GIAC ENTERPRISE

“Password policy and procedure”

GIAC Information Security Officer Practical Assignment V1.2

Christian Chablais

Resubmitted 2/26/2003

Table of Content

Summary

This paper has been prepared for the GIAC Information Security Officer practical assignment v1.2. It includes an overview of GIAC Enterprise, a fictitious financial company, with the details of its information technology infrastructure and business operations. In particular, the paper with explore three areas of critical risk: external intrusion, unavailability of systems and weak authentication. To mitigate authentication's issues, a Password policy is developed, as well as a procedure to write down passwords. Included is a diagram of GIAC Enterprise network.

Assignment 1 : describe GIAC enterprise

1.1 Brief description

GIAC Enterprise (GE) is a relatively small financial company with about 100 employees. Its core business is to manage the assets of private clients. Customers deposit their assets with GIAC Enterprise and then agree on a management agreement, defining the scope and style of management which could be either conservative, dynamic or balanced. The assets are then entrusted to GE's hands, whose role is to achieve the goal fixed with the clients, which is generally to increase the value of the assets over a mid-term horizon. The relationship between GE and its clients is based on trust, good reputation and good financial results. GIAC Enterprise offers no credit (lending) and no e-banking; it offers full banking services in asset management, from the front office (advisory), the middle office (trading room) to the back office (accounting and book-keeping, cash and securities transfer).

1.2 IT Infrastructure, network and resources to protect

GIAC corporate employees are split between two sites (A and B), geographically distant of 500 km, and the critical systems have been duplicated on both sites.

GE applies the Defense In Depth (DID) principle, which states the "placement of defenses such that the compromise on one mechanism does not render one defensless" (Sans GISO course). At network level, this is achieved by dividing it in several sub-nets.
The first layer which protects GE from **Internet** is router Cisco 1700, installed by the ISP together with a 1GB leased line, and then reconfigured with traffic management blocking rules as defined in the Naval Surface Warfare Center Site Security Plan,

section border router http://www.nswc.navy.mil/ISSEC/Guidance/Site_Security_Plan.pdf .

The second layer is an external stateful firewall Iptables [v. 1.2.6a] from Linux Redhat 8 distribution. Its role is to filter as inbound only the necessary access to the DMZ, and as outbound to accept only legitimated traffic to the Internet.

The services required by GE to interact with the Internet are placed on the **DMZ**. The machines there act as bastion hosts, described in "Building Internet Firewall" by Chapman & Zwicky as "our presence on the internet ; they are by definition highly exposed. The general principle is to keep them simple and to be prepared for them to be compromised".

- Mail server : Mimesweeper [v, 4.2.1] acts as smtp server with Internet, and is connected to the internal mail server Exchange 5.5. ; it checks virus with Fsecure 5.5 and logs all the emails.
- Web server : the IIS 4 , Coldfusion [v. 4.5], SQL Server 7 [sp 4], provides public information about investment funds ; there is no e-banking.
- Websense [v.4.2.4] works with the internal firewall. For every Internet access on services http and https, it checks if the station is authorized and logs the access. GE maintains an Internet access policy which clearly states that the access to the Webmail and chat sites are not permitted, and that all activity is monitored.
- DNS server : runs Bind [version 9.2.1].

All hosts are run on Dell PowerEdge [model 2650 - 6650], NT4 sp6, BlackIce 3.5. BlackIce is a host-based firewall with an intrusion detection engine which allows to block intruders on the fly.
All traffic on the DMZ is monitored by an IDS sensor, Snort 1.9, with interface in "stealth mode" on this subnet, and another interface on the internal Admin network. Alerts are sent in MySQL mode. Rules have been tuned with external consultant ; not surprisingly, there is a huge amount of attacks detected on this segment.

The next layer is the internal **firewall** Checkpoint 4.1 [sp 6], which is purposely different from the first layer firewall. This machine, together with the other internal firewalls, is managed centrally from a console in Admin sub-net. It operates a NAT for internal hosts which access the Internet, and allows information flow control between GE internal network, the Internet, the Extranet, the Financial network and the Admin network. All Checkpoint firewalls run on Nokia IP1440.

Then comes the semi restricted network **Extranet**, where the connections of the external mobile users to internal network are handled by a Router Cisco 3600, with a set of modem both analogic and isdn. Every user has a SecureId token and is authenticated by a Server RSA, protocol Radius, located in the internal network. This subnet is monitored by an IDS sensor.

Another semi-restricted network is the **financial net**, serving routers and satellite devices installed by financial services providers like Bloomberg, Reuters and Clearing Houses. This sub-net provides critical information. Only requested services are allowed to pass the firewall, and only some restricted internal hosts are allowed to access them. This is an application of the Least Privilege principle : if a host does not need a service, it won't get it.

Then the **Admin network** which is reserved to the Infosec department :

- The Console Syslog : collects syslog messages from routers and Windows based servers. On every Windows based servers has been installed the utility NTSyslog [v. 1.2] which forwards NT events in syslog format. The server console runs SL4NT [v 2.0], a service which acts like a syslog daemon, and logs the message in a MS SQL database. The messages are viewed via a browser, through an internal program developed with Coldfusion, with a search engine (it has been inspired by the Acid Snort console). GE Policy states that those messages must be reviewed daily.
- On same server, the management firewall software, CP 4.1 [sp 6]. Server is NT4 SP6 Poweredge
- Console Ids, Linux Redhat 8, Apache [2.0.40n, MySQL [3.23], pages web protected by RAS SecureId , Openssh [3.4p1], Acid [0.9.6b]

All Hubs or GE networks are D-Link DE816TP.

