# Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

CONFIDENTIAL
FOR GIAC ENTERPRISES EYES ONLY

# GIAC Enterprises
# Strategic Security Audits (SSA)

**Name: Rhett Saunders**
**Title: Security Officer**
**Company: Strategic Security Audits (SSA)**
**Version: 1.6d**
**Date: July 5, 2001**


© SANS Institute 2000 - 2005, Author retains full rights.

CONFIDENTIAL
FOR GIAC ENTERPRISES EYES ONLY

© SANS Institute 2000 - 2005 Author retains full rights.

CONFIDENTIAL
FOR GIAC ENTERPRISES EYES ONLY

© SANS Institute 2000 - 2005, Author retains full rights.

CONFIDENTIAL
FOR GIAC ENTERPRISES EYES ONLY

© SANS Institute 2000 - 2005 Author retains full rights.

# Table of Contents

**I. Executive Summary** 1

**II. Detailed Findings** 2

A. Operating System Vulnerabilities 2
B. Configuration Vulnerabilities 5
C. Risk Assessment of Installed Third Party Software 7
D. Administrative Practices 8
E. Security Patches 9
F. Sensitive Data 9
G. Internet Connectivity 9
H. Access Restrictions 10
I. Back-Up and Recovery Procedures 11
J. Other Issues/Vulnerabilities 11

**III. Prioritized Security Vulnerabilities** 11

**IV. Endnotes** 15

© SANS Institute 2000 - 2005 Author retains full rights.



© SANS Institute 2000 - 2005 Author retains full rights.

## I. Executive Summary

Introduction

GIAC Enterprises, a new Internet startup company based in San Diego, California, whose primary mission is to sell online fortune cookies, has hired Strategic Security Audits (SSA) to perform an audit of their network infrastructure with emphasis on their production database server. GIAC's need for a security audit is long overdue after the recent fallout of their IT personnel and the lack of a security officer. SSA's team of security professionals, lead by Rhett Saunders, will perform an audit of the database server, known as Topcat, as well as any other outside variables that may affect Topcat.

At the time GIAC Enterprises was commissioned in April 2001, the original system and network administrator teams each were respectively responsible for the security and well-being of the machines. Recently this team had been replaced by contractors due to a middle-management cut. The new team now in place is staffed by contractors; although still at minimum manning, their primary focus, in addition to their mission statement, is security.

Although the overall security level of GIAC Enterprises is medium, all data will be considered and safeguarded at a high security level due to their intellectual property and other rights. This report and all information herein is classified Confidential For GIAC Enterprises Eyes Only.

Purpose of the Study

The study is recommended by their internal auditors and is described in the RFP. GIAC's internal auditors believe that the current RFP is too broad and requires a more specific and revised plan for security. Since GIAC outsourced SSA for the security audit, a more specific and revised report is requested.

Findings

The goals and objectives for the security audit will be revised and respond to the original Request for Proposal as follows:

- Identify the operating system, configuration and any other vulnerabilities;
- Identify the risks from third-party software installed on the database server;
- Analyze the existing administrative practices and provide feedback;
- Ensure that all systems possess the most current security patches;
- Ensure that all sensitive data is encrypted from the intranet to the internet;
- Review and suggest how access should be restricted on a need-to-know basis;
- Provide feedback on the current disaster and contingency plan;



© SANS Institute 2000 - 2005 Author retains full rights.

- Provide a prioritized list of security vulnerabilities and estimates to correcting the issues.

© SANS Institute 2000 - 2005, Author retains full rights.


© SANS Institute 2000 - 2005 Author retains full rights.

## II. Detailed Findings

This portion of the report will outline in detail the vulnerabilities and issues regarding the system known as Topcat. Topcat is a Sun Enterprise 3500 with four 450 MHz Ultra III processors, four Gbytes of memory, 50 Gbytes of hard disk space, three interfaces (one for fail-over), and four Differential SCSI slots running Solaris 2.7.

The Topcat server is the most critical system in the network and has several vulnerabilities and issues surrounding it. For one thing, the security policy is not updated and makes reference to Solaris 2.4. Additionally, the older server on which the database used to reside, is a SPARC 1000, a model for which all support is now discontinued by Sun Microsystems.

