Global Information Assurance Certification Paper

GISO Practical Assignment (v 1.1)

Original Submission, following completion of
SANS Track 9 at Cyber Defense Initiative East
November, 2001

Kevin M. Hanrahan

Assignment 1: Describe GIAC Enterprises

Description of GIAC Enterprises

GIAC Enterprises is a market leader in the Security Information Management space with its flagship product GIACview, which provides a distributed infrastructure for the collection, normalization and processing of security events throughout an enterprise and providing a central console for correlation, reporting and alerting. GIAC Enterprises sells GIACview as an enterprise software solution, and provides security-related professional services to GIACview customers.

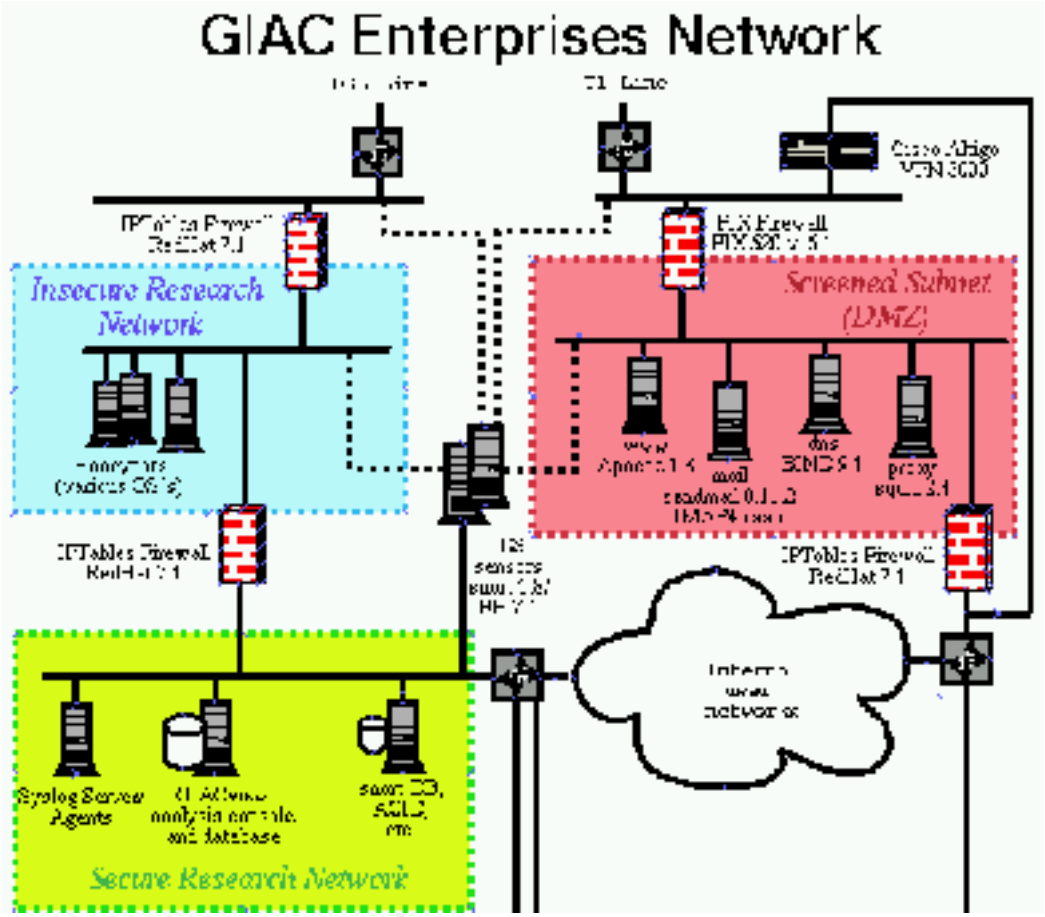
GIAC Enterprises is a relatively small company which has just completed Series B funding and is in the process of transitioning from startup mode to a more established company. With the funding, GIAC Enterprises has sufficient capital to properly deploy a security infrastructure, and implement a proper set of security policies. Because of GIAC Enterprise's growing visibility in the security space, it is imperative to implement a thorough security policy in order to protect against malicious hackers who may want to 'make a statement' by defacing the public website or similar acts, as well as to protect the firm's intellectual capital. Since GIAC Enterprises has been operating in a fast and loose startup-type environment until now, it is imperative that the security policies be clear and understandable and demonstrate the business needs, so as to minimize the inevitable resistance that the policies will generate.

