Global Information Assurance Certification Paper

GIAC Firewall and Perimeter Protection Curriculum
SANS Network Security 2000
Practical Assignment

Jeff Horne

Assignment 1: Security Architecture

Define a security architecture. The goal of your policy is to use filtering routers, firewalls, VPNs and internal firewalls to rapidly implement the VISA "Ten Commandments" to the extent possible at GIAC Enterprises, a new Internet Startup that expects to earn 200 million per year in sales of online fortune cookie sayings. The "Ten Commandments" are listed below:

1. *Install and maintain a working network firewall to protect data accessible via the Internet.*
2. *Keep security patches up-to-date.*
3. *Encrypt stored data accessible from the Internet.*
4. *Encrypt data sent across networks.*
5. *Use and regularly update anti-virus software.*
6. *Restrict access to data by business "need to know."*
7. *Assign unique IDs to each person with computer access to data.*
8. *Track access to data by unique ID.*
9. *Don't use vendor-supplied defaults for system passwords and other security parameters.*
10. *Regularly test security systems and processes*

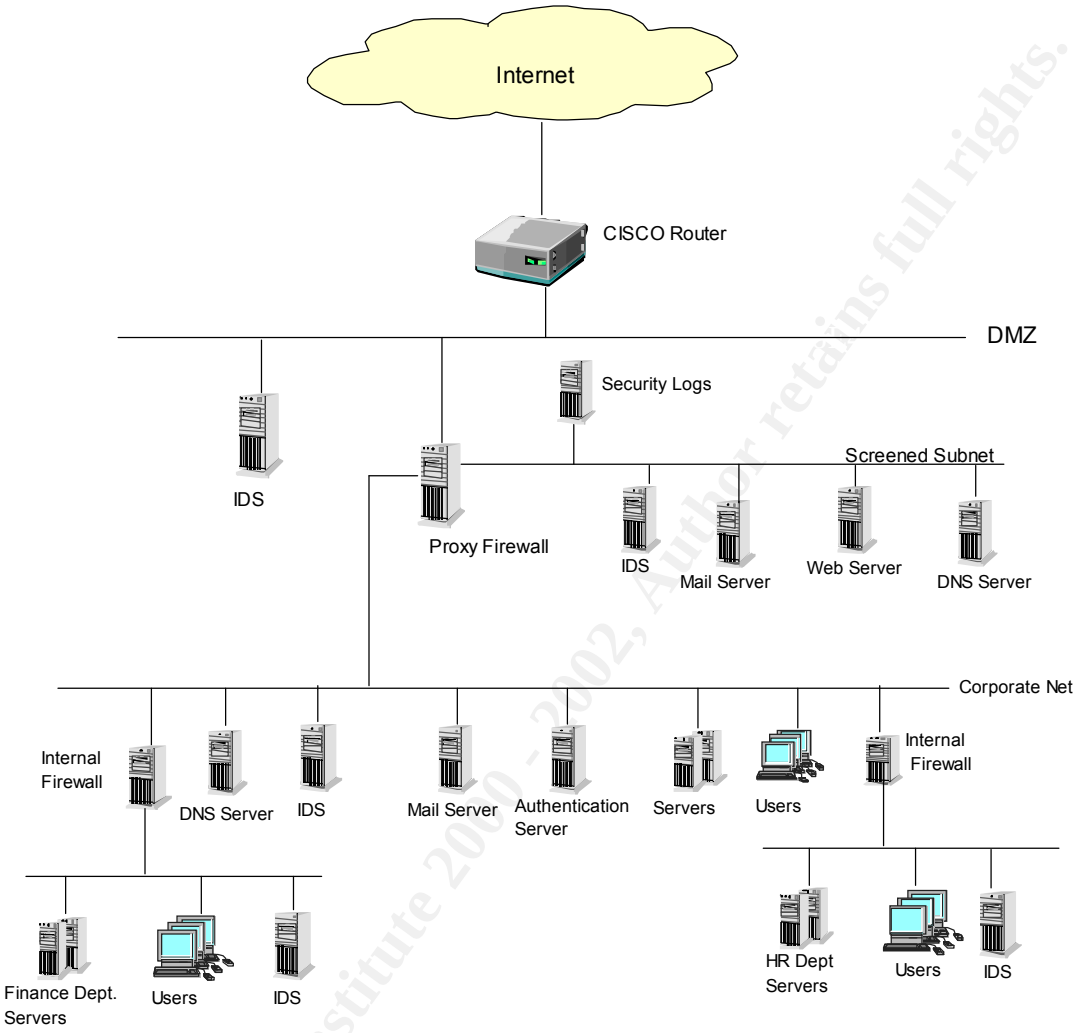
The student assignment is to produce a diagram, or set of diagrams with explanatory text defining how to use perimeter technologies to implement as many of the requirements above as possible. For this assignment you are a large and growing E-business that just completed a merger/acquisition you must consider the need for customers, suppliers, and partners.

