GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

Interested in learning more?

Check out the list of upcoming events offering
"Security Leadership Essentials for Managers (Cybersecurity Leadership 512)"
at http://www.giac.org/registration/gslc

Security Analysis

GIAC Enterprises

Karen Zwolski

Information Security Officer Training
GISO - Basic Practical Assignment
Version 1.2 (February 9, 2002)

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Assignment 1 - Describe GIAC Enterprises

Description of GIAC Enterprises

GIAC Enterprises is a planning, engineering, and architectural consulting company that provides design services to various government agencies and private industries. GIAC employs over eight thousand engineers and designers in fifty offices throughout the United States. Each office specializes in one or more technical disciplines including design and planning of transportation systems, environmental assessments, architectural design, mechanical engineering, and electrical engineering. GIAC's diversity has positioned the company to provide consulting services for large multi-faceted design projects.

IT Infrastructure

GIAC Enterprises Information Technology infrastructure consists of a large LAN at the Corporate Headquarters and several private smaller LAN's at production offices.

The Corporate Headquarters LAN is divided into a private internal network and a screened subnet (or DMZ). The DMZ is protected by Cisco Pix 520 redundant firewalls. Internet connectivity is via a Cisco 3640 border router. A Cisco 4210 Intrusion Detection Sensor is located outside the firewall. All servers in the DMZ are assigned private IP addresses in a 192.168.x.x range. The servers in the private LAN are assigned private addresses in the 10.x.x.x range. Any server that must be reached by server name via the Internet has a public IP address mapped to its private address in a network address translation table on the firewall.

A server diagram is located in Appendix A.

The private Corporate Headquarters private LAN consists of following hardware and software.

- *Six NT 4.0 servers running Domino 5.09a for applications.* Numerous Domino databases comprising the Corporate Intranet are stored on these servers. The databases are accessible using a Lotus Notes Client or Microsoft Internet Explorer browser. These servers can be accessed via private WAN or via the Internet. Internet access is allowed only via the Apache reverse proxy servers or the Domino application proxy servers in the DMZ. The reverse proxy servers and the Domino application proxy servers require authentication before sessions are passed via proxy to the private WAN.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- *Eight NT 4.0 servers running Domino 5.09a for mail.* Each of several thousand employees owns a mail database on one of these servers. The mail is accessible using a Lotus Notes Client or Microsoft Internet Explorer browser. These servers can be accessed via private WAN or via the Internet. Internet access is allowed only via the Apache reverse proxy servers or the Domino application proxy servers in the DMZ. The reverse proxy servers and the Domino application proxy servers require authentication before sessions are passed via proxy to the private WAN.
- *Two NT 4.0 servers running Domino 5.09a SMTP services.* These servers accept inbound connections on port 25 only from the Sendmail servers in the DMZ. Messages received from the Sendmail servers by the SMTP servers are then routed to the appropriate Domino mail server for the intended recipient. All Domino mail servers route outbound Internet mail via these SMTP servers to the Internet. These servers also run Symantec Norton AntiVirus for Lotus Notes.
- *Two NT 4.0 servers running Domino 5.09a LDAP services.* The LDAP servers provide authentication capability when using the browser to access Domino mail and database servers from the Internet. These servers also provide Domino directory services for authentication capability when using the Notes client to access Domino mail and database servers from the Internet.
- *Two Windows 2000 servers running Microsoft DNS services.* The DNS servers resolve internal IP addresses and forward all requests for external IP address resolution to Internet root servers.
- *Two IBM AS400 servers running accounting and human resources applications.* These servers are accessible via the private WAN only using terminals.
- *NT 4.0 server running Cisco Secure Policy Manager.* The purpose of this application is to monitor and manage the IDS sensor, border router, and firewall .
- *Cisco 3640 router.* This router connects the Corporate private LAN to an AT&T managed frame-relay Wide Area Network.

The Corporate Headquarters DMZ consists of following hardware and software.

- *Two Red Hat Linux 6.2 servers running Apache HTTP Server 1.3.* These are reverse proxy servers that provide browser access via the Internet to the Domino mail and database servers in the private Corporate LAN. All HTTP requests from the Internet for Domino mail and applications are routed to the reverse proxy servers. The reverse proxy servers require authentication via the LDAP servers in the private LAN before passing connections to the mail and application servers.
- *Two NT 4.0 servers running Domino 5.09a.* These are Domino Passthru Servers that serve as application proxy servers for Notes client access via the Internet to Domino mail and database servers in the private Corporate LAN. All requests for service to mail and applications in the private LAN using the Notes protocol and Notes client are handled by these servers. These servers require the Notes client/user requesting access to have a public key stored in the Domino directory on the LDAP server.
- *Two NT 4.0 servers running Sendmail Switch version 2.1.1.* All inbound Internet mail addressed to GIAC Enterprises is routed to these servers. These servers perform spam filtering and pass all appropriate inbound messages to the Domino SMTP servers in the private Corporate LAN.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- *Two NT 4.0 servers running Lotus QuickPlace.* QuickPlace is a self-service web tool that allows project managers to create shared team workspace applications.
- *Cisco IDS 4210 Intrusion Detection Sensor.*

Large Production Office LANs consist of the following hardware and software.