IT Infrastructure

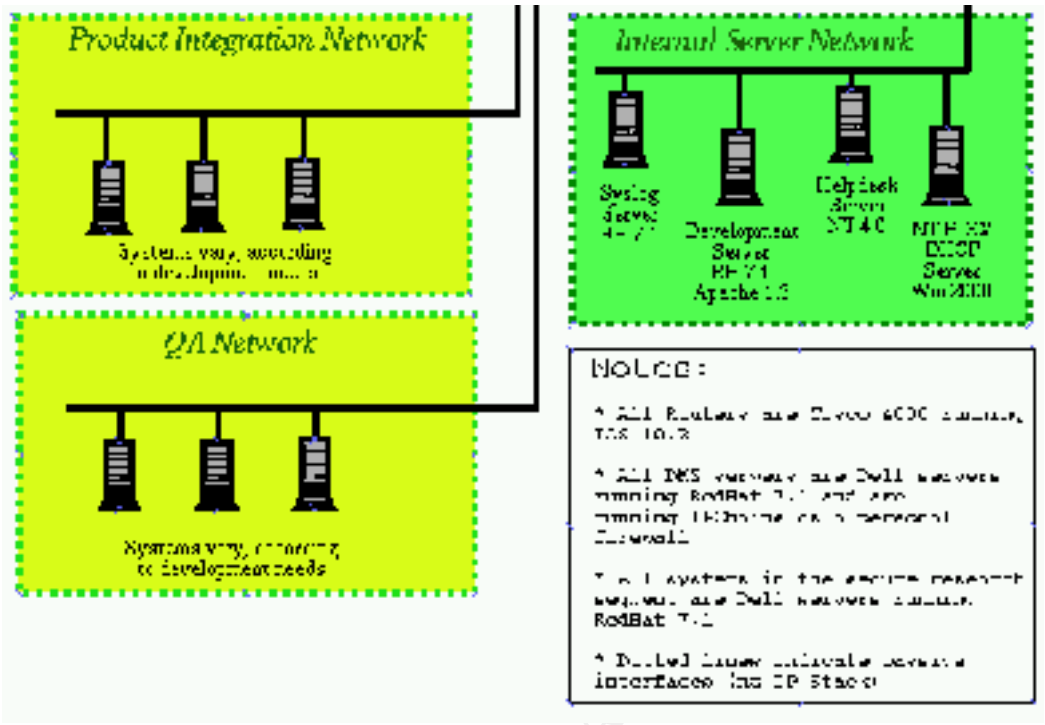
The IT infrastructure at GIAC Enterprises is designed to accomplish the following tasks:

- Provide public access to the corporate webserver
- Provide password-protected access to restricted sections of the webserver to customers, partners and others on an as-needed basis
- Provide a public email gateway
- Provide email access to remote employees, using secure POP, IMAP or web browser access
- Provide an authoritative DNS server for the internet, and an internal DNS server for the internal network
- Provide secure remote access for remote employees via VPN and ssh
- Provide a dedicated subnet for product stress-testing and QA, so that normal internal traffic is not affected by these activities
- Provide a segregated research network, with separate internet access, for the deployment of honeypots and security products

The following two diagrams provide a schematic view of the network:



Network Schematic (top half)



Network Schematic (bottom half)

Business Operations

The operational IT needs for GIAC Enterprises can be classified into the following categories: public access, partner/customer access, employee support, and research/development. The specific needs of each of these areas are listed below.

Public Access

The need for public access is limited to a public website and an SMTP server for incoming mail to employees. Specifically:

- Allow incoming HTTP traffic to www.giacent.com
- Allow incoming SMTP traffic to mail.giacent.com

As we maintain our own authoritative DNS server we further:

- Allow incoming UDP DNS requests to dns.giacnet.com
- Allow incoming TCP DNS requests from our ISP DNS server to dns.giacnet.com

Partner/Customer Access

GIAC Enterprises maintains two login -restricted sections of the public website f or access to non-public materials posted on a webserver. Although the material is not particularly sensitive, it contains intellectual property information that should not be publicly available. In keeping with general principles, this section of the web server is available only through secure http, as usernames and passwords are used. Therefore:

- Allow incoming HTTPS traffic to www.giacent.com

Employee Support

Employee IT services provided by GIAC Enterprises incl ude mail and web access for all internal employees; DHCP, NT file and print sharing for internal Windows users; mail access and VPN access to remote employees. The incoming and outgoing traffic restrictions to server these needs are:

- Allow internal acce ss to secure POP, secure IMAP, and SMTP (for relaying) to mail.giacent.com
- Allow outgoing SMTP traffic to the internet from mail.giacent.com
- Allow internal HTTP and HTTPS pro xt traffic to Squid server on proxy.giacent.com
- Allow outgoing HTTP and HTTPS traffic from proxy.giacent.com
- No NT protocols are permitted onto the DMZ or beyond
- Allow incoming secure POP and secure IMAP from the internet to mail.giacent.com
- Users who have authenticated through the corporate VPN are effectively internal users and are assigned an address on an internal user segment.

- All user desktops and laptops are placed on one of the several internal user networks

Research and Development

In addition to normal IT needs, the research and development users at GIAC Enterprises have additional technical needs. In particular, several specific purpose network segments have been created for their use. Two of these networks, the product integration network and the QA network are segregated out primarily for bandwidth reasons as opposed to security reasons. However, since no user desktops exist on these two networks, the principle of least privilege dictates that access to corporate services from these networks be restricted.