Introduction

The security architecture for GIAC Enterprises, depicted on the following page, follows the principle of layered security or "defense in depth" in order to implement the VISA "Ten Commandments" and to avoid being a security "Tootsie Roll Pop" i.e. hard on the outside but soft and chewy on the inside. To implement this philosophy, a combination of tools such as screening routers, firewalls, intrusion detection sensors and encryption is used. In addition, strong procedures are developed and enforced to ensure the technical defenses are kept secure.

For the purposes of this assignment GIAC Enterprises uses Sun Solaris and Windows NT servers and Windows 98 workstations on the desktop. The company is connected to an ISP via a DS3 connection. CISCO routers are used to subnet the internal network as well as for the border router. Internal firewalls are used to segment the corporate network and limit access to data to those with the appropriate authorization. All employees are allowed E-mail and Web access to the Internet as part of their job function.

On the following pages, each major component of the architecture is discussed briefly followed by detailed discussion of each of the "Ten Commandments".



Filtering Router

Although not listed in the Commandments, an important part of our security architecture is a filtering router installed between the ISP and the DMZ. This router screens all traffic in and outbound, providing another layer of security as mentioned above and reducing overhead processing on the firewall. Specific steps taken to harden the router and router filters are discussed in the Security Policy.

DMZ

The network segment between the border router and the company's firewall is known as the DMZ, or De-Militarized Zone. This piece of the network receives some protection from the filters on the screening router but is not protected as much as the network behind the firewall. This network segment will contain only the router, the firewall, an Intrusion Detection sensor and, periodically, system with vulnerability assessment tools used to scan these devices.

Internet Firewall

Axent Technology's Raptor firewall is used to protect the corporate network from unauthorized access. The firewall is discussed in detail as part of the "Ten Commandments" discussion below.

Screened Subnet

This network segment is intended for systems that must be accessible from the Internet. Because the screened subnet is connected to the firewall, systems connected to it receive some protection, although not as much as systems on the corporate network. Only specific, required services are allowed to each system on this subnet, depending on the function of the system.

Log Server

A syslog server is implemented on the screened subnet to collect data from the router and the other systems on this subnet. Information on the server is pulled into the corporate network using SSH.

Internal Network

The internal Ethernet is subdivided into multiple security domains. Some data and services are accessible to all employees on the corporate network. For example, all employees can send and receive Email and access the Web. Other parts of the network,

such as Finance and Human Resources, are considered to contain sensitive data and are protected from general access by internal firewalls. Protections on the internal network and data access considerations are discussed in detail later under Commandments 6, 7 and 8.

One of the most common ways to subvert perimeter security is to go around it, and one way of doing this is to break in through an unsecured modem on a computer that is also connected to the corporate network. For this reason, modems may not be used on GIAC Enterprises' computer systems. Rare exceptions are made in specific circumstances but the modem must be registered with the security administrators and the system should not be connected to the company network while the modem is in use or afterward, until the system is checked.

Network-based Intrusion Detection is implemented on all of the servers and each subnet of the network with log files and alerts sent to the log server and, in-turn to security administrators based on urgency.

VISA Ten Commandments

1. Install and maintain a network firewall

   In order to fulfill this requirement, GIAC Enterprises will use Axent Technology's Raptor Firewall, running on a Solaris Unix platform. Before the Raptor software is installed, a couple of steps will be taken to further protect the firewall from compromise. First, the Solaris operating system is hardened. This was accomplished using information and tools from the following sources:

   http://www.sans.org/newlook/resources/hard_solaris.htm
   http://www.enteract.com/~lspitz/armoring.html
   http://www.sun.com/blueprints/tools
   http://yassp.org

   After the operating system is hardened, checksum software, such as Tripwire, is installed. A baseline of system files is obtained against which later runs can be compared for evidence of tampering. A copy of the data from the initial Tripwire run is saved on removable media and stored securely away from the system. The baseline must be updated regularly when upgrades are made to the system.

