* servers. Depending on the budget, GIAC Enterprises can choose from a number of fault monitoring packages, ranging from the freely available Big Brother[6] to the feature-rich BMC Patrol.[7] Alternatively, the organization may consider outsourcing monitoring duties of its critical systems to an external company.

Additionally, we suggest deploying integrity verification software such as Tripwire[8] to ensure integrity of critical files on the *redrum* and *bluewiz* servers. This software operates by comparing snapshots of the system's state to the expected configuration, altering administrators when an unauthorized change is detected. In addition to performing host-level intrusion detection, tools such as Tripwire can be used to maintain a historical log of changes made to the organization's critical servers – this information may prove useful in future internal and external audits as well as during routine system administration duties. It is generally recommended to complement host-based intrusion detection systems (IDS) with network-based intrusion detection systems. Network IDS monitor network communications and alert administrators when suspicious traffic is detected. Additionally, a carefully configured IDS can be used for forensic purposes when responding to an incident, allowing the organization to determine an event's severity and circumstances. Finally, an IDS can help the organization detect attacks during reconnaissance stages, before the attacker attempts to compromise a critical system.

## 2.7 Sensitive Data

GIAC Enterprises uses the *redrum* server for hosting its corporate Web site, which consists of static content and several Perl-based CGI scripts. OpenSSL libraries are currently installed on *redrum* without a valid SSL certificate, and this functionality of the Web server is not currently utilized. CGI scripts are being used to obtain contact information from potential customers and to gather feedback from the site's visitors. (Note that the organization's production systems are hosted at a co-location provider and are not subject to this audit.) This is the only information gathered by the Web server, and GIAC Enterprises does not deem it to be sufficiently sensitive to warrant the use of SSL. While such information does not necessarily require that it be encrypted during transport, we invite GIAC Enterprises to analyze the impact of a data intercept, and weigh it against the cost of setting up and maintaining an SSL certificate for the Web server.

We are concerned that the organization uses clear-text IMAP authentication for its remote mail users. This may result in login credentials intercepted en-route by an attacker, which can lead to a server compromise, especially in the light of other IMAP vulnerabilities discussed earlier. We suggest employing IMAPS functionality that is built into UW imapd, which will allow users to encrypt all IMAP sessions via SSL. [9] For proper installation, this will require obtaining a server-side SSL certificate from a company such as VeriSign. On the client side IMAPS functionality is transparently supported by Outlook, which is being used by GIAC Enterprises.

## 2.8 Virus Protection

GIAC Enterprises employs Norton Anti-Virus software on all its Windows-based workstations. However, our analysis showed that approximately 60% of workstations had virus pattern definitions at least 2 months old. We suggest configuring automatic update functionality, available with Norton Anti-Virus, to ensure that virus definitions remain up to date and provide the expected level of protection. Norton Anti-Virus can be configured to automatically update itself by "pulling" software and virus definition updates from Norton's Web site. Alternatively, organizations can configure the corporate edition of Norton Anti-Virus, which GIAC Enterprises owns, to "push" updates to individual workstations from a central server. The latter is the recommended solution, since it offers the most control over the update distribution process.

Anti-virus software is not installed on the organization's UNIX servers, which is acceptable considering the industry's current practice relating to servers that are used solely by system administration staff. However, we recommend configuring the mail gateway to scan incoming and outbound mail messages for viruses, to ensure that malicious code does not enter or leave the corporate network. Such configuration will provide a level of redundancy, since virus checking will be performed at the network's perimeter, as well as at individual workstations.

## 2.9 Access Restrictions

The *redrum* and *bluewiz* servers are remotely administered through the use of OpenSSH and SFTP. SSH is a good protocol to use for this purpose, since it encrypted all aspects of the administrator's session with the server. The organization uses SecureCRT and SecureFX, a well regarded SSH client produced by Van Dyke Technologies,[10] to connect to servers from Windows workstations. Unfortunately, administrators directly log in as root over the network, instead of connecting to the system using individual accounts and then using the "su" utility to obtain administrative access to the system. Logging in directly as root does not allow the organization to keep an audit track of who logged in to the system, and may allow attackers to brute-force root's login credentials. We recommend that this functionality be disabled on the servers by setting the "`PermitRootLogin`" value to "`no`" in the sshd_config file. OpenSSH can also be compiled with support for TCP Wrappers, which will allow the organization to limit which client systems are able to connect to the SSH server; this functionality is not currently enabled on *redrum* and *bluewiz*. Additionally, we suggest using the "sudo" utility to allow administrators that do not require full root access to execute privileged commands in a controlled manner.