In contrast, the research team operates two specialized segments with major security implications. The 'insecure research segment' is used as a honeynet and a proving ground for various security products including GIACview. It uses a separate Internet connection, and a separate internet domain. Although there is a firewall and packet filtering router between the insecure segment and the Internet, the rules on these devices are loose by design in order to attract hostile traffic into this segment. The more critical purpose of the firewall separating the research segment from the firewall is to prevent excessive outgoing traffic from the research segment to the internet. Since systems on this segment are allowed to be compromised, they must not be used as a launching point for other attacks on the Internet.

A second firewall separates this insecure research segment with a secure research segment, which is part of the GIAC internal network. Because of the inherent insecurity of the insecure segment, only extremely limited traffic which is necessary for the monitoring of the honeynet is allowed. Further, systems on the secure research segment are restricted in their access to the remainder of the corporate network, citing POLP.

The security policy for the research segments can be summarized as follows:

- Allow any traffic to any systems from the internet to any honeypot address on the research segment (may be restricted due to research needs)
- Deny any outbound traffic from the insecure segment to the internet, except: the first 5 tcp connections, the first 25 UDP packets (for traceroute), and the first 5 ICMP packets, with a 24 hour period.
- Deny any traffic from insecure segment to secure segment except syslog from a honeypot address to the syslog server on the secure segment
- Deny connections to the DMZ, internet or server segment from addresses in any of the R&D segments

The development organization also maintains two servers, located on the corporate server segment: a development CVS repository accessed through HTTP, and a support helpdesk system, also accessed through HTTP. These systems, like all other servers on the server segment, are only accessible from address on one of the internal user networks.

Assignment 2 - Define Security Policy

Areas of Risk

GIAC Enterprises is an emerging player in the security software industry, and is gaining visibility in both the blackhat and whitehat circles. As a result, we are experiencing a rise in suspicious activity against our perimeter and publicly accessible servers. As our visibility grows, the importance of maintaining credibility in the security and business communities becomes increasingly important.

In order to focus resources in the most important areas, the following five areas of risk are identified. By addressing this risks first, we increase our ability to maintain our technology functionality, intellectual property, and credibility.

Area of Risk: Protection of the Perimeter

The perimeter, defined as the network components which connect the GIAC Enterprises network to the Internet, is of primary importance as it is the first line of defense between our systems and any potential malicious activity. Since it is imperative that the firm remained connected to the Internet, it is critical that the perimeter be as secure as possible while providing the services required.

The primary threat to the perimeter is that through misconfiguration, or faults in the perimeter components, that traffic will be allowed to pass from the internet to an internal system which would allow the internal system to be compromised. Possible results of such a compromise would include a denial of business critical services (such as email), leaking of our intellectual property (compromise of source code repositories), or embarrassment and loss of credibility (such as a web site defacement).

In order to mitigate the perimeter risk, as security policy (defined below) has been created so that the types of traffic allowed to cross the perimeter are minimized. Key points in this perimeter policy include: defense in depth, principle of least privilege, and the enforcement of application proxies in the DMZ so that no connections are permitted between the internet and the internal network.

The effort required to mitigate this risk requires the periodic review of the configurations of the Internet router, external firewall, and internal firewall. This review is performed weekly, and takes approximately one hour or less.

Area of Risk: Enterprise Integrity: Intrusion Detection / Logfile Monitoring

In counterpoint to perimeter defense, which aims to keep out hostile traffic, the enterprise integrity area is focused on ensuring that critical systems are not compromised either by outside or internal users. Our concern is to ensure that systems providing Internet services as well as those providing critical internal functions are secured in order to prevent the unauthorized disclosure or modification of data.

The threat here is twofold: servers in the DMZ are vulnerable to compromise in the

event of exploitation of as-yet unknown bugs in the server software, while these systems, along with internal servers on the server subnet, are vulnerable to potential exploits by internal users.

The possible consequences of failure to detect a compromise can be severe. The exposure of sensitive technical or marketing information to a competitor could result in a loss of business or intellectual property. It must be stressed that this information is more likely to be leaked by disgruntled employees than by an external blackhat under the employ of a competing company. Similarly, internal emails can contain sensitive information that could be potentially damaging as well. In addition to unauthorized disclosure of information, the unauthorized modification of data can result in tangible, although not necessarily quantifiable, damage to the business. For example, if the public website were to be defaced, the public relations damage to the reputation of GIAC Enterprises would be severe.

In order to mitigate the risk to the integrity of the data residing on our servers, we employ intrusion detection and host integrity products within critical segments of the enterprise. The corporate DMZ, which hosts all publicly accessible servers, is the primary focus of this effort. Through the utilization of the "snort" network intrusion detection system, all traffic passing into, out of, or through the DMZ is monitored, with alerts generating emails to both the system administrator and security analyst.

In order to enforce policy more efficiently, the snort rules should be augmented to alert whenever traffic is seen passing directly through the DMZ (policy dictates that no traffic passes directly between the Internet and the internal network).

We further recommend that a full packet capture engine be deployed on the DMZ in parallel with the snort engine. This packet capture should contain at least three days of traffic, so that more in depth analysis and investigation can be conducted when an incident is suspected. The recommended products for this functionality is tcpdump with SHADOW used as a reporting and file management interface.

