Global Information Assurance Certification Paper

Internet Security Handbook

Minimum Levels of Due Diligence

Stewart Caquelin
GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4b - Option 1
August 7, 2003

Abstract:
Establishing site security is a daunting task. Generally speaking it was always thought of in terms of defense, a protective shield and not in terms of civil liability. Today Organizations are being held accountable for their interpretation of appropriate security measures. They must now be able to prove that they have taken reasonable steps to secure and protect the Information systems and the data stored on them.

Introduction

The "Internet" is a worldwide collection of thousands of networks linked by a common set of technical protocols which make it possible for users of any one of the networks to communicate with or use the services located on any of the other networks[1]. It is this worldwide system of interconnecting networks combined with the lack of centralized structure and standardized controls that significantly increases computer security risks and liabilities.

Since the Internets recognized beginning in 1969[2], when the first computer to computer communication was transferred across ARPANET[3] from UCLA to Stanford Research Institute, computer and network security has been voluntary and the responsibility of the site owners. Computer and network security often took a back seat to ease of use, convenience, and features. Security design was mostly ad hoc and usually added to the computer or network after a security breach or incident had occurred.

Traditionally, computer and network security practices on the Internet have been collaborative effort; all sites are expected to help one another respond to security violations. Often this involved tracing connections, capturing packets, tracking violators and assisting law enforcement efforts. Computer and network security controls were almost explicitly designed and implemented to prevent unauthorized access. Viruses, Worms, distributed denial-of-services attacks, Zombies and Robots all evolving weapons in the Hackers war chest have changed the battlefield. Security practices are evolving into a comprehensive collection of technologies performing specific tasks combined with the best practices and procedures that integrate into an overall site security policy.

Since RFC-1244 was released in July of 1991, it has been predicted that in the near future organizations could be held responsible because one of their nodes was used to launch a network attack. Similarly, people who develop patches or workarounds may be sued if the patches or workarounds are ineffective, resulting in compromise of the systems, or, if the patches or workarounds themselves damage systems[4].

The Federal Trade Commission (FTC) has started enforcement actions against companies that fail to take appropriate security precautions especially when consumer information and privacy are involved. Recent privacy and security regulations such as the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")[5] and Gramm-Leach-Bliley (GLB) Act[6] and the Safeguards Rule[7] have mandated specific requirements for companies doing business in these areas.

Recent FTC settlements:

- Microsoft Corporation has agreed to settle Federal Trade Commission charges regarding the privacy and security of personal information collected from consumers through its "Passport" web services. As part of the settlement, Microsoft will implement a comprehensive information security program for Passport and similar services[8].

- Eli Lilly and Company (Lilly) has agreed to settle Federal Trade Commission charges regarding the unauthorized disclosure of sensitive personal information collected from consumers through its Prozac.com Web site[9].

- Guess, Incorporated has agreed to settle Federal Trade Commission charges that it exposed consumers' personal information, including credit card numbers, to commonly known attacks by hackers, contrary to the company's claims[10].

Companies who fail to implement appropriate computer and network security practices are likely to be held accountable for their negligence. Legal liabilities will most likely be determined by a company's failure to show reasonable due diligence. Tort tests will certainly involve what would be considered reasonable and prudent security measures. Knowing of a computer or network system vulnerability, and then taking appropriate measures to minimize the exposure will be essential to preventing future legal problems. This paper is an attempt to set minimum levels of consistent security practices based on today's technology and industry best practices.

Common Security Risks

Hackers, Worms and Viruses show no bias, their goal is to compromise site or system security and then control or infect all vulnerable systems the easiest way possible. In almost all cases the strategy is the same, randomly search for a specific weakness, then exploit that weakness.

Today, hacking tools are being widely distributed and are typically easy to use. Most of the tools use the same strategy. Scan IP addresses and identify known security vulnerabilities. Once a vulnerable computer or network has been located, the Hacker, Worm or Virus strikes and any of the following may happen.

- Unauthorized disclosure of confidential information.
- Modification or deletion of data.
- Authorized access to systems could be denied due to system overload or denial of service attacks.
- The unauthorized use of a system for the processing or storage of data.
- Exploitation of a vulnerable system, using that system to attack others, hiding the attackers true identity while implicating the owner as the perpetrator of the unscrupulous act.
- Changes to system hardware, firmware, or software characteristics without the Network / Systems Administrators knowledge, instruction, or consent.

Security Handbook Goal

This handbook sets minimum computer and network security guidelines and procedures for all computers and networks that are connected to the Internet. These guidelines are fundamental security actions that generally apply to all computers systems and networks regardless of manufacturer or vendor. The guidelines are based on the following generally accepted computer and network security best practices.

Develop a Security Policy - This high level document is the foundation of your commitment to computer and network security. This document should not be adopted in words only, it should be an action plan backed up at the highest level. A policy that is enforced at all levels proves evidence of due diligence, if it is not, it is proof of negligence.

Educate the end users - Training should include the proper use of Email applications and specifically how to handle Email attachments, the use of Anti-Virus software and how to keep the virus definitions updated. Instructions should be given on how to select good passwords. Training should also review and emphasize the importance of the computer and network security policy.

Hold System and Network Administrators accountable - Write computer and network security responsibilities into the Job description of these professionals. This should include keeping all systems updated with vendor released system patches. Hire only qualified candidates for these positions.

Harden all production systems - Hardening is a process of removing all unused and unnecessary services. Installation checklist and scoring tools should be used for each Operating system or device. All system changes should be documented in a central location. If possible, production systems should be restricted to running only a single service.

Systems should be routinely audited - Log files should be reviewed and running services evaluated. All user accounts should be validated. Backup and Restore procedures should also be verified. Ports should be scanned and system security probed for weaknesses. This also gives you an opportunity to learn the system, the network, what to expect and when.

An incident response plan/policy should be developed – This plan should include how to identify a security incident, contact and notification information, damage assessment, containment and recovery plans.

Design defenses in depth security - Use packet filtering and access control list on the border routers to drop unnecessary traffic. Use firewalls for more granular traffic control and logging. Segment networks by services, functions or departments. Use checklist to maintain constantly strong Host level security, where strong password policies are enforced, a layer of physical security and finally an enforced written security policy.

Information Systems Policy

GIAC ENTERPRISES Information Systems are business tools that are provided by GIAC ENTERPRISES to employees to facilitate timely and efficient conduct of business. The goal of this policy is to assure the operational security and integrity of these resources, discouraging practices, which degrade the usability of these network resources and thus the value of our Information Systems. Employees, associates and customers should realize that these resources are finite and costly. GIAC ENTERPRISES encourages all employees and associates to use these resources in a manner that is respectful to others.

Employees must take particular care to comply with and understand the copyright, trademark, libel, slander, and public speech control laws of those countries in which GIAC ENTERPRISES maintains a business presence. Local jurisdiction of data protection laws applies and will be enforced. This policy is intended to be consistent with other GIAC ENTERPRISES policies, including Harassment and Equal Opportunity Employment policies. Information Systems should be used in a manner consistent with these policies. These policies apply to local, mobile, and telecommuting users. Misuse of Information Systems or breech of Information Systems policies may be considered grounds for disciplinary action up to and including termination of employment. GIAC ENTERPRISES reserves the right to amend this policy at any time without notice.

Information Systems Definitions:

- Electronic mail ("Email") is defined as an office communication tool whereby electronic messages are prepared, sent, and retrieved on personal computers and workstations.
- The GIAC ENTERPRISES local and external computer network (“Network”) includes but is not limited to all computers, network devices, communication hardware, software, and accounts that are connected together for the purpose of electronic communications and data sharing.
- On-line services (i.e., the Internet) are defined as communication tools whereby business information, reference material and messages are sent and received electronically.
- Other electronic equipment (i.e., fax machines and faxed messages, and PDA – personal digital assistant) and the media contained are defined as equipment used for electronic communication and data sharing.

