Global Information Assurance Certification Paper

Global Information Assurance Certification (GIAC)
Information Security Officer (ISO)
CERTIFICATION PRACTICAL

IT Security for GIAC Enterprises

Mike Frandsen
Information Security Officer Certification
Version: 1.2 (October 16, 2002)
Resubmission

Abstract

GIAC Enterprises is a company that sells comprehensive fantasy football advice over the Internet and through a mailed newsletter. This paper describes the business process of the company, its IT infrastructure, security risks, and preventative and corrective security measures.

GIAC Enterprises uses a Defense-In-Depth strategy to ensure confidentiality, integrity, and availability of information by applying several different layers of security using industry best practices. This security posture makes it hard for a hacker to gain access to a system because if one layer of security is penetrated, there are several others that must still be bypassed. The GIAC Enterprises network is divided into an Intranet that is only accessible by employees, and a publicly accessible subnet for services that facilitate web page and e-mail traffic.

GIAC Enterprises uses automated tools, software, policies and procedures to ensure the confidentiality, availability, and integrity of its information. Some of the tools used are listed below:

- Anti-Virus Software – to prevent malicious code
- Firewalls – to filter out unwanted electronic traffic
- Intrusion Detection – to monitor and be alerted to potential hacker attacks
- Encryption – to provide secure web and e-mail transmissions
- Vulnerability Scanning – to identify security flaws in systems

The paper includes a vulnerability scanning policy and procedures to ensure that system vulnerabilities are minimized.

TABLE OF CONTENTS

1. Mission of GIAC Enterprises..... 4
2. Description of GIAC Enterprises..... 4
3. Business Operations..... 4
   - 3.1. Business Process Summary..... 4
   - 3.2. Secure Transactions..... 5
4. IT Security Overview..... 5
5. IT Infrastructure..... 6
   - 5.1. GIAC Enterprises Network..... 6
   - 5.2. Network Infrastructure Tables..... 9
   - 5.3. Security and Privacy Statement..... 9
   - 5.4. Physical Security..... 10
   - 5.5. Other Security Measures..... 11
6. Areas of Risk..... 11
   - 6.1. Risk 1: Unauthorized Access Attempts..... 11
     - 6.1.1. Overview of Risk..... 11
     - 6.1.2. Why Risk Concerns GIAC Enterprises..... 12
     - 6.1.3. Consequences if Vulnerability were Exploited..... 12
     - 6.1.4. Steps Taken to Mitigate Risk..... 12
   - 6.2. Risk 2: Instant Messaging Vulnerabilities..... 14
     - 6.2.1. Overview of Risk..... 14
     - 6.2.2. Why Risk Concerns GIAC Enterprises..... 14
     - 6.2.3. Consequences if Vulnerability were Exploited/Steps Taken to Mitigate Risk..... 14
   - 6.3. Risk 3: System Configuration Vulnerabilities..... 16
     - 6.3.1. Overview of Risk..... 16
     - 6.3.2. Why Risk Concerns GIAC Enterprises..... 16
     - 6.3.3. Consequences if Vulnerability were Exploited..... 16
     - 6.3.4. Steps Taken to Mitigate Risk..... 17
7. Security Policy and Procedures..... 18
   - 7.1. Sample Audit Policy..... 18
   - 7.2. Sample Policy Critique..... 19
   - 7.3. GIAC Enterprises Vulnerability Scanning Policy..... 20
   - 7.4. GIAC Enterprises Vulnerability Scanning Procedures..... 24
     - 7.4.1. Scanning Tool Used..... 24
     - 7.4.2. Types of Scans..... 25
     - 7.4.3. Required Actions..... 25
8. References..... 26

1. Mission of GIAC Enterprises

The mission of GIAC Enterprises is to provide subscribers with the best fantasy football information on the Internet.

2. Description of GIAC Enterprises

GIAC Enterprises is a for profit corporation that specializes in providing comprehensive fantasy football advice over the Internet and through a mailed newsletter. The popularity of fantasy football in the U.S. has skyrocketed the last few years and it has become a lucrative web-based business. For a yearly cost of $29.95, consumers can subscribe to information based on projections of how players will perform statistically in the upcoming pro football season. GIAC Enterprises has a team of experts including professional football contacts in the media that provide information to the company. Subscribers then gain expertise that they can use in their individual fantasy football leagues.

3. Business Operations

3.1. Business Process Summary

GIAC Enterprises conducts its business via the World Wide Web, by offering fantasy football advice to subscribers over the Internet or a newsletter by mail. The industry is competitive, with a large and growing number of fantasy football web sites on the Internet. GIAC Enterprises has a full-time staff of 15 employees, and at any one time retains between five and ten part-time consultants. Having part-time employees reduces costs for office space, equipment, benefits, and wages. GIAC Enterprises gets a large part of its revenue from companies who pay GIAC Enterprises to advertise on its web site. The target market for GIAC Enterprises is male sports fans aged 18-54.

Customers provide their credit card numbers over the phone, on the Internet, or by mail to register for the service. Once a customer becomes a member, that membership lasts for one year, and enables the customer to login securely to the company's web site using Secure Socket Layer (SSL) encryption to receive the proprietary information. User IDs and passwords are chosen by the user. Passwords must conform to the requirements listed in the next section.

GIAC Enterprises provides weekly updates on the projected performances of professional football players, and includes player rankings by position, recommendations on which players to start each week, updates on all league transactions, injury reports, columns written by experts, and fantasy mock drafts.

Once a week, one of GIAC Enterprises' experts is available for chatting through instant messaging (IM) programs. Because IM presents several security risks,

GIAC Enterprises has posted guidelines on its web site for employees and subscribers to follow to protect information as much as possible.

