GISO PRACTICAL ASSIGNMENT VERSION 1.2

GIAC Enterprises

Submitted by: Lori Homsher
lhomsher@jjsheeran.com
Date: April 25, 2002

Table of Contents

Section
1

Describe GIAC Enterprises

A digital printing and shipping company

Giac Enterprises is a small business that provides high-speed, digital copying services using several Xerox Docutechs. GIAC's business goal is to provide efficient, fast turn-around of digital print files, including sales training manuals, corporate literature, print-on-demand documents, personalized laser letters, and price sheets.

In addition to printing services, GIAC Enterprises offers repack/distribution and shipping services. GIAC creates training manuals for their customers and ships them to customer sales reps and district managers. Personalized laser letters and corporate literature are shipped to consumers in mailing campaigns or as requested. Although GIAC is a small business of approximately 70 employees, most of GIAC's customers are Fortune-500 companies.

IT Infrastructure

GIAC's IT Infrastructure provides system support for internal employees, as well as remote access for business partners and outside consultants. A diagram of GIAC's network is provided in Appendix A.

GIAC's IT management has chosen Linux as the server of choice because of the low cost, yet high quality software available. As a small business, GIAC needs to provide the latest technology at small-business prices. Most internal servers run Linux RedHat 7.1.

The desktop OS is Windows NT/2000, although a few Windows ME machines found their way onto the network through orders placed outside of IT.

The connection to the Internet is provided over a fractional T1. Currently, the DMZ consists of a Cisco router, external web server, and firewall. All inbound traffic comes through the Cisco router. The router performs basic filtering and sends incoming web traffic to the external web server and all other traffic to the firewall. The external web server holds GIAC's company "brochure" web site. There is no confidential data held there. All services have been removed from the web server except for those needed for Apache. Tripwire is running on the web server and will notify GIAC's IT department of any changes to the server or web site within one hour. In GIAC's DMZ, the Cisco router servers as the firewall that sits between the DMZ and the Internet. The Linux Firewall protects GIAC's internal network from the DMZ.

The filtering provided by the router includes:

- No internal IP addresses passed in or out (all network classes)
- No IP spoofing
- Allow ICMP request & reply only, along with the "can't fragment" messages (type 3, code 4) as suggested by Marc Slemko in *"Path MTU discovery and filtering ICMP"* [1]. The "can't fragment" packets are an integral part of the Internet. Without feedback that the packet being sent is too large, the host will continue to try to resend the packet, and the packet will continue to be silently dropped.
- Block broadcast packets in & out
- Block incoming IP with destination IP not equal to router address (GIAC's internal network uses private, non-routable IP addresses)
- Block all non IP traffic
- Block TCP/UDP packets with a source port of zero

The Linux firewall performs stateful filtering using netfilter and RedHat 7.1. The firewall has been configured using the recommendations found on the Linux Packet Filtering HOWTO, maintained by Rusty Russell[2]. The firewall rule set includes the same filters as the router with these additional filters:

- Deny all except what is specifically allowed. By default, this includes (but is not limited to) deny all incoming port 80 requests (GIAC's internal web server is for Intranet use only), deny all incoming port 53 requests (GIAC uses ISP DNS servers on the outside of the network), and deny all incoming Netbios requests.
- Allow only business partners and remote users into ssh ports. Valid users are indicated in the firewall configuration. Each server requiring remote access runs ssh on a different port. Incoming ssh port indicates to which server traffic should be forwarded.
- Allow ftp access from specified IP addresses only. GIAC's ftp server sits on the internal network and requires a valid ftp logon. It is not an anonymous ftp server. Ftp users have extremely limited access and cannot move outside of their home directories. Details of ftp access are provided below. Tripwire is running on the ftp server.

- Allow incoming mail from ISP only (GIAC uses their ISP as a "Smart Relay" for email)
- Allow outbound traffic from valid network IP address only. Block outbound DNS to servers other than ISP DNS servers. Block outbound Netbios traffic.
- Squid proxy services on firewall control all outbound http requests. Access Control Lists are set to limit outbound requests from internal network only and to restrict port ranges.

Preventative maintenance of firewall includes:

- Firewall log files are reviewed weekly by the system administrator, using some automated scripts. Strange log entries or trends are passed along to IT management for further analysis.
- System administrator also evaluates daily disk usage and processes running on firewall. Firewall is running only the services required to fulfill its function (inetd.conf and c compiler have been removed)
- Software is kept up-to-date
- Tripwire is running on firewall.

The internal network provides resources for printing services, shipping and receiving, and office staff. The key components of GIAC's internal network include the print servers, graphics workstations, ftp servers and inventory control/fulfillment software. Currently, all hardware and software is controlled by GIAC's internal IT department, *with the exception of the print servers,* which are maintained by the Printer Manufacturer*.*

Snort network-based Intrusion Detection is provided on the internal network. Alerts are sent to the system administrator. GIAC doesn't have the IT staff to properly manage the large amounts of data that can be generated from an IDS sitting on the DMZ. Instead, IT management has decided to use Snort on the inside network for help in alerting the system administrator of possible attacks on the network. This includes detection of events that might occur when a hacker tries to find out more information about the network. In *"Hacking Linux Exposed"*, by Brian Hatch, James Lee, and George Kurtz [3], the authors review many types of attacks, including: ping sweepers, port-scanning tools, OS detection software and other scanners such as SAINT, SARA and Nessus. GIAC's IDS is configured with the goal of catching the attacker while he/she is still gathering information about the network.

Symantec network-based anti-virus is configured to 'push' anti-virus updates to all workstations on the network on a daily basis.