Policies:

1. Information Systems remain the property of the company, and no employee should have any expectation of privacy concerning content. Information Systems are not the private property of any employee and should not be considered personal or confidential. Even when a message or material is erased, it may still be possible to retrieve and read it.
2. Use by an employee of Information Systems shall constitute express consent of the employee to monitor and/or disclose the contents. Authorized IT staff and management may audit, monitor, access, and disclose data sent from, received

by, and stored upon its Information Systems to ensure these systems are not abused or misused, and to ensure compliance with this policy, with or without notice to affected employees. GIAC ENTERPRISES Group also reserves the right to disclose information contained in employee assigned Information Systems to law enforcement or governmental officials or to other third parties, without notification or permission from the employees sending or receiving the messages. Such records and messages may be subpoenaed in connection with court or administrative proceedings.

3. Information Systems are intended for business purposes only
4. Personal use of Information Systems to solicit other persons, companies, or entities for commercial ventures, religious or political causes or other non-job-related solicitations is prohibited.
5. Information Systems may not be used in a way that may be disruptive, offensive to others, or harmful to morale.
6. Management of individually allocated Information Systems is the responsibility of the employee. Excessive use or abuse is unacceptable. It is the employee's responsibility to delete unneeded data in a timely manner, archive data that is not needed on active directories, and to keep distribution lists current.
7. Personal mail accounts such as AOL, Yahoo, or Hotmail may not be used for company business. The Company has strict security policies managed on the corporate mail system for all incoming and outgoing mail. Non-corporate accounts may only be accessed from a company computer with express authorization by IT.
8. GIAC ENTERPRISES will not forward communications received for former employees, to the former employee, or will GIAC ENTERPRISES advise the sender of a forwarding address. Action may be taken to forward communications to appropriate internal addresses.
9. Client Email addresses are to be protected and kept confidential. Any Email to multiple clients should not contain their address in the TO: field, but rather in the BCC: (Blind Carbon Copy) field. This ensures the confidentiality of addresses and eliminates the "Replies to All" option for anyone on the list, and the potential for spreading an electronic virus.
10. Log-on identifications and passwords are the property of GIAC ENTERPRISES and the use of passwords for security does not guarantee confidentiality. Employees may not disclose them to anyone. The employee/account holder is responsible for the account activity. An employee obtaining or attempting to obtain a password for an account that is not assigned to the employee is prohibited. Disclosure or discovery of another's account or password is not considered permission to use another employee's account, and is prohibited.
11. Actions that impede the normal operation of Information Systems are prohibited. This may include but is not limited to causing excessive network traffic or monopolizing public storage space.
12. The Information Systems must not be used to send or receive copyrighted materials, trade secrets, proprietary financial information, or other confidential information belonging to the Company to anyone outside the organization without prior management authorization.

13. No employee shall violate the terms of intellectual property rights. Using Information Systems resources in a manner that infringes upon the legal rights of another individual is prohibited.
14. Use of Information Systems' resources is subject to the regulation of the local, state, or country regulations. Abusing the computer and network resources may subject the employee to prosecution under local, state, federal/country or international law and the employee should expect GIAC ENTERPRISES to pursue such action.
15. Software Piracy - GIAC ENTERPRISES supports all copyright laws concerning proprietary data and software duplication. It is the responsibility of department management to administer this policy. All employees' use of computer software will adhere to copyright laws.
16. Employees may distribute "Public Domain" software with management's approval. "Public Domain" software should be analyzed for computer viruses prior to distribution. Anti-viral checking is the responsibility of the users and department management. There should be no expectation of support by IT, and use may be prohibited if system or network problems are suspected. Public Domain is defined as Software in which ownership has been relinquished to the public at large and is distributed without charge.
17. Disabling or uninstalling any software placed on the employees PC or workstation by the IT department, including AntiVirus software is prohibited.
18. Employees may not remove from the premises any hardware, software, files, or data without prior management authorization, and a completed Property Removal Form.
19. Employees are prohibited from connecting personally owned machines to the GIAC ENTERPRISES network without prior authorization from management and IT.
20. Mobile users must abide by these policies as well any site-specific remote policies.

To help clarify these policies, the following are examples of abuse and misuse of Information Systems.

Privacy and Access

a) Employees should not send, receive, or store sensitive personal or private information using GIAC ENTERPRISES Information systems
b) User accountability – Regardless of the circumstances, individual passwords must never be shared or revealed to anyone else besides the authorized user. To do so exposes the authorized user to responsibility for action another party takes with the password. If users need to share computer resident data, they should utilize message-forwarding facilities, public directories on local area network servers, and other authorized information-sharing mechanisms. To prevent unauthorized parties from obtaining access to Information Systems, users must choose a password that is in compliance with the written Password policy contained in this document.

c) Attempting to get false or misleading information to obtain an internal or external account on a Network resource or disguising or attempting to disguise the identity of an account or resource is prohibited. Using any local or external computer or network resources to gain unauthorized access to internal or external Information Systems is prohibited.
d) Misrepresenting, obscuring, suppressing, or replacing an employee's identity on an Information System is prohibited.
e) An employee shall not use another site's mail server to relay mail without the express permission of the site's owner.
f) Attempting to monitor or tamper with another's Information System communications, or reading, copying, changing, or deleting another person's files or software without the explicit agreement of the owner are all considered unacceptable and are prohibited.
g) Do not compromise the confidentiality of information accessed in the course of your daily activity. The information accessible through Information Systems is considered private to the organization, which owns or holds rights to them unless specifically stated. All work done by an employee is considered property of the company.
h) Circumventing or attempting to circumvent data protection schemes, security systems, or uncover security loopholes is prohibited. Interference with service to any employee, host or network including, without limitation, mail bombing, flooding, deliberate attempts to overload a system and broadcast attacks are all considered unacceptable and are prohibited. Employees may not use Information Systems to develop or send any virus or otherwise destructive program.
i) Obtaining or attempting to obtain an IP address without the consent of IT is prohibited. Electronic forging of any kind, or making of identities (Spoofing) to include but not limited to IP addresses, domains, business names, etc. are all considered unacceptable and are prohibited. If the network uses Dynamic Naming (DHCP), consent for a corporate system to obtain an IP address is assumed.

Harassment

j) Possession of sexually explicit images, messages, cartoons, chain letters or messages, or messages containing ethnic slurs, racial epithets, pornography, other discriminating content, or anything that could be construed as harassment or disparagement of others is inappropriate use of Information Systems and is prohibited.
k) Information Systems must not be used to visit sexually explicit or otherwise offensive or inappropriate Web sites, or to send, display, download or print offensive material, pornographic or sexually explicit pictures or any other materials which would be found offensive by most reasonable people.

Software Licensing

l) Distribution of any single licensed software product, or soliciting software from other employees, for the purpose of avoiding the licensing costs is prohibited

m) Installation or use of any single licensed software product on a network where other unlicensed employees would share that product is prohibited
n) Installation of unlicensed software is strictly prohibited. Unapproved software or use of software which does not have a license purchased by GIAC ENTERPRISES is prohibited. Management may approve exceptions, but the user must be able to produce a valid license if requested.
o) Information Systems shall not be used to make unauthorized, unlicensed, or illegal copies of any software or files including movie and audio files.

Resource Usage

p) Employees should be aware that Internet sites accessed from GIAC ENTERPRISES network might identify the employee as the originator of each visit. This may be regarded as representing GIAC ENTERPRISES. Thus, all communication should be professional, appropriate, and not adversely reflect on GIAC ENTERPRISES reputation.
q) Monopolizing Information System resources to the exclusion of others is considered unacceptable and is prohibited.
r) Information Systems may not be used for SPAM. Spam is defined as excessive posting or multiple posting unsolicited Email, and is explicitly prohibited.
s) Non-business related use of computer and network resources to play Internet computer games, participate in Internet Chat Rooms and News Groups, streaming audio/video is considered unacceptable.

Other

t) Properly identify the authorship and where applicable, the authority of the communication's intent. When stating your opinion, please identify this in your communication.
u) Managers must ensure temporary employees, contractors, and other visitors adhere to these policies.

GIAC Enterprises Virus Avoidance

Portions of the content contained in this section "Virus Avoidance" are from a downloadable document template from TechRepublic called "Virus Protection Policy" URL: http://techrepublic.com. This is a free download however it does require you to sign up for a free membership.