This machine is configured in compliance with the Capability Maturity Model (CMM) Level-2 environment. During the audit there was evidence that the bundles shipped over to the machine via configuration management were modified after the bundling process. The policies need to be updated so as to not allow system administrators to modify, create, or delete any portion of the machine that is configured. In general, all policies need to be updated for superusers. This location has 10 different users with root password. This situation can have devastating results when many superusers are logged on at the same time and making changes to the system.

Other issues that pose commonly-overlooked risks are the running of unnecessary services; poorly documented administrative policies; lack of a regular plan to patch the system; the use of a plaintext protocol such as telnet for sending data; and a contingency plan that has never been drilled in its entirety.

### A. Operating System Vulnerabilities

The following information will provide the path of least resistance that the SSA team used to find the exploits against the multiple operating system environment (Solaris 2.5 through 2.7). This access was given after our request for a normal user account be set up on the development server (Garfield – Running Solaris 2.5).

Known Exploits

There were many exploits that could have been used to achieve a compromise of the database server. Three of those were at the top of the list noted from CERT and Security-express.com. These vulnerabilities are:

**CERT® Advisory CA-2001-05 Exploitation of snmpXdmid**

Problem Overview:



© SANS Institute 2000 - 2005 Author retains full rights.

This vulnerability allows an intruder to gain privileged (root) access to the system.

Solution:

For sites not needing this service, the solution is to turn off the service with the following command line procedures:

Disable snmpXdmi
Until patches are available, sites that do not use both SNMP and DMI are strongly encouraged to disable snmpXdmid.

One way to accomplish this is to issue the following commands (as root):
Prevent the daemon from starting up upon reboot.

```
# mv /etc/rc3.d/SXXdmi /etc/rc3.d/KXXdmi
```

Killing the currently running daemon

```
# /etc/init.d/init.dmi stop
```

Verify that the daemon is no longer active.

```
# ps -ef | grep dmi
```

As an additional measure, you may wish to make the daemon non-executable.

```
# chmod 000 /usr/lib/dmi/snmpXdmid
```

Restrict access to snmpXdmi and other RPC services
For sites that require the functionality of snmpXdmi or other RPC services, local IP filtering rules that prevent hosts other than localhost from connecting to the daemon may mitigate the risks associated with running the daemon. Sun RPC services are advertised on port 111/{tcp,udp}. The snmpXdmid RPC service id is 100249; use 'rpcinfo -p' to list local site port bindings:

```
# rpcinfo -p | grep 100249
  100249 1 udp 32785
  100249 1 tcp 32786
```

Note that site-specific port binding will vary.



© SANS Institute 2000 - 2005 Author retains full rights.

For sites that do use DMI (dmispd) and the mapper (snmpXdmid), there are no workarounds

**CERT® Advisory CA-1998-02 Vulnerabilities in CDE**

Problem Overview:

Local users are able to gain write access to arbitrary files. This can be leveraged to gain privileged access.

Local users may also be able to remove files from arbitrary directories, thus causing a denial of service.

Solution:

Sun has a patch for this vulnerability known as the "dtappgather exploit".

Sun Microsystems, Inc.

Sun has released the following patches:

| Patch ID | CDE Version |
|---|---|
| 105837-01 | 1.2 |
| 105838-01 | 1.2_x86 |
| 104498-02 | 1.02 |
| 104500-02 | 1.02_x86 |
| 104497-02 | 1.01 |
| 104499-02 | 1.01_x86 |

To get the patches, go to Sun solve online[2]

**Buffer Overflow with UFSDUMP/UFSRESTORE**

Problem Overview:

This exploit is for any Sun system running an original OEM version of Solaris 2.5. It is possible to create a buffer overflow with UFSDUMP and UFSRESTORE.

Solution

List of Patches

The following patches are available in relation to the above problem.



© SANS Institute 2000 - 2005 Author retains full rights.

| SunOS | Patch ID |
|---|---|
| SunOS 5.5.1 | 104490-05 |
| SunOS 5.5.1_x86 | 104491-04 |
| SunOS 5.5 | 103261-06 |
| SunOS 5.5_x86 | 103262-06 |

To get the patches, go to Sun solve online[3]

These are known exploits that have been circulated among SecurityFocus.com, CERT Advisories, BugTraqs.com, and the rest of the hacker world for the past few years.