GIAC outsources its mail server management to a local ISP. The ISP provides some basic email filtering including: reject email from open-relay mail servers and reject email with obviously inappropriate subjects. All incoming mail passes through the firewall and gets delivered to the individual desktops. Email is not encrypted on a regular basis, although PGP has been used occasionally to receive encrypted files from a customer. Desktops are configured to forward email messages with attachments into a 'quarantine' folder.

The IT department handles Windows operating system and software upgrades whenever time permits. There are no regularly scheduled updates. The IT manager subscribes to several email news lists including: (the CERT mailing list, RedHat-watch-list@redhat.com, incidents@securityfocus.com, focus-virus@securityfocus.com, intrusions-subscribe@incidents.org, to keep up-to-date with the latest vulnerabilities. If a vulnerability is reported that applies to GIAC's systems, the IT Manager forwards the email to the network administrator for follow-up.

Business Operations

Typical "flow" of a printing job at GIAC Enterprises

a. Customer sends print document and shipping list, if applicable, to GIAC's ftp server. The customer's unique login dictates the directory into which the files are stored. Disk quotas are set to restrict disk usage per user.
b. Graphics department at GIAC retrieves document from ftp server (using samba for file sharing). The file length is verified and the document is opened at graphics workstation. Document is checked to ensure formatting has held and fonts are available.
c. Document is sent to print server for final set-up.
d. Printer operator opens document in print server software. At this step, specifics such as finishing (stitching, hot-tape binding, etc) and locations for inserting tabs or offset-printed pages are indicated. The printers perform in-line stitching (stapling), as well as hot-tape binding for documents less than 100 pages. Large binders can be printed, but the finishing is handled as a separate project. GIAC can perform spiral binding, or insert into ring binders.
e. For binders, the following final steps are required:
   - GIAC either shrink-wraps the inside pages, or inserts them into the binder.
   - Binders are then packed for shipment. GIAC can send one binder to each person on a list, or can pack up binders for bulk shipment.
   - For multiple shipments, the address list is loaded onto the shipping software and shipping labels are printed.
   - Shipping data is uploaded into the order fulfillment software.
f. In addition to the standard print process listed above, GIAC's customers will place orders directly on GIAC's fulfillment system

(application server) for training binders and other literature stored in GIAC's warehouse.

Applications and type of access required to carry out business operations

Customers require access to GIAC's ftp server for delivery of documents for printing. This is handled using a Linux ftp server (running wu-ftpd version 2.6.2) with guest user logon. The ftp server does not allow anonymous logon. GIAC's customers are provided with a logon and are placed in a restricted group. The ftp server is configured with the rule says that that all REAL or GUEST users in the ftp group will be treated just like an anonymous user – their home directory becomes their root directory. This type of access is referred to as 'guestgroup' in the ftp configuration files. Under general Linux permissions, it is sometimes referred to as 'chroot', which uses a special root directory (the user's home directory in this case). With this setting, it is impossible for the ftp users to move outside of their home directory. As GUEST users, they are unable to run any programs, unless the programs are specifically placed into their home directory path.

Some of GIAC's customers need access to the inventory control/fulfillment application. These customers access the system to check on inventory levels for upcoming projects and to place orders for literature that is warehoused at GIAC, such as letterhead, brochures and envelopes.

Most of GIAC's remote-access customers use Secure Shell (ssh version 2) with the port set to match the port running on the application server. Secure Shell (ssh) is a remote login program that provides encrypted telnet-like access. According to the ssh 'man' page, it is intended to replace rlogin, rsh and telnet, and provides secure encrypted communications between two hosts. For additional security, the firewall checks the incoming IP to make sure the request is coming from a valid customer, and then forwards the connection to the application server. The application server is running tcpwrappers to limit access to valid domains only.

Each remote-access customer has a unique Unix system logon and password. A second logon is required to access the application, which runs on a proprietary database (Unidata). The application logon indicates which account database this user has access to on the application server. Application-level passwords are set to match the Unix system passwords. They are required by the application to point the user into the proper database, but are not providing additional security at this time. As a convenience to customers, Unix system passwords (along with their matching application passwords) are set to never expire.

There are a few customers who access GIAC's application server using dial-up connections. These customers are local and the dial-up access was provided long before the Internet became available. The modems are also provided as a back up to customers experiencing Internet connection problems. GIAC supplies a bank of approximately 8 modems, which are attached to the serial board on the application server.

GIAC's IT employees often need to access the servers from a remote location. In addition, outside consultants are used to develop new applications requiring specific skill sets. GIAC has a pool of about four IT consultants who provide help to GIAC's two full-time programmers on an as-needed basis. IT employees and consultants both access the system remotely using Secure Shell (ssh), version 2. As with customer ssh connections, consultant's and employee's domains are specified in the ssh configuration. When a consultant or employee changes their home ISP, the domain must be changed in the ssh configuration file and the IP must be changed in the firewall to allow access. As with customers, passwords never expire for remote-access employees and consultants.

Internal employees require file sharing across servers to pick up documents for processing. Since the servers are running Linux and the desktops are running Windows NT/2000, GIAC uses Samba to accomplish file sharing across these platforms. Samba is a GNU utility that allows a Unix machine to act as a file server for Microsoft machines. GIAC also uses samba to automatically backup the networked PCs to a samba file server.

Section

2

Identify Risks

Dial-up Modems

GIAC's dial-up modems were installed 10 years ago to allow customers to access GIAC's application server. The modems were required for access in the pre-Internet days, but now they offer more risk than benefit. The fact that they are attached directly to GIAC's application server makes the modems an even greater risk. The application server holds all order history, customer databases and inventory levels for GIAC's customers. From a hardware/software and customer service point-of-view, the application server is GIAC's "crown jewel".