It is the responsibility of everyone who uses GIAC Enterprises computer network to take reasonable measures to protect our network from virus infections.

This document outlines how various viruses can infect GIAC ENTERPRISES network, how the IT department tries to prevent and/or minimize infections, and how our network users should respond to a virus if they suspect one has infected the GIAC ENTERPRISES network.

How viruses can infect the GIAC ENTERPRISES network

There are actually three various types of computer viruses: true viruses, Trojan horses, and worms. True viruses actually hide themselves, often as macros, within other files, such as spreadsheets or Word documents. When an infected file is opened from a computer connected to the GIAC ENTERPRISES network, the virus can spread throughout the network and may do damage. A Trojan horse is an actual program file that, once executed, doesn't spread but can damage the computer on which the file was run. A worm is also a program file that, when executed, can both spread throughout a network and do damage to the computer from which it was run.

Viruses can enter the GIAC ENTERPRISES network in a variety of ways:

1. **Email -** By far, most viruses are sent as Email attachments. These attachments could be working documents or spreadsheets, or they could be merely viruses disguised as pictures, jokes, etc. These attachments may have been knowingly sent by someone wanting to infect our network or by someone who does not know the attachment contains a virus. However, once some viruses are opened, they automatically email themselves, and the sender may not know his or her computer is infected.
2. **Disk, CD, Zip disk, or other media -** Viruses can also spread via various types of storage media. As with Email attachments, the virus could hide within a legitimate document or spreadsheet or simply be disguised as another type of file.
3. **Software downloaded from the Internet -** Downloading software via the Internet can also be a source of infection. As with other types of transmissions, the virus could hide within a legitimate document, spreadsheet, or other type of file.
4. **Instant messaging attachments -** Although less common than email attachments, more viruses are taking advantage of instant messaging software. These attachments work the same as Email viruses, but they are transmitted via instant messaging software.

Users can be tricked (Social Engineering) into installing any type of virus. For example, a Trojan horse might arrive in email described as a computer game. When the user receives the mail, they may be enticed by the description of the game to install it. Although it may in fact be a game, it may also be taking other action that is not readily apparent to the user, such as deleting files or mailing sensitive information to the attacker.

How the GIAC ENTERPRISES IT department prevents and/or minimizes virus infections

- **Scanning Internet traffic -** All Internet traffic coming to and going from our network must pass through company servers and other network devices. Only specific types of network traffic are allowed beyond the GIAC ENTERPRISES exterior firewalls.

For example, an Email message that originates outside of the network must pass through the Virus scanning software on our UNIX Sendmail server before it is allowed to enter the GroupWare Email servers. The Email is scanned a second time on the GroupWare servers before delivery. If at anytime a Virus is detected it is Quarantined and removed from the system.

- **Running server and workstation AntiVirus software -** All servers run AntiVirus software. This software scans all files saved to these servers.

  AntiVirus software is also installed on all GIAC ENTERPRISES workstations. This software scans all data written to or read from a workstation's hard drive. If it finds something suspicious, it isolates the dubious file on the computer and automatically notifies the help desk.

- **Routinely updating virus definitions -** periodically, the AntiVirus management server checks the AntiVirus update site for updated definition files. These definition files allow the software to detect new viruses. If a new virus definition file is available, the virus scanning software is automatically updated, and then the system administrator is informed.

  When end users turn on their computers at the beginning of the workday, the workstation virus protection program checks with the AntiVirus management server on our network for updates. The workstation program will then download and install the update automatically, if one exists.

How to respond to and report a virus

Even though all Internet traffic is scanned for viruses and all files on the company's servers are scanned, the possibility still exists that a new or well-hidden virus could find its way to an employee's workstation, and if not properly handled, it could infect GIAC Enterprises network.

The IT staff will attempt to notify all users of credible virus threats via Email or telephone messages. Because this notification will automatically go to everyone in the organization, employees should not forward virus warning messages. On occasion, well-meaning people will distribute virus warnings that are actually virus hoaxes. These warnings are typically harmless; however, forwarding such messages unnecessarily increases network traffic.

As stated, it is the responsibility of all GIAC Enterprises network users to take reasonable steps to prevent virus outbreaks. Use the guidelines below to do your part:

- Update your anti-virus software files regularly. Over 500 viruses are discovered each month. Your Virus software should be configured to receive Virus definition updates from our internal servers however, you can run the LiveUpdate process at anytime. Simply open the AntiVirus application and press the LiveUpdate button.

- Never open an unexpected Email attachment unless you are sure it is from a trusted source (and that your trusted source really meant to send it). The old rule was "never open attachments from people you don't know." The new rule is "never open attachments unless you know why you received them." Newer viruses can copy a friend's list of Email addresses out of an Email program and can generate a message to you with an infected file. Never open attachments with the .exe, .com, .vbs, .lnk, .bat or .pif extension. Keep in mind that viruses usually come from someone you know.
- Delete chain emails and junk email. These types of email are considered Spam, which is unsolicited, intrusive mail that clogs up the network. Do not forward or reply, unsubscribe at your own risk. A common trick spammers use is to get you to unsubscribe so they can validate your Email address. If you respond, they've connected; you are a real person. They can add your Email address to a list that they will use or sell. On the other hand, a company you recognize and trust may inadvertently Spam you due to bad Email management. By responding, you've done them a service. So, if you don't recognize the mailer, you probably shouldn't unsubscribe.
- Avoid publicizing your Email address. The more your Email address is seen on Internet bulletin boards and in newsgroups, chat rooms and the like, the more likely you to receive unsolicited Email.
- Never download freeware or shareware from the Internet without express permission of the IT department or your Supervisor.
- If a file you receive contains macros that you are unsure about, disable the macros.

Notify the help desk of all suspicious files

If you receive a suspicious file or Email attachment, do not open it. Call GIAC ENTERPRISES help desk at extension xxxx (xxxx) xxx-xxxx and inform the support analyst that you have received a suspicious file. The support analyst will explain how to handle the file.

If the potentially infected file is on a disk that you have inserted into your computer, the AntiVirus software on your machine will ask you if you wish to scan the disk, format the disk, or eject the disk. Eject the disk and contact the help desk at extension xxxx (xxx) xxx-xxxx. They will instruct you on how to handle the disk.

After the support analyst has neutralized the file, send a note to the person who sent/gave you the file notifying them that they sent/gave you a virus. (If the file was sent via Email, the AntiVirus software running on our Email system will automatically send an Email message informing the sender of the virus it detected.)

If the file is an infected spreadsheet or document that is of critical importance to GIAC ENTERPRISES, the IT department will attempt to scan and clean the file. The IT department, however, makes no guarantees as to whether an infected file can be totally cleaned and will not allow the infected file to be used on GIAC ENTERPRISES computers.

Password Guidelines

Passwords are the last line of defense before a system is compromised. A poorly selected password could expose a single account, a single computer, all trusted hosts or potentially the entire network to unauthorized entry. The object when choosing a password is to make it as difficult as possible for anyone or any process to make educated guess about what you've selected.

What Not to Use

- Don't use your login name in any form (as-is, reversed, capitalized, doubled, etc.).
- Don't use your first or last name in any form.
- Don't use your spouse or child's name.
- Don't use other information easily obtained about you. This includes license plate numbers, telephone numbers, social security numbers, the brand of your automobile, the name of the street you live on, etc.
- Don't use a password of all digits, or all the same letter. This significantly decreases the search time for a cracker.
- Don't use a word contained in (English or foreign language) dictionaries, spelling lists, or other lists of words.
- Don't use a password shorter than six characters.

What to Use

- Do use a password with mixed-case alphabetic characters.
- Do use a password with non-alphabetic characters, e.g., numeric or punctuation.
- Do use a password that is a least six characters in length.
- Do use a password that is easy to remember, so you don't have to write it down.
- Do use a password that you can type quickly, without having to look at the keyboard. This makes it harder for someone to steal your password by watching over your shoulder.