During the rules of engagement, GIAC explained that the production servers be protected at all costs during this audit. The use of the above exploits were only to be the path of least resistance into the network, without disturbing any production systems.

Although the webserver (Jaguar) is running Solaris 2.5, it is highly suggested that this server be upgraded as soon as possible to the most current stable operating system available from Sun Microsystems. The best advice here is that your network is only as secure as your most vulnerable system.

**B. Configuration Vulnerabilities**

This section will describe those vulnerabilities that the OEM version of the operating system creates right from the start. It is imperative that the system be configured properly from the first install of the operating system to insure the highest of security for the system. Once a system has become production before these configurations are made usually by then it's too late to make these changes later. One rule of thumb when installing the operating system is to install a "low fat" core installation on any machine, regardless of it's purpose. You can later add any support you need by way of "piecemeal-ing" those services and/or software installs you need later.

Commonly Trojaned programs/services are discussed below. These include features such as telnet, in.telnetd, login, su, ftp, ls, ps, netstat, ifconfig, find, du, df, and the list goes on. One file that is a prime target is the `/etc/inetd.conf` file.

Below is an explanation of findings using services already installed on the machine to figure out the topography of the network.



© SANS Institute 2000 - 2005 Author retains full rights.

Services Running on the Database Server

As a normal user we could easily telnet, ftp, rsh, and rlogin onto Topcat from the development server. The auditor (with user privileges) found that the NFS mount for `/home` was shared to all the systems. Thus the auditor created a .rlogin file and generated a lists of hosts on the system from a world readable `/etc/hosts` file. Once on Topcat the auditor tried a view command on `/etc/inetd.conf` and found that this was again, world readable.

Here is a list of services running on Topcat:

```
ftp stream tcp nowait root /usr/local/sec/tcpdin.ftpd
telnet stream tcp nowait root /usr/local/sec/tcpd in.telnetd
```

File Transfer Protocol (FTP)[4] -- as far as Washington University is concerned -- has proven to be an extremely useful tool and an extreme vulnerability if not configured properly. After a successful FTP connection from Garfield to Topcat, we tried several exploits to gain control of `/etc/passwd` and `/etc/shadow` on the system. Proving to be successful it was obvious that this protocol was not setup in a `chroot`'ed environment. Another approach is install OpenSSH (http://www.openssh.org) Version 2.9 since it has a version of FTP called sFTP (Secure FTP). This is an alternative to using Washington University's tool.

Telnet is another great tool that helps administrators and users to work remotely. It also helps out hackers very well too. Telnet broadcasts all kinds of information as plaintext. This makes it easy for a hacker to use a tool such as SNOOP to view passwords, commands, and any information passed along this service. Turn off immediately and replace with OpenSSH 2.9.

```
shell stream tcp nowait root /usr/local/sec/tcpd in.rshd
login stream tcp nowait root /usr/local/sec/tcpd     in.rlogind
exec stream tcp nowait root /usr/local/sec/tcpd in.rexecd
comsat dgram udp wait root /usr/local/sec/tcpd in.comsat
talk dgram udp wait root /usr/local/sec/tcpd in.talkd
```

All of the above services including FTP and Telnet are wrapped by way of TCP-WRAPPERS. This is a proper configuration for such services. However, it's strongly encouraged to TCP-WRAP a version of SSH (Version 2.9 and above) and remove the above services from the system, as well as from the `/etc/inetd.conf` file.

```
tftp dgram udp wait root /usr/local/sec/tcpd in.tftpd -s
/tftpboot
```

Trivial File Transfer Protocol (TFTP)[5] uses the User Datagram Protocol (UDP)



© SANS Institute 2000 - 2005 Author retains full rights.

and provides no security features. It is often used by servers to boot diskless workstations, X-terminals, and routers. This feature can most definitely be turned off its not going to be used to boot another system.

```
finger stream tcp nowait nobody /usr/sbin/in.fingerd in.fingerd
systat stream tcp nowait root /usr/bin/ps ps -ef
netstat stream tcp nowait root /usr/bin/netstat netstat -f inet
```