3.2. Secure Transactions

GIAC Enterprises provides secure web-based transactions, and ensures that all of the information it collects from customers, as well as the company's proprietary research information is kept secure. GIAC Enterprises uses 128-bit SSL encryption to ensure the confidentiality of customer credit card transactions. SSL is a protocol that allows client/server communication via encryption. Any third parties who intercept this data in transit will intercept encrypted data that will be unreadable.

When customers enter their personal information into the order form, it is transmitted over the Internet in an encrypted format, and then decoded when it gets to the web site. GIAC Enterprises also encrypts the credit card number when it is stored on GIAC Enterprises IT resources, and when it is forwarded to the credit card company. User IDs and passwords must be between seven and 10 letters, comprised of mixed alphanumeric characters, and changed every two months. Subscribers are prompted to make changes through automated password aging.

GIAC Enterprises provides its employees with secure, private, remote access by "tunneling" through the Internet via Virtual Private Networks (VPNs). VPNs allow GIAC Enterprises employees to send e-mail through the company e-mail server, and access information from the GIAC Enterprises Intranet including the database server and file server. The database server is the key server on which the company's critical information – the proprietary research information as well as customer data – resides.

Remote access is accomplished using a Cisco VPN Concentrator and Cisco Secure VPN Client. Connections are made through cable modems. GIAC Enterprises uses the tunneling protocol IP Security Protocol Suite (IPSec). Remote users have Windows 2000 PCs with the same secure configurations that the PCs on site have, including anti-virus software.

4. IT Security Overview

The need for IT security measures for online companies is increasing dramatically due to new vulnerabilities and threats that are constantly being developed, the interconnectivity of systems on the Internet, and the ease of use of hacker tools.

GIAC Enterprises uses a Defense-In-Depth strategy to ensure confidentiality, integrity, and availability of information by applying several different layers of security using industry best practices. GIAC Enterprises ensures that its IT

resources have a level of security that is appropriate for the level of risk that could result from security breaches.

GIAC Enterprises is a small enterprise, and does not have the resources of a larger corporation. Therefore, GIAC Enterprises accepts the risk for some threats that are unlikely to occur, would not have a devastating impact on the business, or for which costs would be inconsistent with the risk involved.

5. IT Infrastructure

5.1. GIAC Enterprises Network

The GIAC Enterprises TCP/IP based network consists of a public and private subnet. The public subnet includes an E-Mail Server, a DNS Server, and a Web Server. These servers have services (SMTP, DNS, HTTP) accessible from the Internet on the public subnet. The file server, database server, and desktop workstations are not directly accessible from the Internet because they have no need to be accessed outside the GIAC Enterprises Network.

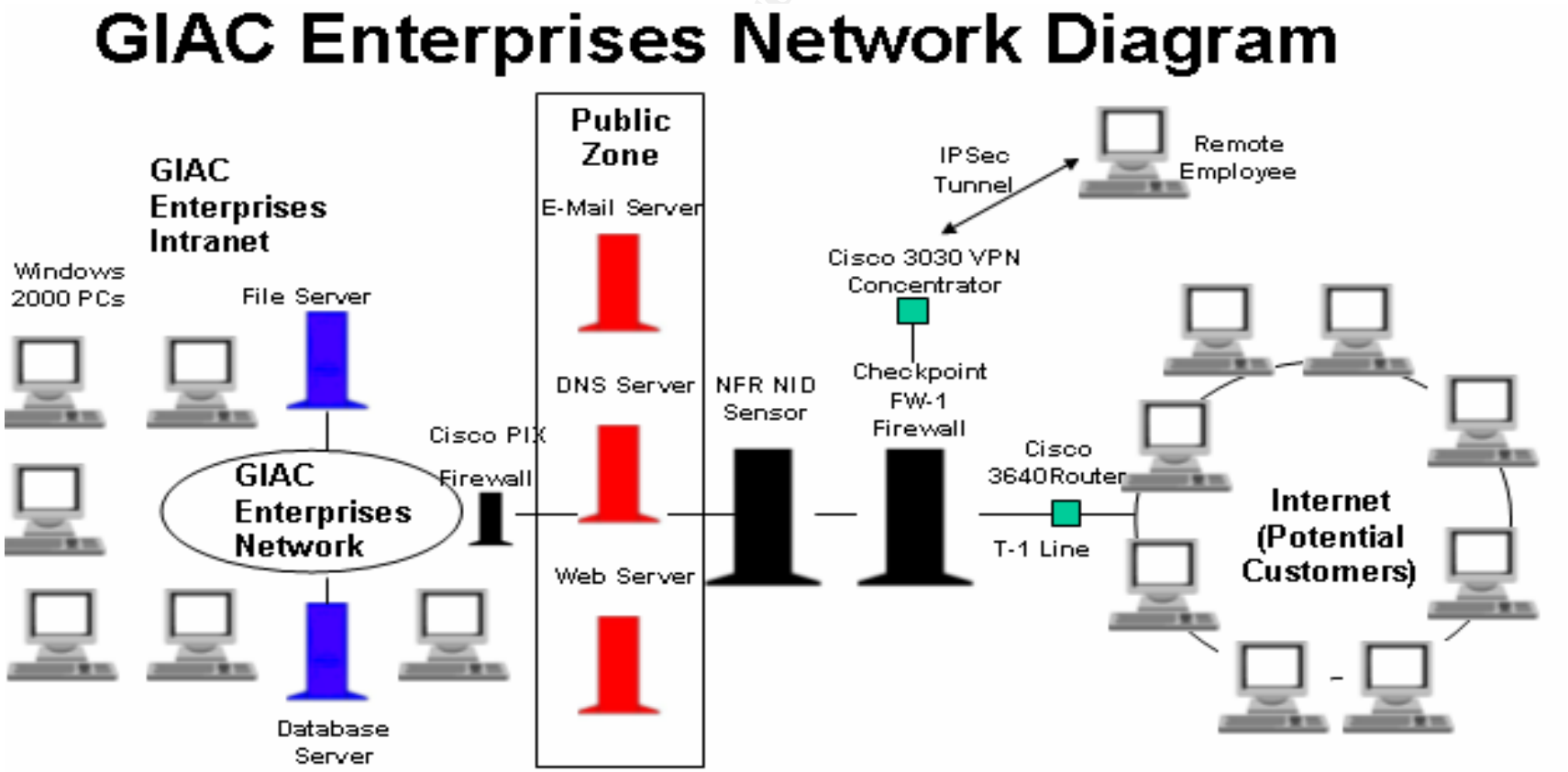
Separating the GIAC Enterprises Network from the Internet is a Checkpoint FW-1 firewall and Cisco 3640 router, while a Network Flight Recorder Network Intrusion Detection (NID) sensor resides on a server between the GIAC Enterprises Network and the firewall. A Cisco PIX 515E Firewall separates the GIAC Enterprises Intranet from the publicly available zone. The NID generates real-time reports on intrusion attempts, denial of service attacks, scans and probes, and other suspicious activity. The firewall rules are set up to "deny all" Internet traffic except what is necessary to operate the business and provide service to the customers. The firewalls restrict access from the Internet to the GIAC Enterprises Intranet, and allow only the ports and protocols necessary to conduct business related transmissions.