Method to Choose Secure and Easy to Remember Passwords

- Choose a line or two from a song, poem or make up a phase, and use the first letter of each word. For example, "Default Operating System Installations are very insecure" would be "dosiavi"
- Use a combination of upper and lower case and alternate between alpha and numeric characters. For example, "Default Operating System Installations are very insecure" would be "D0S1av1" the number 0 was substituted for the letter O and the number 1 was substituted for the letter i. Other common substitutions are 2 for Z, 5 for S, 6 for b, and 9 for g.

Remote Access - Telecommuting Guidelines

Until recently, remote access to the GIAC ENTERPRISES network was characterized by dial-up users accessing our network to read Email. The communications

infrastructure supporting this type of connection, is relatively secure, and poses little or no threat to communications integrity or confidentiality of our internal network. The exceptions are the identification of the phone number required to make the connection and the compromise of the shared secrets (username and password).

Remote access from the Internet is fundamentally the same when compared to a dial-up connection. The major difference is in the entry point. Remote clients are authenticated at our Firewall. The Internet has made it possible for a remote user to connect to our Network from virtually anywhere in the world. Opening up our borders to include the Internet, as an access median to our internal network requires that we extend our security control to the authorized remote user and they're computers.

Requirements

Remote Access into our networks from the Internet requires that each individual user be trained on how to continually monitor and maintain their remote computer. For this reason approval for remote access must come from your Supervisor. Each user requesting remote access must successfully complete the following training courses.

1. GIAC ENTERPRISES Cable/DSL router. This class teaches the basic setup, configuration and connection of the router to the Internet. This prevents the Remote Users Computer from being connected directly to the Internet.
2. GIAC ENTERPRISES VPN software. This class teaches the remote user how to load and verify that the VPN software is working correctly and the steps in the authentication process.
3. GIAC ENTERPRISES Personal Firewall software. This class teaches the remote user how to load and verify that the Personal Firewall software is working correctly.
4. GIAC ENTERPRISES Anti-Virus software. This class teaches the remote user how to load and verify that the Anti-Virus software is working correctly and how to verify definition files and manually download and install them if necessary.
5. GIAC ENTERPRISES system update and maintenance. This class teaches how to update the Operating System software when security patches or updates are released by the vendor.

Conditions

Finally each remote users will be required to sign an acceptable use policy. This is a simply document outlining the following conditions.

- The remote user is expected maintain updated and operational AntiVirus software.
- The remote user is expected to always have the Personal Firewall software running.
- The remote user is expected to maintain all vendor supplied updates once approval is given by the GIAC ENTERPRISES security department.
- The remote user is the only person that is allowed access to the GIAC ENTERPRISES resources.

- The remote user understands and will permit the GIAC ENTERPRISES security department to scan or otherwise attempt breach security being maintained by the remote user.
- The remote user agrees that is their responsibility to report all unusual system events to the GIAC ENTERPRISES security department.

Failure to comply with any of the above conditions is grounds to revoke your remote access status.

System Administration Guidelines

It is the responsibility of the System Administrator to ensure that the systems under their control are available when needed. That confidential information is only available to those with authorized access and that the systems hosting this information are not subject to unauthorized changes or entry.

Security responsibilities

Assurance

- Only system administrators should install or update software on servers. Users may not install software on Internet accessible hosts.
- Systems should be cleanly installed according to the following Operating System Installation Checklists.
  - Unix Security Checklist ver. 2.0[11]
  - Windows NT Configuration guidelines[12]
  - Linux Systems Installation Guidelines[13]
- Disable or remove all services that are not necessary, within the scope or functionally of the Host.
- OS installations and routine maintenance should include the latest recommended patches.
- Only patches from the original software vendor should be applied. Patches should be pre-tested in a test environment, before being applied to production systems.
- Before a Computer is move into production, system administrators will install and run the CIS Security Benchmarks and Scoring Tool[14]. The Computer must meet the minimum-security levels established by GIAC Enterprises for the OS and the Service it will be performing. System administrators are expected to run the CIS scoring tool on a regular basis to monitor the state of the systems security. Updated information on the latest Benchmarks, Scoring Tools and Checklist can be found at Security Consensus Operational Readiness Evaluation (S.C.O.R.E.), URL:http://www.sans.org/score/ or The Center for Internet Security (CIS), URL:http://www.cisecurity.org/
- Disable dynamic routing protocols and remove all services that allow packet forwarding.

- Changes made to a system should be logged in the GIAC Enterprises change log files. At minimum, the log should contain a description of the change and a reason/comment.
- Labels containing the following information should be attached to all machines during installation: Hostname, Machine, IP address(s), MAC address(s), and System Administrators contact information.
- System Administrators will provide GIAC Enterprises, Computer Security Incident Response Team with a currently valid Root/Administrator equivalent Username and Password. The Computer Security Incident Response Team will be notified when changes have been made to this Username or Password.
- System Administrators should stay current with security trends and News. Recommended Internet Security resources are:
  - SANS Information Security Reading Room[15]. This site contains Security news and information.
  - CERT® Coordination Center[16] (CERT/CC) studies Internet security vulnerabilities, handles computer security incidents, publishes security alerts, researches long-term changes in networked systems, and develop information and training to improve Internet Security.
  - Internet Storm Center[17] is a virtual organization of advanced intrusion detection analysts, forensic experts and incident handlers from across the globe. This site consolidates vulnerability data, attack statistics, and general security news in order to create a daily common operational picture of the Internet.
  - GIAC ENTERPRISES strongly recommends that System Administrators subscribe to the CERT Advisory Mailing List[18] and the SANS Newsletter Subscription Service[19].

Identification / Authentication

- User passwords should be unique: (See Selecting Good Passwords).
- Change all default passwords - Many operating systems and application programs are installed with default accounts and passwords. These must be changed immediately to something that cannot be easily guessed or cracked.
- Accounts should only exist for authorized persons, these should allow minimum privileges. When a user is transferred or terminates employment, his/her account should be blocked or deleted immediately.
- Each user must be identified by a name or number and belong to a group. If guest accounts are used, their working environment should be very restricted. It is highly recommend that Guest/Anonymous accounts be disabled on all Internet accessible hosts.
- User accounts and groups should be managed by the administrator (or equivalent), not by users themselves.
- Screen locks or screen savers should be activated after 15 minutes idle time with password protection.
- Systems discovered with null passwords on Username will be disconnected from the Internet/Network immediately.

- If an account is subjected to continuous login failures in short period of time, block or lock the account and notify the account owner.
- Post a legal notice (See Appendix A Sample Banner Page) informing the user of implications of system abuse.
- Logons should only be enabled when necessary (e.g. between 06:00 and 22:00 Monday to Friday.)
- Avoid allowing direct Administrator/Root logon, especially where more than one person administers a system.

Educate your users to keep their accounts secure.

- Users should never lend their accounts to someone else.
- Users should be careful about what other accounts they trust.
- Users should pick good passwords (See Selecting Good Passwords)
- Users should not leave their passwords lying around, written on a Post-It stuck to the computer etc.

On Dialup systems:

- If a user enters a bad login name or password, the error message should be the same for both cases. A possible attacker should not be informed if a user account is valid, The message should simply state that the authentication has failed.
- Configure Dialup systems to disconnect the phone line after 3 unsuccessful login attempts.

Accountability/Audit Trail

- Logging should be enabled to automate audit trail monitoring and analysis to detect security breaches.
- Audit trail logs and programs/utilities should only be accessible to the Administrator/Root equivalent accounts.
- System Administrator activity (Administrator/Root) should be logged.
- Unsuccessful login attempts should be logged, and accounts automatically locked after 3 unsuccessful attempts.
- All production systems will have Network Time Services install and set to retrieve system time from GIAC Enterprises Central Time server.
- When possible important events should trigger system alarms/Email alerts automatically.
- System Administrators should do routine checks of their systems. These checks should include the following:
  - Check log files. (Not just for security incidents; look for other system problems too.)
  - System baselines, what would be normal – CPU utilization, Disk capacity, Daily Log file size and average number of logins.
  - Look for any changes to access controls, user accounts or system files.