- *Cisco Router for WAN Connectivity.* There are over forty large production offices connected to the frame-relay WAN. All end users in the production offices have connectivity to the Corporate private LAN via the frame-relay WAN.
- *Cisco Border Router and Cisco Pix Firewall.* Large production offices have Internet connectivity for outbound browsing only.
- *NT 4.0 and Windows 2000 file and print servers.* Depending on the size of the office, any number of file and print servers are available. These servers provide file storage for project related cadd files and project related word processing documents.
- *NT 4.0 and Windows 2000 workstations.* All users have a workstation with Lotus Notes client software. Depending on the user's job function, Microsoft Office, Autocad, and/or various other engineering design applications are installed on the workstation.

Small Production Office LANs consist of the following hardware and software.

- *Cisco Pix 506 and Cisco Router.* There are ten small offices where the number of users or office location makes a frame-relay connection to the Corporate private LAN cost prohibitive. These offices maintain a DSL, cable modem, or T1 connection to the Internet and access the Corporate LAN via point to point VPN.
- *NT 4.0 and Windows 2000 file and print servers.* These offices may have one or more file and print servers for storing project related information.
- *NT 4.0 and Windows 2000 workstations.* All users have a workstation with Lotus Notes client software. Depending on the user's job function, Microsoft Office, Autocad, and/or various other engineering design applications are installed on the workstation.

Business Operations

GIAC Enterprises provides design services for both small and large projects for private industries and government agencies. Each particular production office may specialize in one or more technical disciplines requiring a specific level of expertise amongst the engineers. Production offices use high-end workstations and file/print servers in NT 4.0 based local area networks. Specific project drawings, design work, and proposal preparation is performed and stored on servers in the production offices.

Large design projects usually require the combined expertise of engineers located in various offices throughout the country. It is essential for geographically dispersed workers to be able to communicate and collaborate with other employees and clients in the design process and management of the project. GIAC Corporate Headquarters

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

maintains a private Domino based Intranet that provides four primary applications for the purpose of communication and collaboration. These four primary applications provide project management capabilities, marketing and proposal preparation tools, basic administrative functions, and email.

Project management databases allow for storage of technical and administrative project related information and client contact information. These databases also contain a discussion section that provides employees working on the project the ability to ask questions about the projects or post items of interest. A project calendar where client meetings and project milestones can be posted along with a "to-do" list is maintained in each project database.

The marketing databases provide information necessary to pursue work, locate expertise, and rapidly build proposals. History on all completed major projects is stored in the marketing databases. Additionally, service profiles, honors and awards, project photography, proposal samples, technical papers, employee resumes, and a complete client contact list are maintained in the marketing databases on the GIAC Intranet.

The administrative applications provide employees with basic administrative services and information. Domino based databases simplify administrative processes and provide easy access to forms, company policies, and various materials intended to educate and keep employees informed about company activities. The following applications are important to GIAC operations and help GIAC keep overhead low.

- GIAC Forms Database - All forms required for purchasing, requesting vacation, travel expense reimbursement, etc. are found in these databases.
- Jobs Posting Database - All job opening are advertised in this database. Employees can apply online or submit referrals to any job opening.
- Policy and Procedures Database - All human resources, accounting, administrative, and computer policy manuals are online.
- Training Library - Various training videos, books, and computer based training software can be checked out using this library database.
- Directory - all employee names, phone numbers, and office locations are kept in this database.
- Resource and Reservations Database - Company resources including conference rooms, projectors, vehicles, cameras, etc. are listed in this database. Employees can schedule conference rooms and reserve equipment using this application.

Email is essential for all employees. The email servers for the entire corporation are centrally located at the Corporate Headquarters private LAN. Corporate communication is managed primarily via email. Communication with clients via email is also a necessity. The requirement that GIAC employees be reachable via email is often designated in client contracts. Many project proposals and job progress reports must be submitted using email.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Every large production office has connectivity to the GIAC Intranet via a private frame relay wide area network managed by a third party vendor. Small production offices have connectivity to the GIAC Intranet via a PIX to PIX Virtual Private Network over the Internet using IPSec. Every user in the small and large production offices uses a Lotus Notes client for access to the GIAC Intranet including email.

Many employees travel frequently or work in client offices. Remote access to GIAC's Intranet and email servers is provided via the Internet using a Lotus Notes client or Microsoft IE browser. Client sites frequently will not allow for the installation of a Lotus Notes client on their workstations. In these cases, the employee must use a browser for access to the Intranet and to email. If using a browser for access, the request for service is directed to the Apache reverse proxy servers in the DMZ. SSL certificates for each server are stored on the Apache servers providing an encrypted tunnel for browser access. The Apache servers request authentication from a LDAP server in the private network. Only after successful authentication, is the employee able to access the Intranet and their personal email database.