Anti-virus software is installed at multiple levels: at the e-mail server and on the personal computers (PCs) connected to the GIAC Enterprises Network. This is consistent with a Defense-In-Depth security posture so that if one layer is penetrated, malicious code must still bypass another layer to gain access to systems. GIAC Enterprises uses the following Network Associates McAfee anti-virus software:

- GroupShield for the e-mail gateway
- VirusScan for desktop workstations and servers

GIAC Enterprises also uses ePolicy Orchestrator, which is management software for Network Associates anti-virus software. ePolicy Orchestrator provides automatic updates of anti-virus definition files to servers and desktop workstations.

See the GIAC Enterprises Network Diagram and GIAC Enterprises IT Infrastructure Tables for more details on IT infrastructure.


GIAC Enterprises Network Diagram
Public Zone
GIAC Enterprises Intranet
E-Mail Server
IPSec Tunnel
Remote Employee
Windows 2000 PCs
File Server
Cisco 3030 VPN Concentrator
DNS Server
NFR NID Sensor
Checkpoint FW-1 Firewall
Cisco PIX Firewall
GIAC Enterprises Network
Cisco 3640Router
T-1 Line
Internet (Potential Customers)
Web Server
Database Server
Servers with services (SMTP, DNS, HTTP) accessible from Internet
Servers that contain proprietary information and are not accessible from the Internet

5.2. Network Infrastructure Tables

GIAC Enterprises System Infrastructure					
Components	**Product**		**Operating System**		**Configuration (examples of major services and/or applications)**
	Brand	**Version**	**Type**	**Version**	
Web Server	Apache	HTTP Server 2.0	Red Hat Linux	8.0 Professional	HTTP(s)
E-Mail Server	Microsoft	Exchange 2000 Server	Microsoft Windows 2000 Professional Server	Service Pack 3	SMTP, McAfee GroupShield Exchange, ePolicy Orchestrator V. 2.5.1.203
File and Print Server	Microsoft	Windows 2000 Professional Server	Microsoft Windows 2000 Professional Server	Service Pack 3	FTP
DNS Server	JHSoftware	Simple DNS Plus	Microsoft Windows 2000 Professional Server	Service Pack 3	DNS
Database Server/File Server	Microsoft	SQL 2000 Server	Microsoft Windows 2000 Professional Server	Service Pack 3	SQL
Personal Computers	Compaq	DeskPro EN Series 1.0	Microsoft Windows 2000 Professional	5, Service Pack 2.	Office 2000; Outlook 2000; Internet Explorer 6.0 SP 1; McAfee VirusScan7, ePolicy Orchestrator V. 2.5.1.203

Network Infrastructure	
Components	**Product/Brand/Version**
Perimeter Router	Cisco 3640, IOS 12.2
Perimeter Firewall	Checkpoint FW-1
Intranet Firewall	Cisco PIX 515E
Network Intrusion Detection System	Network Flight Recorder NID
VPN Concentrator	Cisco 3030

5.3. Security and Privacy Statement

GIAC Enterprises has posted the following statement on its web site.

GIAC Enterprises has applied appropriate managerial, operational, and technical controls to ensure the confidentiality, integrity, and availability of all information on our site as well as all customer information. All personal information will be used only by us for membership purposes and will not be forwarded to any third parties.

Personal Information Collected by GIAC Enterprises includes:

- *Name*
- *Phone Number*
- *Address*
- *E-Mail Address*
- *Age*
- *Credit Card Number and Expiration Date*

GIAC Enterprises does not use cookies, however, advertisers may use cookies that may be activated if customers click on their ads or go to their web sites. GIAC Enterprises uses safeguards such as firewalls, intrusion detection, anti-virus software, vulnerability scanning, and encryption to ensure that all data is secure.

5.4. Physical Security

GIAC Enterprises employs parking turnstiles and electronically swiped badges to gain access to its office space. The LAN closet and the server room are always locked and only the Security Officer has a key. The company also owns fire alarms, extinguishers, and smoke detectors, and follows an evacuation plan in case of emergencies.

