GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

Version 1.5d

Tanya Baccam

CISSP, GCIH, CISA, MCSE, CCNA, CCSE, CCSA, Oracle DBA

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

Security Architecture 3
Requirements **3**
Summary of Proposed Architecture **3**
Network Diagram of Proposed Architecture **4**
Architecture Definitions **4**
Perimeter Security 4
Primary Internal Firewall 5
Segregated Networks 5
Intrusion Detection 6
Physical Security 6
Security Policy 7
Requirements **7**
Sample Security Policy Outline **7**
Security Policy Documented **9**
Border Router **14**
Summary Policy 14
Policy implementation 15
Primary Firewall **18**
Summary Policy 18
Firewall Rule set 19
VPN **21**
Summary Policy 21
Tutorial 21
Audit Your Security Architecture 23
Requirements **23**
Plan **23**
Implementation **24**
Scan for intended services 24
Test available services 24
Test blocking rules 25
Research for Vulnerabilities 27
Analysis **28**
Design Under Fire 29
Requirements **29**
Firewall Vulnerabilities 29
Denial of Service attack 31
Attack plan 31
Bibliography 33

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

Security Architecture

Requirements

Define a security architecture for GIAC Enterprises, a growing Internet startup that expects to earn $200 million per year in online sales of fortune cookie sayings, and which has just completed a merger/acquisition. Your architecture must specify filtering routers, firewalls, VPNs to partners, secure remote access, and internal firewalls. Be explicit about the brand and version of each perimeter defense component. Produce a diagram or set of diagrams with explanatory text that define how to use perimeter technologies to implement your security architecture.

You must consider and define access for:

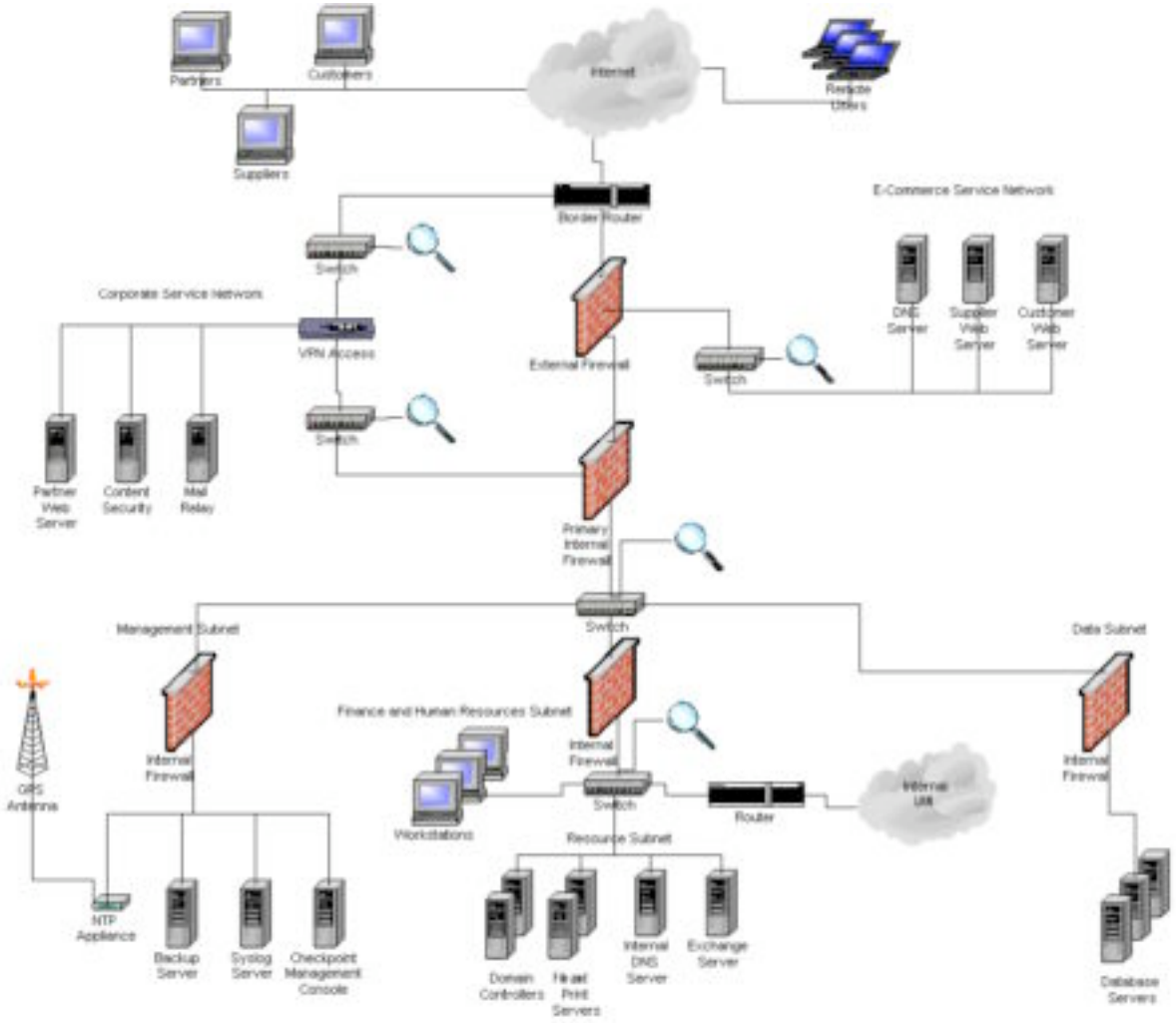
- Customers (the companies that purchase bulk online fortunes);
- Suppliers (the authors of fortune cookie sayings that connect to supply fortunes);
- Partners (the international partners that translate and resell fortunes).

Summary of Proposed Architecture

The environment at GIAC Enterprises will consist primarily of Microsoft, Cisco and Checkpoint products. This is being implemented primarily due to the ease of use and the approximate three person team that will be in place at GIAC Enterprises. The environment will consist of multiple subnets including the corporate service network, the E-Commerce service network, the management subnet, the data subnet, the finance and human resources subnet, the resources subnet and the internal LAN. Each subnet will control access to the other subnets and will be protected by the appropriate technologies.

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

Network Diagram of Proposed Architecture



Architecture Definitions

Perimeter Security

Border Router

The border router in this architecture will function as a filtering router decreasing the amount of traffic analyzed by the firewall. The border router's primary function is to route traffic. The router will also be needed to implement policies, such as the following requirements:

- Implement ingress filtering
- Implement egress filtering
- Control ICMP traffic
- Block source routing

A further, and more detailed, explanation of the router security policy can be found in the "Security Policy – Border Router" section.