   The Raptor firewall provides a separate client called the Raptor Console for Unix or "RCU" that is used by system and security administrators to mange the firewall securely from the corporate network. The management GUI sets up an encrypted tunnel for managing firewall rules and objects and an additional tool provides encrypted telnet for operating system management tasks that require interactive login access.

   The perimeter firewall will have a 3rd Network Interface Card (NIC) connected to a screened or protected subnet. This subnet will hold servers that must be accessible

from the Internet, including the external Email and DNS servers and the public Web server. A network-based intrusion detection sensor is placed on this subnet to detect port scans, DoS attacks, attempted intrusions or other unauthorized access to these systems. Traffic between the corporate network and the screened subnet is encrypted. All traffic to and from systems on this subnet is logged.

The firewall will allow only necessary services to pass to each system on the screened network. For example, only SMTP packets are allowed to pass through the firewall between the Internet and the Email server. SSH connections are allowed from the corporate network to these systems as long as they are initiated on the corporate network.

2. Keep security patches up-to-date

Maintaining the latest operating system and application patches is crucial to keeping the GIAC Enterprises network secure. The following sources of information are accessed via email subscriptions:

SANS NewsBites
SANS Security Alert Consensus
Sun's Customer Warning System (CWS) for security issues related to Solaris
SecurityPortal's Weekly Digests for Axent, Solaris and Tools
SecurityFocus Newsletter

All pertinent patches are downloaded and tested prior to installation on production systems. Security-related patches are given immediate priority for installation, other patch installations are scheduled to provide the least impact on production systems operation.

3. Encrypt stored data accessible from the Internet

Sensitive data stored on the external Web server is encrypted using PGP, 128-bit encryption. Suppliers and business-partners requiring access to this data are sent GIAC Enterprises' public key.

4. Encrypt data sent across networks

- Transactions between GIAC Enterprises and its customers are protected via HTTPS using SSL, 128-bit encryption.
- Data transfers between the company and its business partners and suppliers use VPN links through Raptor's built-in VPN tunneling capability. The firewall can set up encrypted tunnels with other IPsec-compliant servers.
- Remote access traffic is encrypted using RaptorMobile, the VPN client that comes with the Raptor firewall.

5. Use and update anti-virus software

   Norton AntiVirus is used on all desktop machines and servers. Up-to-date virus definitions are obtained via a subscription with the vendor. New definitions are downloaded on demand by the system administrators and distributed to the servers and workstations. Virus definitions are routinely downloaded twice weekly but can be obtained any time a new virus alert is received from a trusted source such as the ones listed in #2 above.

6. Restrict access to data by "need-to-know"

   Access to data on the corporate network is restricted by the use of internal firewalls requiring users to authenticate with their UID and password before being permitted into a secured domain. A Radius server on the internal network is used to provide authentication services for the internal firewalls. Internal firewalls are, by design, not the same type as the perimeter firewall so a compromise of one does not necessarily mean a compromise of the other. On the corporate network, speed is a primary consideration, therefore PIX firewalls are used for this application.

7. Assign unique IDs to each person with computer access to data

   Every computer user in GIAC Enterprises is assigned a unique computer User ID (UID). No multiple-user (shared-password) accounts are allowed. System and network administrators log onto systems with their personal UID and then access administrative accounts with elevated privileges.

8. Track access to data by unique ID

   - Network access is disallowed to admin accounts. Admins must log into systems with their personal UID.
   - Administrators are assigned only the privileges necessary to do their jobs and all accesses to higher-privileged accounts are logged.
   - The Radius server authenticates users who access data on a secured subnet and the access is logged.

9. Don't use default passwords

   All standard login accounts are either disabled or have their default password changed. The default community string is changed on all internal routers and the border router. Each user account is initially assigned a unique password that is pre-expired, forcing the user to change it the first time they log in. Users are informed in writing of the password policy requiring a minimum password length and required

use of special characters. User account passwords expire after 90 days and passwords for administrator accounts expire after 35 days. Passwords for administrator accounts are immediately changed any time someone leaves that job function.