5.5. Other Security Measures

- GIAC Enterprises has published a Rules of Security Engagement on its web site with separate guidelines for employees and subscribers to follow to ensure adequate security. The section for employees is transparent to subscribers. Rules include but are not limited to the following topics:
    - Appropriate Use of the Internet, E-mail, and other IT Resources
    - Remote Access
    - Passwords
    - Security Roles and Responsibilities
- GIAC Enterprises has a Contingency Plan to send information by mail if online services are unavailable. GIAC Enterprises also backs up all of its

data and stores the data off site. Full backups are conducted weekly, and incremental backups are performed nightly. Each tape is labeled with the content and the date.

- All employees are required to sign a Non-Disclosure Agreement, which states that employees will not release company information to unauthorized personnel.

- Only the Security Officer has the authority to make hardware and software changes to the GIAC Enterprises network, or changes to the configuration of employee desktop workstations.

6. Areas of Risk

The information that is most critical to the company is user-provided information and also the player related information. This data is broken down into proprietary information on projected player performance, injuries, and trends; and personal customer information such as name, address, phone number, credit card number and expiration date.

Loss or modification of proprietary company or customer information is the major risk to GIAC Enterprises. These risks are identified into the following main areas:

1. Unauthorized Access Attempts
2. Instant Messaging Vulnerabilities
3. System Configuration Vulnerabilities

If any of these risks are realized, they could cause legal problems, financial losses, or harm to the company's reputation. A loss of proprietary research information and personal customer information could result. Therefore, certain steps are taken to mitigate risks. However, as a small company, GIAC Enterprises accepts some security risks because in some cases the cost of implementing safeguards would be more than the cost of a realized risk.

6.1. Risk 1: Unauthorized Access Attempts

6.1.1. Overview of Risk

Unauthorized access attempts are part of an effort to compromise the confidentiality, integrity, and availability of an IT resource. They are attempts by attackers to read, write, copy, or execute protected files. Unauthorized Access Attempts also may include attempts to gain protected access privileges. The proliferation of "script kiddies," hacker programs that don't require much effort to launch, has made illegally accessing a network easier and more common than in the past. These unsophisticated attacks that are often generated from point-and-

click tools can sometimes cause just as much damage as carefully scripted attacks. Some examples of unauthorized access attempts include HTTP, DNS, and FTP attempts.

6.1.2. Why Risk Concerns GIAC Enterprises

Any network connected to the Internet is potentially vulnerable to unauthorized access attempts. Although the GIAC Enterprises network has been separated into a company-only Intranet and a publicly accessible subnet, the increased frequency of unauthorized access attempts originating from the Internet requires the company to be vigilant in keeping its security safeguards up to date. GIAC Enterprises is a visible company because of its web site. In addition, a large percentage of unauthorized access attempts are HTTP related.

6.1.3. Consequences if Vulnerability were Exploited

Hackers regularly conduct reconnaissance scans and probes and subsequently launch unauthorized access attempts based on their findings. A network is only as secure as its weakest link, and one system compromise can quickly spread to the rest of the network, and even spew attacks on systems outside the network. Therefore, even if a majority of systems are secure, if one system is compromised, it can quickly adversely affect the integrity of the rest of the network. The effects on successful unauthorized access of GIAC Enterprises systems could result in information being deleted, stolen, or modified and cause financial, legal, or public relations damage to the business. Customers could be lost, and ultimately, confidentiality, availability, and integrity of information could be compromised.

6.1.4. Steps Taken to Mitigate Risk

GIAC Enterprises has configured its network firewalls to protect against unauthorized access attempts as much as possible. In order to prevent hackers from exploiting vulnerabilities and potentially changing, stealing, or destroying information, GIAC Enterprises restricts public access to its systems that do not have a business related need to be accessible via the Internet. The public should only see the basic web site, and subscribers should only have access to information they have paid for. Examples of systems that are publicly accessible are servers that run web, DNS, or e-mail services. Examples of systems that are not publicly accessible include personal desktop computers and printers.

Any systems that need to have at least one service open to the public are located on the publicly accessible subnet. These systems include the web, DNS, and e-mail servers. Any systems that have no requirements to be publicly accessible are located on the GIAC Enterprises Intranet. Employees whose systems are located on the GIAC Enterprises Intranet still have the capability of sending electronic traffic outside of the GIAC Enterprises Network, i.e. Internet or e-mail

traffic, however no unauthorized traffic from the Internet will be allowed in to the Intranet.

GIAC Enterprises uses a NID to detect incoming traffic that matches common attack signatures. Reports are generated by the NID and analyzed by the Security Officer. The Security Officer investigates potential incidents to determine if any compromises occur. If systems are compromised, the Security Officer implements corrective actions such as strengthening passwords, reloading the operating system, or applying security patches.

The Security Officer focuses on detecting and analyzing attacks that are launched from GIAC Enterprises. NID alerts that originate from within the GIAC Enterprises network are given a higher priority than external alerts, because if the source of an attack is within the network, it likely means a system has been compromised and can start attacking other systems inside or outside of the network. The Security Officer analyzes activity trends based on NID reports and configures the firewalls accordingly.

GIAC Enterprises uses its firewalls to block Internet traffic from entering its Intranet, and selectively block certain ports and services. GIAC Enterprises uses the System Administration, Networking and Security (SANS) Institute/FBI 20 Most Critical Internet Security Vulnerabilities as a point of reference for what to allow and deny. Some examples of what GIAC Enterprises blocks are included below.

- Incoming HTTP (TCP ports 80, 8000, 8080, and 8888) and DNS (port 53) queries that are not directed to the web and DNS servers.

- TCP port 21 and UDP port 69, because of FTP and TFTP exploits.

- TCP port 1433, the Microsoft SQL default port, to protect its most critical information from external scans and probes and subsequent unauthorized access attempts.

- TCP and UDP ports 137-139 and 445 because NetBIOS is not required to conduct business and contains major vulnerabilities.