## 2.10 Contingency Practices

Both servers that we examined are backed up to tape by performing daily incremental and weekly full backups; this is achieved using the UNIX "dump" utility. However, we are concerned that GIAC Enterprises does not perform periodic test restores to ensure that the tape unit is operating as expected. We are also concerned that while backup procedures are properly documented, there are no policies for performing system restores. We suggest that the organization draft detailed policies that will outline steps necessary to recover from system failures and other security incidents in a prompt and reliable manner. Additionally, the organization should consider making copies of its full backup tapes to be taken for secure off-site storage. This can be performed every week, or twice a month, to provide the organization with a way to recover from an event such as a regional disaster.

The *redrum* and *bluewiz* servers are not deployed in a cluster configuration, as the organization considers it an unnecessarily expensive solution. This is a reasonable assessment, considering that the decision was reached in a formal manner by analyzing the risk of downtime and the cost of recovery. The servers are currently using single disks for their partitions, and the organization is in the process of purchasing a RAID storage system that will introduce a level of redundancy to the servers' storage subsystem.

## 2.11 Miscellaneous Concerns

We are concerned with the apparent lack of security policies in the organization. Although there exists some documentation elating day-to-day computing operations, we would like to see the organization formalize its procedures in writing. This will ensure that all critical areas of the computing infrastructure are addressed in a thought-out and consistent manner, and will create a baseline against which GIAC Enterprises will be able to compare the state of its security practices through internal and third party audits. Effective security policies should address most issues discussed in this document, and define procedures, roles, and responsibilities of the company's personnel and computing resources. Additionally, we highly recommend documenting configuration parameters of the organization's critical systems – this documentation should be maintained separately from the security policy, and will help ensure that proper information about computing infrastructure is always available to authorized personnel.

# Section 3: Prioritizing Issues

## 3.1 Severity Metrics

When prioritizing our concerns, we looked primarily at the impact that a successful exploitation of the vulnerability or misconfiguration will have on the organization's resources, as shown in Figure 3-1 below. We consulted GIAC Enterprises staff when defining severity metrics, to ensure that our discussion is relevant to the organization's concerns and priorities. Note that criticality of the affected service was not considered in depth, since all services and systems analyzed during our audit were deemed to be critical.

| Concern Severity | Description of Severity Criteria |
|---|---|
| High | May result in a remote or local attacker obtaining root-level access, with or without a shell, to the system. Also includes concerns relating to irrecoverable loss of critical data. |
| Medium | May result in a remote attacker obtaining access to system's resources as a non-privileged user. Also includes denial of service concerns relating to services and resources. |
| Low | May result in a local attacker obtaining non-privileged user access to data and resources that should not be accessible to an external user. Also includes concerns relating to highly improbable events. |

*Figure 3-1*

## 3.2 Lists of Concerns

Here we present prioritized lists of vulnerabilities and concerns that we described in greater detail earlier in the document. Proposed resolutions to these issues are presented in the next section. Figure 3-2 below lists concerns to which we assigned the priority of "high."

| Cause of High Concern | Potential Impact | Target |
|---|---|---|
| Vulnerabilities in installed packages may allow local or remote users to assume root-level privileges. | Full control of a compromised system by a non-privileged local or remote user. | Packages on *bluewiz* and *redrum*: tmpwatch, ncurses, modutils, gnorpm, glibc, vixie, kernel 2.2.19, ed, PAM, iputils. |
| A combination of bugs in UW imapd may allow authenticated remote users to obtain root-level access. | Full control of a compromised system by a non-privileged but authenticated user internal to the organization. | The UW imapd package on *redrum*. |

| | | |
|---|---|---|
| Outdated virus definitions on internal workstations. | May result in a remote attacker gaining access to internal systems via a malicious agent. | All systems on the corporate network. |
| Administrators do not perform test restores. | Unnoticed faults in the backup mechanism may lead to lack of data backup. | The *bluewiz* and *redrum* servers. |

*Figure 3-2*

Figure 3-3 below presents concerns to which we assigned the priority of "medium."