Then the Intranet of **site A** : all devices are connected to a Switch Cisco Catalyst 4006 ; there are about 100 hosts, running NT4 sp6 and Office 97.
The main services provided are :

- Financial application and accounting : Sun Solaris [Enterprise 3500]
- Mail server : Exchange 5.5, Internet connector to and from bastion host in the DMZ
- Intranet web server, IIS4, Coldfusion [4.5], MSSQL 7
- RSA server (SecureId) v 5.0.02,
- File and Print servers
- IDS monitors traffic in and out Internet.
- Workstations : Dell, NT4 SP6, Office 97
- Servers configuration : Dell Poweredge, NT4 SP6, 1Gb RAM

The **site B**, distant 500 km, is connected to site A by a 1 Gb leased line. On each access point the traffic is encrypted by a Vpn Cisco 3000 concentrator and then the data are handled by a Cisco 3600 router. The traffic though the routers is monitored by Ids, which transmits the alerts to log server in Admin network.

On Intranet site B there are 50 hosts and 30 users, with basically the same services. This site acts as backup location in case of disaster.
Sevices provided include :

- Active servers : internal mail (Echange 5.5), File and print
- Backup server : Financial application and accounting

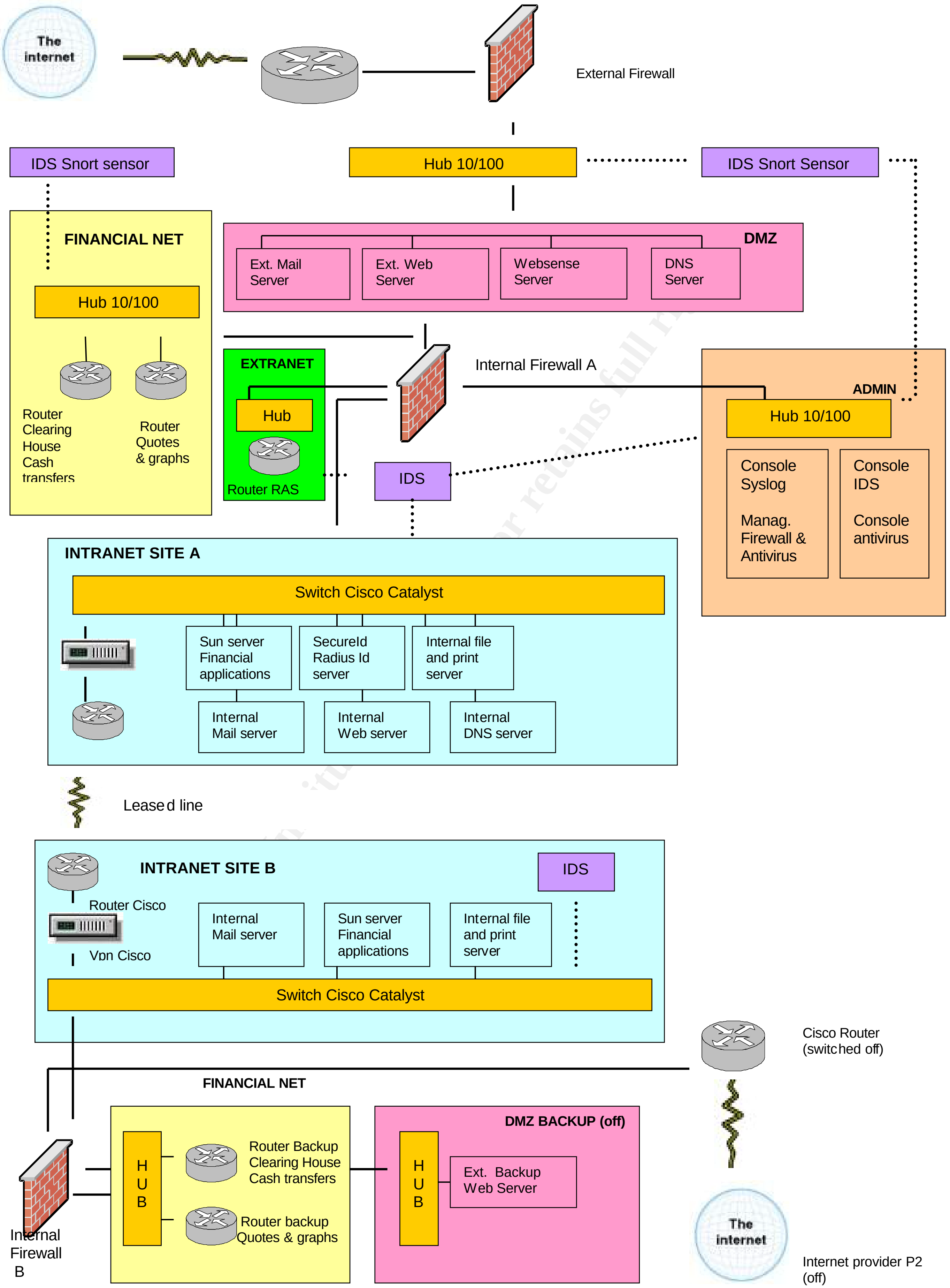
At the next layer is a Firewall CP 4.1, which filters access to the following sub-nets :

- Financial net backups : backup communication devices have been installed by financial services providers Bloomberg, Reuters, and the Clearing Houses. In case of failure of primary devices in Site A, those services are reactivated.
- DMS backup : with a leased line to Internet ; the router and modem switched off. In case the Internet link in site A is broken, they are powered on and the routing tables are manually reconfigured so that GE uses this segment.

All Windows based hosts and servers are running Norton Antivirus. The update and distribution of the virus definition files is centrally managed by a Symantec Norton Antivirus Enterprise 7.6 console on the Admin network.