Remote access using a Lotus Notes client is made available using a Domino passthru server in the DMZ. The passthru server is an application proxy server that request authentication from the LDAP server in the private network. Network port encryption on the passthru server encrypts data passed over the Internet. Passthru servers can be accessed over any Internet connection.

All employees have outbound browser access to the Internet. In many cases, building standards and guidelines, code compliance documentation, and business procurement opportunities are available on various web sites.

Clients have requested access to project databases and project collaboration via the web. Lotus QuickPlace servers have been installed in the DMZ to provide this service. QuickPlace provides the capability to project managers who have little or no programming skills to quickly create web applications. These applications allow for storage of documents, revision tracking with check in/check out capability, and file exchange. Task management and status tracking is available via Gantt Chart. Automatic email notification can be enabled when tasks are due or overdue. Discussion forums may also be added to QuickPlace databases. Access to QuickPlace is controlled by the project manager. A list of authorized users is created when the application is created. QuickPlace is installed on Domino servers. Authentication is managed by an LDAP server in the private corporate local area network.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Assignment 2 - Identify Risks

Risk #1 - Inappropriate Disclosure of Proprietary Information

GIAC Enterprises has made a tremendous investment in engineering, assessment, and architecture of transportation systems, environment, and facilities. The protection of specifications, proposals, employee profiles, and client lists is essential to the success and survival of the company. Consider the advantage to a competitor who obtains an unauthorized copy of a proposal. What if the competitor uses that proposal to better position it's company to win the job? The potential for lost revenue is such a case is obvious. A considerable competitive advantage could also be obtained by using specifications and design work that GIAC spent much time and money developing. Additionally, inappropriate disclosure of certain specifications could present civil liabilities, embarrass the company, or cause loss of client confidence and trust. Inappropriate disclosure of employee profiles may violate employee privacy rights or may facilitate loss of talent due to aggressive employment agency tactics or competitors need to procure specific talents. The disclosure of client lists could present an advantage to competitors or could violate privacy rights of clients.

Threats to GIAC's information include unauthorized access to databases that may be vulnerable due to failure to control access to authorized accounts, inappropriate access control lists, inappropriate application configuration, or failure to secure operating systems. Lack of security policy and/or lack of security policy enforcement could leave data vulnerable to dangerous copying and distribution. The risk is high considering the motivation of a competitor to gain advantage or the motivation of an employee or former employee to obtain client lists and use valuable design work to start his own consulting business.

Malicious code execution is always a threat to the protection of proprietary data. It has the potential to leave backdoors for unauthorized access or automate the distribution confidential data.

The potential for accidental disclosure of private information due to lack of employee security awareness is high. Employees may not understand the consequences of such disclosure or may not be aware of the confidentiality of certain types of data. Careless use of email, careless handling of sensitive documents, careless disclosure of passwords, or just forgetting to log out are all actions that can easily occur and leave proprietary data vulnerable.

The following steps should be taken to mitigate the risk of inappropriate disclosure of proprietary information.

1. Applications must be configured to provide maximum security to prevent unauthorized access to data and unauthorized access to code. This requires the application of appropriate Access Control Lists and proper application configuration according to specified procedures.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2. Harden operating systems and apply all security patches promptly.
3. Deploy network and host-based intrusion detection.
4. Monitor operating system and application logs for anomalies and unauthorized or unusual access attempts.
5. Perform regularly scheduled penetration tests and audits.
6. Secure storage of backup media.
7. Secure physical access to servers.
8. Prohibit use of tools that could compromise security.
9. Manage accounts and passwords properly. Make sure the principal of least privilege is applied.
10. Classify data according to confidentiality and criticality. Make sure employees are aware of and understand the classification.
11. Provide security awareness training to employees.
12. Require the use of S/MIME for transmission of sensitive email.
13. Install malicious code protection and keep pattern files and engines up to date.
14. Prohibit use of chat over the Internet.
15. Encrypt sensitive databases and encrypt remote access to the company Intranet.
16. Tightly control the installation of CD writers on end user machines to prevent copying of large cadd files, specifications, or databases.
17. Develop security policy to address the following issues:
    - Assign rights to intellectual property created by the employee to the employer as appropriate
    - Assign copyright notice to programs created by the company
    - Require signing of non-disclosure agreements as necessary
    - Clearly define business requirements for disclosure to third parties
    - Maintain the right to discontinue service to irresponsible or abusive employees

Risk #2 - Availability of Infrastructure

GIAC'S infrastructure comprises the "crown-jewels" for the company. The availability of the infrastructure is critical to the productivity of the company. GIAC does not manufacture any products. Its revenue is provided strictly through the labor of its employees. The GIAC Intranet provides the following applications that are essential to productivity.