| **Cause of Medium Concern** | **Potential Impact** | **Target** |
|---|---|---|
| Vulnerabilities in installed packages may allow local users to assume elevated, but not root-level privileges. | Limited control of a compromised system by a non-privileged local or remote user. | Package on *bluewiz* and *redrum*: man, slocate, rpm, procmail 3.1.4, sendmail 8.11.1 |
| IMAP users use clear text authentication mechanisms. | Interception of valid user's login credentials, which may lead to a system compromise when combined with existing vulnerabilities in UW imapd. | The UW imapd package on *redrum*. |
| The "nxt" and "tsig" bugs in BIND could allow a remote user to execute code as user named. | Partial control of a local system by a remote user, which may lead to full control via exploitation of local vulnerabilities. | The BIND package on *bluewiz*. |
| Both public and internal systems are hosted on the same network segment. | Compromise of a publicly accessible server is likely to expose internal systems located on the same subnet. | All systems on the corporate network. |
| The "srv", "sig", "maxdname", and "infoleak" bugs in BIND might cause remote denial of service or information loss. | Downtime of the DNS service and possible loss of confidential information. | The BIND package on *bluewiz*. |
| Fault monitoring is performed manually and does not cover all critical resources. | Late discovery of a system compromise. | All systems on the corporate network. |
| Lack of host and network-based intrusion detection systems prevents proper monitoring. | Late discovery of a system compromise. | All systems on the corporate network. |

| | | |
|---|---|---|
| Administrators login to servers directly as “root” over the network. | Lack of audit trail in case of an incident, potential brute-force compromise of root’s login credentials. | The *bluewiz* and *redrum* servers. |
| Servers do not use RAID disks. | Prolonged downtime in case of a disk failure. | The *bluewiz* and *redrum* servers. |
| Misconfigurations in Apache are inconsistent with recommended guidelines | Potential loss of confidential data or service associated with HTTP, potential execution of restricted commands. | The HTTP service on *redrum*. |
| Lack of documented security policies and procedures. | Inconsistent service configurations, ineffective incident response, lack of auditable baseline. | All systems on the corporate network. |

*Figure 3-3*

Finally, Figure 3-4 below presents concerns to which we assigned the priority of “low.”

| **Cause of Low Concern** | **Potential Impact** | **Target** |
|---|---|---|
| Systems contain packages or features that are not necessary or that are not being used. | Potential elevated access by a non-privileged user. | Packages on *bluewiz* and *redrum*: xinetd, openssh, knfsd, portmap, XFree86, GNOME, Netscape Communicator. |
| The “zxfr”, “sigdiv0”, and “infoleak” bugs in BIND might result in an unlikely DoS attack. | Possible, but unlikely, downtime of the DNS service. | The BIND package on *bluewiz*. |
| Installed OpenSSL libraries may be vulnerable once SSL functionality is enabled. | Potential compromise to integrity of SSL-encrypted data. | The HTTPS and IMAPS services on *redrum*, once they are being used. |
| A vulnerability in Apache exposes directory contents. | A remote user may be able to view directory contents despite presence of the “index.html” file. | The HTTP service on *redrum*. |
| Misconfigurations in BIND are inconsistent with recommended guidelines | Potential loss of confidential data or service associated with DNS. | The BIND package on *bluewiz*. |
| Copies of backup tapes are not stored off-site | Lack of backup in case of a local or regional disaster. | The *bluewiz* and *redrum* servers. |

*Figure 3-4*

# Section 4: Recommendations

## 4.1 Risk Mitigation Strategy

In the previous section we outlined priorities for our concerns relating to information security of the organization's *redrum* and *bluewiz* servers. When deciding which of those concerns to address first, GIAC Enterprises should take into account the severity value we assigned to the issue, and weigh the cost of mitigating the issue against the value of the targeted resource. This section proposes an action plan for mitigating discovered risks that is based on our perception of resources' value, while taking into account the approximate cost of implementing our recommendations. As a general rule, we placed the most importance on mitigating concerns marked as "high", with the assumption that the organization may be willing to rapidly implement these recommendations at the cost of possibly delaying the mitigation of issues of "low" priority. (Budget constraints were articulated to us in the beginning of the project, and have been guiding our efforts throughout this engagement.)

## 4.2 Proposed Action Plan

Figure 4-1 below outlines the proposed action plan for addressing our concerns described earlier in the document. We listed suggested actions in the order of importance that we assigned to them, starting with the most important action. We also included the estimated cost of performing suggested action; however, our calculations do not include the cost of maintenance that might be associated with some of the items.