- TCP and UDP port 111 and ports 32770-32789 so that Remote Procedure Call (RPC) services do not allow hackers to successfully access the Unix operating system on which the web server resides.

- Attack signatures for which there are no known false positives.

6.2. Risk 2: Instant Messaging Vulnerabilities

6.2.1. Overview of Risk

Security for Instant Messaging and Chat (IM) programs is not keeping pace with the rapid increase in the usage of these programs. Many of the same vulnerabilities that exist in e-mail programs are also present in IM programs. Examples include buffer overflows, viruses, spoofing, spamming, and messages sent in clear text. However, because IM programs use different ports and protocols than e-mail services, virus software is not yet mature for IM and this is a security hole that can enable hackers to bypass the traditional security controls such as virus software. In addition, the ports and protocols that IM programs use can change, making it hard to configure firewalls to manage IM traffic.

6.2.2. Why Risk Concerns GIAC Enterprises

IM is an integral part of GIAC Enterprises because of the real time communication that facilitates the rapid updating of information for the web site, as well as communication between subscribers who choose to exchange information. All employees and subscribers to GIAC Enterprises must agree to adhere to GIAC Enterprises IM Guidance. The table on the next page describes common IM vulnerabilities and the recommended actions to ensure that information exchanged via IM is kept secure. Because employees and subscribers may use different commercially available IM programs, vulnerabilities and guidance apply to IM programs in general rather than any specific software.

6.2.3. Consequences if Vulnerability were Exploited/Steps Taken to Mitigate Risk

See the table on the next page. In addition to the security measures GIAC Enterprises has implemented for IM, the use of Internet Relay Chat (IRC) programs is banned and access to ports 6665 through 6669 is blocked at the firewalls. According to the Department of Energy Computer Incident Advisory Capability, IRC activity often indicates hacker activity.

IM Vulnerabilities	Details on Threats/Consequences if Vulnerabilities were Exploited	GIAC Enterprises Recommended Actions/ Steps Taken to Mitigate Risk
1. Buffer overflows	Holes in IM programs can allow attackers to execute arbitrary code and cause denial of service attacks.	Use the latest patched versions of IM programs.
2. Viruses	• Infected Files can be exchanged via IM and spread through the IM address book/buddy list. • Antivirus software isn't fully developed for IM yet because of the different ports and protocols IM uses. IM viruses can circumvent anti-virus software at the e-mail and firewall gateways, leaving desktop protection as the last defense.	• Don't accept files or click on URLs unless they are from a trusted source because of the risk of downloading malicious code or being directed to a compromised server. Use e-mail to send files or URLs. • Periodically download the latest antivirus software because anti-virus software for IM is still being developed. • Disable file transfer capabilities
3. Lack of encryption	IMs are sent through clear text. Some IM programs are developing encryption but this is still in the early stages.	Never send sensitive information in IM, and use encrypted e-mail instead if possible.
4. Logging vulnerabilities	• Even if users disable logging features, the users they are exchanging IMs with can log IMs. • Some IM company servers retain logs and can be hacked.	Only communicate with trusted users.
5. File sharing vulnerabilities	• IM programs can be set up to share files, giving external users access to a directory on hard drives of internal users. • Both users of an IM peer-to-peer link must sign off before the connection is completely terminated.	Never send sensitive information in IM, and use encrypted e-mail instead if possible.
6. IP addresses can be visible	IP addresses of IM users and ports used can be detected by monitoring software.	• Configure IM program to restrict peer-to-peer transmissions to avoid showing IP address. If possible, configure IM program to hide IP address as much as possible. • Log off the IM program when it's not being used.
7. Spoofing/Stealing Screen Names	• Stealing screen names and passwords to masquerade as another user can be done more easily via IM than via e-mail.	• Change IM passwords frequently and develop passwords with alpha and numeric characters because of increased risk of spoofing. • Configure IM program so password is not saved.
8. Spamming	Unless IM programs are configured to communicate only with buddy list, spamming is possible.	Configure IM program to only accept and send IMs to a specified list of users.
9. Bandwidth issues	IMs and file sharing can eat up bandwidth, especially when large attachments are exchanged.	• Do not send attachments via IM.
10. Release of personal information	• Personal information in a profile is viewable by other users.	Configure IM program so that personal information is not listed, and users cannot search for you.

6.3. Risk 3: System Configuration Vulnerabilities

6.3.1. Overview of Risk

Malicious users can take advantage of incorrectly configured systems to corrupt data or disrupt the normal operation of systems. Potential incidents may include storing hacker programs or defacing web pages without the knowledge of GIAC Enterprises employees. System configuration vulnerabilities include extraneous services that are turned on that may expose systems to outside attack. These problems include unpatched software vulnerabilities in operating systems, Internet browsers, or e-mail programs. Often systems arrive "out of the box" with unnecessary services enabled as part of their default configuration. This is a problem for both Windows and Unix systems. This risk focuses on hardening the configuration of systems, rather than using a firewall to filter out electronic traffic.

6.3.2. Why Risk Concerns GIAC Enterprises

The IT systems at GIAC Enterprises contain the company's most critical and sensitive information: proprietary research information and customer data. GIAC Enterprises uses a variety of operating systems and versions, and therefore these systems must be periodically scanned to identify vulnerabilities and recommend corrective actions such as upgrading or reloading operating systems, turning off unnecessary services, applying software patches, or modifying access by adding or strengthening passwords or restricting permissions. For more information on system configuration vulnerabilities and the actions necessary to remediate them, see the GIAC Enterprises Vulnerability Scanning Policy and Procedures.