Recommendations for ensuring host integrity include extending the deployment of the "tripwire" utility to all servers containing sensitive information, regardless of the system's location within the network. Currently, tripwire is used to detect changes on all DMZ servers. In all cases, tripwire is configured to monitor critical system files. Additionally, tripwire will monitor changes made in any of the files used in the public website.

The upfront costs to monitor the DMZ traffic with snort are minimal, as this product is deployed on a surplus desktop running the Linux operating system with a replacement cost of $1800.00. If the recommendation to deploy a separate packet capture system is implemented, a similarly priced system, along with additional disk space, be used; this system will cost approximately $2600.00. The cost of the snort software, as well as the packet capture software

Area of Risk: Honeynet Research Lab

GIAC Enterprises maintains a separate network for the purposes of conducting security research (see above diagram). This network has its own internet connection

separate from that used for normal corporate purposes, and utilizes a different, and changing, domain name. Because this lab is used to conduct the honeynet research in which GIAC Enterprises, the systems on this segment are, by design, compromised by blackhats.

The unusual nature of this lab poses a unique risk with respect to the enterprise security posture. The risks are twofold: that the corpo rate network could be compromised through the alternate connection, and that a blackhat could use resources on the research network as a launching point for attacks against third parties.

That the research lab could serve as an alternate path into the cor porate network is the more straightforward of the two issues to address. In terms of consequences of this risk being exploited, the damage is identical to that of the normal perimeter defense described previously. The steps taken to mitigate the risk are similar as well, but have some unique differences. Referring again to the network diagram, note that the honeynet portion of the lab (the "insecure" research lab) is separated from the management portion of the lab ("secure" research lab) by a firewall. Unlike the firewall separating the corporate DMZ from the internet, however, the firewall which divides the insecure and secure lab segments is configured to pass no traffic, other than TCP connections established from the secure segment into the honeynet segment, while only syslog messages are passed into the secure administration segment.

In order to further mitigate this risk, we recommend that this firewall be further restricted so that no IP traffic be allowed to flow through this firewall in either direction; management of the honeypot network should only be possible through the consoles, and syslog should be forwarded to the admin segment only through promiscuous sensing of the honeynet segment. In this configuration, no compromise of corporate reso urces is possible from the honeynet segment.

The second risk deriving from the honeynet segment is that these systems, once compromised, can be used as a launch point for attacks against other systems on the Internet. The most likely scenario is that de nial of service software, such as Trinoo or TFN, are installed and are later used to flood a third -party target. Also possible is that a blackhat will use a compromised system as a staging point for compromising other systems.

In either of these situatio ns, the possible consequences can be serious. As mentioned previously, the reputation of GIAC Enterprises is critical to its success in the marketplace; if systems owed by GIAC are used in illegal activities, the reputation of the company as a security fi rm could be seriously harmed. Moreover, such activity could expose GIAC to lawsuits. Although the case law in this area is still unclear, a strong case of negligence can be made against the firm if the strongest possible steps are not taken to ensure tha t these systems are not used against other internet sites.

In order to mitigate this risk, we control outbound traffic from the honeynet to the internet by limiting the number of connections that can be established from the research segment. Currently, w e limit the connections to five, as recommended by the Honeynet Project, so that blackhats have the opportunity to test connectivity and download tools to a compromised honeypot, but little else. Ideally, the blackhat will

not me aware that subsequent tra ffic, especially UDP or ICMP based denial of service attempts, never reach the intended destination.

Further research is ongoing to refine this restriction policy, but any future policy changes will be biased towards containment of the attacker rather tha n to prevent the attacker's detection that he is in a honeypot environment.

The costs to implement the recommended security policy are included as part of the operations of the research lab.

Area of Risk: Remote Access to Corporate Resources

Although GIAC Enterprises maintains a corporate headquarters where the majority of employees work, there are a significant number of salespeople and SE's who work in home offices in other regions of the country, and spend significant amounts of time on the road. These users, along with local employees at home or away from the office, need access to email and intranet applications. The company strives to provide these users with the maximum functionality while outside the office.

For the most part, the risks in the remote access capability are related to ensuring the integrity and confidentiality of corporate information. Like most companies, email is the lifeblood of corporate communication at GIAC, and that information frequently contains sensitive information . GIAC also provides a corporate intranet server from which users can, among other things, download corporate -confidential and other documents designated for internal use only, or disclosure under NDA.

While the consequences of compromise of a remote acc ess account are intangible, the prevention of information flow to a remote salesman would impair his ability to generate revenue. Disclosure of internal information to competitors could jeopardize GIAC's marketing efforts or leak the firm's intellectual p roperty. As such, assuring the confidentiality, integrity and availability of email and intranet access is of highest priority.

In order to mitigate the risks inherent with remote access, GIAC Enterprises has been gradually tightening the once open infra structure it inherited from its parent company. Paramount in this effort is the mandatory use of encrypted communication for the transfer of email or intranet documents outside the corporate network. The long overdue implementation of SSL secured POP m ail access in the Netscape mail client has made this cutoff possible. Likewise, all password -protected web pages maintained by the company have been converted to use SSL.