A Cisco 3660 router with IOS 12.2 will be used as the border router. Reference information for this router can be found at http://www.cisco.com/univercd/cc/td/doc/pcat/3600.htm#fea. The router has a redundant power supply. The router will also run HSRP (Hot Swappable Routing Protocol) for maximum

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

up time. The Cisco 3660 provides a module hot-swap capability that will be implemented. The Cisco 3660 series was designed for higher-availability with optional power redundancy and network module hot-swap capability.

External Firewall

The external firewall will be a Checkpoint Firewall-1 Version 4.1 with Service Pack 4. The external firewall will be the first line of defense after the border router. The firewall will protect the E-Commerce environment that includes the customer and supplier web server and the primary DNS server. Additionally, the firewall will assist in protecting the internal environment that includes the management subnet, the data subnet, the finance subnet, the resource subnet and the internal network.

VPN

The Corporate Service Network will utilize Checkpoint VPN1 4.1 with Service Pack 4 to control access to the environment. This server has three network interface cards: one for the external connection, one for the internal connection and one for access to the Corporate Service Network.

Primary Internal Firewall

The primary internal firewall will serve as a secondary line of defense for the internal network. This firewall will run a Cisco PIX 520 running version 6. By implementing multiple brands of firewalls, it will be more difficult for a hacker or cracker to break into the environment, since it is assumed that two firewall vendors will not have the same vulnerabilities at the same time.

Segregated Networks

E-Commerce Service Network

The E-Commerce Service Network will consist of three primary servers. The primary external DNS server will be implemented in this environment, as well as supplier and customer web servers. The DNS server will run BIND 9.1.2. The supplier and customer web servers will run IIS4 on a hardened NT4.0 platform with service pack 6a. An ASP will be utilized to handle the management of uploading and downloading of cookie files, billing and supplier relations. Additionally, an ASP will be utilized to handle customer queries, purchases and billings. The backend of the customer and supplier web servers will be a SQL server that will be stored in the data subnet.

Corporate Service Network

The Corporate Service network will provide access to network resources for partners and remote users. The proxy server will run Microsoft Proxy 2.0 and will be responsible for handling the web traffic from the internal network. The partner web server will be a hardened NT 4.0 with service pack 6a running IIS4. Access to this server will only be supplied via VPN. This server will have an SQL server backend that is stored in the data subnet.

Management Subnet

The management subnet will be protected by a Checkpoint Firewall-1 running service pack 4 on a hardened NT 4.0 platform. This subnet will require MAC authentication to tighten security. A very limited number of administrative personnel will have access to this subnet. The management subnet will contain an ntp server, backup servers, syslog servers and checkpoint management console. The servers consist primarily of hardened NT 4.0 servers.

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

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

Resource Subnet

The resource subnet will contain the domain controllers including both primary and secondary servers, the file and print servers, the internal DNS server and the exchange server. The resource subnet will be protected by a Checkpoint Firewall 1 running service pack 4 on a hardened NT 4.0 platform. The internal DNS server is being implemented here to enforce a split DNS architecture. The servers will be hardened NT4.0 servers with server pack 6a applied. The internal DNS server will run BIND 9.1.2.

Data Subnet

The data subnet will contain database servers running on a hardened NT4.0 server with a SQL server database. The data subnet will be protected by a Checkpoint Firewall-1 on an NT platform with service pack 6a. Access to this subnet will be obtained primarily by logging on to other servers in the environment. Access will be highly restricted and monitored to ensure that the data is only flowing to the appropriate subnets and users. The primary focus of GIAC Enterprises, the sayings for fortune cookies, will be stored in this environment, so it will be extremely important to ensure that the data is secure.

Finance and Human Resources Subnet

The finance and human resource subnet will also be a separate subnet since financial and human resource data is highly confidential. This subnet will consist primarily of hardened NT4.0 servers and workstations. Access to this subnet will be provided to authorized users only.

Internal LAN

The internal LAN will consist primarily of hardened NT4.0 servers and workstations. The internal LAN will provide access for the everyday users. A Cisco 3620 router running IOS 12.2 and the installed firewall package will be utilized to protect this subnet. The router will assist in filtering the appropriate access to the finance and human resources subnet as well as the resource subnet.

Intrusion Detection

Intrusion Detection systems will be utilized through out the environment, and the data will be sent to the syslog server for analysis. Intrusion Detection systems will be utilized on all switches in the environment. Due to the scope of this assignment, details on the configuration of the intrusion detection systems will be eliminated.

Physical Security

Physical security is a key to any environment. Without physical security, the logical security implemented will be incomplete and possible ineffective. Resources such as computer hardware and software, peripheral devices, storage media and information systems documentation must be protected. Physical access to these resources makes it possible for users to view, damage or misuse the equipment. Physical security must be implemented and administered to ensure that only authorized personnel have access to the information in the environment. Physical security includes devices, such as locks and keys, key cards, combination door locks, personnel to screen visitors, guards to patrol facilities, biometric devices, fire detection and suppression equipment, alternate power supplies, humidity monitors and temperature monitors. Consideration for the environment should also be addressed when implementing physical security. For example, in the case of GIAC Enterprises, security guards who patrol the perimeter of the facilities may not be necessary; however, receptionists utilized to screen visitors entering the facility would be a control that should be implemented.

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

Security Policy

Requirements

Based on the security architecture that you defined in Assignment 1, provide a security policy for AT LEAST the following three components:

- Border Router
- Primary Firewall
- VPN

You may also wish to include one or more internal firewalls used to implement defense in depth or to separate business functions.

By 'security policy' we mean the specific ACLs, firewall ruleset, IPSec policy, etc. (as appropriate) for the specific component used in your architecture. For each component, be sure to consider internal business operations, customers, suppliers and partners. Keep in mind you are an E-Business with customers, suppliers, and partners - you MAY NOT simply block everything!
(Special note VPNs: since IPSec VPNs are still a bit flaky when it comes to implementation, that component will be graded more loosely than the border router and primary firewall. However, be sure to define whether split-horizon is implemented, key exchange parameters, the choice of AH or ESP and why. PPP-based VPNs are also fully acceptable as long as they are well defined.)
For each security policy, write a tutorial on how to implement each ACL, rule, or policy measure on your specific component. Please use screen shots, network traffic traces, firewall log information, and/or URLs to find further information as appropriate. Be certain to include the following:

1. The service or protocol addressed by the ACL or rule, and the reason these services might be considered a vulnerability.