6.3.3. Consequences if Vulnerability were Exploited

If vulnerabilities are exploited, attackers could conduct their own scans and probes to collect information useful to launch denial of service attacks, spread malicious code, or try to gain access to company information. The following consequences could result:

Consequence	Example	Confidentiality, Integrity, or Availability
Damage to the credibility of GIAC Enterprises.	Example: A web site defaced through web server vulnerabilities could cause subscribers to lose confidence in GIAC Enterprises.	Integrity and Availability
Loss of research information, or loss of access to information	A successful denial of service attack that resulted from unpatched vulnerabilities could prevent	Availability

Consequence	Example	Confidentiality, Integrity, or Availability
by subscribers.	subscribers from accessing the web site and getting the most up-to-date information.	
Unauthorized disclosure of confidential information.	A release of personal customer information due to a hacker that gained access through an extraneous service could result in stolen credit card information.	Confidentiality
Financial consequences.	A release of proprietary information by hacking into the database server could allow hackers to modify information, or other companies to gain access to information and thus an advantage over GIAC Enterprises.	Confidentiality and Integrity

6.3.4. Steps Taken to Mitigate Risk

The GIAC Enterprises IT security program uses multiple layers of safeguards so if one layer is breached, an intruder does not gain access to a system. IT system configuration is an important component of this strategy because systems must be configured correctly and software versions must be kept up-to-date to prevent hackers from exploiting vulnerabilities and changing, stealing, or destroying data. Systems that contain a service that must be accessible externally are still configured to keep only the minimum of services available to run the business. Because systems that are accessible in the "public zone" of GIAC Enterprises are by definition more vulnerable than the closed systems behind the second firewall, they are scanned for vulnerabilities more often than the systems on the Intranet.

By using secure software versions, applying security patches, and modifying access controls, GIAC Enterprises protects against

- GIAC Enterprises uses an Apache web server on a Red Hat Linux operating system instead of Microsoft's Internet Information Server (IIS). IIS is vulnerable to many HTTP unauthorized access attempts in its default configuration. Even if vulnerabilities are patched, based on trends of the past two years, it is likely more security holes will be discovered in IIS. According to the SANS Institute/FBI 20 Most Critical Internet Security Vulnerabilities[1], "IIS is prone to vulnerabilities in three major classes: failure to handle unanticipated requests, buffer overflows, and sample applications."

[1] http://www.sans.org/top20/

- GIAC Enterprises downloads the latest security patches from Apache at http://www.apache.org/dist/httpd/patches/. RPC services are disabled on the Linux system.

- GIAC Enterprises uses the latest version of Internet Explorer (IE6, SP2) to minimize vulnerabilities. Earlier versions of IE that do not contain service packs have major vulnerabilities, according to the SANS Institute/FBI 20 Most Critical Internet Security Vulnerabilities.

- GIAC Enterprises ensures that strong passwords are used on all its administrator and user accounts that conform to the password requirements listed in Section 5.2.

New system configuration vulnerabilities and related exploits are constantly being discovered and developed. GIAC Enterprises employs an automated vulnerability scanning program to detect possible vulnerabilities and take corrective action. Vulnerability scans of computers, servers, and routers must be ongoing because of changes in hardware, software upgrades, operating system patches, and new security patches. Each network node is examined to determine what weaknesses exist. For more details on the GIAC Enterprises vulnerability scanning program, see the policy and procedures in the next section.

7. Security Policy and Procedures

The sample policy is taken from the SANS Security Policy Project.

7.1. Sample Audit Policy[2]

1.0 Purpose
To provide the authority for members of <Company Name>'s InfoSec team to conduct a security audit on any system at <Company Name>.

Audits may be conducted to:

- *Ensure integrity, confidentiality and availability of information and resources*
- *Investigate possible security incidents ensure conformance to <Company Name> security policies*
- *Monitor user or system activity where appropriate.*

2.0 Scope

2. SANS Security Policy Project/Audit Policy web site: http://www.sans.org/newlook/resources/policies/Audit_Policy.pdf.

This policy covers all computer and communication devices owned or operated by <Company Name>. This policy also covers any computer and communications device that are present on <Company Name> premises, but which may not be owned or operated by <Company Name>.

3.0 Policy
When requested, and for the purpose of performing an audit, any access needed will be provided to members of <Company Name>'s InfoSec team.

This access may include:

- *User level and/or system level access to any computing or communications device*
- *Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on <Company Name> equipment or premises*
- *Access to work areas (labs, offices, cubicles, storage areas, etc.)*
- *Access to interactively monitor and log traffic on <Company Name> networks.*

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Revision History

7.2. Sample Policy Critique

The above policy meets the requirements of Michele Guel's SANS course "Proven Practices for Managing the Security Function." These requirements state that a policy must be:

- Implementable and enforceable
- Concise and easy to understand
- Balances protection with productivity

However, the policy is too general and needs to be customized for a business depending on its requirements. The following comments will be incorporated into a revised policy that focuses on vulnerability scanning, which is one of several subcategories of auditing.

Purpose

This policy is being established to enable security personnel to conduct security audits. It states the objective for performing audits: to ensure the confidentiality, integrity, and availability of information and resources. However, the policy lacks specificity regarding the types of audits it discusses. Regarding the statement "Monitor user or system activity where appropriate," the word "user" doesn't apply

to GIAC Enterprises because the Company President does not believe in monitoring user activity. The purpose should explain what types of audits the policy addresses.

Background

There is no background section. A background section that explains why the policy is important and provides information about the company security program would be helpful.

Scope

The policy describes what the policy covers – devices owned and operated by the company, or that reside on company premises. The second sentence in the scope, though, covering " any computer and communications device that are present on <Company Name> premises, but which may not be owned or operated by <Company Name>," is good for large organizations that may interface with other companies but does not apply to a small company such as GIAC Enterprises. The policy does not specify the stakeholders who are covered within the scope.