The VPN used at GIAC plays a limited role. The corporate issue tracking system, which uses legacy help -desk software that requires the Windows NT operating system and IIS webserver, needs occasional access by SE's in the field who may need to view or update the status of issues relevant to their accounts. Since corporate policy forbids the deployment of Microsoft IIS and Windows operating systems on the DMZ, this server can be accessed remotely only through VPN. As only a few users have VPN access, and VPN addresses are restricted by the firewall to access only the help desk server, th e VPN is not considered a significant risk in our environment.

Still at issue is the insistence on some users in using their ISP mail addresses as their only mail account, and demanding that all corporate email be forwarded to their private account. The proposed security policy would prohibit such forwarding, on the grounds that email, which may contain proprietary information, can only be sent out of the control of the firm through explicit action by a user - not through automated actions. The resistance to implementing this proposed policy is a clear indication of another area of risk: user education and awareness, described below.

Fortunately, the cost to mitigate this risk is near zero. Due to the support of SSL secured POP and IMAP protocols in the current versions of most major mail user agents allows for a trivial implementation for most users. Most costs for this implementation were measured in terms of time, for those users who needed to upgrade their mail UA's to a more current version (Netscape users in particular). As SSL based webservers, as well as POP and IMAP servers, are part of the standard Red Hat distributions, the deployment costs on the server side were also minimal and were only time, not dollar, costs.

Area of Risk: User Awareness and Education

It may seem ironic that user awareness and education would be a significant risk for a company focused on security. In fact, however, a large portion of the employees at GIAC are not security professionals, but are in the sales, marketing, finance, HR, and other fields that exist to support the core business. Moreover, many of the technical employees, such as programmers and help desk technicians, are not (nor are expected to be) security professionals. In this light, it should be no surprise that GIAC Enterprises is no different than other companies in that the human element may be the weakest link in the corporate security posture.

The specific threats in the human area include the compromise of passwords, through carelessness or easily guessed passwords, and the denial of service to a specific employee as the result of virus or other malicious code.

The password compromise issue is of particular concern, as a recent execution of the "crack" program against the mail server revealed a large number of bad passwords, particularly with salespeople who tend to be remote users. Although the compromise of a salesman's email password would not be likely to cause damage beyond the one compromised individual, such a compromise could easily hinder that person's ability to work effectively until the compromise was detected and repaired. Since salespeople's productivity has an immediate impact of the corporate bottom line, the consequences of a compromise here can be serious.

The mitigation of this threat must be two pronged: enforcement and education. To enforce password security we recommend a more aggressive password expiration policy, a preprocessor to prohibit bad passwords when changed, and the periodic running of the crack program and disabling of accounts that are cracked.

Although GIAC has had little actual damage as a result of email viruses, the constantly evolving nature of this threat ensures that it will remain a priority from the security standpoint. Like password enforcement, education of best practices plays a major role in virus threat mitigation, but more technology options can be implemented

to help the threat.
Currently, all incoming mail is scanned for viruses prior to delivery, while anti-virus software on the user's desktop/laptop has not been standardized at the corporate level. Our recommendation to mitigate the virus risk is to standardize the Windows users on a single anti-virus product, in which updates are announced by the system administration team. We also recommend that the corporate mail server add a second virus scanner, providing defense-in-depth against email viruses.

To educate users on security best practices, we recommend the following be implemented:

- During new employee orientation, a security best practices guide be provided to each employee. As with the acceptable use policy, the employee must sign that he has read the password policy
- On a monthly basis, a brief security best practices email be sent to all employees. Emphasizing one particular facet of the best practices, the email will help promote security awareness on an ongoing basis, without being overwhelming or heavy-handed.

The cost of mitigating the password vulnerabilities is estimated to be three to five hours per month for system administration tasks, including weekly "crack" runs, user notification of bad and/or expired passwords, and user assistance. Mitigation of the virus threat would involve the purchase of a commercial a/v product, and associated maintenance and support, for all Windows-based systems and the mail server. Administration of signature updates can be expected to run about two hours per month.

Security Policies

note: the following policies were derived from templates provided by the SANS Security Policy Project

GIAC Enterprises Password Policy

Purpose
The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change. Such a policy is necessary because mos t access to corporate resources, accessed both internally and from the Internet, is controlled by passwords. Because the compromise of a password, due to user negligence or due to a choice of a bad password, can result in disruption of business, the loss of corporate intellectual property, and embarrassment to the firm, GIAC Enterprises considers adherence to the policy to be of the utmost importance for all employees.

Scope
This policy applies to all employees, for passwords pertaining to:

- email access
- intranet access
- login to windows domain controllers
- personal desktops and laptops, whether corporate -owned or personally owned, that connect to the corporate network or VPN
- any other password protected resource administered by GIAC Enterprises , such as routers, firewalls, or software applications.

Policy

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.), except those for individual workstations, must be changed on at least a quarterly basi s, and adhere to the escrow provions below
- All network-level passwords (e.g. routers and firewalls) must be change on a quarterly basis, and adhere to the escrow policy
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- All user-level and system-level passwords must conform to the guidelines described below

Guidelines

A. General Password Construction Guidelines

The selection of a good password is the first step in password security. The proliferation of password cracking utilities makes it imperative that passwords are not guessable or easily broken by such programs. Poor, weak passwords have the

following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The words "GIAC", "GIACEnt", "sanjose", "sanfran" or any derivation.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Are easily remembered so that they need not be written down.