10. Regularly test security systems and processes

    Periodic vulnerability scans are performed on all border and internal security systems. Auditing is also done to ensure compliance with company procedures on user account passwords and data protection. Scans are run at least quarterly on the firewall and border router from a system on the DMZ. Scans are also run at any time a significant change is made to the configuration of either of these systems. Quarterly scans are performed on all DMZ systems and internal servers. War dialing is performed quarterly against the range of phone numbers assigned to GIAC Inc. to detect unauthorized modems. A password-cracking program is run against the company's user database every six months to detect weak or non-compliant passwords.

Assignment 2: Security Policy

For the purposes of this assignment, your security policy should be focused on implementation of requirement number 1 above "Install and maintain a working network firewall to protect data accessible via the Internet." For a baseline policy, use the filtering recommendations located at www.sans.org/topten.htm. You DO NOT need to repeat that information. Instead, focus on ADDITIONAL filtering you would recommend and why. Keep in mind you are an E-Business with customers, suppliers, and partners, you MAY NOT simply block everything! Your policy should implement your design above.

Write a tutorial on how to implement each additional recommended action in the filtering policy below on your firewall or perimeter defense solution. Be explicit about the brand and version of perimeter defense. The base policy is taken from the recommended perimeter defense actions in the "Top Ten" document. Screenshots, network traffic traces, firewall log information and URLs to find further information should all be used. Be certain to include the following:

1. *The reason these services might be considered a vulnerability*
2. *Relevant information about the behavior of the protocol or service on the network*
3. *Syntax of the filter*
4. *Description of each of the parts of the filter*
5. *Explain how to apply the filter*
6. *If this filter is order dependant, what other rules should this filter precede and follow***
7. *Explain how to test the filter*
8. *Be certain to point out any tips, tricks, or gotcha's.*

*** You may find it easier to create a section of your practical that describes the order you would apply all of the rules rather than trying to do it with each policy cluster. Be certain to explain your reasons for the order you choose, we cannot read your mind.*

Base Security Policy

Please note, we are not asking you to repeat the blocking instructions for the "top ten" security vulnerabilities. You may wish to reference one of the later practicals in your work since they were focused on blocking the "top ten" they can be found: http://www.sans.org/giactc/gcfw.htm

In this section, we list the base security policy so you know what additional services to recommend blocking. These are ports that are commonly probed and attacked.

Blocking these ports is a minimum requirement for perimeter security, not a comprehensive firewall specification list. A far better rule is to block all unused ports. And even if you believe these ports are blocked, you should still actively monitor them to detect intrusion attempts. A warning is also in order. Blocking some of the ports in the following list may disable needed services. Please consider the potential effects of these recommendations before implementing them.

1) *Block "spoofed" addresses-- packets coming from outside your company sourced from internal addresses or private (RFC1918 and network 127) addresses. Also block source routed packets.*

2) *Login services-- telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), NetBIOS (139/tcp), rlogin et al (512/tcp through 514/tcp)*

3) *RPC and NFS-- Portmap/rpcbind (111/tcp and 111/udp), NFS (2049/tcp and 2049/udp), lockd (4045/tcp and 4045/udp)*

4) *NetBIOS in Windows NT -- 135 (tcp and udp), 137 (udp), 138 (udp), 139 (tcp). Windows 2000 - earlier ports plus 445(tcp and udp)*

5) *X Windows -- 6000/tcp through 6255/tcp*

6) *Naming services-- DNS (53/udp) to all machines which are not DNS servers, DNS zone transfers (53/tcp) except from external secondaries, LDAP (389/tcp and 389/udp)*

7) *Mail-- SMTP (25/tcp) to all machines, which are not external mail relays, POP (109/tcp and 110/tcp), IMAP (143/tcp)*

8) *Web-- HTTP (80/tcp) and SSL (443/tcp) except to external Web servers, may also want to block common high-order HTTP port choices (8000/tcp, 8080/tcp, 8888/tcp, etc.)*

9) *"Small Services"-- ports below 20/tcp and 20/udp, time (37/tcp and 37/udp)*

10) *Miscellaneous-- TFTP (69/udp), finger (79/tcp), NNTP (119/tcp), NTP (123/tcp), LPD (515/tcp), syslog (514/udp), SNMP (161/tcp and 161/udp, 162/tcp and 162/udp), BGP (179/tcp), SOCKS (1080/tcp)*

11) *ICMP-- block incoming echo request (ping and Windows traceroute), block outgoing echo replies, time exceeded, and unreachable messages.*

GIAC Enterprises' perimeter defense solution consists of a screening router and a firewall with its associated-screened subnet. The sections below address how the security policy is implemented on each component.