2. Any relevant information about the behavior of the service or protocol on the network.

3. The syntax of the ACL, filter, rule, etc.

4. A description of each of the parts of the filter.

5. An explanation of how to apply the filter.

6. If the filter is order-dependent, list any rules that should precede and/or follow this filter, and why this order is important. (Note: instead of explaining order dependencies for each individual rule, you may wish to create a separate section of your practical that describes the order in which ALL of the rules should be applied, and why.)

7. Explain how to test the ACL/filter/rule.

Be certain to point out any tips, tricks, or "gotchas".

Sample Security Policy Outline

An IT security policy is foundational to the information security within an organization. Security policies must be complete, up to date and must reflect the corporate needs. Once policies have been developed, compliance must be obtained. Compliance requires that all employees understand the policies and the circumstances for which the policies apply. To this end, policy documents should be written clearly, concisely and address key points that an organization's management wishes to communicate. A corporations security policy should be less than ten pages. Employees should be educated on the policies and must understand how they should comply to the policies.

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

Below is a complete outline for a security policy. In a complete policy, all areas should be addressed. For this assignment only select areas will be expanded upon based on the requirements of the assignment.

1) Introduction
   a) Summary
   b) Objectives
   c) Security Standards
      i) Authorization
      ii) Confidentiality
      iii) Integrity
      iv) Access
      v) Appropriate Use
      vi) Employee Privacy
2) Personnel Standards
   a) Hiring
   b) Friendly Terminations
   c) Unfriendly Terminations
3) IT Systems
   a) Specific Systems
      i) Firewalls
      ii) Routers
      iii) VPN
      iv) Strategic Servers
      v) Email
      vi) Internet
      vii) Telephone and Communications
      viii) Data Center
      ix) Desktop Machines
      x) Legacy Systems
   b) System Requirements
      i) Password Standards
      ii) Administrative Access
      iii) Physical Access
      iv) Backups
      v) Auditing & Monitoring
      vi) Disaster Recovery
4) Security Incident Handling
   a) Preparing and Planning for Incident Handling
   b) Notification and Points of Contact
   c) Identifying an Incident
   d) Handling an Incident
   e) Follow-up of an Incident
   f) Forensics and Legal Implications
   g) Public Relations Contacts
   h) Key Steps
      i) Preparation
      ii) Identification
      iii) Containment
      iv) Eradication
      v) Recovery
      vi) Follow-Up

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

i) Responsibilities
5) Ongoing Activities
a) Incident Warnings
i) Virus warnings
ii) Intrusion Detection
iii) Security Patches
6) Violations
7) Contacts, Mailing Lists and Other Resources[1]

Security Policy Documented

----------Begin GIAC Enterprise Security Policy Manual----------

Introduction

Summary

The policies in this document were developed by GIAC Enterprises in order to define GIAC Enterprise's information technology security requirements. These policies are the minimum level of security acceptable to GIAC Enterprises. GIAC Enterprise relies heavily on their information technology systems for the effective management of its business. The importance and critical nature of the information, software, hardware, telecommunications and facilities must be recognized by all GIAC employees, as an asset to be protected through the company security program.

Objectives

GIAC Enterprise's will establish and promulgate guidance for the protection of the organization's information technology resources and sensitive information.

Security Standards

Authorization

Authorization allows users to do or have something. GIAC Enterprise consists of multiple computer systems. The personnel to whom an employee directly reports will authorize access for the systems and define the privileges of use. This includes, but is not limited to, hours of access, file directories, application systems and Internet access. The system administrator will review the authorized access and define the individual user profiles for the system. Authorization must be reviewed every three months. At this time, a review and verification of the current employees on the system will be conducted. Any employees who do not demonstrate a valid business purpose to access the systems will be removed.

Confidentiality

Confidentiality is the degree to which the privacy or secrecy of something can be maintained. Confidential information is information at GIAC Enterprises pertaining to its operations, that upon disclosure could have a negative financial or operational impact. The unauthorized disclosure of confidential information to competitors or other third parties presents a threat to GIAC Enterprises.

Integrity

Integrity refers to the assurance that information can be accessed or modified by only authorized individuals. Methods such as limiting physical access, restricting logical access and maintaining rigorous authentication practices will be utilized to help ensure that only authorized access to the systems is obtained.

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

Access

Access is the ability to obtain what an employee needs to do his/her job. Access for all employees must be approved by the appropriate manager and reviewed on a regular basis.

Appropriate Use

GIAC Enterprises computing resources are for business purposes only. GIAC Enterprise management has the latitude to allow the use of GIAC Enterprise computing assets for personal and professional growth at the discretion of the manager. In such a case when personal use policies are acceptable to a manger, a standards document applicable to the individual department must be written and submitted by the department to the Information Systems Steering Committee. The Information Systems Steering Committee is responsible to review and approve or disapprove the standards. If no such standards are in place, then the default policy is in effect.

Employee Privacy

Messages sent over the enterprise network, computer and communications systems are the property of GIAC Enterprises. Management has the right to examine all the data stored in or transmitted by any GIAC Enterprise systems in order to properly protect and manage GIAC Enterprise property. GIAC Enterprise is not responsible for the message protection services such as encryption. Therefore, GIAC is free from all responsibility pertaining to the disclosure of information sent over GIAC Enterprise networks.

Personnel Standards

Hiring

Employees will have access to applicable systems on their first day of employment. The manager of each new employee must complete and sign a 'New Employee Access Request' form containing proper approval prior to the new employee arriving on site. The form must be signed by the owners of the data to which the employee requires access. Upon proper approval, the form will be submitted to the GIAC Enterprise Information Technology team, and the team will set up the appropriate User Ids and passwords. The manager who submitted the form will be notified when the user setup is complete.

Friendly Terminations

Upon employment termination on friendly terms, the employee is required to do an exit interview with the department of Human Resources. At this time, the Manager of Human Resources will complete and sign an 'Employee Termination' form which should be submitted to the Information Technology team. The Information Technology team must remove all employee access within 48 hours of termination.

Unfriendly Terminations

Upon employment termination on unfriendly terms, the employee will be requested to leave the facilities immediately. Two escorts will be provided to assist in this process. As soon as the Manager of Human Resources becomes aware of such terminations, they must immediately complete and sign an 'Employee Termination' form. This form must be submitted to the Information Technology team and followed up with a phone call. The Information Technology team must remove any employee access immediately upon employee termination. Information pertaining to unfriendly terminations is confidential and should only be discussed with appropriate personnel.