A popular scheme for creating and remembering good passwords is to choose a theme, such as songs from a particular group, movies, or book titles. Derive a password from the theme based on the first letters of each word, maybe replacing some letters with numbers or special characters. For example, if your theme is golf winners, choosing "Tiger Woods, 2001, 16 under par (a record!)" may yield a password of "01TW-16!".

B. Password Protection Standards

Do not use the same password for GIAC Enterprises accounts as for other non-corporate access (e.g., personal ISP account, option trading, benefits, etc.). Do not use the same password for your email and your workstation.

Do not share passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential information.

Remember: The system administrati on staff at GIAC Enterprises will never ask you for your passwords. No administration task in our environment will require such information.

Do not use the "Remember Password" feature of Outlook, Netscape, or other applications.

Password cracking or guessing may be performed on a periodic or random basis by system administrators. If a password is guessed or cracked during one of these scans,

the account may be disabled, the user will be required to contact the system administrator in order to to change it .

Password Escrow

Root, administrator, enable, and other systems -level passwords for each production server or infrastructure systems will be stored in a labeled, sealed, dated envelope signed by the person responsible for the s ystem and provided to corporate systems administration for secure storage. Servers used for development or QA GIACview builds are exempt from this requirement, but systems used for demos or support are not.

The password escrow envelops will be audited periodically by the office of the CTO in order to enforce compliance with this section.

Responsibility and Enforcement

User password expiration and quality enforcement is performed by system administration staff, using system utilities provided with app lications and operating systems, and the "crack" and "l0phtcrack" utilities.

Auditing of systems level passwords and escrow procedures are performed by the CTO, or designated representative.

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

Effective Date: December 15 2001 - Initial Creation

GIAC Enterprises Email Access and Processing Policy

Purpose

To prevent the unauthorized or inadvertent disclos ure of sensitive company information, and to protect the integrity of the netForensics mail server infrastructure.

Background

GIAC Enterprises realizes the importance of fast and easily accessible email communications, especially with respect to account managers and systems engineers who work in remote or home offices. At the same time, all employees need to realize that such email frequently contains information that, if leaked to competitors, clients, or others outside the company, could impede our abi lity to close sales or effectively market our product. It is critical, therefore, that GIC Enterprises and its employees adhere to procedures that control and safeguard our intellectual property.

Scope

This policy covers email access, including automatic email forwarding, and thereby the potentially inadvertent transmission of sensitive information by all employees, vendors, and agents operating on behalf of GIAC Enterprises.

Policy

A. Forwarding

Employees must exercise utmost cau tion when sending any email from inside GIAC Enterprises to an outside network. In order to prevent unauthorized disclosure of proprietary or sensitive information due to the lack of control of the security of third - party email providers, GIAC email will not be automatically forwarded to an external destination.

B. Remote Email Access

GIAC Enterprises currently provided a secure webserver application for browser - based access to email, as well as secure post -office protocol (POP) and interactive mail access protocol (IMAP) access for mail client applications. These are the only mechanisms available for remote users to access mail from the Internet.

The insecure version of POP will remain available to internal users through January 31, 2002, so that Ne tscape 4.x users have sufficient opportunity to migrate to Netscape 6.x, Outlook, Eudora, or other secure POP aware user agent.

C. Mail Relaying

Because of the potential abuse by email spammers, the GIAC Enterprises mail server cannot be used as an outgo ing SMTP relay server to unknown systems on the Internet.

Remote employees with static IP addresses, either at home or remote offices, may provide their addresses to the system administration team so that they can use the corporate mail server as a relay . Remote users with Linux systems in default configuration can simply use "localhost" as a mail relay.

Users with randomly assigned IP addresses (i.e. dialup users) must use their ISP's designated relay host for outgoing mail. Note that this does NOT prevent you from using the GIAC Enterprises POP or IMAP server as an incoming mailbox, nor does it prevent you from configuring your identy and return address as you@giacenterprises.com.

Mail Scanning

Any mail delivered to GIAC Enterprises is scanned for malicious code attachments, such as viruses. GIAC Enterprises reserves the right to implement automated scanning programs for incoming mail in order to block harmful attachments, spam, or mail which would violate the corporate Acceptable Use Policy.

Email Privacy

GIAC Enterprises does not currently monitor email communications for acceptable use violations, and has no plans to do so. However, senior management (VP and above) may request such monitoring of specific employees in the event that there is reason to believe that violations of the Acceptable Use Policy are being committed by the employee.

When an employee leaves the company, all email to that emplyee will be forwarded to his manager.

Responsibility and Enforcement

The office of the CTO, during periodic firewall audits, will ensure that internet access to the mail server is limited to the protocols approved for remote access, and that the mail server is not running non-compliant process.

System administrators will ensure that system alias file /etc/aliases does not contain remote addresses, or assist users in the creation .forward files which perform forwarding to outside systems.