- Project management and tracking databases. These databases provide project calendars, task assignment, submittal tracking, and technical expertise sharing amongst geographically dispersed engineers who comprise project teams.
- Marketing databases contain information that allows professional staff to locate expertise and quickly produce proposals.
- Administrative databases save time and streamline overhead processes by providing ready access to forms, procedures, contract templates, and training materials.
- Email helps engineers, administrators, and technicians to communicate project information throughout the company and to communicate easily with clients. Many

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

client contracts specify the ability to reach project team members via email. Some clients will only accept proposals via email.
- Engineers must have access to cadd and various design applications to produce specifications and plans.

The lack of availability of the above applications would severely hamper or stop production. No production means no revenue. Availability of applications will also impact GIAC's ability to meet contractual obligations to clients. Failure to meet obligations could result in significant embarrassment and expose GIAC to civil liability. Availability also impacts the ability of the staff to meet proposal deadlines. Inability to meet proposal deadlines will likely result in lost work.

There are many threats to the availability of GIAC's infrastructure. Hardware failure, accidental or intentional data or hardware destruction, theft, natural disaster, malicious code execution, inappropriately configured applications, and installation of untested or malfunctioning software or utilities could all make systems or data unavailable. The likelihood of many of these events is fairly high. Hardware frequently fails, and employees can easily accidentally delete data. Administrators lacking time and resources may install untested utilities or mis-configure applications. Storms, power failures, or other disasters are hard to predict but can be devastating if they occur.

The following steps should be taken to mitigate the risk of lack of availability.

1. Develop and practice a disaster recovery and business continuity plan.
2. Perform daily backups of databases. Keep current backup media on site for quick recovery. Keep another backup copy offsite.
3. Build redundant servers for database applications and deploy hardware such as Cisco LocalDirector to provide automatic failover and load balancing.
4. Cluster mail database servers using Domino clustering technology to provide failover and load balancing.
5. Build servers with all available redundant options such as dual power supply, hardware based raid arrays, and dual fans.
6. Keep spare parts on the shelf.
7. Build test server(s) and workstations. Test servers can be used to test new applications or utilities. Test servers can also be used to replace failed servers.
8. Use multiple Internet Service Providers with Internet connections at different physical locations. In addition to the SMTP servers at Corporate Headquarters, install a backup SMTP server at different physical location where Internet access is available.
9. Design the frame relay network to provide redundant paths to the Corporate Headquarters Data Center.
10. Deploy monitoring with HP OpenView. Monitor power, server room environment, server availability, application availability, and network availability. Page on-call technician when failure is detected.
11. Provide remote VPN access to on-call technicians.
12. Install utility such as Compaq Insight Manager to log pending hardware failure.
13. Establish and comply with change control policy and procedure.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

14. Establish regular maintenance windows during late night or weekend hours.
15. Physically secure server room and control access.
16. Install anti-virus software and keep pattern files and engines up to date.
17. Install appropriate Uninterrupted Power Supply (UPS).
18. Document power down and power up methods so operators can power done equipment safely and bring servers back on line quickly. This is especially important in surviving power failures where UPS is limited.

Risk #3 - Inappropriate Use of the Internet

GIAC provides Internet access including email services and web browsing to all employees for the purpose of performing research and communicating with clients and other employees. Inappropriate use of the Internet presents significant threat to productivity, effective use of resources, legal liability, and reputation.

Loss of productivity in a consulting firm is a significant problem. GIAC's revenue is derived solely from billing clients for the labor of its employees. Employees who waste time browsing non-business related web sites could reduce billable hours.

Computing resources are expensive. Excessive web browsing and abuse of email can clog expensive bandwidth and degrade performance resulting in higher expenses for more bandwidth or productivity loss. Downloading of large files and storage of large files received via email consume disk space and affect backup cycles and result in higher equipment cost.

GIAC is responsible for the use of its resources and may face significant legal problems if the resources are inappropriately used. For example, downloading, displaying, or emailing of sexually explicit materials or jokes may be construed as allowing a hostile work environment leaving the company exposed to lawsuits. If downloaded or emailed materials make derogatory reference to race, gender, religion, or disability, the company could be charged with violating discrimination laws.

Employees have the ability to post materials to web sites and chat rooms. Those materials could potentially contain confidential information, false statements about employees or competitors, or false press releases. This could result in defamation law suits or charges such as illegal stock price manipulation.

Employees have the potential to conduct other illegal activity using the company's Internet resources. What if an employee uses GIAC's resources to launch an attack against another company's computing resources or participate in a child pornography ring? If GIAC did nothing to control this type of activity, GIAC could face civil or criminal charges. GIAC could face significant penalties for employees who use GIAC resources to violate copyright laws by downloading and distributing copyrighted materials.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

GIAC's reputation and the reputation of its employees is also at risk due to inappropriate use of the Internet. Even if the actions mentioned in previous paragraphs do not result in litigation or criminal charges, the actions could result in significant embarrassment and damage to GIAC's reputation.

The likelihood that GIAC's resources will be inappropriately used is high. Every employee has access to Internet resources. Inappropriate behavior causes problems that cannot be controlled by technology. Controlling inappropriate behavior is a huge challenge that cannot be fully accomplished. Technology has resulted in high availability of illicit or illegal materials, anonymity of access in many cases, and ease of use - all creating a high level of temptation that may be hard to resist.