IT Systems

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

Specific Systems

Firewalls

A GIAC Enterprise approved firewall and/or other access control technology or processes as specified by the Information Technology Steering Committee must protect all connections between GIAC Enterprise internal networks and the Internet or any other external computer network.

Routers

A border router will be utilized at the perimeter of GIAC Enterprise networks. All traffic must flow through an approved filtering router.

VPN

GIAC Enterprise users must complete an approved VPN access training course prior to being granted privileges to use dial-up or any other remote access data communications system. Partners and Suppliers will be provided VPN access only upon an appropriate signed agreement, a copy of which will be provided to and approved by the Information Technology Steering Committee.

Strategic Servers

Access to strategic servers will be monitored on a regular basis. A review of the users and the access provided should be done every three months, or more frequently, depending on the confidentiality of the data or the operational impact of the server.

Email

During an employee's working business hours, email usage should pertain to only business correspondence. Limited personal use will be allowed during breaks and non-business hours. GIAC Enterprise will monitor this usage; therefore, this privilege should be controlled carefully. GIAC Enterprises will not condone the sending of large files, such as, email executable jokes, generating high volumes of personal mail through third party sales or e-mail groups, or soliciting non-GIAC Enterprise business. GIAC Enterprise has the right to disallow an employee any personal use of the e-mail systems if improper usage is suspected. These cases will be documented and signed by the appropriate management.

Internet

Internet access will be provided after completing an 'Internet Access Request' form. These forms must be signed by the user and their management. Access will only be provided when there is a valid business reason for such access. Internet access will only be allowed for valid business usage.

Telephone and Communications

Communications are the foundation to GIAC Enterprise business. Electronic mail, telephone, and video conferencing have become foundational to any business. A communications network enables the transfer of data between users, hosts, partners, suppliers, customers, applications and other facilities. During the transfer, data is susceptible to either unintentional or deliberate access or alteration. The Information Technology team, along with the owners of the information will establish and maintain security controls to detect unauthorized attempts to access or modify data in transit. Follow-up procedures will be in place to detect any suspected unauthorized attempts.

Data Center

All multi-user computers or servers and critical systems must reside in a data center. Each data center

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

must be physically secure and access will only be provided for valid business reasons. Additionally, access will only be supplied to systems administrators, operators, senior information technology management and support personnel. A 'Data Center Access Request' form must be signed and submitted by a user's manager to ensure that only proper access is granted. The data center will be equipped with a fire suppression system, uninterruptible power supplies, alarms, video monitoring, humidity controls and air conditioning.

Desktop Machines

Each employee's desktop machine is the property of GIAC Enterprises. GIAC Enterprises retains the right to obtain access to an employee's desktop machine at any time.

Legacy Systems

** This section is not applicable to GIAC Enterprises and is only being included as a sample for readers.

System Requirements

Password Standards

Personnel are responsible for their own passwords. Passwords must be chosen that are difficult to guess. Passwords should not be related to an employee's job or personal life. Additionally, passwords must not be a word found in a dictionary. Each password must be substantially different from the pervious password. Passwords must be changed every 60 days and can not be the same as the last ten passwords utilized. Passwords must never be shared or revealed.

System administrators are responsible for the passwords that are utilized on their systems. Passwords may not be stored in a readable format, i.e. clear text. This includes passwords stored in any file or on any medium including, put not limited to, passwords files, notepads, scripts and macros. Additionally, default passwords must be changed on all systems prior to moving the systems to the production environment.

If it is suspected that a password is known, the password must be immediately changed.

Administrative Access

Administrative access to strategic servers will be closely guarded. Access must be approved by the appropriate management to each specific strategic server. This includes, but is not limited to, the servers on the E-Commerce, data, corporate, management and resource subnets.

Physical Access

Physical access to the facilities will be restricted to authorized personnel. All visitors must sign in at the reception desk and be escorted by authorized personnel while in the facilities.

Access to telephone wiring closets, computer data centers, systems development offices, network switching rooms, and other work areas containing confidential information and must be physically restricted. All transmission media, such as cables and connectors, must be covered and protected. The Information Technology department must approve physical access to all critical systems. Critical systems must be stored in locked computer data centers.

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

Backups

All systems will be backed up on a regular basis. An incremental backup will be performed daily, Monday through Saturday and will be retained for two weeks. A full backup will be performed on Sunday and retained for four weeks. The first Sunday of the month will be a monthly backup and will be retained for two years. This will replace the weekly backup for the first Sunday of the month.

Auditing & Monitoring

Personnel are subject to electronic monitoring while on GIAC Enterprise premises. The GIAC Enterprise Information Technology team is responsible for monitoring all critical systems. Automated tools must be utilized to assist in verifying the security status of the computer. Tools must include mechanisms for the correction of security problems.

Intrusion Detection systems must also be utilized throughout the environment to monitor for malicious activity.

Disaster Recovery

Disaster Recovery Plans will exist for all critical systems. Disaster Recovery Plans will be updated on an annual basis. Disaster Recovery Plans older than one calendar year are considered to be expired and invalid.

Security Incident Handling

** This section of the policy manual is not applicable to this assignment, and therefore will not be expanded upon. To find further information pertaining to vulnerabilities and incident handling, multiple SANS students have submitted papers that can be found at www.sans.org/giactc/gcih.htm.

Ongoing Activities

Incident Warnings

Virus warnings

GIAC Enterprises will determine the appropriate virus scanning software to be installed and utilized on all GIAC Enterprise systems. The software will be updated every 30 days to ensure that the highest level of virus protection is being obtained.

To prevent infection by computer viruses, users must not use any externally provided software from a person or organization other then a known and trusted supplier. Whenever software/files are received from any un-trusted external entity or downloaded from the Internet, the files must be scanned by software approved by GIAC Enterprises. Scanning must take place prior to being run by any program or being executed.

Intrusion Detection

Intrusion Detection systems must be utilized, logged and monitored within the GIAC Enterprise environment. Intrusion Detection Systems are required at the perimeter for all incoming traffic. Traffic entering the network must be monitored and logged by the Intrusion Detection system. These logs must be reviewed daily and on an ongoing basis by Information Technology personnel.

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

Security Patches

Security patches must be tested in a test environment prior to applying them to production systems. All patches must be applied to information systems as they become available, assuming that they have been tested and that they do not hinder activities in the GIAC Enterprises environment. The Information Technology team is to ensure that the most recent patches have been applied to all systems.

Violations

The GIAC Enterprise employees who willingly and deliberately violate this policy will be subject to disciplinary action up to and including termination.