Systems without effective logging are blind and make it difficult to learn what happened during an attack, or even whether an attack actually was successful.[20]

Access Control

- All systems that require authentication or privileged access should present an online warning Banner Page to inform each user of the rules for access to the system. Without these warning, internal or external attackers can often avoid prosecution. (See Appendix A Sample Banner Page).

- All users should be authorized. Access to all objects on the system should be controlled (files, printers, devices, databases, commands, applications etc.).
- Users should only be able to set the privileges of objects belonging to them in their environment.
- Administrator/ Root login should only be allowed via the System Console.
- Users should not be able to examine the Access Control granted to other users.

Reliability of Service

- System configuration, user files and database backups will be preformed daily.
- Backups will be normal so that the archive bit is set when the information changes.
- If possible, backups will be conducted after business or at low activity times.
- All system administrators will use GIAC Enterprises backup system. It is their responsible to load the client application and make the node available for backup.
- All system administrators will check the restore procedures monthly. Restore test will be conducted to separate restore test area on the system. Data integrity will be conducted on restored files.

Network Systems Guidelines

It is the responsibility of the Network Operations Staff to ensure that the Physical Networks under their control are available when needed. That confidential information is only available to those with authorized access and that the Enterprise Networks are not subject to unauthorized changes or entry.

Security responsibilities

Assurance

- All IP addresses must be requested through Network Operations. Requests can be submitted on-line through the GIAC Enterprises IP Address request form or in person at the Help Desk. Each IP address will be stored in the IP Maintenance database and updates are sent to our internal DNS server.
- Copies of all Router configuration files will be stored in text file format, backed up on a separate Host. Network Operations Staff will supply the GIAC Enterprises Computer Security Incident Response Team with a currently valid Root/Administrator/Enable equivalent Username and Password. The GIAC Enterprises Computer Security Incident Response Team will be notified when changes have been made to this Username or Password.
- All Cisco Routers will be audited using the CIS Security Benchmarks and Scoring Tool. Network System administrators are expected to run the CIS scoring tool on a regular basis to monitor the state of the systems security. Updated information on the latest Benchmarks, Scoring Tools and Checklist can be found at Security Consensus Operational Readiness Evaluation (S.C.O.R.E.), URL:http://www.sans.org/score/ or The Center for Internet Security (CIS), URL:http://www.cisecurity.org/
- Physical Switch/Hub port connection information is located with the IP maintenance database.
- GIAC ENTERPRISES Corporate WAN information and statistics are located on the GIAC Enterprises network operation Web portal.
- GIAC ENTERPRISES Corporate Server information and statistics are located on the GIAC Enterprises network operation Web portal.

Identification / Authentication

- Computers on the GIAC ENTERPRISES network will have a documented IP address, Host name and operator. This information will be stored in IP Maintenance database.
- All Routers and Switches that require authentication or privileged access should present an online warning (Banner Page) to inform each user of the rules for access to the system. Without these warnings, internal or external attacker's can often avoid prosecution. (See Appendix A Sample Banner Page).
- Default system accounts should be deleted, disabled or renamed.
- Every username or system account should have a unique password.

- Systems discovered with null passwords on username will be disconnected from the Internet/Network immediately.

Accountability/Audit Trail

- All users are accountable for their actions and the computers that they are assigned too.
- All network traffic in and out of the GIAC Enterprise network will be log to file. These log files will be archive to CD-ROM on a monthly basis.
- GIAC Enterprise Firewall log files will be regularly analyzed for security breaches.
- The Access Control Lists of the GIAC Enterprise border routers will be audited monthly.

Access Control

- All network routers will be labeled by IP Network address in and out.
- All perimeter routers should be configured according to the document title "Help Defeat Denial of Service Attacks: Step by Step"[21] located on SANS Web site. This document contains step by step instructions for immediate actions requested of all organizations connected to the Internet. These procedures will reduce the chances that our network could be used to damage other networks.

  The following is a list of source addresses that should be filtered at the perimeter routers.

  0.0.0.0/8 - Historical Broadcast
  10.0.0.0/8 - RFC 1918 Private Network
  127.0.0.0/8 - Loopback
  169.254.0.0/16 - Link Local Networks
  172.16.0.0/12 - RFC 1918 Private Network
  192.0.2.0/24 - TEST-NET
  192.168.0.0/16 - RFC 1918 Private Network
  224.0.0.0/4 - Class D Multicast
  240.0.0.0/5 - Class E Reserved
  248.0.0.0/5 - Unallocated
  255.255.255.255/32 - Broadcast
  xxx.xxx.xxx.xxx/16 -GIAC Enterprise Network

  In addition to reviewing and implementing the above recommendations, information contained in the "Consensus Roadmap for Defeating Distributed Denial of Service Attacks"[22] should be reviewed.

The following is a list of service ports that should be filtered at the perimeter routers.

Service Name	Port Number	Protocol
Bootp	67	udp
Trivial File Transfer Protocol	69	udp and tcp
Sun Remote Procedure Call	111	udp and tcp

Simple Network Management Protocol	161	udp
Simple Network Management Protocol Traps	162	udp
NetBios Name Service	137	udp and tcp
NetBios Datagram Service	138	udp and tcp
NetBios Session Service	139	udp and tcp
Microsoft-ds	445	tcp and udp
Routing Information Protocol	520	udp
Echo		icmp
Echo-reply		icmp

Additionally the ports listed at - SANS What port numbers do well-known trojan horses use? URL: http://www.sans.org/resources/idfaq/oddports.php should also be monitored.

Reliability of service

- The network is required 24 hours, 7 days a week. Maintenance window Saturday 06:00-0800.
- Maximum down time during office hours shall be 15 minutes, maximum frequency once every two months.
- The network shall be monitored for errors and performance problems. Preventative action should be taken before serious network disruptions occur, where possible.
- Updates and configuration changes shall be logged in to the GIAC Enterprise Network Operations log files.
- All Network devices will be labeled with the following information. Hostname, IP address, MAC address, cabling node ID and helpdesk telephone number.

GIAC ENTERPRISE - Wireless Network Architecture and Connection Procedures

The purpose of this document is to establish procedures to ensure the Appropriate level of protection for GIAC ENTERPRISE data communication over wireless forms of transmission and reception

Much of the content contained in this section “Wireless Security Threats” is from David Chye Hock Quay, “Formulating A Wireless LAN Security Policy: Relevant Issues, Considerations and Implications.”
URL:http://www.giac.org/practical/David_Quay_GSEC.doc

WIRELESS SECURITY THREATS

All wireless computer systems face security threats that can compromise its systems and services. Unlike our wired corporate network, the intruder does not need physical access in order to pose the following security threats:

Security and access control unless steps are taken to protect them; wireless LAN installations are open to anyone within range of the access point. If a wireless access point is connected to the GIAC ENTERPRISE network without restrictions, anyone with

the proper equipment will be able to access the GIAC ENTERPRISE network, even from outside the building.

Eavesdropping this involves attacks against the confidentiality of the data that is being transmitted across the network. In the wireless network, eavesdropping is the most significant threat because the attacker can intercept the transmission over the air from a distance away from the premise of the company.

Tampering the attacker can modify the content of the intercepted packets from the wireless network and this result in a loss of data integrity.

Unauthorized access and spoofing the attacker could gain access to privileged data and resources in the network by assuming the identity of a valid user. This kind of attack is known as spoofing. To overcome this attack, proper authentication and access control mechanisms need to be put up in the wireless network.

Denial of Service In this attack, the intruder floods the network with either valid or invalid messages affecting the availability of the network resources. The attacker could also flood a receiving wireless station thereby forcing to use up its valuable battery power.

Other security threats. The other threats come from the weakness in the network administration and vulnerabilities of the wireless LAN standards, e.g. the vulnerabilities of the Wired Equivalent Privacy (WEP), which is supported in the IEEE 802.11 wireless LAN standard.

SCOPE

These procedures shall apply to all employees, contractors, consultants, temporaries, and other workers at GIAC ENTERPRISE, including those workers affiliated with third parties who access GIAC ENTERPRISE information systems and networks. These procedures apply to all wireless computer and data communication systems owned by and/or administered by GIAC ENTERPRISE Currently.