Of all servers on GIAC's network, the application server, print servers and firewall are the most critical (the ftp server is critical, but is quickly and easily replaced). If the firewall or application server goes down, the ssh customers can't access GIAC's application server. If the print servers go down, GIAC can't run any print jobs internally. Since GIAC is a service company, they do everything with customer service in mind and have manual processes in place as a work-around for internal network problems. The golden rule at GIAC is: The customer should never be inconvenienced (but inconvenience is perfectly acceptable for internal employees).

The threat to GIAC is of someone gaining access to the application server using war dialing and password cracking. Placing dial-up modems on the application server makes GIAC vulnerable to this threat. Since both war dialing and password cracking software are easy to find and run, and since GIAC has a policy of never expiring passwords, this threat is a high-risk threat to GIAC.

The consequences to GIAC if the application server was exploited include any or all of the following:

- The application server could be disabled, causing GIAC's customers to have disruption of service. This could be accomplished through a DoS attack, root access could be gained using a buffer overflow vulnerability, and Trojan or backdoor programs could be loaded onto the server. Historically, GIAC has provided high-availability to their customers. All system upgrades are scheduled around their customer's business hours. As a result, GIAC's customers have high expectations regarding system availability. They expect the application server to be available every business day. A disruption of service to the application server may cause GIAC's customers to lose confidence in GIAC's ability to provide continued high level of service. In addition, GIAC's customers would be inconvenienced – and this is a direct violation of GIAC's golden rule of "never inconveniencing the customer".

- The data on the application server might be compromised. Files could be corrupted; data could be wiped out. Some worms simply corrupt the backup data for weeks until no good backups can be found, then the data on the disk is destroyed. In this case, GIAC would be unable to provide their customers with order history and inventory data. Customer confidence will be shaken if the integrity of the data is not maintained.
- If an exploit were made public, GIAC would suffer bad publicity. This is particularly worrisome for a company like GIAC, since they work with large, nationally known corporations. Bad publicity would most likely result in lost business. There is no shortage of small businesses ready to replace GIAC as a preferred vendor to their customers.

GIAC has prepared their customers to have high expectations in the level of service provided by GIAC. These high expectations are great when everything is working properly. However, when the application server is unavailable due to a security issue the same high expectations serve to amplify the problem in the customer's mind.

Steps to be taken to mitigate the risk

1. As an immediate, partial solution, the bank of modems can be turned off each night. This will reduce the window of opportunity for war dialing to take place. This solution has no set-up cost, but does require someone to remember to turn the modems off and back on each day. Since this solution fully relies on user intervention, there is a high probability of error (someone forgetting).

2. For a more long-term solution, GIAC should notify customers that their dial-up accounts will be replaced with a more secure remote access solution, like Secure Shell (ssh). The complete project should also include steps to minimize the need of a dial-up account as a backup for Internet connection problems. A backup firewall can be configured to minimize down time if the firewall goes down. This will take care of Internet access problems (as a result of firewall issues) on GIAC's side, but doesn't provide a backup solution to Internet access problems on the customer's end. If the customer loses their Internet connection, or if GIAC's Internet connection goes down due to something other than the firewall, it is

suggested that the customer fax their orders to the customer service representative at GIAC, who will enter the orders locally.

The recommendations for handling Internet connection problems will be as follows:

a. If GIAC's firewall goes down, the IT staff hot-swaps the newly configured firewall into place. Downtime should be under one hour.

b. If GIAC's T1 goes down, or if the customer's Internet connection is down for any reason, the customer faxes their orders to their GIAC customer service representative, who will enter them into the system within 30 minutes of receipt.

3. Implement ssh public-key authentication for remote clients, as outlined in the Secure Shell FAQ: http://www.employees.org/~satch/ssh/faq/ssh-faq-4.html#ss4.5 [4]. With this technology, remote clients can use the convenience of public-key authentication to access the servers rather than hassling with passwords.

   The costs to implement solution #2 is approximately $3000 for the cost of a replacement server, 16 hours of the system administrator's time to configure and test the firewall, and 4 hours to notify the customers of the new procedures. Ongoing costs include the time required for the customer service reps to enter the orders each time the customer's Internet connection or GIAC's T1 is down.

   Ssh public-key authentication can be implemented after solution #2. There are no software costs involved, but many hours of training will most likely be required.

Lack of Password Policy

GIAC's golden rule – "never inconvenience the customer" – applies to password policy as well. Nobody likes to memorize a password, especially if a new one is assigned automatically and is meaningless.

Currently, GIAC's IT staff uses the mkpasswd command in Linux to generate a good password for all users (employees, consultants and customers). Each user is assigned his or her user name and password, which stay with them until someone in IT realizes they have left the company. There is no expiration of passwords, or automatic regeneration of new passwords. Also missing is a defined process for removal of old user accounts. Employees who have been gone for months may still have active accounts on the system.

The current lack of password policy creates the following risks to GIAC:

- The greatest risk is of employees who gain access to the system after they've quit (or worse – after they've been fired). Since GIAC has a bank of modems attached to the application server, an ex-employee could use dial-up to access the system. Of particular concern are employees who worked in IT or customer service and had access to the dial-up customer's logon information. Even for employees working outside of these departments, it is easy to get customer login and password information from other employees. There is no policy or training in place to prevent this. The ex-employee (or current employee who can see the 'writing on the wall') might have dial-up and login information for accounts other than his/her own.
- Over time, employees have become lax with their passwords, even sending them over email to fellow employees or posting the password on their monitors for ease-of-use. An external hacker might come across the dial-up number and user login information on an unencrypted email intended for GIAC's customer.
- After a hacker or ex-employee has gained entry to the application server, they have all the time in the world to wreak havoc, since the password will never expire.
- Since there is no policy, GIAC has no process for punishing employees who are careless with their passwords.