On the next page : network diagram of Giac Enterprise

Network diagram of Giac Enterprise



1.3 Business Operations

GIAC manages the financial assets of its clients.

First, the customer comes to the bank and speaks with his portfolio manager (PM). This is defined as the Front office. They agree about the style of management, which can be either conservative, aggressive or balanced. Over the next meetings, they will evaluate the situation and decide if the investment policy is appropriate, based on the performance, the expectations and the markets. During those meetings, the PM prints a valuation of the client's account. This valuation must be accurate (i.e. up to date), and different portfolio analyses are quickly printed. The customer may have questions about the markets, and the PM has to be able to retrieve answers from the financial services (Reuters, Bloomberg, etc.) From an IT perspective, the important point at this stage is the Availability of systems and the Integrity of data.

To take investment decisions, the PM relies on a team of Analysts, which follow markets, companies and brokers' recommendations. The Analysts rely heavily on financial resources, via Internet or direct provider access ; for them too, the crucial point of the infrastructure is Availability and Integrity. They publish their opinions on intranet site, and their advises are digitally signed : the IT has to assure Confidentiality of data, so that their opinion is not forged.

Based on the customer's chosen investment policy and the analyst advice, orders are generated : buy or sell stocks and bonds, deposit money or exchange currency. The order is digitally entered in the Account System Program and sent to the Middle Office. The job of the Middle Office is to go on the market and find the best price. They use real time quotes to check prices and go to brokers, by telephone or direct electronic ordering. Every telephone call is recorded ; every trade is digitally registered. Of primary importance is Integrity and Availability of those data. A delay of 5 minutes in getting a quote may result in substantial financial loss. When placing online orders, Confidentiality must be guaranteed by appropriate authentication system, via smart card, passwords and encryption devices.

Once the order has been placed, it goes to the Back Office to be implemented. What the Middle Office has done so far is just to agree for a deal with a counterpart : they made the deal on a security, one Buys it and the other Sells it at a certain price. Now the buyer must deliver the money, and the seller the security. This happens in a clearing house, where both have an account. The Back office of both sides gives the corresponding order, and when both orders match in the clearing house, the deal is set. If one side fails, nothing happens. This is a simplified description which gives an idea, and the importance of Back Office function. It connects to the clearing house system and place the order. Here we have the 3 pillars of Infosec : Confidentiality, Integrity and Availability. The system must be Available, because the order has to be placed within a determined period of time, usually the same day. Integrity : data transmitted must be accurate and not alterated. Confidentiality : strong authentication mechanism ensures that transfers orders reflect what has been transmitted by Middle Office.

Sound decisions by the Portfolio Manager generate positive financial results for the customer. Sound execution of orders breeds trust, so that the customer keeps it assets in GE. Client satisfaction is the core strength of GE and is one of value added business advantages that sets it apart from its competitors. This goal is reached by taking care of what is definitely the “crown jewels” of GE: its clients’ assets.

Assignment 2 : Identify Risks

2.1 Areas of Risk, three most critical

Every single step of the GIAC Enterprise processes rely in some way on IT infrastructure. Every breakdown in IT results in break in GE operations and affects its results. I will evaluate the three most critical risks with the formula : Risk = Value x Threat x Vulnerability (ref. Sans GISO course).

2.1.1 External intrusion

Threat

- Intrusion from external point via a modem, connected directly on an individual host with a RAS software active like PCanywhere. This can originate from any host on the network, and it could be detected by a war dialer (free programs are available), or by an ex-employee who knows the access numbers and what software is installed.
- From Internet into DMZ servers : DMZ hosts by definition connected to Internet, they are here to provide a service (Web, e-mails out, dns) or get a service (e-mails in, dns). The threat may come from a badly configured system (unnecessary services active, weak or no password, or default passwords not changed), vulnerability of the OS (Microsoft), a vulnerability of a service application (IIS, DNS Bind, Coldfusion), poor application coding (Coldfusion cfm code) : vulnerabilities are discovered every day, there are a lot of exploits widely distributed. Attackers may range from scripts, kiddy, sophisticated attacker or Worm (Code red). GE DMZ systems could be used as a zombie to launch an attack ; GE Web pages could be defaced.
- Access from Internet into internal network : an attacker may gain access to a DMZ system and uses it as relay to attack internal systems, or enters directly in a badly configured firewall (open inbound connection). Another threat is active code malware : a user connects to a site, allows ActiveX code, and the machine gets compromised because of simple browsing. Instant messaging is another growing threat : most Instant messaging systems use now port 80, they allow access to local drives and software installations, which may result in Trojan-ed systems ; in this case, the illegitimate access is hidden under normal http traffic originated by a an internal user and, even worse, the hacker will be informed automatically every time the compromised host is on line (ref. http://online.securityfocus.com/infocus/1657).
- For all attacks from Internet there are millions of potential attackers.

Threat = very high

Value

- Using our hosts as zombies : not pleasant.
- GE web page defaced: as GE provides no e-banking service, but only information on investment funds, this is tedious but not critical. More serious is the damage to the reputation of GE : clients may lose trust, they might not feel comfortable entrusting their assets with the “insecure” GE.

- Once an attacker is inside, he may launch a DOS attack. Systems unavailability will result quickly in financial losses.
- Once inside, an attacker may launch more serious attacks to gain access to more resources. The principle of escalation, described in the book "Hacking exposed", shows how : plant back doors in systems, scan networks and hosts (enumeration), assess vulnerabilities, gains access to vulnerable systems, crack password, gain information about customers and GE systems. Finally, if the attacker is sophisticated enough to have knowledge of financial transactions, and provided he has the access and the systems and the passwords, he may place orders for his own benefice, and finally get hold of the crown jewels of GE : clients' assets. Such an intruder could drive GE out of business.