Contacts, Mailing Lists and Other Resources

** Information pertaining to specific employees, vendors, mailing lists and other resources applicable to GIAC Enterprises would be recorded here. Due to the scope of this assignment, this will not be addressed.

----------End GIAC Enterprise Security Policy Manual----------

Border Router

Summary Policy

The border router will be responsible for filtering incoming and outgoing traffic. A border router will assist in filtering traffic, but it does not function as a firewall. The border router for GIAC Enterprises will be responsible for the following items:

- Inbound filtering
  - Ingress filter will be applied by dropping and logging traffic coming from private and non-routable address spaces. See RFC 1918 for further information on reserved subnets.
  - Login services will be blocked.
  - RPC and NFS services will be blocked. NFS runs on 2049 and lock runs on 4045. Locd are services that are subject to exploits from RPC calls.
  - NetBIOS services will be blocked.
  - X-windows services will be blocked.
  - Only TCP packets which have been ACKed will be allowed on the network.
  - Allow SMTP traffic to only the mail servers.
  - Allow DNS traffic to only the name servers.
  - Allow ntp traffic to only the time servers.
  - All other traffic will be logged.
- Outbound filtering
  - Egress filtering will prevent outbound spoofing.
  - All other traffic will be logged.
- The router must also be armored.
  - SSH access to the router and monitoring server will be limited.
  - Access to SNMP services will be restricted.
  - Source routing will be disabled so that packets cannot be re-routed to another system.
  - Password encryption will be utilized.
  - The echo service will be disabled.
  - The discard service will be disabled.

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

- The chargen service will be disabled.
- The daytime service will be disabled.
- The finger service will be disabled.
- Http servers will be disabled.
- Bootp servers will be disabled.
- Malicious directed broadcasts will be prevented from causing denial of service problems.
- ICMP unreachable messages will be disabled.
- Only specific ICMP messages will be allowed.
- CDP will be prevented.
- A warning banner will be added.
- Enable UNIX syslog logging.

See http://pasadena.net/cisco/secure.html and http://www.cisco.com/warp/public/707/21.html for additional information.

Policy implementation

** *a.b.c.d represents the applicable host IP. w.x.y.z represents the applicable subnet.*

Inbound Access List

```
        Interface Serial 0
                ip address a.b.c.d w.x.y.z
                ip access-group 101 in

!
!       Ingress filtering
!
access-list 101 deny ip 10.0.0.0 0.255.255.355 any log
access-list 101 deny ip 172.16.0.0 0.15.255.255 any log
access-list 101 deny ip 192.168.0.0 0.0.255.255 any log
access-list 101 deny ip 127.0.0.0 0.255.255.255 any log
access-list 101 deny ip 224.0.0.0 7.255.255.255 any log
access-list 101 deny ip 240.0.0.0 63.255.255.255 any log
access-list 101 deny ip 255.0.0.0 63.255.255.255 any log
access-list 101 deny ip host 0.0.0.0 any log
!
!       Block Login services and log any activity
!
access-list 101 deny tcp any any range ftp telnet log
access-list 101 deny tcp any any range exec lpd log
!
!       Block RPC and NFS and log any activity
!
access-list 101 deny udp any any eq sunrpc log
access-list 101 deny tcp any any eq sunrpc log
access-list 101 deny udp any any eq 2049 log
access-list 101 deny tcp any any eq 2049 log
access-list 101 deny udp any any eq 4045 log
access-list 101 deny tcp any any eq 4045 log
```

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

```
!
!       Block NetBIOS and log any activity
!
access-list 101 deny tcp any any 135 log
access-list 101 deny udp any any 135 log
access-list 101 deny udp any any range 137 138 log
access-list 101 deny tcp any any eq 139 log
access-list 101 deny tcp any any eq 445 log
access-list 101 deny upd any any eq 445 log
!
!       Block Xwindows and log any activity
!
access-list 101 deny tcp any any range 6000 6255 log
!
!       Allow only ACKed tcp packets to our network
!
access-list 101 permit tcp any a.b.c.d w.x.y.z gt 1023 established
!
!       Allow SMTP traffic to only the mail server(s)
!
access-list 101 permit tcp any a.b.c.d 0.0.0.0 eq 25
!
!       Allow DNS traffic to only the name server(s)
!
access-list 101 permit tcp any a.b.c.d 0.0.0.0 eq 53
access-list 101 permit udp any a.b.c.d 0.0.0.0 eq 53
!
!       Allow HTTP traffic to only the web server(s)
!
access-list 101 permit tcp any a.b.c.d 0.0.0.0 eq 80
!
!       Allow ntp traffic to only the time servers
!
access-list 101 permit tcp ant a.b.c.d 0.0.0.0 123
access-list 101 permit udp ant a.b.c.d 0.0.0.0 123
!
!       Log everything else (inbound):
!
access-list 101 deny ip any any log
```

Outbound Access List

```
        Interface Ethernet 0
                ip address a.b.c.d w.x.y.z
                ip access-group 102 in

!
!       Allow IP addresses from GIACs network outbound
!
access-list 2 permit a.b.c.d w.x.y.z any
!
```

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

```
!       Allow outbound web server replies
!
access-list 102 permit tcp a.b.c.d 0.0.0.0 any gt 1023 est
!
!       Allow outbound replies from the mail server
!
access-list 102 permit tcp a.b.c.d 0.0.0.0 any gt 1023 est
!
!       Allow outbound replies from the DNS server
!
access-list 102 permit tcp a.b.c.d 0.0.0.0 any gt 1023 est
!
!       Allow outbound DNS traffic from the DNS server
!
access-list 102 permit udp a.b.c.d 0.0.0.0 any eq 53
!
!       Allow only DNS traffic permitted above
!
access-list 102 deny udp a.b.c.d w.x.y.z any
!
!       Egress filtering and logging any activity
!
access-list 102 deny ip 192.168.0.0 0.0.255.255 any log
access-list 102 deny ip 172.16.0.0 0.15.255.255 any log
access-list 102 deny ip 10.0.0.0 0.255.255.255 any log
access-list 102 deny ip any 192.168.0.0 0.0.255.255 log
access-list 102 deny ip any 172.16.0.0 0.15.255.255 log
access-list 102 deny ip any 10.0.0.0 0.255.255.255 log
!
!       Log everything else
!
access-list 102 deny ip any any log
```