General Rules

All data communication and activity within the Wireless network will be considered UN-trusted.

Access to the Internet will be controlled in the same manner as our Corporate LAN. All users on the Wireless network must follow the conditions and terms of the GIAC ENTERPRISE Information Systems Policy.

IP Addressing will be via DHCP only. No static addressing will be supported.
The Wireless system is provided as a supplement to the “wired” network, not a replacement of it. It is intended more for convenience than for business critical application use.

User Security Awareness

Users shall never assume privacy when using a wireless access system. It is the sole responsibility of the user to ensure their privacy and the protection of privileged information and / or intellectual property.

All users connecting to the wireless network must agree to all of the terms set fourth under the Remote Access - Telecommuting Guidelines section of this document.

Access Points Administration and Maintenance

- Access points will be wired into the buffer zone. This buffer zone is defined as the area between the Firewall and the Internet border router.
- Access to GIAC ENTERPRISE internal systems and data will only be allowed via GIAC ENTERPRISE VPN software. This virtual private network (VPN) runs transparently over a wireless LAN. The VPN also allows authentication, which ensures that only authorized users can send and receive information over the wireless LAN.
- Each Wireless network card must be registered at the Access Point, this is called MAC address control. This causes the Access Point only to talk to specific wireless devices that are registered.
- The Access Points will be controlled and monitored by GIAC ENTERPRISE Network operations staff.
- The Access Point will have IP address and port filtering enabled. Outbound and inbound traffic is subject to the filters that are applied to our corporate network.
- The Access Point should have system logging capability.

Incident Handling Guidelines

Much of the content contained in this section Incident Handling Guidelines, is from Request for Comments document (RFC 2196) "Site Security Handbook" URL:http://www.faqs.org/rfcs/rfc2196.html, It is after all, the intended purpose of (RFC 2196) "to provide practical guidance to administrators trying to secure their information and services. The subjects covered include policy content and formation, a broad range of technical system and network security topics, and security incident response."

This section contains guidelines that should be followed if there is a suspicion our Network or one of its Hosts may have suffered a break-in or other type of security incident.

The best way to handle an incident is to stop it from happening in the first place. Security is everyone's responsibility.

Security Incident Definition

Security is understood to include protection of the privacy of information, protection of information against unauthorized modification, protection of systems against unauthorized access and protection of systems against denial of service.

Listed below are activities that are recognized as being in violation of our GIAC Enterprise security policy. These activities include but are not limited to:

- Any Attempt (either failed or successful) to gain unauthorized access to any system or it's data.
- Any unauthorized use of any system for the processing or storage of data.
- Any unwanted disruption or denial of service.
- Any changes to any system hardware, firmware, or software characteristics without the Network / Systems Administrators knowledge, instruction, or consent.

GIAC Enterprise encourages anyone to report any activities that meet these criteria for being an incident. Local and/or federal laws may further dictate your behavior regarding the handling of computer security incidents.

- GIAC Enterprise Security response hotline – (xxx) xxx-xxxx
- GIAC Enterprise Help Desk – (xxx) xxx-xxxx
- Email - systemsecurity@GIACEnterprises.com

Did a Security Incident really occur?

Many of the signs often associated with virus infection, system intrusions, malicious users, etc., are simply anomalies such as hardware failures or suspicious system/user behavior. To assist in identifying whether there really is an incident, it is very important to capture an accurate picture of the system as soon as possible. Audit information is also extremely useful, especially in determining whether there is a network attack.

Obtain a system snapshot as soon as you suspect that something is wrong. Many incidents cause a dynamic chain of events to occur, and an initial system snapshot may be the most valuable tool for identifying the problem and any source of attack. Finally, it is important to start a logbook. Recording system events, telephone conversations, time stamps, etc., can lead to a more rapid and systematic identification of the problem, and is the basis for subsequent stages of incident handling.

Indicators or "symptoms" that an incident may have happened

- System crashes or hangs.
- Unexplained new user accounts, or high activity on a previously low usage account.
- Unexplained new files or unfamiliar (usually with novel or strange file names).
- Accounting discrepancies (in a UNIX system you might notice the shrinking of an accounting file called /usr/admin/lastlog, something that should make you very suspicious that there may be an intruder).
- Unexplained changes in file lengths or dates especially in system executables files.
- Unexplained attempts to write to system files or changes in system files.
- Unexplained data modification or deletion (files start to disappear).
- Denial of service or inability of one or more users to login to an account.

- Unexplained, poor system performance
- Suspicious probes (there are numerous unsuccessful login attempts from another node).
- Suspicious browsing (someone becomes a Root/Administrator and accesses file after file on many user accounts.)
- Unusual time of usage (more security incidents occur during non-working hours than any other time).
- An indicated last time of usage of a user account that does not correspond to the actual last time of usage for that user

By no means is this list comprehensive; just a short list of common indicators. It is best to collaborate with other technical and computer security personnel to make a decision as a group about whether an incident is occurring.

Steps in Evidence Collection:

1. Capture as accurate a picture of the system as possible.
2. Keep detailed notes. These should include dates and times of suspicious events.
3. Minimize changes to the data as you are collecting it. This is not limited to content changes; you should avoid updating file or directory access times.
4. When confronted with a choice between collection and analysis you should do collection first and analysis later.
5. Remove all external avenues for change or access.

Security Incident Notification

Anyone suspecting that a Security Incident has occurred should notify the GIAC ENTERPRISES Computer Security Incident handling team at the GIAC Enterprise Security response hotline – (xxx) xxx-xxxx, additional the following groups of people should be notified.

- Network / System Administrator, Administrative contacts of affected servers and involved sites.
- Internal communications. Notification by an all GIAC ENTERPRISES Email, if systems are available. This should include a brief description of the incident and corrective action or current status.
- Law enforcement and investigative agencies. In the event of an incident that has legal consequences, it is important to establish contact with investigative agencies (e.g. the Local Law enforcement and the FBI.) as soon as possible
- Notification of the GIAC ENTERPRISES Public relations department.

Protecting Evidence and Activity Logs

Document all details related to the security incident. This will provide valuable information to yourself and others as you try to unravel the course of events. Recording details will provide evidence for prosecution efforts, providing the case moves in that direction. Documenting an incident will also help you perform a final assessment of damage (something management, as well as law enforcement officers, will want to

know), and will provide the basis for later phases of the handling process: eradication, recovery, and follow-up "lessons learned."

At a minimum, the following information should be recorded to log:

- All system log files (Web Server Logs)
- All system events (audit records)
- All actions you take (time tagged)
- All external conversations (including the person with whom you talked, the date and time, and the content of the conversation)

This information will be maintained in electronic log files, located at GIAC ENTERPRISES network operations web site accessible from any Computers browsers. Events recorded to this file will be a centralized, chronological source of information when you need it, instead of requiring you to page through individual sheets of paper. Much of this information is potential evidence in a court of law.

Type and Scope of the Security Incident

Along with the identification of the incident is the evaluation of the scope and impact of the problem. It is important to correctly identify the boundaries of the incident in order to effectively deal with it and prioritize responses.

In order to identify the scope and impact a set of criteria should be defined which is appropriate to the site and to the type of connections available.

Some of the issues include:

- Is this a multi-site incident?
- Are many computers at your site affected by this incident?
- Is sensitive information involved?
- What is the entry point of the incident (network, phone line, local terminal, etc.)?
- What is the potential damage of the incident?
- What resources could be required to handle the incident?
- Is the press involved? If so has the GIAC ENTERPRISES Public relations department been notified.
- Should law enforcement be notified?

Assessing the Damage and Extent

The analysis of the damage and extent of the incident can be quite time consuming, but should lead to some insight into the nature of the incident, and aid investigation and prosecution. As soon as the breach has occurred, the entire system and all of its components should be considered suspect. System software is the most probable target. Preparation is key to be able to detect all changes for a possibly tainted system.

Assuming original vendor distribution media are available, an analysis of all system files should commence, and any irregularities should be noted and referred to all parties involved in handling the incident. It can be very difficult, in some cases, to decide which

backup media are showing a correct system status. Consider, for example, that the incident may have continued for months or years before discovery, and the suspect may be an employee of the site, or otherwise have intimate knowledge or access to the systems. In all cases, the pre-incident preparation will determine what recovery is possible.