The above services can definately be removed from the system, since there is not reason to continue to run these services for potential "system crackers". This does not turn the binary functionality of these services off when using them at the command line.

```
walld/1 tli rpc/datagram_v wait root
/usr/lib/netsvc/rwall/rpc.rwalld rpc.rwalld
```

The wall daemon can be used for denial of service, social engineering attacks, or to execute remote commands. So remove this service as well.
http://cve.mitre.org/board/archives/1999-07/msg00096.html

```
printer stream tcp nowait root /usr/lib/print/in.lpd in.lpd
```

The Solaris 2.6 lpd exploit allows one to create or destroy files and filesystems just by using the innocent printer daemon lpd. Unless your system is a print server, turn this off or patch the lp daemon with the most current recommended patch from Sun Microsystems.

```
http://www.cosc.brocku.ca/~cspress/HelloWorld/1999/02-feb/secur
ity.html
```

```
xaudio stream tcp wait root /usr/openwin/bin/Xaserver Xaserver -
noauth -inetd
```

Unless audio is required on this server, it is recommended to turn this service off.

```
bootps dgram udp wait root /usr/sbin/bootpd bootpd
```

Bootp and bootps are used for boot parameter service. Shut these down if you're not making use of bootp.

```
pop3 stream tcp nowait root
/usr/local/sec/tcpd/opt/gnu/bin/popper -s
```

Unless this system is used to check mail via QPOPPER http://www.eudora.com/qpopper/ there is no reason to have pop3 running as a service. It is highly recommended to turn this service off.



© SANS Institute 2000 - 2005 Author retains full rights.

### C. Risk Assessment of Installed Third Party Software

The risks and factors of installing third party software can introduce countless vulnerabilities to a system. Below are a few third party software bundles that created noticable security holes.

1. Tripwire Version 2.2.1

   This a great tool to do a checksum of all file locations and for monitoring any modifications to any directory location you choose, namely system files. In the wrong hands Tripwire can be "trojan'ed" by a system cracker and report bogus information regarding the status of system files. On Topcat, it was noted that in the usual location of Tripwire `/opt/TSS` (which can be changed during the installation of tripwire to give a system cracker a harder time detecting the use of Tripwire), that the Tripwire database was located on the hard disk under `/opt/TSS/db/Topcat.twd`.

   The main issue is that it's located on the hard disk. A possible solution is to burn this database to a CD-ROM, insuring that the CD is not kept in a writable CD-Burner. The vulnerability created here without a CD-ROM version of the Tripwire database is: your erroneous Tripwire report of system files can lead to an undetected compromised system.

2. OpenSSH Version 1.5

   The buffer-overflow in version 1 of SSHD can be exploited to gain root privileges. This vulnerability is present in most SSHD implementations including: SSH2 2.x with SSH1 fallback support, SSH1 1.2.x versions newer than 1.2.24, F-Secure SSH 1.3.x, OpenSSH prior to 2.3.0 (with version 1 support enabled), OSSH 1.5.7, and others that are derived from SSH1 or OpenSSH. Versions that are not vulnerable include OpenSSH 2.3.0, Cisco SSH, and LSH. It is highly recommended to upgrade to the most current stable version of OpenSSH 2.9.[6]

3. Apache Version 1.2

   Apache was found under `/opt/apache` on the database server. It was bundled to Topcat during the CMM-Level 2 process of configuring the machine. Since this process can become mundane to the configuration manager, extra precaution should be taken when sending all bundles to a server that does not require web access, nor web server software.

   In any event, this version of Apache may display a directory listing when it



© SANS Institute 2000 - 2005 Author retains full rights.

should display an error message. It has been reported that all versions of Apache prior to 1.3.19 are affected.[7]

## D. Administrative Practices

With a little social engineering, administrative practices can lead to a safe and secure environment with little worries. Unfortunately all systems are prone to a lot or little threat depending on how integrated with the internet they are. A system on the internet should be regarded as a system in a hostile environment. There are numerous tools available to the system administrator and sometimes it can be overwhelming at times, depending on the resource allocation for security and reviewing reports.