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

Effective Date: December 15, 2001

GIAC Enterprises DMZ and Internet Access Policy

Purpose

To provide the highest possible security from hostile traffic on the internet, while allowing all necessary i nternet traffic necessary for business operations.

Background

The very existence of GIAC Enterprises and its products is based on the knowledge that the Internet provides individuals with unprecedented ability to attack, infiltrate, disable, or otherwise compromise computer networks and systems globally from the comfort of their own homes. As GIAC Enterprises becomes increasingly visible in the security marketplace, many of these hostile individuals, also referred to as "blackhats", will view GIAC Enterp rises as a tempting target for hostile activity ranging from website defacement to denial of service to theft of our source code.

In order to protect against such activity, GIAC Enterprises enforces restrictions on how traffic is permitted to flow between the corporate network, our publicly accessible servers on the DMZ, and the Internet.

Scope

The restrictions and guidelines described herein apply to the corporate network, production servers, and the firewalls and routers which connect them to the Inter net via the giacenterprises.com registered domain addresses.

This policy does not apply to configuration and activity on the specific honeynet research networks.

Policy

The overarching guidelines in this policy are Principle of Least Privilege, and Defe nse in Depth. The former, POLP, specifies that only the minimum amount of traffic, and the minimum number of services, are permitted to operate on any DMZ or Internet component. Defense in Depth dictates that redundant procedures will be used to secure the infrastructure.

All servers which are accessible from the internet must be located in the DMZ, a network segment which is protected from the Internet by a packet filtering router and a stateful inspection firewall (Cisco PIX). This firewall is hereaft er referred to as the "external firewall".

Following the principle of Defense in Depth, both the external router and the PIX firewall are configured to pass only specific traffic necessary for the specific access to the DMZ servers. Following the Princip le of Least Privilege, they are configured to deny anything but specifically allowed traffic.

The DMZ is further separated from the internal network by a second stateful firewall, which is of a different vendor than the Internet firewall. This firewall is hereafter

referred to as the "internal firewall".

A. Traffic from the Internet to the DMZ

The routers connecting GIAC Enterprise to the internet will perform filtering based on the following rules:

- Only traffic originating from legitimate internet addr esses will be allowed. Traffic appearing to originate from GIAC's own address space or from private address spaces will be blocked.
- Only TCP traffic destined for ports on which GIAC provides legitimate service will be allowed (see implementation guideline s for specific ports). The specific addresses need not be specified on the router. Traffic to all other TCP ports is blocked.
- All UDP traffic will be blocked.
- Only ICMP Destination Unreachable and Time Exceeded packets are allowed; all other ICMP packets are blocked.
- Any other protocol will be blocked.

The external firewall will be configured to the following guidelines

- Only traffic originating from legitimate internet addresses will be allowed. Traffic appearing to originate from GIAC's own address sp ace or from private address spaces will be blocked.
- Only TCP traffic directed to a specific port on a specific system which is approved to run the corresponding service will be passed. All other TCP traffic is blocked.
- All UDP traffic is blocked
- Only ICMP Destination Unreachable and Time Exceeded packets are allowed; all other ICMP packets are blocked.
- Any other traffic will be blocked.

B. Traffic from the DMZ to the Internet

The internet firewalls are configured as follows:

- Only traffic originating fro m GIAC's own public address space will be passed. All other traffic is blocked .

The external firewall will be configured to the following guidelines

- Only traffic originating from a known DMZ server will be permitted.
- Only the proxy server residing on the DMZ will be able to intiate outgoing TCP connections on any port. Only the mail server can initiate outgoing mail connections. Only the DNS server can initiate outgoing DNS TCP connections. All other TCP traffic must be respiles to an externally initiat ed connection.
- No outbound UDP traffic is permitted, except high -port requests as would be generated by traceroute.
- No outbound ICMP traffic is permitted
- All other traffic is blocked.

C. Traffic from the DMZ to the Internal network

The internal firewall is configured to the following guidelines:

- No DMZ system can initiate a connection to the internal network.
- Only syslog and SNMP UDP traffic can pass into the internal network
- Only ICMP Destination Unreachable and Time Exceeded packets can pass

D. Traffic from the Internal Network to the DMZ

The internal firewall will be configured to allow traffic from the internal to the DMZ according to the following guidelines:

- Only traffic originating from the internal address space will be allowed.
- Only TCP traffic directed to a specific port on a specific system which is approved to run the corresponding service will be passed. All other TCP traffic is blocked.
- All UDP traffic is allowed
- ICMP packets are blocked..
- Any other traffic will be blocked.

E. Traffic from the Internet to the Internal Network

No traffic is passed.

F. Modification of Firewall Rules

Any change in either the external or internal firewall rules must be approved by the CTO, or designated representative.

Responsibility and Enforcement

Responsibility for the implementation of this policy resides with the system administration staff.

On a monthly basis, the CTO, or designated representative, will review the firewall configurations.

Unauthorized modification of firewall rules which result in traffic being able to pass which was previously denied is grounds for termination, or other disciplinary action.