Router Policy

The following items are used to secure the router and to reduce traffic allowed into the DMZ. This layer of security slows down potential attackers, reduces the load on the firewall and reduces the amount of "background noise" in the firewall logs. Items already covered in the base policy are not repeated and additional entries are explained in detail. The router entries can be implemented in the order presented and items from the base list will appear in ACL 101.

The following URLs are good sources for router security information:

http://pasadena.net/cisco/secure.html
http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/scoverv.htm

The router's passwords are normally stored in plain text but the following command makes the password display as an encrypted string. This only encrypts the password on the router; it is still transmitted in plain text over the network.
service password-encryption

All unused services should be disabled on the router. The http management interface is not configured or used on the router therefore it should be disabled.
no ip http server

The bootp service is another service that is not configured or used on the router so it should also be disabled.
no ip bootp server

Malicious hosts can send craft broadcasts with a spoofed source address. The spoofed source becomes the target of a DoS attack when all the hosts on the receiving network reply to the broadcast. Blocking broadcast traffic from entering the network prevents our network from being used as an intermediary in these Smurf-type attacks.
no ip directed-broadcast

Systems running older versions of the Windows operating systems can be vulnerable to a DoS attack caused by a remote host's malicious modification of the target's routing table. IP redirects should not be allowed to enter the network.
no ip redirect

Use a SNMP community name other than "public" or "private" and add an access-list to allow only certain IP addresses to access the router.
snmp-server community secret RO 21
access-list 21 permit <GIAC_internal_IP>

A log server is installed on the screened subnet to collect syslog information from the router and public servers. By default the router sends log info to "LOCAL7" so the destination of the log server must be specified. Individual ACL entries must specify "log" or "log-input" to be logged.
logging <ip-of-log-server>

We will provide a warning banner stating that unauthorized entry or tampering is unwelcome.
*banner \ WARNING – No unauthorized access permitted – WARNING *

Several Trojan and DDoS programs place backdoors on systems that listen on specified ports. We will block some of the more common ports although the list changes frequently.
access-list 101 deny tcp any eq 33270 (Trinity DDoS)

access-list 101 deny udp any eq 12345 (NetBus)
access-list 101 deny udp any eq 12346 (NetBus)
access-list 101 deny udp any eq 20034 (NetBus)
access-list 101 deny udp any eq 31337 (Back Orifice)
access-list 101 deny udp any eq 5631 (PCAnywhere)
access-list 101 deny tcp any eq 5631 (PCAnywhere)
access-list 101 deny tcp any eq 5632 (PCAnywhere)
access-list 101 deny udp any eq 5632 (PCAnywhere)

We block "Ident" from coming into our network because it may be used to gather information for a potential attacker.
access-list 101 deny tcp any any eq 113

Finally, we must allow whatever we have not blocked. This should be the last entry for this access list.
access-list 101 permit ip any any

interface FastEthernet 0/0 !external interface
ip address <GIAC "Legal" IP address>
ip access-group 101 in

Egress filtering is applied on the inside interface to prevent GIAC's network from being used in a DDoS attack on someone else. Only valid GIAC Enterprises IP addresses are allowed to pass the inside interface of the router outbound. All others are dropped.
access-list 102 permit ip <GIAC_IP_addresses> any (GIAC's legal address space)
access-list 102 deny ip any any log

interface FastEthernet 1/0 !internal interface
ip address <GIAC Internal IP address>
ip access-group 102 in

The following commands: *sh access-list 101* and
sh access-list 102

are used to view each access list and display how many matches have occurred per filter. This can be used to provide some validation of the access lists.

Firewall Policy

When evaluating rules in the rule set, Raptor does not do a "first match", instead it does a "best match", comparing all rules except for those outside the current time window. The "best" rule is considered to be the most specific one that fits the criteria. Raptor's default action is to drop all traffic not specifically allowed by a rule. Also, detailed logging is

done by default on every rule – it must be re-configured manually to disable or modify the logging level. In the following rules, assume high-level logging unless otherwise specified.

Rule configuration for Raptor allows the following options to be specified:

Source
Destination
Permit/Deny
Services
Time Window
Permit Users/Groups
Deny Users/Groups
Authentication Type

Note 1: For easier reading, only the source, destination, permit/deny, services and user groups are shown below.