These risks, along with the associated threat of system abuse, are of particular concern to GIAC because they frequently lay off employees during slow seasons. Unless the IT system administrator happens to know that someone was let go, the laid-off employee's system account remains active until the system administrator gets around to listing current users and figuring out who is no longer employed by GIAC.

The consequences of these risks are similar in many ways to the dial-up modem consequences, but the damage may be greater since "insiders" may perform the attack. Someone from the inside may know GIAC's points of weakness better than an outsider. Also, an ex-employee knows GIAC's competition and may be better able to use that knowledge to hurt GIAC.

- Unauthorized use of system resources: An ex-employee could use the application server as his own personal server -- to run outbound email campaigns, write and run programs for his C class, download and test some new software (IT has trouble keeping up with software versions now, just imagine how confused they will be when software starts changing on its own!). The firewall will allow outbound email from the internal network, so the use of the application server as a spam server may be a quick and easy way for the ex-employee to make some money while waiting for his unemployment check. Even though the application server is not configured as an open relay mail server, the results of multiple spam campaigns may be enough to get GIAC's server (the outside IP address) placed on a blacklist like the MAPS Relay Spam Stopper.

- Damage done by retaliation from an angry ex-employee: Of particular concern is the damage an ex-IT employee can cause. The entire system could be wiped out, or small annoying problems might creep in over time. The application server may be disabled, causing a disruption of system availability to GIAC's customers.
- Data integrity problems: an ex-employee with information about competitors (or someone who has left GIAC to work for a competitor) may download data files containing confidential information, or change or corrupt data files to ruin the integrity of GIAC's database.

System availability and integrity may be compromised, resulting in decreased level of service to GIAC's customers. Any of these consequences would result in bad publicity to GIAC if provided to the Press.

Steps to be taken to mitigate the risk

1. Change system settings to automatically expire passwords on a regular basis, such as every 90 days.

2. Implement password limitations to require all passwords to be at least 8 characters in length, contain at least 3 alpha, 3 numeric and 2 special characters.

3. Perform User Awareness Training to teach users how to pick meaningful, yet strong, passwords. For example: use actor's names from your favorite movie, but vary the spelling (perhaps swapping first and second half of the name). Combine this with a meaningful number on each end and a '.' in the middle.

4. Also part of User Awareness Training – how to properly store passwords so that they are accessible by the employee, but not by hackers (do not store on PDA, post on monitor, etc).

5. Enforcement of good passwords using crack, or another utility on a regular basis.

6. Remove dial-up access.

Costs of implementation

Costs for implementing good password procedures are hard to estimate. The administration of passwords can be automated at the server and should only take an hour or two per server to set up. However, User Awareness Training is ongoing and can take several hours per month to implement properly. Therefore, the costs for mitigating this risk are ongoing and should be a part of the yearly IT budget. Estimate two hours per employee per year.

Upgrades and Patches

The IT Department currently applies software upgrades and patches as filler work whenever time permits. The IT Manager subscribes to several mailing lists to keep notified of virus updates, security vulnerabilities, and RedHat-specific issues, but there is no procedure in place for how quickly the updates should be applied. The responsibility for applying the updates is not clearly defined and there is no follow-up to confirm that the updates were actually applied. There are no standards for security settings on Microsoft software, including Internet Explorer, Windows and Office.

The IT Infrastructure includes the following Operating Systems:

- RedHat Linux (firewall, ftp server, web server, file server, Intrusion Detection System, 3 desktops)
- AIX (application server)
- Solaris (print servers for large Laser Printers)
- Windows 2000 Server (NAV & network print server)
- Windows NT/2000 (~ 30 desktops)
- Windows ME (2 desktops)

Software running on the various systems includes (this list in not all-inclusive because GIAC's IT has not completed a thorough inventory of all software running on the individual systems):

- Firewall: NetFilter iptables, squid, Secure Shell, tripwire
- ftp server: wu-tftp, sendmail, samba, Secure Shell, tripwire
- Internal web server: Apache, Perl, xdm, nPulse (network monitoring software), sendmail, samba, Secure Shell, tripwire
- External web server: Apache, Secure Shell, tripwire
- File server: samba, sendmail, Secure Shell, tripwire
- Intrusion Detection System: Snort, samba, sendmail, Secure Shell, tripwire
- Application server: AIX, Unidata (application software), samba, sendmail, Apache (used for AIX's help system), tripwire
- Solaris: unknown – maintained by Printer Manufacturer
- Windows 2000 Server: Symantec Norton Anti-virus – corporate edition, Terminal Server, default Windows services

- Windows NT/2000 desktops: Internet Explorer, Eudora e-mail, Microsoft Office (versions vary)
- Windows ME: Internet Explorer, Eudora e-mail, Microsoft Office (versions vary)

The risk to GIAC of continuing with the current (lack of) upgrade procedures is: Unpatched Windows systems could be compromised using an existing or new exploit. Since the Unix servers are running tripwire, IT is notified immediately of any changes to those systems, so the greatest risk is really on the desktops and the Windows server. Of course, the Unix servers should be updated as well, so any policies created to address upgrade procedures must include all servers.

GIAC's desktops and the Windows server run Internet Explorer and Microsoft Office – both known to have new vulnerabilities announced monthly. There is no current standard for security settings at GIAC, so IE configurations may include runtime permissions on ActiveX or JavaScripts, and Office may be set to run macros. GIAC's network sends all web traffic through the proxy software running on the firewall. The proxy software checks for traffic on standard ports, but no filters are set to prevent access to specific web sites. Some employees have installed WebShots and other free-but-unnecessary software on their systems. This type of software often installs hidden programs that run in the background.