Value = minimal to very high

Vulnerability

The options available to deal with risk are : Eliminate, Accept, Minimize or Transfer it (ref. GISO Sans course). Eliminate the risk is not possible : GE needs external connections to conduct its business, and the threat will not disappear. Accept the risk would drive GE out of business quickly, by losing the trust and the assets of its clients. Transfer could be an option with the outsourcing of security. But GE, as all other financial institutions, has to report to the legal authorities about its infrastructure and is responsible in the first place for this. For this reason, a full outsourcing is not possible. Minimize the risk could be achieved with partial outsourcing and internal measures (co-sourcing), always lead by an internal infosec department.

Minimizing the Vulnerability allows to reduce Risk, in application of formula Risk = Value x Threat x Vulnerability. So rather than Vulnerability, I will speak about Reducing the Vulnerability, as both Threats and Values are high with External Intrusion :

Reducing Vulnerability

- External access via modem : - GE modem policy states that no modem can be installed on any workstation. If it is necessary for software support, it should be an external model, it must always be turned off, turned on only when needed, and as the intervention is over, immediately turned off. Such modems are listed, with their justification. External providers must sign a non disclosure agreement. On a random basis the Infosec dials all numbers owned by GE and controls that no modem is answering.
  - External accesses are allowed only through RAS modem pool : there is one single access point, authentication is acceptable only with SecureId tokens ; those are distributed only to few people, and each one of them must justify why he needs it. All the accesses are logged, the log reviewed weekly and the tokens not used for one month are deactivated.
- Compromising a DMZ Host. The principle regarding those hosts is "keep it simple", so there is one service - one machine (web, mail relay, dns). So if one server is compromised, only one service is affected ; this is an application of Defense In Depth and Least Privilege principles.

DMZ Active Patching : the DMZ policy states that every 15 days each system is patched. Audit is enabled, a policy states that this log is reviewed weekly. Passwords are 10 characters long and must contain special characters.
- The DMZ Subnet is screened by an IDS sensor.
- BlackIce is installed on every machine :BlackIce is a host-based firewall and IDS, with feature auto-block enabled, which means that if it detects an attack, it blocks the intruder IP. This exposes GE to a denial of service if someone spoofs a legitimate IP address. It has been a business decision : better not to offer a service for a limited period of time than to suffer an actual intrusion.
- Except for the e-mails, there is no traffic from DMZ to the internal, and no DMZ host is trusted from inside. Only explicitly permitted services are allowed by the firewall.
- DMZ Penetration testing by a an external consultant takes place twice a year.

- External access / Firewalls : both firewalls do not allow direct internal service from outside. To mitigate firewalls configurations errors, changes are restricted to authorized persons, every change is logged, with person name, what, when and why. Every firewall change must be consistent with GE DMZ and external access policies.
- Active code threat (activeX, Java): GE applies the guideline of Least Privilege. Users are granted access only to those sites they need - this is controlled by Websense filtering - and denied the others. Of course, you have to trust the few sites you visit. User awareness is a plus ; meetings are organized every three months.
- Instant messaging : the first measure is “GE Internet acceptable use” policy, which states that no chat is allowed. Then, GE limits the access to Internet sites only to those which are required.
- Inside the network, GE applies Defense in Depth, so that if an attacker eventually breaks in, he may be caught somewhere else. Details about DID inside the network are beyond this discussion at this point.

Reducing the Vulnerability allows GE reduce the risk of External Intrusion to an acceptable level. This is a never ending job which requires from GE the constant evolution of its defenses to stay in business.

2.1.2 Unavailability of the systems

Threat

The Systems of GE may be unavailable for the following reasons :

- crash of OS or application, software bug
- host hardware failure
- Human error
- network malfunctions : cables failures, by accident or malicious manipulation, switch or hubs crash
- power failure
- virus attack
- DOS attack
- fire, earthquake, airplane crash

Threat = high

Value

- System unavailability in Front Office results in poor service to client and loss of trust.
- The Analysts may not be able to take correct decision in accurate time, they miss opportunities, which may result in financial loss.
- The Middle Office cannot place orders anymore, which may result in financial loss.
- Back Office: settlement of transactions does not occur and orders are not placed : potential financial loss.
- Unavailability of the main site A, due to fire accident for example, may paralyze all GE activity for a long time.

Value = high

Vulnerability mitigation

- Critical servers are duplicated on 2 distant sites where data are replicated during night,
- A business continuity plan for critical services is ready for Front, Analysts, Middle and Back Office departments. It is tested twice a year, where people have to move physically and actually test the systems.
- On both sites, the Critical network devices are duplicated (routers & firewalls), others have contact 4-hour intervention.
- Strong backup procedures : all data is saved daily, and then tapes are moved off site.
- Physical access to critical systems is restricted ; the computer room door is closed by a code, every access is logged.
- Every system in the computer room is powered by UPS.
- DOS attack : see point “2.1.2 External intrusion”.
- Virus attack : The e-mails are checked against virus on the e-mail bastion host ; every host internally has an antivirus from a different vendor. The virus definition file update is distributed and monitored centrally by Norton AV Enterprise.

2.1.3 Weak authentication

Threat

“Authentication is more important than encryption” says Bruce Schneier in his free newsletter Cryptogram of February 2003 : “If your computer is controlled by someone on the other end of a Trojan, it doesn’t really matter what kind of encryption you have implemented.” Schneier is the author of “Applied Cryptography”, so we would rather expect him to give priority to encryption issues, but he does not : “Encryption is important ; authentication is more important.”