Armoring the Router

```
!
!       Limit SSH access to the router to the monitoring server:
!
        access-list 10 permit host a.b.c.d
                line vty 0 4
                        transport input ssh
                        access-class 10
                        login
!
!       Restrict access to SNMP services
!
        access list 11 permit host a.b.c.d
        snmp server community giacpublic RO 10
        snmp server community n01shouldn0 RW 11
!
!       Disable source routing so that packets cannot be re-routed to another system
```

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

```
!
        no ip source-route
!
!       Enable password encryption
!
        service password-encryption
!
!       Disable unneeded services such as echo, discard, chargen, and daytime
!
        no service tcp-small-servers
        no service udp-small-servers
!
!       Disable finger service
!
        no service finger
!
!       Disable http and bootp servers
!
        no ip http server
        no ip bootp server
!
!       Prevent malicious directed broadcasts from causing denial of service problems
!
        no ip direct-broadcast
!
!       Stop ICMP unreachable messages on all interfaces
!
        no ip unreachables
!
!       Prevent CDP
!
        no cdp enable
!
!       Add a warning banner.  Add exec, incoming, login, and motd !banners
!
        banner login
!
!       Enable UNIX syslog logging.
!
        logging a.b.c.d
        logging trap debug
        logging console emergencies
```

Primary Firewall

Summary Policy

The firewall will prevent outsiders from accessing the private network. It protects GIAC Enterprise resources. Generally, firewall rules should be listed from specific to general and from the most utilized to the least utilized. The firewall for GIAC Enterprises will be responsible for the following items in this order:

1. Firewall Administration

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

2. Stealth rule
3. Syslog rule
4. Inbound e-mail
5. Inbound Web
6. VPN
7. Client encrypt
8. Reject restricted sites
9. DNS queries and zone transfers
10. Block Chatty Protocols
11. Protect Networks
12. Anti-virus
13. Protection of internal networks from corporate service network
14. Protection of corporate service network from internal networks
15. Allow NTP updates
16. Cleanup rule

Firewall Rule set

The "Cleanup rule"[16] should be created first to block any traffic coming in through the firewall. This rule will be at the end of the rule listing and will drop all traffic not explicitly allowed. The cleanup rule will also allow for logging of any traffic that is being dropped so that the traffic can be analyzed by Intrusion Detection specialists at GIAC Enterprises.

The management network is allowed access to administer the firewalls.[1] This includes SSH traffic, whose administrators will manage the firewall. Secure Shell (SSH) is encrypted traffic between the client and the servers. Only personnel coming from the management network will be allowed to manage the firewall. Any other IP addresses will be dropped.

The stealth rule[2] is utilized to prevent users from connecting directly to the firewall. This rule should be placed at the beginning of the rule listing to ensure that it is protecting the firewall. If anyone attempts to connect to the firewall from an IP address not on the management subnet, an alert will be triggered. This will allow GIAC Enterprise's Intrusion Detection analysts to follow up on the issue.

All GIAC Enterprise servers and routers are logging to the syslog server. Therefore, since the border router must go through the firewall to reach this server, the syslog rule[3] must be added to allow traffic to travel to the syslog server.

E-mail traffic will also be allowed into the GIAC Enterprise networks.[4] Therefore, SMTP (Simple Message Transport Protocol – TCP/25), POP3 (Post Office Protocol TCP/110), and IMAP (Internet Message Access Protocol – TCP/143) will be allowed to communicate to the Microsoft Exchange server. All e-mail traffic is sent to a content security server to scan for viruses. [12]

HTTP (Hypertext Transport Protocol) traffic will be filtered via a web security content server.[5] This server will check for malicious strings that are place in URLs, as well as verifying that unapproved sites are not being visited.[8]

Since GIAC Enterprises has partners that translate and resell information fortunes, a Virtual Private Network (VPN) solution has been utilized to allow connectivity between the networks. CheckPoint's VPN-1 is being utilized as a firewall-to-firewall VPN connection. The partners will need access to the database servers at GIAC Enterprises in order to conduct business. Two rules must be in place to allow a firewall-to-firewall VPN Connection.[8] These rules must be configured on GIAC Enterprises and the

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

partners rule bases. The first rule will create the IPSec firewall-to-firewall communication including encryption and authentication parameters. The second rule will determine the type of data each network can access.

For Client Encryption, SecuRemote is being utilized. Client encryption rules include the following:[7] the first rule will define the list of users from the partners that are allowed access to the Corporate Service Network. The second rule allows VPN clients to retrieve their encryption domain information. This is done when attempting to exchange security key information. The final rule allows internal personnel to authenticate to the firewall and gain access to the internal network.

DNS queries and zone transfers must also be allowed in order for GIAC Enterprises to have an Internet presence. [9] Two rules are created. The first allows DNS queries (UDP-53) to be conducted from the Internal Network to the DNS servers. The second allows zone transfers (TCP-53) to occur from the secondary name server to the primary names server.

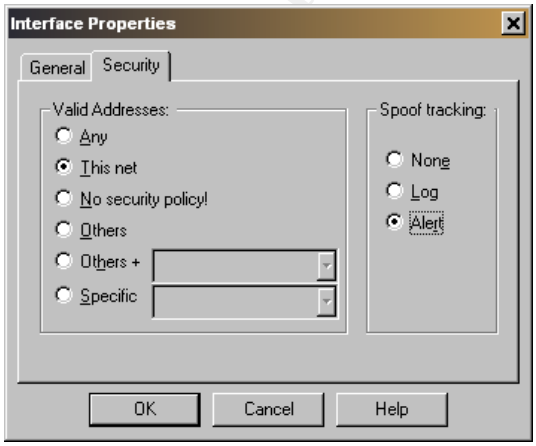
Chatty protocols[10] are blocked to ensure that unauthorized information is not sent out to the Internet. Ident (TCP-113), Bootp (UDP-67), NBDatagram (UDP-138), NBName (UDP-138), NBSession (TCP-139), and MSPortMapper (TCP-135) are not allowed to send information to the Internet.

Protection Rules are put in place to alert administrators in the event that Internal users attempt to access the screened networks or subnets. These rules are placed at the end of the rule base to ensure that all other appropriate access is authorized first.

The corporate service network must be protected from the internal networks as well as the internal networks being protected from the corporate service network. [13 and 14]

The ntp server must also be allowed to receive updates from the Internet. [15]

Once the above rules have been implemented, there are two additional utilities available to CheckPoint-1 that should be utilized. First, Firewall-1 has capabilities to limit IP spoofing attempts. Firewall-1 will examine the IP addresses of incoming packets to validate that these are being received from authorized networks. Second, Firewall-1 has a tool that is designed to stop SYN Flood denial-of-service attacks This tool is called SYN-Defender and should be utilized on the firewall.