The following steps should be taken to mitigate the risk of inappropriate use of the Internet. These steps will not completely eliminate inappropriate use but can demonstrate a good faith effort on GIAC's part thus diminishing legal liability. These steps will also slow productivity loss, reduce the risk of downloading or receiving malicious code via email, reduce the probability of sending or receiving inappropriate email, or visiting inappropriate web sites.

1. Develop and implement Acceptable Use Policy that clearly defines what is acceptable and what is not acceptable.
2. Conduct awareness training to communicate the policy and explain the risk to GIAC of non-compliance.
3. Conduct sensitivity training so that employees understand what is considered offensive conduct.
4. Deploy email monitoring product that can filter content and block specific types of attachments.
5. Deploy web monitoring product that can block access to prohibited sites and filter downloading of specific file types.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Assignment 3 - Evalutate Security Policy

Evaluation of Existing Policy

Password policy can be used to address the risk of inappropriate disclosure of proprietary information. The password policy that is being evaluated was taken from the SANS Security Policy Project section on the SANS web site. This policy and the URL where the policy can be found are located in Appendix B.

General Evaluation: It is clear that this policy is supposed to address the issue of passwords as they relate to security. The general leaning of the policy is towards end user password use. However, the inclusion of SNMP usage, application development standards, and the mention of public/private key systems increase the scope beyond that which can be thoroughly addressed in this policy. The steps that should be taken to address the policy are stated, but it is not always clear who is responsible for taking the steps. For example, *who* is allowed to change passwords? It might be useful to separate administrator duties from end user duties. More specific analysis is provided below.

Purpose and Background: The purpose of this policy is clearly stated. Additional justification for the policy would be useful. End users may be more cooperative if the policy explained that simple passwords are easy to guess and that password cracking programs are readily available and used by intruders. It may also be useful to explain social engineering tactics that are used by to obtain passwords.

Scope: The scope appropriately states who and what is covered by the policy, i.e., all systems and all users who use accounts/passwords to access systems.

Policy Statement: This policy does a nice job of listing requirements that enable users to meet the stated purpose of the policy. Specific requirements for creating, protecting, and changing passwords are all explained. The requirements are easy to understand and reasonable to implement.

The policy goes beyond what is typically expected in a policy document. Specific requirements and rules are appropriately listed. However, some of the guidelines explaining the characteristics of weak and strong passwords and the list of "dont's" are more appropriately suited to a standards and guidelines document. It would be sufficient to refer users to a "Standards and Guidelines" document on creating and safeguarding passwords.

Overall, the policy is advantageous to GIAC because it protects passwords from being guessed or inappropriately exposed thus reducing the risk of unauthorized access.

Responsibility: This policy does make it clear that end users have specific responsibilities for creating secure passwords, changing passwords, and protecting

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

passwords according to requirements specified in the policy. There is no specific statement regarding requirements of administrators when creating or changing passwords or deploying features of operating systems or software that will enforce policy. This could prevent GIAC from taking advantage of security features built into operating systems or software.

There is no information regarding who can draft, review, approve, or modify the policy. This could affect how the policy if perceived and whether or not the policy is enforceable.

Action: The policy appropriately states actions that can be taken to create secure passwords, protect passwords, and change passwords. For example, the policy specifically tells users to create passwords with at least eight characters, containing a mix of characters, and are not a word in any language. The policy also instructs users to change their passwords every four to six months. Requirements for protecting the password are also stated. For example, password protection actions mention not including passwords in email messages, not sharing passwords, not storing passwords in unencrypted form, and reporting suspected comprises to authorities.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Revised Security Policy

The following password policy was rewritten to address shortcomings described above and specifically meet the needs of the GIAC organization.

GIAC Password Policy

1.0 Overview and Background

The password policy is intended to address the risk of unauthorized access to GIAC systems. Unauthorized access can potentially result in the disclosure of proprietary information or destruction and damage to applications and data. Passwords that are not appropriately composed and protected can be compromised by guessing, "social engineering", or the use of sophisticated password cracking programs. Social engineering is a technique used by intruders who may pose as a company official in order to fool an employee into disclosing his password.

2.0 Purpose

The purpose of this policy is to establish requirements for creating, changing, and protecting passwords. These requirements are intended to prevent the compromise of passwords. Adherence to these requirements will make passwords difficult to guess or crack and minimize the risk of inappropriate disclosure of passwords.

3.0 Scope

This policy applies to all personnel including system administrators, managers, and end users as specified below who use a password to access GIAC systems. All systems owned by GIAC or residing in a GIAC owned facility are covered by this policy.

4.0 Policy

4.1 Construction Requirements: These construction requirements apply to all users and administrators when creating passwords.

- Passwords must be at least eight characters long.
- Passwords must contain a mix of characters including uppercase and lowercase characters and at least one non-alphabetic character.
- The password must not be found in any dictionary.
- Proper names, birthdays, phone numbers, etc. or other personal information should not be used when composing passwords.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Keyboard patterns such as "qwertyui" and number patterns such as "1234554321" should not be used.
- Different passwords should be constructed for each account used.