If the system supports centralized logging, go back over the logs and look for abnormalities. If process accounting and connect time accounting is enabled, look for patterns of system usage. To a lesser extent, disk usage may shed light on the incident. Accounting can provide much helpful information in an analysis of an incident and subsequent prosecution. Your ability to address all aspects of a specific incident strongly depends on the success of this analysis.

Security Incident Containment

The purpose of containment is to limit the extent of an attack. An essential part of containment is decision making (e.g., determining whether to shut a system down, disconnect from a network, monitor system or network activity, set traps, disable functions such as remote file transfer, etc.).

Sometimes this decision is trivial; shut the system down if the information is classified, sensitive, or proprietary. Bear in mind that removing all access while an incident is in progress obviously notifies all users, including the alleged problem users, that the administrators are aware of a problem; this may have a deleterious effect on an investigation. In some cases, it is prudent to remove all access or functionality as soon as possible, then restore normal operation in limited stages. In other cases, it is worthwhile to risk some damage to the system if keeping the system up might enable you to identify an intruder.

Acceptable Risks: (System may remain on-line)

- Nuisance (non-destructive) Virus/Worm infections.
- Compromise of non-critical User accounts.

Unacceptable Risks: (System must be taken off-line and rebuilt)

- System or Root level compromise.
- Compromise of confidential information.
- Alteration of critical System files.
- Malicious (destructive) Virus/Worm that threatens other connected systems.

Recovering from an Incident

CERT® Coordination Center.

Links to CERT® Coordination Center - documents related to Security Incident recovery.

- **Steps for Recovering from a UNIX or NT System Compromise**
  URL:http://www.cert.org/tech_tips/win-UNIX-system_compromise.html, provides help with recovering from a computer security compromise.

- **The Intruder Detection Checklist** URL:http://www.cert.org/tech_tips/intruder_detection_checklist.html, and Windows NT Intruder Detection Checklist URL:http://www.cert.org/tech_tips/win_intruder_detection_checklist.html, help you to determine whether or not your system may have been compromised.
- **The UNIX Configuration Guidelines** URL:ttp://www.cert.org/tech_tips/unix_configuration_guidelines.html, includes descriptions of common UNIX system configuration problems that have been exploited by intruders and recommended practices that you can use to help deter several types of break-ins.
- **Windows NT Configuration Guidelines** URL:http://www.cert.org/tech_tips/win_configuration_guidelines.html, does the same for Windows NT systems.
- **The List of Security Tools** URL: http://www.cert.org/tech_tips/security_tools.html, provides information about tools to help you secure your system and deter and detect break-ins.
- **Windows NT Security and Configuration Resources** URL: http://www.cert.org/tech_tips/win-resources.html, points to resources for Windows systems.

CERT® Coordination Center also offers tech tips URL: http://www.cert.org/tech_tips/, on various incident types, including denial of service attacks URL:http://www.cert.org/tech_tips/denial_of_service.html, email bombing and spamming URL:http://www.cert.org/tech_tips/email_bombing_spamming.html, and problems with viruses URL:http://www.cert.org/tech_tips/virusprotection.html and more.

Summary:

Internet security is evolving into a set of generally accepted principles and best practices. Security is not complete after a policy is in place; it is work in progress, it is a constantly moving target, it is a game and we as security practitioners control the playing field. We can diligently protect the assets under our control by proper planning, constant assessment and fine-tuning our defense.

I believe that this paper has covered all aspects of what would be considered Industry best practices and common sense security measures. The true test of due diligence is not in the policy but in its enforcement.

Appendix A - Sample Banner Page

```
##########################################################################
#                                                                        #
#  GIAC Enterprises                                                      #
#                                                                        #
#                                                                        #
#                                                                        #
#   WARNING:    You are requesting access to a secure                    #
#               service. This service is being provided                  #
#               for AUTHORIZED PERSONNEL ONLY !                          #
#               You must have a valid USERNAME and                       #
#               PASSWORD that has been assigned to you                   #
#               by the GIAC Enterprises security administrator           #
#                                                                        #
#   NOTICE:     All access to this service is MONITORED.                 #
#                                                                        #
#                                                                        #
##########################################################################
```

Appendix B - Security Links

The purpose of the information contained in this appendix is to improve the ability of the Network / System Administrators to secure the systems which they are responsible for. Network / System Administrators are strongly encouraged to get all security advisories that pertain to your system(s), and to install the patches or workarounds described in the advisories. They are also encouraged to check with vendor(s) regularly for any updates or new patches that relate to their systems.

The CERT® Coordination Center URL:http://www.cert.org, publishes Current Activity URL:http://www.cert.org/current/current_activity.html, which is a regularly updated summary of the most frequent, high-impact types of security incidents and vulnerabilities currently being reported. Incident notes URL:http://www.cert.org/incident_notes, provide the Internet community with information about current intruder activity. They also publish vulnerability notes URL:http://www.cert.org/vul_notes that provide information about vulnerabilities to the user community.
Technological holes account for a great number of the successful break-ins, but people do their share, as well. Here is a list of Common Security Mistakes URL:http://www.sans.org/resources/mistakes.php, people make that lead to Computer Security Vulnerabilities. Finally, make sure to review How To Eliminate The Ten Most Critical Internet Security Threats URL: http://www.sans.org/top20/top10.php, The Experts' Consensus.

CERT® Coordination Center

- CERT/CC® Security Improvement Modules URL:http://www.cert.org/security-improvement/
- Security Improvement Incident Notes and Vulnerability Notes URL:http://www.cert.org/nav/securityimprovement.html
- Basic information on a variety of Internet security issues. URL:http://www.cert.org/tech_tips/
- Security Tools: Information and Sources URL:http://www.cert.org/other_sources/tool_sources.html
- Training and Education in Network Computing Security URL: http://www.cert.org/nav/training.html
- CERT Alerts Url:http://www.cert.org/nav/alerts.html
- Other Incident Response Teams and Security-Related Organizations URL: http://www.cert.org/other_sources/other_teams.html

Internet Security Information

- AntiOnline maximum Security for the Online World, URL: http://www.antionline.com/
- The Center for Internet Security (CIS), is a not-for-profit cooperative enterprise that helps organizations reduce the risk of business and e-commerce disruptions

resulting from inadequate security configurations. Home of the CIS Benchmark and Scoring Tools URL:http://www.cisecurity.org/

- Common Vulnerabilities and Exposures (CVE). A list of standardized names for vulnerabilities and other information security exposures URL: http://cve.mitre.org/
- Public Security Groups and Organizations, URL:http://www.alw.nih.gov/Security/security-groups.html
- Computer Security Resource Center, URL:http://csrc.ncsl.nist.gov/
- Department of Energy CIAC - Computer Incident Advisory Capability, URL:http://ciac.llnl.gov/
- Internet FAQ Archive, RFC Information and More, URL:http://www.faqs.org/rfcs/
- United States Department of Homeland Security, Federal Computer Incident Response Capability URL:http://www.fedcirc.gov/
- Guidelines for the Secure Operation of the Internet, RFC 1281 URL:http://www.faqs.org/rfcs/rfc1281.html
- Internet Assigned Numbers Authority, (Iana), URL: http://www.iana.org
- Security Newgroups pointers to the USENET newsgroups that provide information about computer security, URL:http://www.alw.nih.gov/Security/security-newsgroups.html
- Symantec – Security Check, Internet Security for the Home URL:http://security.symantec.com/ssc/home.asp?langid=ie&venid=sym&plfid=23&pkj=AEGNESLHFEPGEVVSDUX
- World Wide Web Consortium W3C Technology and Society Domain, W3C Security Resources URL:http://www.w3.org/Security/

Linux Security Information

- Lance Spitzner, Armoring Linux, URL:http://secinf.net/info/unix/lance/linux.html
- LinuxSecurity.com, Linux Security Documentation, URL:http://www.linuxsecurity.com/news/articles_documentation-1.html