Desktop exploits may result in changes to the Windows Registry, stealing of desktop data (including the 'auto-fill' data for various web pages), installation of backdoor programs or trojans that force pop-up ads or repeated visits to domains or IPs. The fact that GIAC's IT doesn't know what is supposed to be running on the machines indicates that they probably wouldn't recognize a problem if something new started running.

In addition to the typical desktop exploits, the consequence of an exploit on the Windows 2000 server may cause disruption of service to the anti-virus clients. The Windows 2000 server runs corporate-edition anti-virus for all desktops. This disruption of service could, in theory, continue for weeks before IT realizes the problem. In fact, their first clue may be when the desktops start getting infected by viruses.

Steps to be taken to mitigate the risk

1. Take inventory of the current versions of Operating Systems and software running on all servers and desktops.

2. Uninstall any software that is not needed on the servers and desktops, and institute an acceptable use policy for desktop users.
3. Establish security standards for systems settings in IE, Office and Windows.
4. Define a reasonable timeline and procedures for implementing updates to OS and software.
5. Install software like tripwire for the Windows 2000 server, to automatically notify IT of any system changes to the server.
6. Clearly identify the persons responsible for keeping the servers and desktops up-to-date.
7. Create a test environment for testing new updates before loading them onto production systems.

Costs of implementation

The most substantial cost is in creating a test environment. GIAC has many different OS flavors, which will make it costly to create duplicates in a test environment. If a test environment is not possible (due to costs), then reasonable procedures should be developed to define how to roll out updates. For example, an update to Windows NT should first be applied to only a few machines. After two weeks of successful use, the upgrade can be applied to the remaining machines.

Section
3

Evaluate and Develop Security Policy

The security policy chosen is for remote access. By eliminating dial-up access and defining appropriate remote access, we remove the risks associated with dial-up access from customers, ex-employees, and others. While the risks associated with a lack of password policy is also very high, the dial-up modem risk can quickly and easily be resolved in GIAC's situation, making this the "low hanging fruit". It is recommended that the password policy be developed as soon as the dial-up access risk is mitigated.

Evaluate Security Policy

The original security policy, included in Appendix B and obtained from http://www.sans.org/newlook/resources/policies/policies.htm addresses Remote Access. GIAC's most important server is its application server. It is into this server that 90% of all remote access takes place (the other 10% is remote access by IT employees into other servers for remote support). The application server holds all order history and customer data, and is used by GIAC's customers for order entry and order status queries. The dial-up modems attached to the application server create unnecessary risk to GIAC and can be replaced with more secure remote access. This policy intends to define appropriate remote access.

Evaluation of the security policy in Appendix B:

- **Purpose:** The security policy clearly states its purpose in the first paragraph – "to define standards for connecting to the network from any host". The reason for establishing these standards is stated as "to minimize the potential exposure from damages which may result from unauthorized use of resources". I think the purpose in the sample policy does a good job of defining the reason for the Remote Access Policy's existence.

- **Background:** The sample security policy does not include the optional component of background. In GIAC's policy, it may be helpful to define the type of remote access GIAC is providing to its customers, since it is different from the typical remote access into a network for email and web purposes.

- **Scope:** The scope of the policy identifies the audience as all employees, contractors, vendors and agents, which effectively covers anyone who may need remote access in the future. However, the remote access connections are defined specifically as "reading or sending email and viewing intranet web resources", which doesn't match GIAC's remote access needs. GIAC needs to provide remote access for customers into the application server and for IT staff into any of the servers for support purposes. Email and web browsing capabilities are not included in GIAC's remote access policy.

  The various remote access implementations covered by the policy identify every type of remote access, even though some of them are clearly home Internet-type connections (cable modems and DSL). The sample policy seems to cover both the Company remote access options, as well as the user's personal Internet access options. It is not clear to me, without access to the supporting documents mentioned throughout the policy, why the home Internet connections are included in the sample policy.

- **Policy Statement:** The policy statement in the sample security policy doesn't define the specifics of providing remote access to a corporate network. There are references to other policies for details on "protecting information" while attached to the corporate network, but I couldn't find any details or guidance on how a user should access the company network remotely. There is reference to a "Remote Access Services" website, which may include this detail (no link was available for me to evaluate the content of that site).

  In GIAC's case, the policy statement will provide standards for remote access into GIAC's servers. The goal of GIAC's remote access policy will be to provide GIAC's customers and IT support staff with the policy on how to access GIAC's servers remotely and in a secure fashion.

  The "General- Policy" section doesn't entirely apply to GIAC and I find parts of it confusing. In the first sentence: "it is the responsibility of employees, contractors, vendors and agents. . . to ensure that their remote access connection is given the same consideration as the user's on-site connection to the company" -- it isn't clear to me what is being suggested, since contractors, vendors and agents may not have an on-site connection. Defining specifically what considerations are expected rather than simply comparing the 'remote access connection' to the 'on-site connection' would clear up this confusion.

  The "Requirements- Policy" section does a good job of defining remote access authentication using one-time passwords or public/private keys, but it doesn't define what is considered a strong pass-phrase (there is reference to a Password Policy, however, which may address this). The section also does a good job of identifying rules of behavior regarding keeping passwords private, use of non-company email accounts, and updating anti-virus software.

Missing from the "Requirements-Policy" section is:

a. What is considered non-standard hardware? Section 3.2, number 8 says that non-standard hardware must be approved, but the policy doesn't define what standard or non-standard hardware is.

b. What are the "personal equipment requirements" of the company? Section 3.2, number 10 states that all personal equipment used to connect to the company's network must meet the requirements of the company-owned equipment for remote access, but the policy doesn't define what these requirements are and there is no reference to another document in which to find this information.