Policy Statement

The policy statement describes the types of access to systems and information that must be provided to the company's information security team. However, the policy statement fails to describe what the auditing process will entail and the different steps necessary to ensure security. It should mention the frequency of scans for the Intranet and public zone, while more detailed information should be included in scanning procedures.

Responsibility

The policy implies, but does not explicitly state, that users are the ones who must grant access to the InfoSec team for audits. The policy does not contain a separate section outlining the responsibilities of various stakeholders. The implied responsibilities lack detailed roles for management, security personnel, and other employees.

Action

The policy focuses on the access that must be granted to the InfoSec team. A separate "Action" section is not necessary, but the policy statement should contain specific actions on how audits will be conducted. The procedures should be even more detailed, listing step-by-step actions.

7.3. GIAC Enterprises Vulnerability Scanning Policy

The Sample Audit Policy has been customized to meet the requirements of GIAC Enterprises and to focus on vulnerability scanning, an auditing process that focuses on identifying and fixing vulnerabilities in systems.

Vulnerability Scanning Policy

1.0 Purpose

The purpose of this policy is to provide the authority for the GIAC Enterprises Security Officer to conduct a vulnerability scan on any system at GIAC Enterprises and conduct necessary remediation. Vulnerability scans are conducted to ensure the integrity, confidentiality and availability of information and resources. Vulnerability scanning identifies security flaws in networks or systems that are susceptible to being exploited so that corrective actions may be taken to prevent security incidents from occurring.

The policy focuses on removing extraneous services that could lead to exploits by hackers. This document establishes a policy for conducting vulnerability scans of GIAC Enterprises IT systems to reduce security risks and direct resources to the areas in most need of security. This policy will be enforced partly by monitoring system activity where appropriate. In addition to outlining a policy for scanning all GIAC Enterprises systems, this policy provides a scanning process to be followed when GIAC Enterprises systems have been compromised by hackers.

- The GIAC Enterprises vulnerability scanning program is designed to:
  - Ensure that security vulnerabilities are swiftly identified and addressed.
  - Periodically check for new vulnerabilities.
  - Categorize and prioritize vulnerabilities based on severity and the criticality of the system at risk.
  - Submit reports to the Company President that recommend corrective actions.
  - Implement corrective actions/Verify that appropriate remediation has been conducted.

2.0 Background

Protecting the security of GIAC Enterprises plays a vital role in facilitating the GIAC Enterprises mission of providing the best fantasy football information on the Internet. GIAC Enterprises will provide the security safeguards needed to protect information while enabling customers to gain access to that information. GIAC Enterprises will ensure that systems run only services that are necessary

to conduct business related requirements, and keep security patches current. This policy is necessary to outline what actions need to be taken so that GIAC Enterprises identifies vulnerabilities before hackers discover them.

3.0 Scope

This policy covers all computer and communication devices owned or operated by GIAC Enterprises. The policy outlines responsibilities for the stakeholders in GIAC Enterprises, which includes the Company President, Security Officer, and Employees.

4.0 Policy

- Standard scans will be conducted monthly on systems that reside on the company's public zone and quarterly on systems that are located on the company Intranet as well as systems that employees use to get remote access to the GIAC Enterprises network.
- When requested, and for the purpose of performing a vulnerability scan, employees will provide any access needed to the Security Officer.
- This access may include:
  - User level and/or system level access to any computing or communications device.
  - Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on GIAC Enterprises equipment or premises.
  - Access to work areas (labs, offices, cubicles, storage areas, etc.).
  - Access to interactively monitor and log traffic on GIAC Enterprises networks.
- The Security Officer will perform all vulnerability scans.
- The Security Officer will notify employees of any vulnerability scans before they are conducted. The vulnerability scan notifications will identify the systems that are scheduled to be scanned, the times of the scans, and the IP address of the system from which the scans originate.
- The Security Officer will address vulnerabilities based on the following priorities:
  - Fix critical problems within 24 hours.
  - Fix areas of concern within one week.

  - Fix potential problems within two weeks, or accept the risk if the cost of fixing the problem is prohibitive.

- The Security Officer will block access to and from GIAC Enterprises systems that are involved in system compromises or web site defacements. Systems for which access has been blocked at the GIAC Enterprises firewalls will be scanned by the Security Officer to verify that remediation has been completed before unblocking the systems.

- The Security Officer and Company President will ensure that the scanning tool minimizes false positive results and addresses the SANS Institute/FBI 20 Most Critical Internet Security Vulnerabilities.

5.0 Responsibilities

The policy focuses on the responsibilities of the Security Officer. Since GIAC Enterprises is a small company, the Security Officer is concerned with the operational security needs of the business. Employees are responsible for the security of their own systems to the extent that is specified in the GIAC Enterprises Rules of Engagement. Oversight is conducted by the Company President.

Company President

- Review scan summary reports.
- Authorize Security Officer to conduct corrective actions to address vulnerabilities.
- Work with owner of scanning tool to ensure that GIAC Enterprises uses latest version of tool minimizes false positive results and checks for SANS Institute/FBI 20 Most Critical Internet Security Vulnerabilities.
- Approve any exceptions to this policy.
- Arrange for a yearly audit of the vulnerability scanning program to ensure that required actions are carried out in an efficient manner.
- Review, approve, or modify policy on an annual basis.

Security Officer

- Notify employees of scans.
- Perform scans.
- Analyze results.
- Prepare reports for the Company President identifying, categorizing, and prioritizing vulnerabilities; recommending corrective actions; and justifying why it is important to conduct remediation.
- Implement corrective actions based on severity of vulnerabilities.

- Use firewalls to block systems that pose a severe risk to the company until remediation is complete.
- Work with owner of scanning tool to ensure that GIAC Enterprises uses latest version of tool minimizes false positive results and checks for SANS Institute/FBI 20 Most Critical Internet Security Vulnerabilities.
- Recommend policy changes annually to the Company President.