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

VPN

Summary Policy

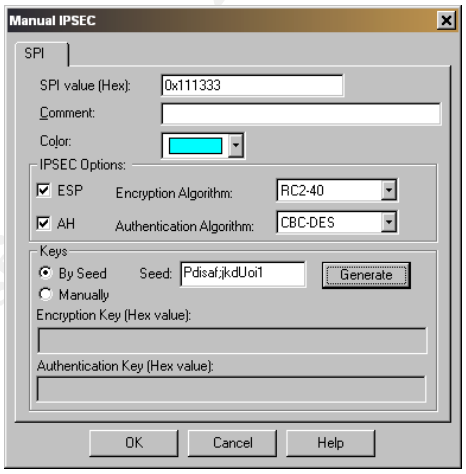
Firewall-1 supports three encryption schemes: FWZ, Manual IPSec, and SKIP. Manual IPSec is being implemented for GIAC Enterprises. IPSec utilizes a security association (SA) which consists of functionality, including whether the packet is encrypted, authenticated or both; algorithms which specify the encryption algorithm and authentication algorithm; keys used in the above algorithms; and additional data. A Security Parameter Index (SPI) identifies a specific SA.

A firewall-to-firewall VPN connection will be configured for all partners. Each personnel requiring access will utilize the SecuRemote client software. This is utilized so the data will be encrypted before it leaves the laptop. When SecuRemote is configured, the users, authentication, encryption and routing must be specified. An internal database of partner user names will define the limitations of SecuRemote such as type of authentication method, locations available, acceptable encryption type and the time of day when access is granted.

Tutorial

Firewall-to-Firewall VPN

The key exchange process is a manual process for Manual IPSec. The IP packets will be encrypted with the Encapsulated Security Payload (ESP) standard. The authentication header (AH) contains the message digest. The authentication algorithm will be CBC-DES and the encryption algorithm will be RC2-40 as seen in the diagram below.



Two rules must be configured on both firewalls to create a firewall-to-firewall VPN. When configuring a rule to allow a firewall-to-firewall VPN connection, the two following rules must be configured on both firewalls rule base.

1. An IPSec firewall-to-firewall rule which defines the encryption and authentication parameters utilized.

2. The VPN rule, which determines what type of data each network can access.

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

FireWalker Hades	Hades FireWalker	IPSEC	accept	Long	Gateways	Any

Client Encrypt Rule

A rule must be created that contains a list of users that have access to the corporate service network.

All Users@Partner_Net	ScreenNET	http https ftp smtp pop-3	Client Encrypt	Long	Gateways	Any

Users must also be able to fetch their encryption domain information when exchanging security key information. The rule below allows clients to complete this.

Any	MgmtConsoles	FireWall1	accept	Long	Gateways	Any

Internal users are also allowed to authenticate with the firewall and gain access to the internal network. The data between the client and the firewall will be encrypted.

All Users@Any	LocalLAN	Any	Client Encrypt	Long	Gateways	Any

* Selected diagrams have been utilized from Daniel Martin's assignment. The assignment can be found at http://www.sans.org/y2k/practical/Daniel_Martin_GCFW.doc.

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

Audit Your Security Architecture

Requirements

You have been assigned to provide technical support for a comprehensive information systems audit for GIAC Enterprises. You are required to audit the Primary Firewall described in Assignments 1 and 2. Your assignment is to:

1. 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.

2. Implement the assessment. Validate that the Primary Firewall is actually implementing the security policy. Be certain to state exactly how you do this, including the tools and commands used. Include screen shots in your report if possible.

3. Conduct a 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: DO NOT simply submit the output of nmap or a similar tool here. It is fine to use any assessment tool you choose, but annotate the output.

Plan

An audit or assessment of the architecture should be conducted in order to mitigate risk. Risk can not be completely eliminated. However, by mitigating the risk, there is a less likely chance the GIAC Enterprise networks will be compromised.

The following series of steps will be conducted to audit the primary firewall.

1) The time and dates of the audit will be determined.
2) The users will be notified of the time and dates of the audit.
3) A scan of the primary firewall will be conducted to ensure that intended services are running.
4) Tests will be conducted to ensure that available services are working properly.
5) Tests will be conducted, via scans, to ensure that each of the blocking rules on the firewall are blocking the intended services.
6) Research will be conducted to identify additional vulnerabilities that may not have been considered.
7) The results will be analyzed.

A few key points should be considered when planning the audit.

1) Due to the load on the network and inherent risks of a scan, the scan should be conducted outside of normal business hours.
2) A full backup of the systems should be completed prior to conducting any testing.
3) GIAC Enterprises should conduct audits on a regular basis to ensure that the environment remains as secure as possible.

The following items will be required in order to complete the audit.

1) A network diagram of GIAC Enterprises which includes applicable IP addresses.
2) A port scanner such as Nmap.
3) A vulnerability scanner such as Nessus and/or Internet Security Scanner (ISS).
4) A sniffer such as tcpdump.

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

The cost of the assessment follows.

Action	Effort
Planning	1 Day
Review network diagram and gather information	1 Day
Conduct analysis	2 Days
Analyze results	1 Day
Closing Meeting	1 Day
Total estimated cost	$15,000 ($2500/day)

Implementation

Scan for intended services

The following command can be utilized using nmap to scan the primary firewall. This command will return all the services that are being run. Only services which are intended to be running and which should be running should be returned by the scan. A scan must be conducted of each interface on the firewall. Any identified services that should not be running should be disabled.

nmap –v –g53 –sS –sR –P0 –O –p 1-65535 –o firewall.out *ip_address*

This command does the following:

–v: verbose mode, nmap returns additional information
–g53: sets the source port number utilized for the scans
–sS: conducts a SYN scan
–sR: conducts a RPC scan
–P0: do not conduct pings before scanning (utilized when ICMP messages are blocked)
–O: activates remote host identification via TCP/IP fingerprinting
–p 1-65000: ports to be scanned
–o firewall.out: output file to send the results to
ip_address: the IP address to be scanned

Test available services

Test access to the Web Server

Attempt to access the web server via an external connection. Complete a transaction to ensure that the web servers are functioning as intended. Follow the transaction through to completion.

Test SSH access

An attempt to access the firewall should be made from the management network using SSH. Utilize a sniffer such as tcpdump to observe the traffic being sent.