Note 2: The host names below are used for ease of reading only. I would not name a firewall "GIACFW" or the DNS server "ExtDNS", instead I would use names like "pluto" and "daffy" which do not advertise the systems' function. There is no point in making systems any more enticing to attackers.

The following user and network "Entities" are defined on the Raptor firewall:

- Inside - Corporate network
- Protected - Screened network
- Outside - DMZ-side network
- Inside_HME0 - Inside interface of the firewall
- Outside_HME1 - DMZ-side interface of the firewall
- GIACFW - The hostname of the firewall
- ExtDNS - External DNS server
- ExtWeb - External Web server
- ExtMail - External E-mail server
- ExtRoute - Filtering router
- LogSrvr - Syslog server
- IntDNS - Internal DNS server
- IntMail - Internal E-mail server
- GIAC_Users - Internal Users
- IT_Admin - Group of Server Administrators
- Sec_Admin - Group of Firewall/Security Administrators
- Universe* - Any IP address

- Screened_IT - Group of net entities including: ExtDNS, ExtWeb, ExtMail
- Screened_SEC - Group of net entities including: ExtRoute and LogSrvr

Source	Dest.	Service	Action

Allow any source to access the external web server using HTTP (Port 80) or Secure HTTP (Port 443). These services allow customers to access our fortune cookie data.

*Universe**	*ExtWeb*	*HTTP/HTTPS*	*Allow*

E-mail. Allow any source to send SMTP to the external mail server, external mail server to send SMTP out and the internal server to get mail from the external server. E-mail is a big target but we allow SMTP traffic only between the outside world and our external mail server. The internal server forwards outgoing mail to the external server and retrieves inbound mail.

*Universe**	*ExtMail*	*SMTP*	*Allow*
ExtMail	*Universe**	*SMTP*	*Allow*
IntMail	*ExtMail*	*SMTP*	*Allow*

The Ident protocol (Port 113/TCP) can be used to gather information about our corporate network by potential attackers and it is not necessary to allow it through the firewall. We choose to drop this traffic at the internal interface. The logging level will be turned down for this rule because of the amount of this kind of traffic.

Inside	*Internal_HME0*	*Ident*	*Deny*

NetBIOS traffic should not leave the corporate network and is also dropped at the internal firewall interface. Logging will be turned down on this rule because it will generate a lot of entries.

Inside	*Internal_HME0*	*NetBIOS_all*	*Deny*

Allow any source to query the external DNS server using UDP only. The external DNS server contains no information about our inside network. Also, allow the external web server to use both TCP and UDP port 53 to request information from other DNS servers.

*Universe**	*ExtDNS*	*DNS_udp*	*Allow*
ExtDNS	*Universe**	*DNS_all*	*Allow*

Allow system administrators to access a group of systems on the screened subnet using SSH.

IT_Admin	*Screened_IT*	*SSH*	*Allow*

Allow security administrators access to the syslog server on the screened subnet using Secure Shell (SSH). Also allow them to connect to the router using telnet after authenticating on the firewall. SSH is not available for the router.

Sec_Admin	*LogSrvr*	*SSH*	*Allow*
Sec_Admin	*ExtRoute*	*Telnet*	*Authenticate*

Allow GIAC Enterprises' employees access to the World Wide Web

GIAC_Users	*Universe**	*HTTP/HTTPS*	*Allow*

VPN tunnels are set up separately from the rulebase both for subnet-to-subnet and for the remote client VPN access. Each remote user must be defined along with authentication and type of VPN access, i.e. ISAKMP, IPSEC or SWIPE. RaptorRemote supports MD5 and DES.

Assignment 3: Audit your security architecture

For the purposes of this assignment please assume that you have been assigned to provide technical support for a comprehensive information systems audit for GIAC Enterprises, a electronic commerce facility that is the largest supplier of electronic fortune cookie sayings in the world. The firewall analyst has set their firewall up according to their base + recommended enhancements security policy that happens to mirror your assignment 1 security policy exactly. Your assignment is:

Plan the assessment. Describe the technical approach you recommend to assess your perimeter. Be certain to include considerations such as what shift or day you would do the assessment. Estimate costs and level of effort. Identify risks and considerations.
Implement the assessment. Validate that the firewall or perimeter router is actually implementing the security policy. Be certain to state exactly how you do this, including the tools and commands used. Screenshots when possible should be included in your report.
Perimeter analysis. Based on your assessment and referring to data from your assessment, analyze the perimeter defense and make recommendations for improvements or alternate architectures. Diagrams are strongly recommended for this part of the assignment.