| Recommended Action | Estimated Cost Calculations | Estimated Cost |
|---|---|---|
| Update packages on *redrum* and *bluewiz* servers to patch high, medium, and hopefully low vulnerabilities. | Locate and research patches: 4hr x $125/hr = $500<br>Verify patch compatibility: 4hr x $125/hr = $500<br>Install patches: 4hr x $125/hr = $500<br>Test system stability: 2hr x $125/hr = $250 | $1,750 |
| Disable direct logins as "root". | User account creation: 1hr x $125 = $125<br>SSH server configuration and testing: 1hr x $125 = $125 | $250 |
| Deploy centralized anti-virus software update mechanism and update virus definitions on internal workstations. | Install and test software: 8hr x $125/hr = $1,000<br>Install updates on workstations: 1hr x $125/hr = $125 | $1,125 |
| Define and perform backup test restore procedures. | Defining procedures: 2hr x $125 = $500<br>Verify procedures: 2hr x $125 = $500 | $1,000 |

| | | |
|---|---|---|
| Employ SSL-protected IMAP functionality on *redrum*. | Cost of Thawte 128-bit SSL cert for 1 year[11] = $125<br>Obtain and install SSL certificate: 3hr x $125 = $375<br>Enable and test SSL with WU imapd: 2hr x $125 = $375<br>Reconfigure user workstations: 4hr x $125 = $500 | $1,375 |
| Fine tune Apache and BIND configurations. | Perform additional research: 1hr x $125 = $125<br>Implement changes: 1hr x $125 = $125<br>Test configuration: 2hr x $125 = $250 | $500 |
| Install and configure Big Brother system monitoring software on *redrum* and *bluewiz*. | Install and test software on a lab: $4hr x $125 = $375<br>Install software in production: 3hr x $125 = $375<br>Configure and test setup: 4hr x $125 = $500<br>Fine tune alert thresholds: 3hr x $125 = $375 | $1,625 |
| Move publicly accessible servers (*redrum* and *bluewiz*) to a dedicated screened subnet. | Reconfigure PIX for new subnet: 2hr x $125 = $250<br>Install switch for new subnet: 0.5hr x $125 = $63<br>Move servers to new subnet: 1hr x $125 = $125<br>Configure and verify NAT on PIX: 1hr x $125 = $125<br>Reconfigure and verify PIX rule set: 1hr x $125 = $125<br>Test final configuration: 1hr x $125 = $125 | $813 |
| Install Tripwire on *redrum* and *bluewiz*. | Cost of Tripwire: Contact vendor for price quote<br>Install software: 2hr x $125 = $250<br>Configure software: 8hr x $125 = $1,000<br>Test configuration: 2hr x $125 = $250<br>Fine tune alert thresholds: 2hr x $125 = $250 | $1,750+ |
| Initiate a project to create documentation, policies, and procedures relating to security of critical systems. | This is a significant undertaking, requiring careful planning and well-defined goals and deliverables. | N/A |
| Remove unused packages that are unnecessary. | Investigate ramifications of removal: 3hr x $125 = $375<br>Remove unnecessary packages: 2hr x $125 = $250<br>Test configuration: 2hr x $125 = $250 | $875 |
| Maintain copies of backup tapes off-site. | This requires purchasing additional tapes and possibly tape copying equipment. There are services that will maintain tapes off-site in a highly secure manner. | N/A |
| Consider installing network IDS | Cost includes hardware, software (could be free Snort), configuration, testing, fine tuning, monitoring. | N/A |
| Continue the process of obtaining RAID for servers. | Already in progress and paid for. | N/A |

*Figure 4-1*

# Section 5: References

[1] Red Hat. “Red Hat Linux 7.0 Security Advisories.” URL: http://rhn.redhat.com/errata/rh7-errata-security.html (January 2005).

[2] Internet Software Consortium. “BIND Vulnerabilities.” URL: http://www.isc.org/index.pl?/sw/bind/bind-security.php (January 2005).

[3] Holt Sorensen. “Secure Installation of BIND.” 8 February 2001. URL: http://www.securityfocus.com/infocus/1361 (January 2005).

[4] Apache HTTP Server. “Module mod_cgi.” URL: http://httpd.apache.org/docs/mod/mod_cgi.html (January 2005).

[5] OpenSSH. “OpenSSH Homepage.” URL: http://www.openssh.com (January 2005).

[6] Big Brother System and Network Monitor. URL: http://www.bb4.org (January 2005).

[7] BMC Software. URL: http://www.bmc.com (January 2005).

[8] Tripwire Homepage. URL: http://www.tripwire.com (January 2005).

[9] UW IMAP Server Documentation. “SSL Build and Installation Notes for UNIX.” URL: http://www.washington.edu/imap/documentation/SSLBUILD.html (January 2005).

[10] Van Dyke Technologies, Inc. URL: http://www.vandyke.com (January 2005).

[11] Thawte. “Digital Certificate Centre.” URL: http://www.thawte.com/pricing (January 2005).