System administration staff may, without prior approval, modify firewall rules to restrict traffic if there is reason to believe that host ile or suspicious activity is happening. In such a case, incident handling procedures must be invoked.

Effective Date: December 15, 2001

Assignment 3 - Define Security Procedures

GIAC Enterprises Firewall Modification Procedures

Purpose:

As the first defense against malicious activity from the Internet, the proper configuration of the corporate firewalls (including the internet border routers) is critical.

Actions to Be Carried Out

This document specified the procedures to be taken when any of the following events needs to take place:

- modification of the access control lists on the internet border routers
- modification of the conduit or outbound directives on the external firewall
- modification of the /etc/sysconfig/iptables rules on the internal firewall

Implications and Importance

The internet border routers serve as GIAC's first line of defense against malicious activity. Proper configuration of these routers allows better defense against a number of denial of service attacks and certain ot her relatively unsophisticated attacks. By using the routers to screen obviously bogus traffic, we relieve the firewall of this burden so that it has more cycles available to perform the more complex stateful firewalling necessary.

The external firewall controls the traffic passing between the Internet and our DMZ, where systems that provide services public to the internet are located. With the exception of DNS all traffic is TCP, and therefore uses stateful inspection techniques to ensure that packets a re part of a legitimate session. As this firewall provides a major component of the defense of the systems most likely to be attacked first, it is considered the most important of the three systems covered in this procedure.

This firewall, as well as the internal firewall, serve a secondary purpose of containing and minimizing the damage that may be done if a DMZ server is compromised. As such, the external firewall restricts the traffic that can flow out of the DMZ.

The internal firewall servers to pro tect the internal network in the event that DMZ systems are compromised, as well as to prevent the direct flow of traffic from the Internet to the internal network. When considering the modification of the internal firewall rules, the assumption is that t he DMZ systems will be compromised and are therefore not trusted; there are few reasons to permit DMZ systems to connect to the internal network, and none of them currently apply to GIAC Enterprises.

Changing Firewall Rules (non -emergency)

The following steps will be taken whenever a non -emergency change is made to the configuration of any of the three components.

1. The current configuration of the firewall/router is saved in a manner that will permit quick restoration should the change need to be rolled back.
2. The system administrator will describe to the approving authority (CTO or designated representative) what the change will be, what the business need for the change is, who requested the change, and when it needs to be implemented. This description must be via email, and should also include a personal discussion.
3. The approving authority validates both the business need and technical correctness of the proposed change, as well as its compliance with the DMZ policy. Approval to effect the proposed cha nge must be granted via reply to the email. If changes to the request are required, the email audit trail must document the changes.
4. The system administration staff will implement the change at the desginated time, and perform any required tests to valida te the desired result.
5. The administrator making the change will email all system administrators, the approving authority, and other interested parties that the change has been made.

Changing Firewall Rules (emergency)

Any GIAC Enterprises employee with t he appropriate technical knowledge can implement an emergency firwall rule change if there is reason to believe that a GIAC system has been compromised and is communicating with an external system.

The following steps are to be taken is such activity is suspected:

1. The discovering party immediately contacts system administration, the CTO, or any person with the technical knowledge to perform the necessary change (in that order)
2. If the person who will make the change does not have the appropriate password , he will obtain it from the password escrow cabinet (see receptionist or CEO for key).
3. The minimum change to block the suspicious traffic is determined - usually this will be blocking of a specific IP address or range, or a specific port. The change shou ld be made on the external firewall, if possible, otherwise on the internal firewall or the internet border router (in that order).
4. The person effecting the change will save the current configuration in the most expedient manner possible, usually a cut and paste will suffice.
5. The change will be made.
6. The corporate incident handling procedures will be invoked.

Verification and Audit

The CTO, or designated representative, will review all firewall and router ACL configurations on a monthly basis. Every "per mit" and ACCEPT rule will be verified for business necessity and compliance with the DMZ policy.

In the event of an emergency change, the CTO will validate the change at the earliest

possible opportunity, and approve or modify the change as appropriate, and notify all administrators and interested parties of the change, and how long the change will be in effect.

On a periodic basis, the CTO will direct a member of the security research department, or other qualified individual to perform an assessment of the various firewalls and ACL routers. This check should be performed quarterly, or as needed. The results of these scans are compared to the firewall configuration logs and the DMZ security policy document. Any discrepancies will be reviewed by the CTO.

Resources:

The SANS Institute, "The SANS Security Policy Project Website"
URL: http://www.sans.org/newlook/resources/policies/policies.htm

Cisco Systems, "Network Security Policy: Best Practices White Paper"
URL: http://www.cisco.com/warp/public/126/secpol.html

Frederick M. Avolio, "Best Practices in Network Security" , March 20, 2000
URL http://www.networkcomp uting.com/1105/1105f2.html

Lance Spitzner, "Auditing Your Firewall Setup" , December 13, 2000
URL: http://www.enteract.com/~lspitz/audit.html

The Honeynet Project, *Know Your Enemy,* Addison Wesley 2001

Chaiw Kok Kee, "Security Policy Roadmap - Process for Creating Security Policies" , October 2, 2001, URL: http://rr.sans.org/policy/roadmap.php