Schneier gives the example of a Trojan-ed system. Another very common authentication issue on GE systems is : how to be sure that the user at the other end is who he pretends to be ? Some systems use tokens to control authentication : the scheme is something you have (the token) and something you know (password). But most of them rely only on the password scheme. Knowing someone else’s password may allow an attacker to steal his identity and gains access to unauthorized resources. There are several ways for an attacker to steal a password :

- shoulder surfing : looking over the shoulder of a user while he types his password
- password guessing : poor password, like children’ or favorite football team’s name

- brute force attack, if the attacker possesses the Sam Database (Win) or shadow password file (Unix).
- keyboard logging : program that silently logs on a file any key typed on the keyboard
- social engineering : an attacker calls the helpdesk and gets admin password pretending to be an executive.
- Sysadmin and users of most departments of GE must remember from 5 to 8 critical passwords. Temptation exists to write them on a piece of paper, or store them in an unencrypted file.

Threat = high

Value

- When an external attacker gains access to GE network, stealing passwords is a step of privilege escalation, as discussed in point "2.1.1 External intrusion".
- Any internal attacker could change the contractual salary amounts in the reserved DB.
- GE, as a financial company, applies the "four eyes principle" for each transaction. This means that you need, for example, two persons for a cash transfer : the first one enters the transaction, and the other one validates it. The validator cannot enter the transaction, and the person who inputs the transaction can not validate it. If one of them could steal the other's password, he may then be able to create and validate a cash transfer, taking money from a customer's account and transferring it to his private, external account. This is a direct attack to GE crown jewels : the customers' assets.

Value = high

Vulnerability mitigation

- Lots of systems lock the account after 3 unsuccessful attempts : this is the case of all the programs that deal with cash or securities transfers, but of course not for root or admin password, which would result in denial of service.
- Antivirus protect partially against download of Trojan programs with embedded keyboards loggers. GE Acceptable Use policy states that programs on workstations may only be installed by the IT team.
- Whenever possible, GE systems use authentication with ***token scheme*** : for example every remote user authenticates with a SecureId token. Some clearing house applications offer token identification as well ; in this cases special care is taken with token management. They are kept in a safe, then distributed to users at beginning of the day, and they return to the safe at the end of the day.
- Most user authentication rely on password only authentication. All employees are aware of password importance, but there is no actual written policy in GE. It is a major security breach, and to fill this gap, a Password Policy must be written, approved and distributed, with related training sessions. It is the object of the Assignment 3. To mitigate the threat of passwords written on a piece of paper of stored in an encrypted file, procedures must be provided to users to educate them :
  - ♦ It is acceptable for GE to write down passwords on a piece of paper only if it is closed in an envelope and if the envelop is stored in a safe. The related procedure is the object of the assignment 4 "Writing down passwords".
  - ♦ It is acceptable to store passwords in a file only with the program "Password Safe" (ref. http://www.counterpane.com/passsafe.html). Password Safe is Windows utility

of Counterpane Labs which allows to keep passwords on computers : a single Safe Combination – just one thing to remember – unlocks all them. Password Safe protects passwords with the Blowfish strong encryption algorithm, and therefore is an acceptable way of storing passwords in a file, if it is used correctly. A step by step procedure will be provided to user (it is not included in this practical), and training sessions will be organized.

Assignment 3 : Evaluate and develop Security Policy

Model Password Policy
The text of this Password Policy has been taken from the “Sans Security Project” at http://www.sans.org/newlook/resources/policies/Password_Policy.pdf. It was the most appropriate existing model I could find. It will be evaluated and then revised to fit GE’s specific requirements. The original policy text is in Courier 9 font , and my comment in the usual Arial 12.

3.1 Evaluate security policy

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.

This introduction focuses on the security aspect of poorly chosen password. In other words, passwords are one of the first lines of defense. I would insist on the authentication function of passwords : people should be aware that passwords are used to identify them on systems, then to give access to whom they are supposed to. A chance-guessed password can result in theft of identify.
Saying that a poorly chosen password could result in the compromise of GE’s network is a little bit excessive : although it can be correct, one has to remember that password management is only one part of GE’s protection (ref. Defense in Depth concept).

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.

Very clear statement. As we’ll see hereafter, the text of the policy is broader and includes other aspects, such as SNMP issues, rather than focusing on just those 3 points : standard for strong password, protection and 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.

It is important to say that anybody who has an account in any form on any system is concerned. As the audience is broader than the personnel of GE, and includes as well members of GE’s board or financial consultants, I would extend the scope from “personnel” to “anybody”.

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.

The policy’s purpose “frequency of change” is treated in points 1 and 3. The SNMP point is important, but it may be confusing to find it here, especially for the average user of GE Systems. I would rather have a separate and specific policy to treat this issue. The same applies for the production system-level passwords and the “sudo” programs points. The revised policy of GE will be less complete, but (hopefully) less confusing. The statement that passwords must not be inserted in communications could be treated further in the policy (protection standard). For these reasons, I would only deal with the frequency of change in this paragraph.
The 4 month interval for the system-level passwords can be considered to be technically sound , however, it would be best to extend this period to 6 months factoring in inefficiency and a general uneasiness when following deadlines . User-level passwords should also be extended to 9 months considering the same ideology. These time frames will allow users and sysadmins to take more care in choosing a strong password while at the same time the effort to remember it.
This point shall be introduced as a bullet point stating that, whenever it is possible, systems will be configured to automatically require that users change their passwords when they expire. For example this is achieved by the policy of Windows NT or the /etc/shadow file in Redhat Linux.

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.
  - 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)

Excellent enumeration. Other weak passwords examples are the auto license plate number, bank account number, which are related to personal information too.
The comment "everyone *should* be aware" shall be substituted with "everyone *must* be aware". The phrase importing the word "should" conveys the impression that compliance with this policy is optional.

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!