NOTE: Assignment 3 should be primarily focused on VISA requirement number 1, "Install and maintain a working network firewall to protect data accessible via the Internet." and your base + recommended security policy. Credit towards honors status will be given to students that are able to design an audit that can test all or a good deal of the VISA requirements.

General

Information systems security is composed of several components. First, there are policies and procedures that define the security architecture and how it will be implemented and maintained. Then there are technical components, including physical security, firewalls, routers, intrusion detection systems, etc., used to implement the policies. Perhaps the most important yet challenging components of information systems security are the people who use and administer the systems. In the end, employees decide how effective a company's information security is by how they adhere to, or ignore security policies and procedures.

A complete audit of a company's security architecture involves many components; however the scope of this assignment is to assess the security of our network firewall and border/screening router. In the following pages some of the basic ingredients required by a good security analysis are covered briefly. Particular attention is given to analyzing our firewall and perimeter security.

Resources required for the security assessment include the following personnel and tools:

- Firewall Analyst: 3-5 days
- Technical Specialist: 3-5 days
- Dedicated NT computer system of sufficient speed and processing power to run CyberCop and other vulnerability assessment tools.
- One network sniffer - ~$10,000.00*

- Network Associates' CyberCop scanner software licensed for 500 IP addresses - ~$15,000.00*

Initial cost of these tools is high but recurring costs are only for support and software maintenance.

The first step of the overall audit is to review the company's security policy and procedures. The policy should be clearly written and comprehensive and the procedures should provide the basis for implementing and enforcing the security policy. The policy and the procedures should be signed by IS and corporate management and copies should be available to those responsible for implementing them. The technical portion of the audit will be configured according to the information in the security policy manual.

The next phase of the audit is to scan the external and internal systems for known vulnerabilities. Because vulnerability scans induce additional overhead processing on the target systems and could disrupt services, they are run during other than normal business hours. GIAC Enterprises primarily works the day shift, Monday through Friday, but backups are done at night and on weekends and there is some batch processing done during these times. It is decided that scanning will be done between the hours of 6 PM and midnight. Also, scans should be scheduled to preclude interference with month-end or year-end processing. Appropriate technical support management and/or staff will be notified prior to any scanning in case production systems are impacted.

CyberCop (http://www.pgp.com/products/cybercop-scanner/default.asp) a commercial, Windows NT based vulnerability scanning tool will be used for our audit. A laptop computer is used for our scans because it can be relocated and reconfigured easily to scan different parts of the network. An initial scan is run by connecting the laptop to the internet outside the screening router. The primary purpose of this scan is to verify the filters on the router. The firewall, the inside interface of the screening router, and systems on the screened subnet can all be scanned for vulnerabilities from the DMZ. This system will also be used to probe GIAC Enterprises' external DNS server using "nslookup" or "dig" for information that might prove useful to an attacker. Following the external scans, the laptop is reconfigured and used to perform internal vulnerability scans on all internal firewalls, servers, and desktop workstations.

Part of GIAC Enterprises' security policy includes rules for creating secure passwords. To check for nonexistent, weak or default passwords we will use password-cracking tools. Although password-cracking capability is included in CyberCop, we will do our cracking "offline" by using a copy of the servers' password databases. We choose this method to keep from overloading the network with a network-based tool. Because GIAC Enterprises utilizes two server platforms, NT and Unix, two password-cracking tools, L0phtCrack for NT (http://www.l0pht.com/l0phtcrack) and Crack for Unix (ftp://coast.cs.prudue.edu/pub/tools/unix/crack) are used to do the password cracking.

As stated earlier, modems can subvert an organization's perimeter security by allowing an intruder to compromise a system without going through the firewall. Once one target system is compromised it provides a base for information gathering or

spreading of viruses, worms, etc. on the internal network. Our audit includes war-dialing the phone numbers assigned to GIAC Enterprises to identify modems attached to users' workstations and to detect any vulnerabilities that might allow an attacker to break into GIAC's network. THC-Scan (http://thc.inferno.tusculum.edu) is a war-dialer that works on Windows NT so we can use the same laptop used for the vulnerability scans for this part of the audit. This scan is performed during non-business hours but will not be announced prior to execution so users will not be warned to disconnect modems they may have connected.