Employees

- Allow access to the security officer to physical work space, IT systems, and information.
- Do not add unauthorized software or services to user workstations.
- Review the Roles and Responsibilities listed in the GIAC Enterprises Rules of Engagement.

6.0 Enforcement

Any user found to have violated this policy may be subject to disciplinary action, up to and including termination of employment pending a review by the Company President.

7.0 Compliance Date

All employees must comply with this policy by October 20, 2002.

8.0 Revision History

This policy will be reviewed on an annual basis and updated as appropriate.

7.4. GIAC Enterprises Vulnerability Scanning Procedures

7.4.1. Scanning Tool Used

GIAC Enterprises uses the Security Administrator's Integrated Network Tool (SAINT™) to conduct vulnerability scans. SAINT was derived from the Systems Administrators' Tool for Analyzing Networks (SATAN) tool, which was developed by Dan Farmer and Wietse Venema and released in 1995. SAINT includes many enhancements from the original tool. GIAC Enterprises selected SAINT for reasons that include the following:

- Finalist for *Information Security* 2002 Information Security Excellence Awards, which recognize the IT security industry's leading products as voted by the magazine's subscribers.
- Based on SANS Institute/FBI 20 Most Critical Internet Security Vulnerabilities.

- SANS/Institute for Security Technology Studies (ISTS) Certified.
- Updated every two weeks or more often if necessary to address a critical vulnerability announcement.
- Contains multiple modes of operation, configurable scan levels, and good reporting tools, according to the SANS Reading Room.

GIAC Enterprises uses the SAINTwriter™ reporting tool to generate vulnerability assessment reports in a user-friendly format. Reports include an executive summary, a list of vulnerabilities for each system, and descriptions of recommended corrective actions.

7.4.2. Types of Scans

- New Host Scans – Scans that assess new hosts before they are added to the network.
- Standard Scans – Thorough scans that search for all known vulnerabilities. These are conducted on a quarterly basis for systems on the Intranet, and on a monthly basis for systems on the public zone.
- Specialized Scans – Quick scans that detect one or more major vulnerabilities, usually conducted when a new exploit occurs. These are conducted on an as needed basis.
- Verification Scans – Scans that ensure that vulnerabilities or incidents have been addressed with appropriate corrective actions. These are conducted one month after standard scans, on a quarterly basis for systems on the Intranet, and on a monthly basis for systems on the public zone.

7.4.3. Required Actions

For All GIAC Enterprises Systems

1. Company President ensures that GIAC Enterprises uses the most up-to-date version of SAINT.

2. Security Officer develops scan schedule.

3. Security Officer informs employees of scan schedule. Security Officer e-mails employees notifications three days before each scan that identify the:

   A. IP addresses of the systems that are scheduled to be scanned
   B. Dates and times the scans will begin and are expected to end
   C. IP address of the system from which the scans originate.

4. Security Officer conducts scan against the systems owned by GIAC Enterprises.

5. Security Officer generates comma separated values (.csv) files.

6. Security Officer develops scan reports. Security Officer analyzes the results of the report and writes an executive summary to the Company President explaining the most critical vulnerabilities, including how and why they need to be addressed.

7. Security Officer evaluates report for accuracy and submits it to management.

8. Company President approves remediation plan based on scan report.

9. Employees allow the Security Officer to conduct appropriate remediation.

10. Security Officer addresses vulnerabilities based on severity using configuration management and the following methods:

    A. Applying software patches or "fixes"
    B. Modifying access
    C. Upgrading or reloading operating systems
    D. Disabling services.

For GIAC Enterprises Systems that are Compromised

1. Security Officer blocks access to and from GIAC Enterprises systems that are involved in system compromises or web site defacements.
2. Security Officer conducts remediation.
3. Security Officer scans systems based on steps above to verify that remediation has been completed.
4. Security Officer unblocks systems.

Note: If fixing vulnerabilities results in a loss or degradation of needed services, management can decide to accept the risk rather than fix the vulnerability. For this to occur, the manager will meet with the Security Officer to review the costs and benefits of remediating vulnerabilities. For example, a vulnerability categorized with a severity of "low" may be an acceptable risk if it means keeping a service enabled to meet business requirements.

8. References

1. Rayome, Jerry. "IRC on Your Dime? What You Really Need to Know About Internet Relay Chat." June, 1998. http://ciac.llnl.gov/ciac/documents/CIAC-2318_IRC_On_Your_Dime.pdf.
2. Checkpoint web site: http://www.checkpoint.com/products/protect/firewall-1.html.

3. Cisco web site: http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/index.html.
4. Guel, Michele. "Proven Practices for Managing the Security Function." 2001. SANS Security Policy Project web site: http://www.sans.org/newlook/resources/policies/policies.htm.
5. Network Flight Recorder web site: http://www.nfr.com/products/NID.
6. Red Hat Linux 8.0 web site: http://www.redhat.com/mktg/rhl8/.
7. SAINT web site: http://www.saintcorporation.com/about.html.
8. SANS Security Policy Project/Audit Policy web site: http://www.sans.org/newlook/resources/policies/Audit_Policy.pdf.
9. SANS Institute/FBI 20 Most Critical Internet Security Vulnerabilities: http://www.sans.org/top20/.
10. Apache security patches: http://www.apache.org/dist/httpd/patches/.
11. A joint whitepaper from IBM Corporation and Microsoft Corporation, "Security in a Web Services World: A Proposed Architecture and Roadmap. Version 1.0. April 7, 2002. http://www.verisign.com/wss/architectureRoadmap.pdf.
12. Viksnins, Rebecca. "Protect Your Instant Messenger." May 10, 2002. http://www.zdnet.com/products/stories/reviews/0,4161,2865184,00.html.