### 1. Daily Reports

Management explained that GIAC Enterprises employees are overworked and will need more help before reviewing any of the following reports:

- COPS
- Tripwire Version 2.2.1
- Crack
- Backup Reports
- Lastlogin Reports
- Network
- Returned Mail Notices
- UUCP Reports
- Log Checker
- Attempted Access Report (Source: TCP WRAPPERS)

Recommended Strategies:

- Appoint an existing employee to be the local security officer;
- Create, contract, or outsource a position for a local security officer;
- Divide the tasks and reports up with the current employees;
- Start reviewing this reports as soon as possible.

### 2. Training the Force

A security awareness program has not been implemented for GIAC Enterprises that ensures all employees are given periodic refresher training in security concepts, techniques, best practices etc. In the absence of a formal ongoing security awareness program, individuals may not



© SANS Institute 2000 - 2005 Author retains full rights.

understand management's security objectives and intent.

### E. Security Patches

Currently there is no policy for updating security patches system-wide. An easy solution is to download the recommended security patches directly from Sun's website at:

http://sunsolve.sun.com/pub-cgi/show.pl?target=home

The Sun Security Coordination Team investigates reports of security vulnerabilities, responds to customer inquiries about security problems with Sun software, and publishes Sun Security Bulletins.

Security Bulletin Subscription

To receive security bulletins directly from the Sun Security Coordination Team, send an email to security-alert@sun.com and include subscribe cws *[your email address]* in the **subject**. For example: *subscribe cws alex.smith@sun.com*

Contact Sun Security Coordination Team

Send an email to security-alert@sun.com. Please encrypt sensitive mail using the Sun Security Coordination Team's PGP key.

Security Resources

- FIRST (Forum of Incident Response and Security Teams)
- CERT Coordination Center [8]

### F. Sensitive Data

Some information gathered from analyses performed on the database server provides GIAC Enterprises with the up-to-date fortune cookie sayings. The sensitivity of most GIAC Enterprises data is not high in relation to U.S. Government data, but the well-being of GIAC Enterprises and all copyrighted data is sensitive for the period of time prior to public disclosure.

Since this information is located on the database server (Topcat), it's imperative that all R-Services and plaintext protocols such as rsh, rlogin, ftp, telnet, and rcp be turned off immediately and a current stable version of OpenSSH be installed as soon as possible.



© SANS Institute 2000 - 2005 Author retains full rights.