Clarification is also needed for section 3.2, number 3, which states that "remotely connected computers must not be connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user". For GIAC's IT staff to access the servers remotely via Secure Shell, they first need to access the Internet, presumably through an ISP. At that point, they are connected to the ISP's network, which is not under the complete control of the user. Similarly, GIAC's customers will access the application server through their corporate network, which the individual remote-access user does not completely control. It is unclear to me how the sample policy can enforce this item, since most (if not all) remote-access users will access the Company Network through an ISP or a corporate network – neither one under the "complete control of the user".

- **Responsibility:** It is not clear in the attached sample policy who is responsible for administration of the policy itself. The sample policy defines the user as being responsible for their remote access connection, but no information is included on who can modify or approve the policy. There is an "Enforcement" section, which explains the disciplinary actions for violation of policy, but it doesn't state who (if anyone) monitors for violations. Additionally, there is no accountability assigned to a specific entity for monitoring and enforcing the policy.

- **Action:** There are no action items pertaining to the administration of the policy. It includes a "Revision History" section, but is lacking a policy start date and any type of review process.

- **Enforcement:** I like the enforcement section of the policy. It makes it clear that a violation of policy will not be tolerated. However, with no responsibility assigned for monitoring remote access, the company will not easily know when they have a violation.

- **Definitions:** For the sample policy, the definitions are appropriate to define terms used throughout the policy that may not be familiar to all remote access users. GIAC's policy does not include many technical terms so a definitions section was not included in the revised policy.

The sample policy is good for defining who is eligible for remote access and the various remote access uses for the sample company (email and intranet web access). It also provides references to more detailed policies on specific types of remote access. (VPN, Wireless, etc) However, it is not a good overall security policy because of the lack of accountability for review and enforcement of the policy. Without some kind of review process, the company won't know whether the employees, contractors, customers and vendors are complying with the policy. And, if the policy isn't enforced, there's really no point in having the policy at all.

Revised Security Policy

GIAC Remote Access Policy

1.0 Purpose

The purpose of this policy is to define standards for customers, employees, and consultants connecting to GIAC's internal servers. These standards are designed to minimize the potential exposure to GIAC from damages, which may result from unauthorized use of GIAC resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, and damage to GIAC internal systems.

2.0 Scope

This policy applies to all remote access users, including but not limited to customers, consultants, and employees of GIAC who require remote access into any of GIAC's internal servers.

3.0 Background

GIAC allows their customers remote access into the application server for the purpose of entering orders and checking on inventory status. IT employees and consultants also require remote-access into GIAC's servers for support purposes.

4.0 Policy

4.1 General

Remote access into GIAC's servers is provided using Secure Shell (ssh). Each server runs Secure Shell on a unique port. The firewall forwards approved incoming ssh requests to the proper server based on port number. All customer ssh users must be approved by their GIAC Sales Rep and all IT ssh users must be approved by the IT Manager for remote access. Upon approval, the Network Administrator establishes the remote access user accounts.

4.2 Responsibilities and Requirements

a. The Network Administrator will download and install the client copy of Secure Shell (ssh) for customer and employee use. Consultants must download and install their own copy of ssh client.

b. Ongoing administration of remote access users will be performed by the Network Administrator. Users will be prompted to change their passwords every 90 days. The Network Administrator will monitor account activity and expire any accounts that are inactive for 90 days. If an account is needed after it has been expired, a request must be made in writing to the Network Administrator, who will reactivate the account. These procedures are outlined in detail in the "Administration of remote ssh users" document.

c. It is the responsibility of the remote access user to keep their login and password private. This information cannot be shared with anyone, at any time, for any reason.

d. Remote access to GIAC's servers must be used for business purposes only. Misuse of GIAC's system resources is considered a violation of this policy.

e. All hosts that are connected to GIAC's internal servers via remote access must use the most up-to-date anti-virus software.

5.0 Enforcement

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

6.0 Responsibility of this Policy

The IT Manager maintains this policy. It is the responsibility of the IT Manager to ensure that the policy is current, relevant, and enforced. This policy will be reviewed by the IT Manager on a quarterly basis.

7.0 Actions

The Network Administrator must ensure that all remote-access users comply with this policy by September 30, 2002.

IT Manager will review this policy every 3 months.

Remote-access users will change their passwords every 90 days.

8.0 Revision History

Original Policy written on April 23, 2002.

Section

4

Develop Security Procedures

Administration of remote ssh Users

The Network administrator is responsible for ongoing administration of remote ssh users. These procedures are important to GIAC because they provide the framework for secure remote access by GIAC's customers. Without defined procedures, unauthorized personnel may be given remote access, or may use inactive accounts. Administration of ssh clients includes the following set of procedures:

- *Process to request remote access:* New IT users may request remote access into GIAC's application server by submitting a written request (via paper or email) to the IT Manager. Upon approval, the request is given to the Network Administrator for setup.

  New customers requiring remote-access will normally notify their GIAC Sales Representative. The Sales Rep will approve the written request and provide it to the Network Administrator for setup. If the customer request comes into IT instead of Sales, the Network Administrator will provide a copy of the request to the GIAC Sales Rep. This copy serves to notify the sales rep of an additional remote access user (for billing purposes). It also provides a second level of validation to protect against unauthorized requests for remote access, since GIAC's sales rep will be aware of any customer employee requiring remote access into GIAC's server.

- *Process to approve remote access:* GIAC's sales rep provides the approval for remote access customers to the Network Administrator by initialing the original request. The sales rep is responsible for notifying the customer of any additional charges that may apply for the remote access. The IT Manager provides approval for remote access IT users.

- *Process to enable access:* The Network Administrator works with the customer's IT staff to install and configure the most recent ssh client version. On GIAC's servers, the following changes will be performed by the Network Administrator to enable remote access for a new user:

  - Firewall must be configured to allow incoming access from the customer's IP. Details on how to change the firewall configuration can be found in the "Firewall Configuration Manual".