Microsoft Windows Security Information

- Lance Spitzner, Armoring Windows NT URL:http://secinf.net/info/unix/lance/nt.html
- Steve Gibson, Gibson Research Corporation, ShieldsUP, URL:http://grc.com/x/ne.dll?bh0bkyd2, Internet Security Check for Windows 95/98/NT Machines
- Microsoft TechNet, Security Best Practices URL:http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/Default.asp
- Microsoft, Security and Privacy, URL:http://www.microsoft.com/security/default.asp
- Microsoft, Security Tools and Checklists. URL:http://www.microsoft.com/technet/security/tools.asp

- NTBugtraq URL:http://www.ntbugtraq.com/NTBugtraq is a mailing list for the discussion of security exploits and security bugs in Windows NT, Windows 2000, and Windows XP plus related applications.
- NT Security News Windows and .net magazine URL:http://www.ntsecurity.net/
- Windows NT Security Guidelines, A Study for NSA Research,URL: http://www.trustedsystems.com/tss_nsa_guide.htm
- WindowsSecurity.com, URL:http://www.windowsecurity.com/

Personal Firewalls

- Zone Labs, URL:http://www.zonelabs.com/,offers free firewall software to individual users. The freeware, ZoneAlarm, monitors all activity on your computer, including each time an application tries to access the Internet.
- Sygate Technologies, URL:http://www.sybergen.com/, Sygate Personal Firewall: provides protection from hackers and other malicious intruders-both on and off the corporate network. Now FREE for consumer use!
- Kerio Personal Firewall™, URL:http://www.kerio.com/kpf_home.html, represents smart, easy-to-use personal security technology that fully protects personal computers against hackers and internal misuse.

System Administration, Networking and Security (SANS)

- SANS Institute, Home Page URL:http://www.sans.org/newlook/home.htm
- SANS Institute, Information and Computer Security Resource URL:http://www.sans.org/newlook/resources/index.htm
- SANS Institute Security Newsletters and Digests, URL:http://www.sans.org/newlook/digests/index.htm
- SANS Institute, Bookstore URL:http://www.sans.org/newlook/publications/index.htm
- SANS Institute, What port numbers do well-known trojan horses use?, URL:http://www.sans.org/resources/idfaq/oddports.php
- Security Consensus Operational Readiness Evaluation (S.C.O.R.E.) “Dedicated to providing community consensus minimum standard for procedures, and checklists for overall infrastructure security”, URL: http://www.sans.org/score/
- The SANS Security Policy Project, http://www.sans.org/resources/policies/

Unix Security Information

- Armoring Solaris, URL:http://secinf.net/info/unix/lance/armoring.html
- How to install Solaris and have a good host security, URL:http://yassp.parc.xerox.com/
- Solaris Hardening and Security, URL:http://www.softpanorama.org/Security/sos.shtml

Reference materials

Symantec Corporation, Assets, Threats and Vulnerabilities: Discovery and Analysis
A comprehensive approach to Enterprise Risk Management
URL: http://enterprisesecurity.symantec.com/PDF/AxentPDFs/RiskMgmt.pdf

Federal Trade Commission Facts for Business
Security Check: Reducing Risks to your Computer Systems
URL: http://www.ftc.gov/bcp/conline/pubs/buspubs/security.htm

Federal Trade Commission Facts for Consumers
You've got Spam: How to Can unwanted Email
http://www.ftc.gov/bcp/conline/pubs/online/inbox.pdf

David A. Curry, IMPROVING THE SECURITY OF YOUR UNIX SYSTEM
Information and Telecommunications Sciences and Technology Division
ITSTD-721-FR-90-21
URL: http://www.alw.nih.gov/Security/Docs/unix-security.html

Peter Norton and Mike Stockman, Network Security Fundamentals

Stephen Northcutt, Lenny Zeltser, Scott Winters, Karen Kent Frederick and Ronald W. Ritchey, Inside Network Perimeter Security

The NIST Handbook, An Introduction to Computer Security:
URL: http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

TechRepublic, "Virus Protection Policy" URL: http://techrepublic.com

RFC 2196 Site Security Handbook URL:http://www.faqs.org/rfcs/rfc2196.html

David Chye Hock Quay, "Formulating A Wireless LAN Security Policy: Relevant Issues, Considerations and Implications."
URL:http://www.giac.org/practical/David_Quay_GSEC.doc

Sean Boran, IT Security Cookbook
URL : http://www.boran.com/security/index.html

State of Colorado – Standards Working Group - Email, Directory Services and Security
URL:
http://www.oit.state.co.us/resources/docs/cio_enterprise_services_standard_report.pdf

CERT® Security Improvement Modules URL:http://www.cert.org/security-improvement/

[1] Network Working Group - Request for Comments: 1594 - Answers to Commonly asked "New Internet User" Questions". 3.1 What is the Internet? URL: http://www.faqs.org/rfcs/rfc1594.html

[2] Hobbes' Internet Timeline v6.1 URL: http://www.zakon.org/robert/internet/timeline/

[3] History of ARPANET Behind the Net - The untold history of the ARPANET Or - The "Open" History of the ARPANET/Internet By Michael Hauben
URL: http://www.dei.isep.ipp.pt/docs/arpa.html

[4] Network Working Group - Request for Comments: 1244 – Site Security Handbook
URL: http://www.faqs.org/rfcs/rfc1244.html

[5] United States Department of Health and Human Services, Office for Civil Rights - HIPAA
URL: http://www.hhs.gov/ocr/hipaa/

[6] Financial Privacy: The Gramm-Leach-Bliley Act
URL: http://www3.ftc.gov/privacy/glbact/

[7] The Gramm-Leach-Bliley Act: The Safeguards Rule
URL: http://www3.ftc.gov/privacy/privacyinitiatives/safeguards.html

[8] Microsoft Settles FTC Charges Alleging False Security and Privacy Promises Passport Single Sign-In, Passport "Wallet," and Kids Passport Named in Complaint Allegations
URL: http://www.ftc.gov/opa/2002/08/microsoft.htm

[9] Eli Lilly Settles FTC Charges Concerning Security Breach
Company Disclosed Email Addresses of 669 Subscribers to its Prozac Reminder Service
URL: http://www3.ftc.gov/opa/2002/01/elililly.htm

[10] Guess Settles FTC Security Charges; Third FTC Case Targets False Claims about Information Security
Agency Alleges Security Flaws Placed Consumers' Credit Card Numbers at Risk to Hackers
URL: http://www.ftc.gov/opa/2003/06/guess.htm

[11] CERT® Coordination Center - Unix Security Checklist Ver 2.0
URL: http://www.cert.org/tech_tips/usc20_full.html

[12] CERT® Coordination Center - Windows NT Configuration Guidelines
URL: http://www.cert.org/tech_tips/win_configuration_guidelines.html

[13] Linux Online - Linux Installation and Getting Started
URL: http://www.tldp.org/LDP/gs/gs.html

[14] The Center for Internet Security – A not-for-profit cooperative enterprise that helps organizations reduce the risk of business and e-commerce disruptions resulting from inadequate security configurations.
URL: http://www.cisecurity.org/

[15] SANS InfoSec Reading Room – Computer Security White Papers
URL:http://www.sans.org/infosecFAQ/index.htm

[16] The CERT® Coordination Center (CERT/CC) Center of Internet security expertise
URL: http://www.cert.org/

[17] InternetStormCenter URL: http://isc.incidents.org/

[18] CERT® Advisory Mailing List URL: http://www.cert.org/contact_cert/certmaillist.html

[19] SANS Newsletter Subscription Service URL: http://www.sans.org/newsletters/sac/

[20] State of Colorado – Standards Working Group Email, Directory Services and Security URL:
http://www.oit.state.co.us/resources/docs/cio_enterprise_services_standard_report.pdf

[21] Help Defeat Denial of Services Attacks : Step by Step
URL: http://www.sans.org/dosstep/index.htm

[22] Consensus Roadmap for Defeating Distributed Denial of Service Attacks
URL: http://www.sans.org/dosstep/roadmap.php

Last Updated: May 23rd, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event