### G. Internet Connectivity

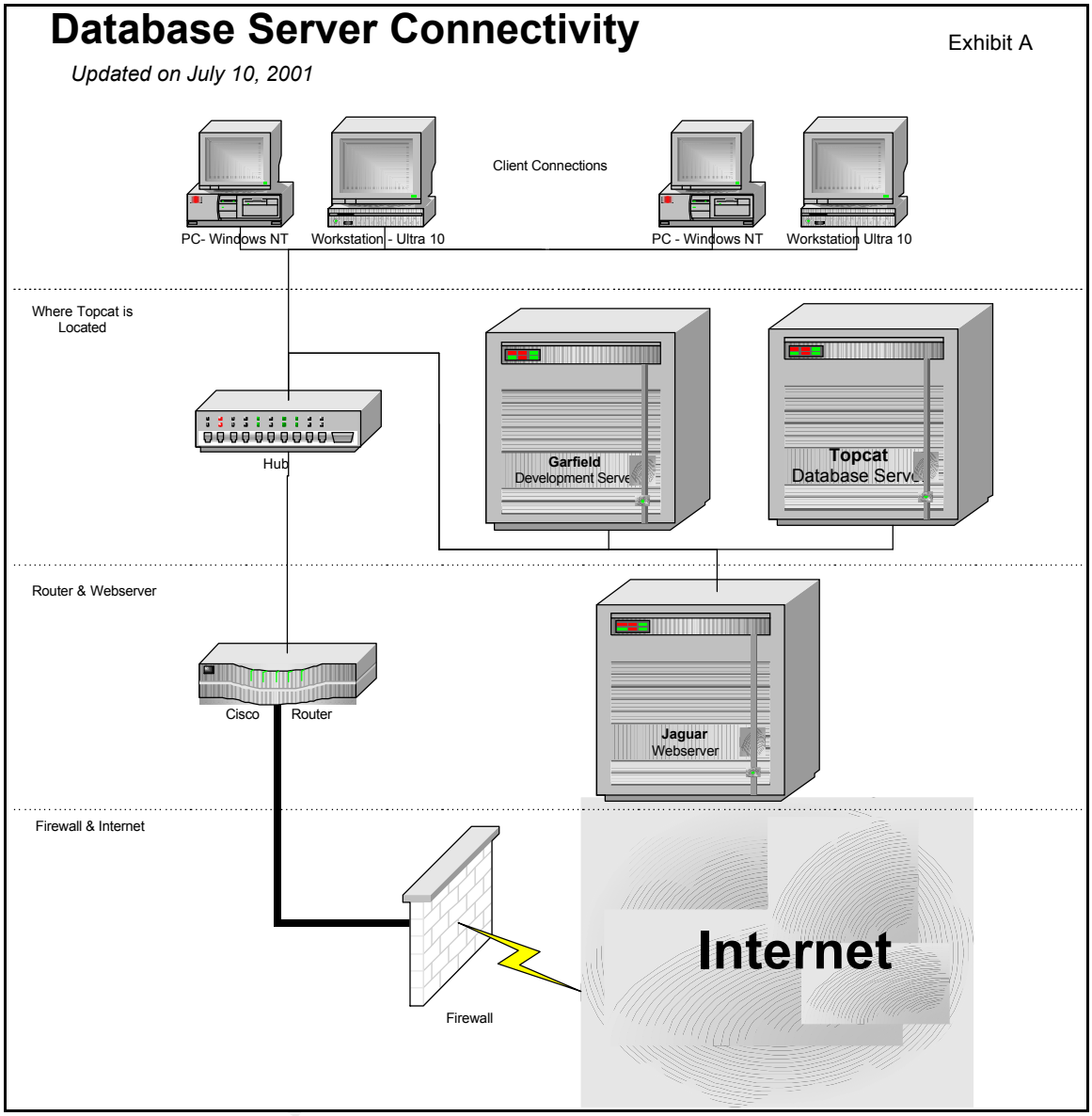
The GIAC Enterprises Unix system does have a connection to the Internet through a crypto-room. At the present time, restriction to the network is controlled by crypto-room. Access to the Unix systems is controlled by host based and user-based authentication, and is limited to a small subset of the services provided by the Solaris platform. Only e-mail connections from the Internet were permitted.

### Exhibit A: Database Server Connectivity

© SANS Institute 2000 - 2005, Author retains full rights.



© SANS Institute 2000 - 2005 Author retains full rights.




## H. Access Restrictions

Our previous audit noted that security related personnel policies and procedures could be strengthened for GIAC Enterprises. Personnel policies and procedures do not adequately encompass the identification of individuals requiring background checks and re-investigations, the use and maintenance of confidentiality agreements for employees and the contractors, the use of current job descriptions that include security responsibilities, and an employee training and professional development program.

1. Root Password

Currently root password is shared among 10 different system, webserver,



© SANS Institute 2000 - 2005 Author retains full rights.

database and network administrators. This is unsatisfactory because there is no formal paperwork or instructions that explain the accountibility and responsibility one has when possessing these passwords. Another problem with this setup is that having superuser privileges implies that conflict may occur if there is more than one superuser logged in at a time. On a need to know basis, a system administrator does not need to keep up with the web server administrator, and the database administrator does not need to keep up with the system administration and so forth.

Recommended Strategies:

- Limit who has root password on what system;
- Construct a formal standard operating procedure to who has what power on each of the systems;
- Create formal paperwork which outlines those powers one has with root or any other superuser access;
- Use sudo or a wheel account to restrict access and certain functions that users can perform without the need for superuser passwords.

2. Badges

Currently there are badges used to control a magnetically locked door. Although during the auditor's visit, the cleaning person, electrician, and a few unidentified people to the GIAC Enterprises secured area were permitted inside without any sanitation of systems, badge, or sign-in.