Implementation

A strong perimeter defense is not the only important piece of our security architecture; however a properly configured firewall and screening router certainly serve as the foundation for the rest of our defenses. As stated above, the focus of this assignment is assess our network perimeter security. In order to check our security architecture from different network perspectives the sniffer and laptop computer will be used at a couple of different network locations.

In order to scan the border router from an external view, an account is obtained from a local, commercial ISP specifically to be used for security analysis. The laptop computer is used to access the internet via this account and run the initial scan directed at the external IP address of our firewall. CyberCop is used for the scan and is configured to do a high-level of scanning, including DoS attacks but excluding password cracking. This scan is primarily to verify that the security policy is implemented correctly on the screening router. The sniffer is connected to the DMZ to verify that traffic that is supposed to be blocked is not passing the router. (A router was not available for this portion of our testing; therefore no actual data is included.)

Next, our scanning host is connected to the DMZ and CyberCop is configured, as above, to do a high-level of scanning, including DoS attacks and excluding password checks. The scan is again configured with the address of the outside interface of our firewall.

Analysis

Although the focus of this section is to audit the network firewall, some general comments are included on the overall audit process. The vulnerability scan of the firewall is addressed last.

Following completion of all audit activity, the results are compiled and a report is produced. This report includes all aspects of the audit: the policy/procedure review, system scans, password cracking and war-dialing. The report is delivered to IS management for review and a meeting scheduled with the audit team to discuss the results in detail. The meeting is to address all the vulnerabilities found, identify any false positives and develop plans for corrective action. Corrective actions are prioritized by the severity of the vulnerability.

Any discrepancies between the security policy and the actual operating environment should be reviewed in detail. Occasionally, a company's IS requirements change over the course of time to reflect evolving business needs and the paperwork lags behind the actual configuration. In such cases, the security policies should be updated as needed. If, however, the policies are correct then steps need to be taken to ensure they are implemented as designed.

The problem of users having weak passwords is always present. If the password policy is too strict users simply write the passwords on sticky notes and paste them to their computer. Results of the password-cracking program should be reviewed and users with weak or non-compliant passwords should be notified to change their password.

Vulnerabilities found on authorized modems should be corrected immediately. The system(s) using these modems should be removed from the network and thoroughly checked for viruses, trojans, etc. prior to being cleared for re-connection. If unauthorized modems are detected by the scan, further investigation should be done to determine whether someone is deliberately subverting security or simply not following procedures.

The CyberCop scan from our DMZ listed several potential low-risk vulnerabilities on our firewall. These vulnerabilities, as shown in the example below, indicate open ports that might be vulnerable to port scans. In our case these ports are required for servers on the screened subnet to communicate with the outside world.

TCP SYN port scanning **11/19/00 7:40:56AM**

Risk Factor:	Low
Complexity:	Medium
Popularity:	Popular
Impact:	Intelligence
Root Cause:	Insecure Design
Ease of Fix:	Difficult
Description:	This check can be used as a much faster alternative to regular TCP port scanning. This check scans a target host for listening TCP ports in much the same way as the regular TCP port scanning, however does so by sending a packet to initiate a connection and watching for a response. The difference in using this method is that a complete connection to the remote host is not actually opened. The drawback in using this method is that it may be unreliable due to packet loss on the network.
Security Concerns:	
Suggestion:	The scanner will return which TCP ports are listening. You should check these ports to see if they are running services that you have approved. If they are running services which are undocumented, or which you do not wish to run, we suggest you disable them. Many operating systems are shipped with a large number of services that are not required for normal operation. In some cases these services may contain known or unknown security problems. It is recommended that any services which are not required be disabled.

TCP Port 80 (www) active
TCP Port 443 (https) active
TCP Port 53(dns) active
UDP Port 53(dns) active
TCP Port 25 (smtp) active

During the initial audit review a schedule should be developed during which all legitimate findings should be addressed, either by correcting the problem or documenting why an exception to the policy is necessary. A follow-up meeting should be held some reasonable time in the future to review progress made toward resolving issues raised by the audit. Audit reports should be saved for comparison with data from future audits. Since information security is an ongoing process it will take continuous monitoring and refinement to maintain GIAC Enterprises' security at an acceptably high level.