These seem to be good suggestions. I would add this one: take two common words, join them, and add between the two digits or punctuation, for example "giac!*enterprise". Related to point 2 (punctuation characters), I would add to mix special characters with some selected from the "extended Ascii codes" (ref http://www.asciitable.com) .

To evaluate the effect of this guidelines with my modifications, I have simulated a password list with both poor and strong passwords, and run password cracker against them. I used LC4 version 4.00 from http://www.atstake.com/., on a Dell Optiplex Gxi, P2 233 mhz, 200 Mb ram, NT4 Sp6. LC4 configuration was : brute force with char A-Z, 0-9, spec. Char.

The first step was to choose a password and classify it as was "weak" or "strong", following the criterion of the policy guideline. Then running LC4 against them to see which ones were discovered, how long it took, and then I draw the conclusions of the test.

Password list :

Weak passwords - Why

1) ***giac*** : weak, because it is the company name, < 8 char
2) ***Giac*** : idem, but with Maj - Min
3) ***enterprise*** : weak, it is a word found in dictionary, but it has 10 char

4) ***Enterprise*** : idem, but with Maj – Min
5) ***Enterprise1*** : weak, all of the above preceded or followed by a digit

Medium to strong passwords - Why

6) ***Enterprise**** : both upper and lower case char, punctuation char, >8 char, but derived from a dictionary name
7) ***Enterprise*[]*** : idem, with more punctuation char
8) ***3nt3rpr1s3*** : idem, replaced “e” with “3” and “i” with “1”
9) ***IKAPWIAGP*** derived from a phrase : “I Know A Phrase Which Is A Good Password.” -> but all in uppercase
10) ***Ikapwiagp*** same with Maj-Min, but without digits or special characters
11) ***1kapw1agpw*** same with digits but without special characters
12) ***1kap*[]w1agp*** same with digits and special char
13) ***dancer!water*** two dictionary words (<8 char) with special character inbetween
D@nc3r!W@t3r idem with numbers and Min/Maj
14) ***telephone(organism*** two dictionary words (>8 char) with special character inbetween
15) ***T3l3ph0n3(0rg@n1sm*** idem with numbers and Min/Maj
16) ***EnterPrise*** common dictionnary word with Min/Maj inside
17) ***dancer• water•*** two common words with 2 extended ascii char

Result of the LC4 cracking session

Password	Discovered in	method
01) ***giac***	8 min 28 sec	brute force method
02) ***Giac***	8 min 28 sec	brute force method
03) ***Enterprise***	4 sec	dictionary
04) ***Enterprise***	4 sec	dictionary
05) ***Enterprise1***	1min 37 sec	hybrid
06) ***Enterprise****	1min 37 sec	hybrid
07) ***Enterprise*[]***	4 days 19 hours	brute force method
08) ***3nt3rpr1s3***	14 h 38 min	brute force
09) ***IKAPWIAGP***	23 h 42 min	brute force
10) ***Ikapwiagp***	23 h 42 min	brute force
11) ***1kapw1agpw***	1 day 2 hours	brute force
12) ***1kap*[]w1agp***	*	
13) ***dancer!water***	2 min 7 sec	hybrid
14) ***D@nc3r!W@t3r***	*	
15) ***telephone(organism***	*	
16) ***T3l3ph0n3(0rg@n1sm***	*	
17) ***EnterPrise***	4 sec. Dictionnary	
18) ***dancer• water•***	*	

* not discovered after 20 days

Conclusion

The weak passwords were all discovered in less that 9 minutes (1->5). The hybrid attack was very efficient against two dictionary words of less than 8 characters joined by a special character (13), and against dictionary names preceded or followed by a digit (5) or some special characters (6-7). It is worth noticing that brute force attack has cracked the non dictionary passwords (9-10-11) in about one day. Anyway, none of the discovered passwords fulfilled completely the guidelines for strong passwords, because none had both mixed uppercase-lowercase AND digits AND special characters.
The good news came from those that resisted : (12) non dictionary with at least 3 special characters, (14-16) two modified dictionary words with special characters ; Extended ascii characters proved very resilient.

As a conclusion, I would say that the passwords created correctly following these guidelines have passed this little test. The guidelines of the policy are therefore effective and clear enough to help anybody in creating strong passwords.
We have to take into account as well that "eventually, any password can be brute forced, given sufficient time and resource" (reference : Navy's password management guidelines http://www.nswc.navy.mil/ISSEC/Guidance/password_management.html). Think that LC4 can be used in distributed mode. This should be stated in the policy, otherwise GE staff and management would develop a false sense a security, thinking that they are absolutely safe because they followed those guidelines. Strong passwords are but one line of the defense, they improve GE's global security.
Other aspects of defense against password guessing are : restrict the access to Sam DB or unix password files, monitor and detect suspicious activities on the network and on the hosts. These aspects are beyond the scope of this policy.

For GE requirements, the guideline "Passwords should never be written down and stored on line" should be moved into the section "Protection standard" and discussed there.

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> acce ss 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.

"Do not use the same password …" is correct, it is the same idea as "leave your password at work" (reference : Navy's password management guidelines). It is important because lots of people now have a personal Internet account at home and are tempted to mix passwords. But, to avoid abuse, I will fix a limit to this and add: " the same password can not be used on more than 3 different systems."
A further issue arises when re-using the same passwords on external services. As described in the Business operations section, GE utilises many external services, clearing houses is an example, which require a strong password to assure correct authentication. These passwords are stored in external databases which may be compromised. . If an attacker can access these passwords, he could attempt to access internal GE resources. Therefore the policy should prohibit the use of the same password on both external AND internal systems.