  - User's domain must be added to the hosts.allow file on the application server.

  - Unix system accounts must be enabled on the appropriate server. Passwords must contain at least 8 characters with 3 alpha, 3 numeric and 2 other. Passwords will be set to automatically prompt for change after 90 days. User account name is set to last name and first initial. The following command can be used to add new users to the server:

    ```
    useradd –D –p pwd username
    ```

    This command uses the –D flag, which uses the default settings from /etc/login.defs. The default settings for GIAC's server includes the following:

    - Expire password in 90 days
    - Passwords have restrictions as described above
    - Allow 30 days after password has expired for user to reassign a new password. After 30 days, account is disabled.
    - Put user in 'staff' group
    - Create home directory and copy files from /etc/skel to user's home directory

  - Application accounts must be configured to point to the appropriate database for customer access. From within the Unidata database, run the following command to copy an existing user record to the new user record. Use the same username as was created for the Unix system account:

    ```
    cp   users   existing.user   username
    ```

    The user record must now be edited to include information unique to this user, such as user name and database account for access.

    ```
    ed users username
    ```

- *Process to monitor account activity:* The Network Administrator will check the log files monthly and make note of any remote user who hasn't accessed the system in 90 days. This process can be accomplished on the application server, where user logon information is kept until specifically removed from the log files. The following command can be used, which will show the most recent access for each user specified:

```
last | grep username | tail
```

The Network Administrator may choose to create a script to simplify monthly monitoring of the log files. The script can be similar to the following, with output redirected to a file, if necessary:

```
#!/bin/bash
for var in ‘cat /home/netadm/usernames’
do
        last | grep $var | tail
done
```

- *Process to expire inactive user accounts:* Inactive user accounts are expired by the Network Administrator by locking the account. Prior to flagging an account as inactive, the Network Administrator will notify the appropriate GIAC Sales Rep for approval. If approved for expiration, the Network administrator expires the account using the following command:

  ```
  usermod –L username
  ```

- *Process to reactivate expired user account:* The Network Administrator can reactivate an expired account when requested by the remote access user and approved by the GIAC Sales Rep. The following command can be used to reactivate an account:

  ```
  usermod –U username
  ```

- *Process to permanently remove an inactive account:* In cases where the remote user will never again need access, the account can be permanently removed from the system by following these steps:
  - The Network Administrator must first review the files in the user’s home directory and move any critical files to another location on disk.
  - After the files have been moved, the following command can be used to remove the user account and the user’s home directory:

    ```
    userdel -r   username
    ```

- *Process to audit policy procedures:* The IT Manager is responsible for verifying that the security policy is working as intended. Quarterly review of this policy is the IT Manager’s responsibility. The Network Administrator will provide a report to the IT Manager on the first week of each quarter. The report should include:

- A listing of all current remote access users and the date of last access.
- The name of the person who approved the user for remote access
- User's company name (if applicable), IP address and domain
- Any users currently flagged for inactivity
- Any users permanently removed during the last quarter
- Any users requesting reactivation during the last quarter

With this information, the IT Manager will verify that:

- Inactive users do not remain on the system indefinitely
- All new users have been approved by either the GIAC Sales Rep or the IT Manager
- All customer users represent a customer of GIAC's
- Requests for reactivation have appropriate approvals

List of References

1. Slemko, Marc. "Path MTU discovery and filtering ICMP". 18 January 1998
URL:http://www.worldgate.com/~marcs/mtu/ (27 March 2002)

2. Russell, Rusty. "Linux Packet Filtering HOWTO". 20 November 2001
URL:http://netfilter.samba.org/unreliable-guides/packet-filtering-HOWTO/packet-filtering-HOWTO.linuxdoc.html (10 April 2002)