4.2 Changing Passwords (Users): All users must adhere to the following requirements for changing their passwords.

- Users must change their passwords every 90 days.
- Users must not reuse any password for a period of one year.

- Users should not simply add a number or use a cyclical pattern when changing passwords. For example, if a previous password was "jan&wentir", the new password should not be "feb&wentir" or "1jan$wentir".
- Users who forget their passwords must complete a "Password Request" form and submit the form to their System Administrator.
- Users must immediately change their email password (Lotus Notes) after the Lotus Notes client is initially installed.

4.3 **Changing Passwords (System Administrators):** All System Administrators must adhere to the following requirements when changing passwords.

- System Administrators can change passwords for users who forget their passwords. System Administrators will only change passwords when an appropriate "Password Request" form is received.
- Administrators will immediately lock accounts if the user reports that the password has been compromised. System Administrators will then change passwords when an appropriate "Password Request" form is received.
- When changing passwords for a user, the System Administrator must adhere to Construction Requirements as specified in section 4.1 of this document.

4.4 Password Protection: All users are must adhere to the following requirements necessary to protect passwords.

- Do not disclose your password to anyone, even someone claiming to be an important company official. System Administrators and company officials will not ask for your password.
- Do not store your password in an unencrypted fashion in text files, email, or on PDA's, etc.
- Passwords must not be displayed where others can see them. If you write your password down, it must be stored in a secure location such as a safe or locked cabinet in a room with controlled access.
- Do not share or allow your coworkers, subordinates, or supervisors use your password.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Users must notify a System Administrator immediately if you suspect your password was compromised.

5.0 Actions

The following features must be implemented by System Administrators to facilitate policy implementation if the operating system or application provides the listed procedure. Additionally, System Administrators must follow any additional procedures regarding passwords as specified in *Procedures* documents for specific applications.

- Automatic checking of length and complexity of passwords as they are constructed or changed.
- Notification of approaching password expiration and lockout of accounts when passwords are not changed as required by policy.
- Password history storage and prevention of constructing previously used passwords.
- Impose a limit of three unsuccessful attempts to provide a password. When the limit is exceeded, the account should be locked.
- On systems requiring ID files and ID file passwords, passwords should be checked against passwords stored on the server.

6.0 Compliance

The Security Manager will monitor compliance by attempting to guess passwords or running password cracking programs on a random basis. System Administrators should monitor compliance by watching for obvious violations such as posting of passwords on computer monitors.

7.0 Enforcement

Any employee known to have violated this policy is subject to disciplinary action up to and including termination.

8.0 Policy Creation and Maintenance

8.1 The GIAC Security Manager is responsible for creation and maintenance of this policy.
8.2 This policy and all changes to this policy must be reviewed by the Chief Information Officer of GIAC.
8.3 This policy and all changes to this policy must be approved by GIAC's Director of Human Resources.
8.4 For further information or clarification, please contact the GIAC Security Manager.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Assignment 4 - Develop Security Procedures

Procedure for Creating Secure Lotus Notes Client Passwords

Overview

Lotus Notes provides the capability to secure passwords by implementing a specific level of password complexity, password checking, password history, and forced password changing. Password Policy mandates that the following procedures be followed.

Why This Procedure is Important

When accessing a Domino server using a Lotus Notes client, a Lotus Notes ID file and the password for that ID file must be used. If an unauthorized user obtains the ID file and its password, that user would normally be able to freely access the Domino server and any database (including mail) that allows access to that user according to the ACL. Lotus Notes ID files are created by the Lotus Notes Administrator when the user is registered. The ID file and the initial password must be sent to the local support technician who uses the ID file to install the client software. According to Password Policy, the end user must change his/her Lotus Notes password immediately after the client software is installed. If password checking is enabled, the server is made aware that the ID file password was changed. Thereafter, users having a copy of the ID file and original password will not be able to access the server. This will prevent unauthorized access to ACL protected databases and promotes the principle of non-repudiation.

Lotus Notes provides the capability to enforce password complexity, password changing, and password history. Implementation of these features will ensure that Password Policy is adhered to and will result in secure passwords that are difficult to guess or crack.

Responsibility

Lotus Notes Administrator(s) are responsible for following the steps listed in Part I and Part II of this document when creating Lotus Notes client passwords.

Part I - Steps Required to Enforce Required Password Complexity

These steps should be followed prior to registering users and will enable a default password quality of "10". The password quality setting does not adhere to a precise set of rules, but a setting of "10" generally requires passwords containing at least eight characters and containing at least two non-alphabetic characters or a password containing at least twelve characters that does not include dictionary words.

1. Launch the Domino Administrator Client
2. From the menu bar, select File - Preferences - Administration Preferences

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

3. From the Administration Preferences Dialog Box, click the Registration Icon - then click the ID File Settings button
4. In the ID File Setting Dialog Box, set Person Password Quality to 10.