Here is a list of "don’ts":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an e -mail message
- Don't reveal a password to the boss
- Don't talk about a password in front of o thers
- 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

It is correct not to reveal one’s password to anybody, including the boss. The challenge now is to have this policy signed by him.
All these “don’t” are good hints ; I would move the statement: “passwords must not be inserted into e-mail messages or other forms of electronic communications” in first position.

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

This is an example of how policy protects people. If a superior asks somebody’s password, any GE employee can refer him to this text to justify his refusal. If they have any doubt, they just have to follow this guideline and they will be protected.

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

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.

Partially correct : passwords must not be written down and stored in the office, but they must be written down and stored somewhere. There are at least two reasons. First the sysadmin may leave without notice for a lot of reasons that will not be discussed here. If he is not here next week, how can we access the systems without the passwords ? He surely has applied the password policy recommendation and his password will resist brute force attack. Second, any employee may apply correctly the principle “do not send any sensitive data on the Internet unless it is encrypted”. But then GE must be able to review any communication, as stated in the “Acceptable Use policy” document which has been signed by everybody.
So the passwords can be written down, but it is only acceptable to store them in a sealed envelope. A procedure must explain how to do it, where the envelope is to be kept (in a safe), that it has to be signed, who can have the authority to open it, why and how. This procedure will be developed in Assignment 4.

The statement “do not store passwords in a file without encryption” should be changed in “… strong encryption approved by infosec.” Procedures must be provided to the users to explain them how to do it.

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.

This point should already have been treated.

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

Yes

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.

I will treat this aspect in the "enforcement" section.

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 u ser 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 retr ieval, wherever possible.

Like SNMP and SUDO, this point is important, but it may be confusing for the average user of GE Systems to find it here. I would treat this issue on a separate and specific policy.

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.

Remote access is object of a separate policy, where the only acceptable authentication is with SecureId.

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 pass phrase 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 characte rs. An example of a good passphrase:

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

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

This is a valuable statement, because sooner or later GE staff members will have to deal with public / private key creation and management. But as it is not directly related to the purpose of policy – the creation of strong passwords, their protection and the frequency of change -, and in order to keep it as simple as possible, this paragraph will be skipped.

5.0 Enforcement

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

Necessary ; a policy that can not be enforced will fail.
As previously mentioned the “Password cracking” section is applicable in this section . In the case a password is found, the user will firstly be requested to change the password. If the problem is not resolved, he/she will be required to undertake training sessions. Finally, in the case of “lack of good will”, disciplinary sanctions shall apply with one exception: “If a password is required which is mandatory to continue working, and neither the System Administrator, infosec team member or Security Officer is available,, you are allowed to ask it to a staff member. This incident must be reported and the password reset when the situation normalizes” .

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).

Finally, the responsibility section is lacking, specifically who is responsible for revising, evaluating and enforcing the policy. Moreover , as this policy is business wide, each Department Manager shall be responsible for the dissemination and confirmation that the policy is understood by his/her staff.

3.2 Revised security policy

Password policy

1.0 Overview

Passwords are used to manage and control access to our computers and networks. Another function of passwords is to authenticate users and to give them access to the resources they need. A poorly chosen password may result in the compromise of Giac Enterprise corporate network, inappropriate or criminal use of Giac Enterprise resources or theft of identify. As such, all Giac Enterprise employees (including contractors and vendors with access to Giac Enterprise 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 anybody 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 Giac Enterprise facility, has access to the Giac Enterprise network, or stores any non-public Giac Enterprise information.

4.0 Policy

4.1 Frequency of change

- *All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed at least every 6 months.*
- *All user-level passwords (e.g., e-mail, web, desktop computer, etc.) must be changed at least every 9 months. The recommended change interval is every 6 months.*
- *Whenever it is possible, systems will be configured to automatically require that users change their passwords when they expire.*

4.2 Guideline for the creation of strong passwords

Passwords are used for various purposes at Giac Enterprise. 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 must 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.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The words "Giac", "sanjose", "sanfran" or any derivation.
    - Birthdays and other personal information such as addresses, phone numbers, auto license plate number, bank account number
    - 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, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Contain extended Ascii codes such as "• • • " (see http://www.asciitable.com for a complete list with the corresponding numbers). To obtain an extended Ascii code, press the alt key and type alt + character number with the numeric keyboard.
- 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.
- 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.
- Another way is to take two common words, like "dancer" and "water", mix upper and lower character and join them with a special character : "Danc3r• wat3r• "

Of course, do not use either of these examples as passwords!

NOTE : It is an unfortunate reality that given sufficient time and resources any password can be "brute forced", since there are a limited number of characters to fill a string of limited length. These guidelines DO provide a framework within which to operate at an appropriate level while ensuring an appropriate control mechanism.

4.3 Password Protection Standards

- **Leave you password at work** ! Do not use any of the password for Giac Enterprise systems outside of Giac Enterprise accounts.
- Where possible, **don't use the same password for various Giac Enterprise access needs**. For example, select one password for the NT account and a separate password for the UNIX account. In any case, the same password cannot be utilised on more than 3 different systems. Furthermore, it is not allowed to use the same password on external systems and GE internal systems.

- ***Do not share Giac Enterprise passwords** with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential Giac Enterprise information.*
- *You may **write passwords down** only in a sealed envelop which should be kept in a safe. For this operation refer to Giac Enterprise procedure. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without strong encryption. Only programs approved by Infosec will be used.*

Here is a list of "don'ts":

- *Don't reveal a password in an e-mail message messages or other forms of electronic communication*
- *Don't reveal a password over the phone to ANYONE*
- *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*
- *Don't use the "Remember Password" feature of applications (e.g., Eudora, OutLook, Netscape Messenger).*

If someone demands a password, refer them to this document or have them call someone in the Information Security Department. If an account or password is suspected to have been compromised, report the incident to InfoSec and change all passwords.