3. Hatch, Brian; Lee, James; Kurtz, George. Hacking Linux Exposed. McGraw-Hill Professional. April 2001. Chapter 3

4. Acheson, Steve. "Secure Shell FAQ". 16 February 2001.
URL: http://www.employees.org/~satch/ssh/faq/ssh-faq.html

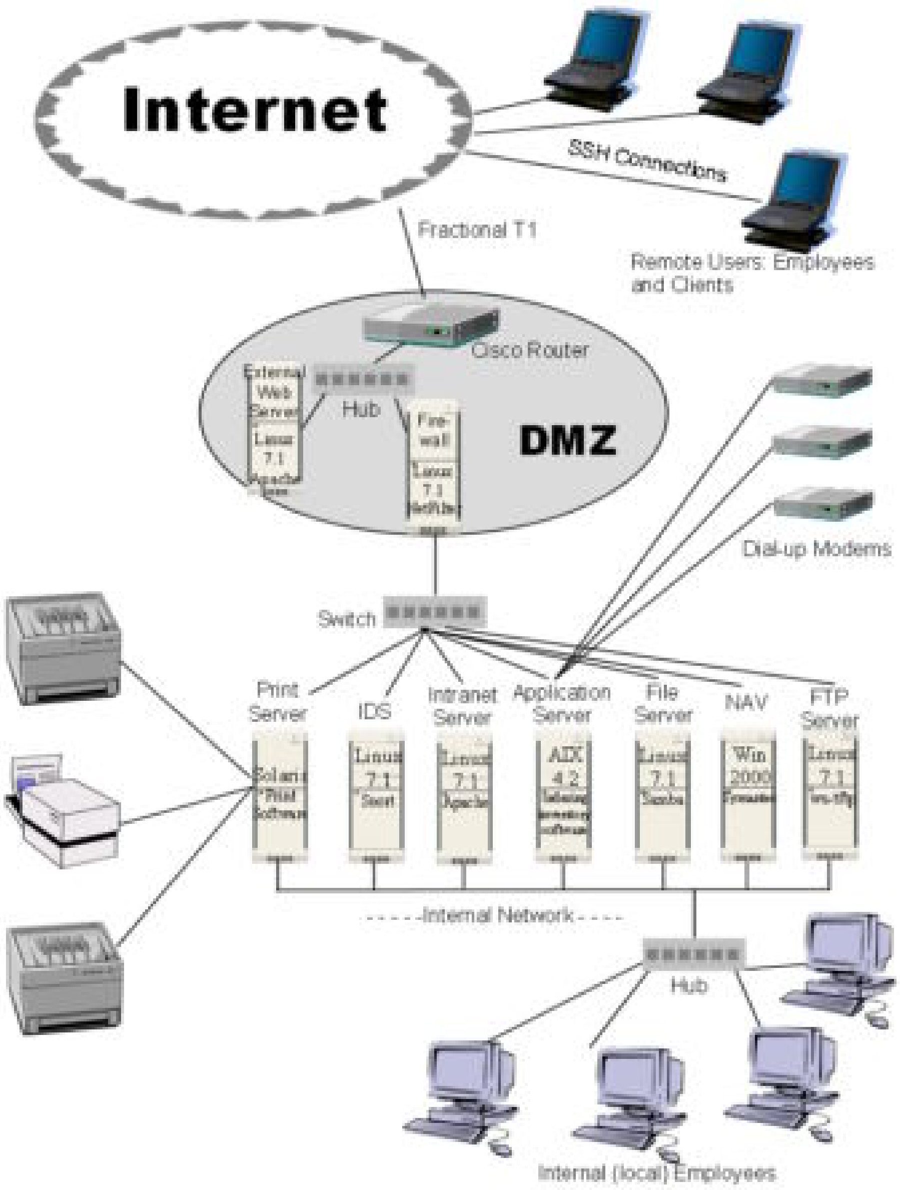
Other books used for research and information:

Ziegler, Robert L. Linux Firewalls. New Riders Professional. November 1999

Zwicky, Elizabeth; Cooper, Simon; Chapman, D. Brent; Russell, Deborah. Building Internet Firewalls. O'Reilly & Associates. 15 January 2000

Garfinkel, Simson; Spafford, Gene. Practical Unix and Internet Security. O'Reilly & Associates. April 1996

Appendix A: Network diagram



Appendix B – Security Policy

The following security policy was obtained from:

http://www.sans.org/newlook//resources/policies/policies.htm

Remote Access Policy

1.0 Purpose

The purpose of this policy is to define standards for connecting to <Company Name>'s network from any host. These standards are designed to minimize the potential exposure to <Company Name> from damages which may result from unauthorized use of <Company Name> resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical <Company Name> internal systems, etc.

2.0 Scope

This policy applies to all <Company Name> employees, contractors, vendors and agents with a <Company Name>-owned or personally-owned computer or workstation used to connect to the <Company Name> network. This policy applies to remote access connections used to do work on behalf of
<Company Name>, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

3.0 Policy

3.1 General

1. It is the responsibility of <Company Name> employees, contractors, vendors and agents with remote access privileges to <Company Name>'s corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to <Company Name>.
2. General access to the Internet for recreational use by immediate household members through the <Company Name> Network on personal computers is permitted for employees that have flat-rate services. The <Company Name> employee is responsible to ensure the family member does not violate any <Company Name> policies, does not perform illegal activities, and does not use the access for outside business interests. The <Company Name> employee bears responsibility for the consequences should the access be misused.

3. Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of <Company Name>'s network:
    a. *Acceptable Encryption Policy*
    b. *Virtual Private Network (VPN) Policy*
    c. *Wireless Communications Policy*
    d. *Acceptable Use Policy*
4. For additional information regarding <Company Name>'s remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., go to the Remote Access Services website.

3.2 Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Password Policy.
2. At no time should any <Company Name> employee provide their login or email password to anyone, not even family members.
3. <Company Name> employees and contractors with remote access privileges must ensure that their <Company Name>-owned or personal computer or workstation, which is remotely connected to <Company Name>'s corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
4. <Company Name> employees and contractors with remote access privileges to <Company Name>'s corporate network must not use non-<Company Name> email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct <Company Name> business, thereby ensuring that official business is never confused with personal business.
5. Routers for dedicated ISDN lines configured for access to the <Company Name> network must meet minimum authentication requirements of CHAP.
6. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
7. Frame Relay must meet minimum authentication requirements of DLCI standards.
8. Non-standard hardware configurations must be approved by Remote Access Services, and InfoSec must approve security configurations for access to hardware.
9. All hosts that are connected to <Company Name> internal networks via remote access technologies must use the most up-to-date anti-virus software (place url to corporate software site here), this includes personal computers. Third party connections must comply with requirements as stated in the *Third Party Agreement*.
10. Personal equipment that is used to connect to <Company Name>'s networks must meet the requirements of <Company Name>-owned equipment for remote access.

11. Organizations or individuals who wish to implement non-standard Remote Access solutions to the <Company Name> production network must obtain prior approval from Remote Access Services and InfoSec.

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

5.0 Definitions
Term **Definition**
Cable Modem Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.

CHAP Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function. DLCIData Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network, and has local significance only to that channel.

Dial-in Modem A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.

Dual Homing Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Corporate network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on a <Company Name>-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into <Company Name> and an ISP, depending on packet destination.

DSL Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).

Frame Relay A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the telephone company's network.

ISDN There are two flavors of Integrated Services Digital Network or ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signaling info.

Remote Access Any access to <Company Name>'s corporate network through a non-<Company Name> controlled network, device, or medium.

Split-tunneling Simultaneous direct access to a non-<Company Name> network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into <Company Name>'s corporate network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

6.0 Revision History