## I. Back-Up and Recovery Procedures

Controls surrounding the storage of backup tapes for GIAC Enterprises could be improved. Specifically:

- Policies and procedures for the safeguarding, monitoring, and maintenance of backup tapes do not exist.
- GIAC Enterprises does not maintain inventory records of magnetic tapes stored off-site.
- Backup tapes (stored in containers) and the keys to the containers are not adequately secured prior to being picked up by the off-site storage vendor.
- Annual and quarterly backup tapes are not rotated off-site.

Implementation of Disaster Recovery Plan - A copy of the GIAC Enterprises Disaster Recovery Plan is not stored at the off-site facility. The inability to recover/locate a plan in the event of a declared emergency increases the risk the



© SANS Institute 2000 - 2005 Author retains full rights.

objectives of the plan may not be achieved.

The GIAC Enterprises current Disaster Recovery Plan has only been drilled on a piecemeal basis. However, GIAC Enterprises has yet to test the contingency plan in its entirety.

### J. Other Issues/Vulnerabilities

GIAC Enterprises has a website which includes information about all personnel and systems. This information is available to anyone who wants to gain access to their systems. This website needs to be sanitized from all system names, and names of personnel, as well as removing the downloadable picture of the network topography.

## III. Prioritized Security Vulnerabilities

The matrix presented below will describe the findings/conditions with its respective recommended action and time frame to respond.

| Finding/Condition | Recommended Corrective Action | Time Frame |
|---|---|---|
| GIAC Enterprises has not adopted a formal security awareness training program. In addition, security awareness training is not a requirement for the GIAC Enterprises staff. This information was not specifically addressed by the GIAC Enterprises Security Plan. | GIAC Enterprises management should implement a mandatory, biannual security awareness training session for its employees. In addition, GIAC Enterprises should record these large training sessions and offer it to those staff unable to attend the course in person. | FY 2002 |
| GIAC Enterprises has tested its Disaster Recovery and Contingency plan on a piecemeal basis. Portions of the contingency plan have been tested as minor failures occur; however, GIAC Enterprises has yet to test the contingency plan in its entirety. | GIAC Enterprises should test the Disaster Recovery and Contingency plan in its entirety. The testing should be done on an annual basis or whenever significant changes are made to the IT architecture plan or when key personnel changes. In addition, the Disaster Recovery and Contingency Plan should be updated to reflect such changes. | FY2002 |


© SANS Institute 2000 - 2005 Author retains full rights.

| | | |
|---|---|---|
| GIAC Enterprises does not have documented Rules of Behavior to govern staff use of the computer system. This information was not specifically addressed by the GIAC Enterprises Security Plan. | 1. Require all employees and contractors to review these Rules of Behavior and sign an agreement stating that they will act according to these Rules of Behavior to grant user access.<br><br>2. Conduct a yearly review of the Rules of Behavior ensuring that it reflects GIAC Enterprises's current environment. | August 2001 |
| GIAC Enterprises needs to enforce their security policy and federal guidelines on password management. Testing revealed:<br><br>Most passwords were guessed which assumes that the system administrator is not checking a form of Crack Report.<br><br>No passwords assigned to some accounts.<br><br>No password aging and expiration for any account. | 1. At a minimum, a process could be established to periodically run a password-cracking program to identify and change all easy-to-guess passwords. Security software could be used to enforce the use of strong passwords.<br><br>2. Passwords should immediately be assigned to accounts that currently have no passwords associated with them. If no user is associated with the account, the user id should be locked or removed from the local password file.<br><br>3. Password aging and expiration should be set in accordance with OWS security policy or federal guidelines. | August 2001 |
| GIAC Enterprises has not removed the permission for world-writeable and setUID/setGID files and directories from all systems. | 1. All writeable-by-other files be reviewed. Unless the writeable-by-other permission is needed for the proper functioning of the system, the permission should be changed.<br><br>2. All setuid/setgid files be reviewed. If setuid/setgid is required , the program should be compiled and all access to the source code should be restricted. Otherwise, the setUID/setGID permissions should be removed. | August 2001 |


© SANS Institute 2000 - 2005 Author retains full rights.