5.0 Enforcement

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. If the password is "cracked" during a successive scan, the user will need to undergo training sessions, until the password he/she creates complies with this policy. In the case of "lack of good will", disciplinary sanctions shall apply..

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

Exception(s) to this policy: :

- *If a password is required which is mandatory to continue working, and neither the System Administrator, infosec team member or Security Officer is available, , you are allowed to ask it to a staff member. This incident must be reported and the password reset when the situation normalizes .*

6.0 Responsibility

- ***Any user of GIAC resources**, as defined in the "Scope section", is responsible for choosing, storing and changing passwords in compliance with this policy.*
- *The **Security officer** is responsible for reviewing this policy once year. He/she will organize technical and information training sessions at the minimum once a year.*
- *Each **department manager** shall be responsible for distributing and confirming that the policy is read and understood by each employee The department manager will also ensure that all new hires will be provided a copy of the policy as part of their orientation.*
- ***Infosec** shall be responsible for auditing IT resources to ensure compliance with this policy on a random selected basis, but not less than twice a year.*
- ***System administrators** shall configure the systems and provide adequate support in the implementation of this policy.*
- ***Internal auditor** shall be responsible for the periodic review of IT resources to ensure compliance with this policy and reporting to authorities.*

7.0 Definitions

***External system** : any system which is not located in the GE internal network. A good example is an internet Web server, but it can be a financial service as well.*

8.0 Revision History

Effective date : 19th February 2003
Next revision : March 2004

Assignment 4 : Develop security procedures

The text of the following procedure is based upon some paragraphs of Navy's "Password management guidelines ", which have been tailored for GE's use.

Procedure : Writing down passwords

1.0 Background
Passwords are personal and should be treated as sensitive, confidential information. There are two reasons to write down passwords : (a) to remember them when they have been forgotten, or (b) when the authorized management staff needs to access them.

2.0 Purpose
This procedure refers to GE Password Policy, in particular to the Password's protection section. It establishes how to write down passwords and seal them in an envelope, how to store them and retrieve them appropriately.

3.0 Scope
The scope of this procedure includes anybody 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 Giac Enterprise facility, has access to the Giac Enterprise network, or stores any non-public Giac Enterprise information.

4.0 Action
4.1 Storing passwords

- *Write the password(s) down on opaque paper, and for each password indicate what it is for.*
- *Fold the sheet twice and place it in an envelope.*
- *On the outside of the envelope, write down your name, the content of the envelope and who is authorized to open it on an everyday basis if you are not present. Consult with your department head or the Infosec to ensure that this last information is compatible with your department policy and organization.*
- *After you close and seal the envelope, sign your name and date across the seal.*
- *Take the envelope and give it personally to the Safe Officer who will store it in a safe.*
- *You may use one envelope for one password, or one envelope for all you passwords. In this case, whenever the envelope has been opened by an authorized person different from yourself, you will have to change all passwords stored in the envelope.*

4.2 Retrieving passwords

- *If you ever forget your password, or if you need to change it, ask the authorized officer to open the safe and retrieve the envelope.*
- *While you stay at the Safe Officer's desk and in his/her presence, recall or modify the password, and place it in a new envelope.*
- *Sign and seal the new envelope as above.*

- *If you use a new piece of paper, you must shred the one with the old password. Ask the Safe Officer or a delegate to accompany you and witness shredding of the paper ("four eyes" principle).*
- *If someone else, who is authorized to access your information in your absence, needs your password (this must be negotiated and documented in advance), they can use the procedure above except they will write on the envelope when and why they opened it. When you return to work, change your password and place the new one in an envelope as described above.*

5.0 Frequency of change

Do update the password(s) stored in the envelope every time you change them, either as a routine periodic change or when it has been necessary to use your account in an emergency during your absence.

6.0 Responsibility

- *The **Safe Officer** is responsible for the storage of the envelopes and of their release to their owner or to a legitimate staff member. He'll make sure that no copy of any kind is made of the envelope's content, and that discarded papers are actually shredded*
- *The **Infosec department** must control that at least one envelop exists for every admin level password. In case of legitimate suspicion, the Infosec team member may open an envelope to control that the password does exist and to test it. This action must be approved by the Security Officer and two persons must be present ("four eyes" principle).*
- *Each **department manager** shall be responsible for distributing and confirming that the procedure is read and understood by each employee The department manager will also ensure that all new hires will be provided a copy of the procedure as part of their orientation.*
- *The **Security officer** is responsible for reviewing this procedure once a year.*
- ***Internal auditor** shall be responsible for the periodic review of safes with password envelopes to ensure compliance with this procedure and reporting to authorities.*

8.0 Revision history

Effective date : 19th February 2003
Next revision : March 2004

References

Internal :

Naval Surface Warfare Center Site Security Plan, section border router
http://www.nswc.navy.mil/ISSEC/Guidance/Site_Security_Plan.pdf .
Navy's password management guidelines :
http://www.nswc.navy.mil/ISSEC/Guidance/password_management.html

External :

Bastion host : "Building Internet Firewall", Chapman & Zwicky, Ed. Oreilly

Instant Insecurity : http://online.securityfocus.com/infocus/1657
Enumeration and privilege escalation : “Hacking exposed”, Scambray, McClure & Clure, Ed. Osborne/McGraw-Hill
Ascii codes reference table : http://www.asciitable.com/”
Software LC4 : http://www.atstake.com/.
“Applied cryptography”, Bruce Schneier, John Wiley & Sons
“The importance of authentication”, Bruce Schneier, Crytpogram February 2003, http://www.counterpane.com/crypto-gram-0302.html