Part II - Steps Required to Enable Password Checking and Enforce Password Changing and Password History

Following the steps in Part II will enable password checking and enforce password changing and history checking. After these steps have been completed, the server will store a password digest of the user's password. The user ID files will store the necessary information to enforce history checking (by storing the last 49 passwords) and will store the date of the latest password change, the number of days until the password expires, and the number of days a user can wait before changing the password.

You must follow the steps below for each server where password checking is to be enabled.

1. Open the Domino Directory on the Administration Server and select the relevant server document.
2. On the Security Tab of the server document, set the "Check passwords on Notes ID's" field to Enabled.
3. Save and close the server document.
4. Replicate the Administration Server Domino Directory to all effected servers.
5. Restart the Domino server application on all effected servers.

The above procedures enabled password checking for the servers. You must now enable password checking for each registered user. Follow this procedure immediately after registering new users.

1. Open the Domino Directory on the Administration Server and select the "People" view.
2. Select the person documents of newly registered uses.
3. From the menu bar, select Actions - Set Password Fields
4. You will prompted to confirm the change process. Click "Yes" to confirm the change process, and you will be presented with a dialog box requesting more information.
5. Enter the following information in the dialog box:
   Check password
   Required change interval = 60
   Grace period = 30
6. Click OK in the dialog box. You will be notified that the operation completed successfully.

Verify that Action have been Performed and are having the Desired Effect

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The following warnings will be displayed to the user if the procedures above have been correctly followed.

When a user is changing his password, if the password is not sufficiently complex, the following message will be displayed.

> *Your password is insufficiently complex. Add more characters or varied characters.*

When the password expiration date is near, the following message will be displayed once per day until the password is changed.

> *Warning: Your password will expire on dd/mm/yyyy.*

Once the password renewal date has passed, the following message will be displayed when the user provides the ID file password, before the server is accessed.

> *You must change your password. It expired on dd/mm/yyyy.*

During the grace period, if the user attempts to access the server anyway, the following message will be displayed. At this point, the user can still change his/her password.

> *Your password has expired. You cannot access this server until you change it.*

After the grace period passes, if the user still has not changed his password and tries to access the server, the following message will be displayed.

> *Server Error: Your password expired and your account is locked out. See your System Administrator to reset it.*