| | | |
|---|---|---|
| The development, test and production instances of the database for the GIAC Enterprises application are all running on the same server. The Informix database will allow users with access to the operating system (Unix) to have access to all three instances. | GIAC Enterprises should segregate the production environment in a manner that would prevent an unauthorized user from disrupting the production environment. In addition, a policy regarding this segregation approach should be created and incorporated as part of the system development life cycle methodology. | September 2001 |
| Management of user accounts on the OWS system needs to be improved. 183 users on the database server have a command shell. | 1. Users should be restricted from having command-line access to the OWS system.<br><br>2. Generic Operating System and Test accounts should be removed from the local password file.<br><br>3. Any accounts that have not been accessed for an extended period of time should be disabled. | August 2001 |
| Two UNIX servers were susceptible to known security vulnerabilities - specifically the dtappgather vulnerability and the ufsrestore vulnerability. The penetration testing team exploited these known vulnerabilities to gain root access to two Unix servers. | Install applicable patches or upgrade to a newer version of the operating system that resolves these security vulnerabilities, in accordance with documented software maintenance plan. | August 2001 |
| Trust relationships between Unix machines facilitated remote access without requiring passwords. The penetration testing team exploited trust relationships to transfer user and root access from compromised Unix servers to those that trusted them. | Use SSH in lieu of old R-Services. | August 2001 |



© SANS Institute 2000 - 2005 Author retains full rights.

| | | |
|---|---|---|
| Configuration of NFS mounted directories allowed escalation of privileges. Using a server where the network security penetration testing team already had root access, the team copied a command shell to a directory which was being exported via NFS, and made it setuid root. Then, from a target machine that had mounted the exported directory, the team ran the command shell to gain root access. | For NFS mounted locations used nosuid. | August 2001 |
| Accounts existed with the same username and password on UNIX as on NT. The penetration testing team used compromised usernames and passwords gained from Windows NT to access Unix servers. | Use different usernames and passwords on different systems | August 2001 |
| FTP software identified which usernames were valid and which were not by giving different error messages during authentication. The penetration testing team used this flaw to screen for valid usernames, based on the compromised Windows NT accounts, and found a valid username and password on a Unix server within 85 minutes. | Switch to a version of FTP that gives the same error message regardless of whether or not the username is valid. | August 2001 |
| Excessive information was available via DNS. The penetration testing team quickly obtained complete lists of the registered machines names and IP addresses and clues about the purposes of those machines. This helped the team to focus their attack more efficiently. | Set the DNS servers to allow zone transfers only to other authorized DNS servers. | August 2001 |

© SA



© SANS Institute 2000 - 2005 Author retains full rights.

## IV. Endnotes

[1] Carnegie Mellon Software Engineering Institute. "CERT® Advisory CA-2001-05 Exploitation of snmpXdmid" 30 March 2001. URL: http://www.cert.org/advisories/CA-2001-05.html (10 July 2001).

[2] Carnegie Mellon Software Engineering Institute. "CERT® Advisory CA-1998-02 Vulnerabilities in CDE" 30 March 2001. URL: http://www.cert.org/advisories/CA-1998-02.html (10 July 2001).

[3] McGann, Seth. "Buffer overflows in Solaris 2.6 ufsdump and ufsrestore" 23 April 1998. URL: http://www.security-express.com/archives/bugtraq/1998_2/0154.html (10 July 2001).

[4] INT Media Group, Inc. "FTP" 1 Sept 1996. URL: http://webopedia.internet.com/TERM/F/FTP.html (10 July 2001).

[5] INT Media Group, Inc. "TFTP" 1 Sept 1996. URL: http://webopedia.internet.com/TERM/T/TFTP.html (10 July 2001).

[6] O'Reilly & Associates, Inc.. "Linux Kernel Problems; SSH Design Flaw" 13 February 2001. URL: http://linux.oreillynet.com/pub/a/linux/2001/02/13/insecurities.html (10 July 2001).

[7] O'Reilly & Associates, Inc.. "Apache Insecurity Reveals Directory Contents" 20 March 2001. URL: http://linux.oreillynet.com/pub/a/linux/2001/03/20/insecurities.html (10 July 2001).

[8] Sun Microsystems. "Sunsolve Online Security Information" 10 July 2001. URL: http://sunsolve.sun.com/pub-cgi/show.pl?target=security/sec (10 July 2001).

© SANS Institute 2000 - 2005, Author retains full rights.



© SANS Institute 2000 - 2005 Author retains full rights.