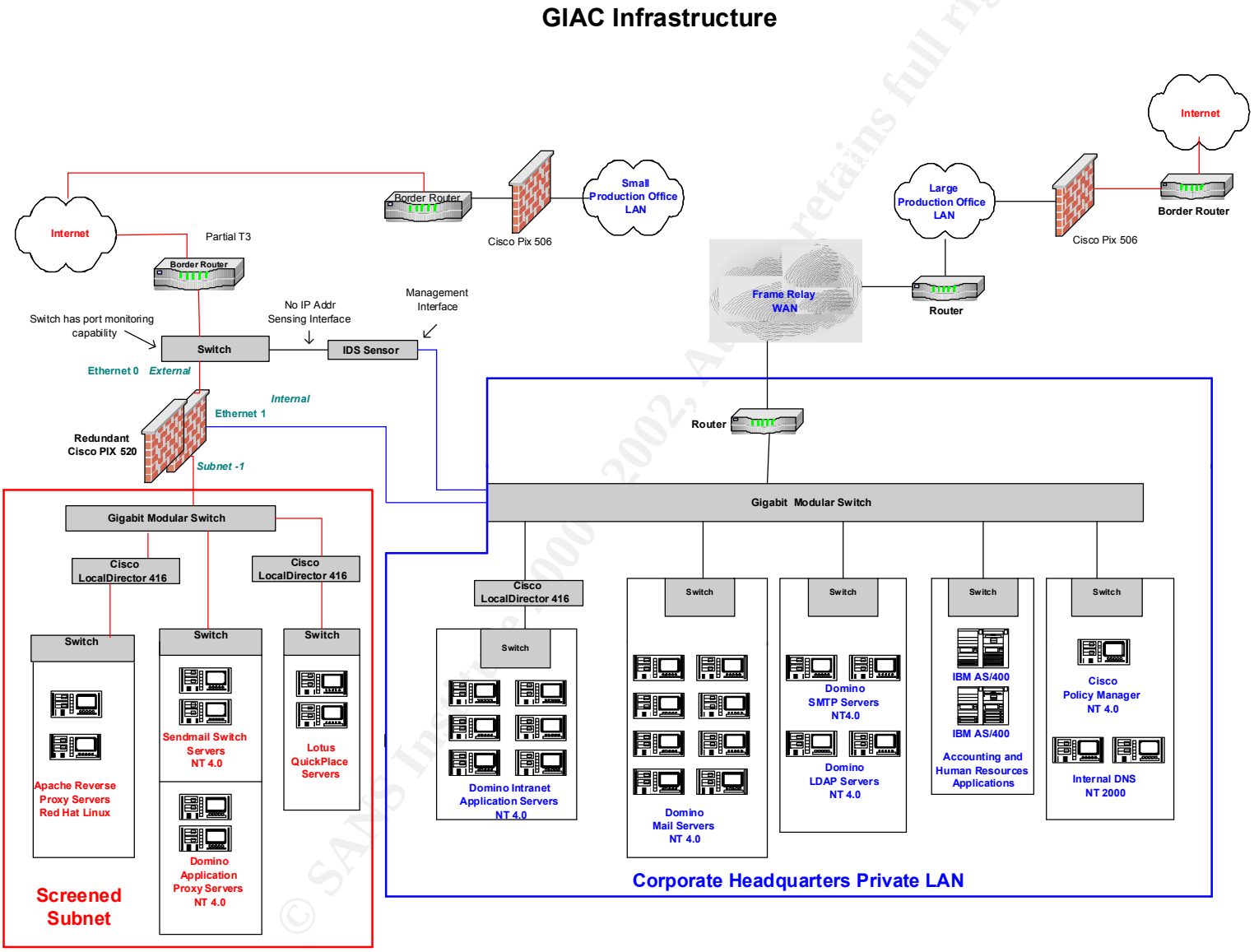
Testing Your Procedures

Before implementing these features, you should set up a test server and set grace periods and change intervals to one or two days. Try accessing the server with test accounts to make sure the messages above are appropriately displayed.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Appendix A - Infrastructure Diagram



© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Appendix B - Password Policy

This policy was copied from the SANS Security Policy Project section on the SANS web site: http://www.sans.org/newlook/resources/policies/Password_Policy.doc

Password Policy

1.0 Overview
Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of <Company Name>'s entire corporate network. As such, all <Company Name> employees (including contractors and vendors with access to <Company Name> systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 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.

3.0 Scope
The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any <Company Name> facility, has access to the <Company Name> network, or stores any non-public <Company Name> information.

4.0 Policy
4.1 General

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All production system-level passwords must be part of the InfoSec administered global password management database.
- 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.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All user-level and system-level passwords must conform to the guidelines described below.

4.2 Guidelines
A. General Password Construction Guidelines
Passwords are used for various purposes at <Company Name>. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

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.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Computer terms and names, commands, sites, companies, hardware, software.
- The words "<Company Name>", "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.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

B. Password Protection Standards
Do not use the same password for <Company Name> accounts as for other non-<Company Name> access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various <Company Name> access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for an NT account and a UNIX account.

Do not share <Company Name> passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential <Company Name> information.

Here is a list of "dont's":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in the Information Security Department.

Do not use the "Remember Password" feature of applications (e.g., Eudora, OutLook, Netscape Messenger).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once every six months (except system-level passwords which must be changed quarterly). The recommended change interval is every four months.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

If an account or password is suspected to have been compromised, report the incident to InfoSec and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by InfoSec or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

C. Application Development Standards
Application developers must ensure their programs contain the following security precautions. Applications:

- should support authentication of individual users, not groups.
- should not store passwords in clear text or in any easily reversible form.
- should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

D. Use of Passwords and Passphrases for Remote Access Users
Access to the <Company Name> Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

E. Passphrases
Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

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

6.0 Definitions

Terms	**Definitions**
Application Administration Account	Any account that is for the administration of an application (e.g., Oracle database administrator, ISSU administrator).

7.0 Revision History

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

References

Allen, Julia H. The CERT Guide to Systems and Network Security Practices. Addison-Wesley Pub Co., 2001.

"Configuring a Simple PIX-to-PIX VPN Tunnel Using IPSec". 15 Apr 2002. Online. Available http://www.cisco.com/warp/public/110/38.html

Cornaia, Mark. "Under the Microscope: Password Checking". Lotus Developer Domain. 04 Sep 2001. Online. Available http://www-10.lotus.com/ldd/today.nsf/f01245ebfc115aaf8525661a006b86b9/55e4cbd0f3257be685256abc001a5c7c?OpenDocument

"Guide to Internet Usage and Policy". Elron Software Incorporated. 2002. Online. Available http://www.elronsoftware.com/pdf/IUP_Guide.pdf

"Password Protection Policy". The SANS Security Policy Project. Online. Available http://www.sans.org/newlook/resources/policies/Password_Policy.doc

"Quickplace - Instant Team Collaboration". Online. Available http://www.lotus.com/home.nsf/welcome/quickplace.

SANS Institute, The. "Certified information Security Officer Training" Track **9**

Schreiber, Mark E. "Employee E-mail and Internet Risks: Policy Guidelines and Investigations". Elron Software. Online. Available http://www.elronsoftware.com/pdf/Schreiberwp.pdf

Williams, Christie. "Understanding Password Quality". Lotus Developer Domain. 04 Sep 2001. Online. Available http://www-10.lotus.com/ldd/today.nsf/f01245ebfc115aaf8525661a006b86b9/098c9f7d4a0cccbd85256abc0011e4f0?OpenDocument

Woods, Charles Cresson. Information Security Policies Made Easy. Pentasafe Security Technologies, Inc., May 2001.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.