Test VPN

VPN access should be tested by attempting to access the network from an external connection. The traffic should be monitored by using a tool such as tcpdump to ensure that the data is being encrypted.

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

Test Mail Access

Mail access should be tested by attempting to send mail from the external mail server to a valid Internet address. Additionally, an email should be sent from a valid Internet address to the external mail server.

Test DNS Access

DNS access can be tested by performing a DNS lookup from a valid Internet address to the external DNS server. Additionally, a DNS lookup should be conducted from the external DNS server to a valid DNS server on the Internet. An attempt to conduct a zone transfer should also be completed.

Test Access from the E-Commerce Service Network

Tests should be conducted to ensure that the E-Commerce Service Network can only access appropriate resources. Tests such as PING, TELNET, TCP, etc. should be conducted from the machines on the E-Commerce Service Network to the management subnet, data subnet, resource subnet, finance and HR subnet and the internal subnet.

Syslogs

Syslogging should be checked to ensure that proper logs are being sent and stored on the log servers.

Backups

Backups should be verified to ensure that they are being conducted properly and that the data can be retrieved from the tapes.

NTP Server

To verify whether the NTP server is working correctly, observe the time on the NTP server as well as the time on a machine in the E-Commerce Service Network. The times on the machines should be the same.

IDS Check

During this process, all activity should be logged. Review the logs to verify that the IDS have been able to monitor and log all service attempts.

Test blocking rules

Each firewall rule which blocks traffic should be tested to ensure that the traffic is not getting through the firewall. Additionally, ingress filtering, egress filtering and fragmentation should be tested to ensure that the firewall responds as expected.

Ingress filtering test

Tests should be conducted to ensure that ingress filtering is being blocked as expected. Each non-routable address and internal network address should be tested to ensure that these packets cannot get past the firewall. A command such as the following should be utilized.

nmap –sS –P0 –v –p 80 –o ingress.out –S *source_ip_address* -i eth0 *dest_ip_address*

This command does the following:

–sS: conducts a SYN scan
–P0: do not conduct pings before scanning (utilized when ICMP messages are blocked)
–v: verbose mode, nmap returns additional information
–p 80: port(s) to be scanned
–o ingress.out: output file to send the results to

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

–S *source_ip_address*: the ip address (non-routable and internal network addresses) being utilized as the source
–i eth0: the interface to utilize
–*dest_ip_address*: the destination IP address to be scanned

Egress filtering test

Tests should also be conducted to ensure that egress filtering is being blocked as expected. Each internal address should be utilized to ensure that the cannot leave the network. A command such as the following should be utilized.

nmap –sS –P0 –v –p 80 –o egress.out –S *source_ip_address* -i eth0 *dest_ip_address*

This command does the following:
–sS: conducts a SYN scan
–P0: do not conduct pings before scanning (utilized when ICMP messages are blocked)
–v: verbose mode, nmap returns additional information
–p 80: port(s) to be scanned
–o egress.out: output file to send the results to
–S source_ip_address: the ip address (non-routable and internal network addresses) being utilized as the source
–i eth0: the interface to utilize
–dest_ip_address: the destination IP address to be scanned

Fragmentation test

A fragmentation test should be completed to ensure that services which are not allowed through the firewall normally are still not allowed through the firewall when fragmented. A command such as the following can be utilized to complete this test:

hping2 –V –I eth0 --data 40 --count 3 --syn –p 22 *ip_address*
hping2 –V --frag –I eth0 --data 40 --count 3 --syn –p 22 *ip_address*

The first command does the following:

–V: verbose mode
–I eth0: interface name
--data 40: data size
--count 3: packet count
--syn: sets the SYN flag
–p 22: sets the destination port
ip_address: sets the destination address

The second command does the following:
–V: verbose mode
--frag: split packets in more fragments
–I eth0: interface name
--data 40: data size
--count 3: packet count
--syn: sets the SYN flag
–p 22: sets the destination port
–*ip_address*: sets the destination address

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

The second command contains a fragmented packet. If the rules are set up correctly, both commands should return nothing. Using a tool such as tcpdump, you can observe if the second command does, in fact, generate traffic.

Chatty protocols test

A test should be conducted to ensure that the chatty protocols are blocked from leaving the network. A sniffer such as tcpdump can be placed on the external interface and utilized to ensure that unauthorized packets are not sent out to the Internet. Hping can be utilized to craft packets in an attempt to send the requests to the border router. The following services should be tested:

– Ident (TCP-113)
– Bootp (UDP-67)
– NBDatagram (UDP-138)
– NBName (UDP-138)
– NBSession (TCP-139)
– MSPortMapper (TCP-135)

Firewall Administration and Stealth test

An attempt should be made to access and connect to the firewall from a machine other than those on the management network. This attempt must be denied.

Research for Vulnerabilities

The following vulnerabilities were identified for CheckPoint Firewall-1.

1) Passive FTP Vulnerability

   "FireWall-1's parsing of the FTP control connection was manipulated via MTU such that a FTP server PASV port number, as processed by FireWall-1, was associated with the port number of a service with a known security issue (in this case, ToolTalk port vulnerability on a un-patched Solaris 2.6 system). This enabled the client to exploit the server's vulnerability (i.e., an in.ftpd that returned client-controlled data in an error message and running a possibly unnecessary service: ToolTalk) to gain root access on the machine. This vulnerability was reported to BugTrag on Wednesday, February 9th by John MacDonald of DataProtect." See http://www.checkpoint.com/techsupport/alerts/pasvftp.html for further information.

2) IP Fragment-driven Denial of Service Vulnerability

   "It has been determined that a stream of large IP fragments can cause the FireWall-1 code that logs the fragmentation event to consume most available host system CPU cycles. It should be noted that no unauthorized access, information leakage, or fragment passing occurs.

   The vulnerability was discovered by Lance Spitzner (lance@spitzner.net) and has been confirmed by Check Point. Testing by Check Point indicates that versions 4.0 and 4.1 of FireWall-1 can be impacted (versions earlier then the 4.0 version were not tested)." See http://www.checkpoint.com/techsupport/alerts/ipfrag_dos.html for further information.

3) Fast Mode Vulnerability

   "Check Point Software Technologies has been made aware of a TCP-fragment-based security issue associated with the use of the "Fast Mode" option for individual TCP services (NOTE: Fast Mode is synonymous with "FASTPATH" in the product GUI). Current Service Packs (v4.1 SP3 and v4.0 SP8) address this issue and a workaround is also available.

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

Additionally, performance enhancements in recent VPN-1/FireWall-1 releases eliminate the need for the Fast Mode option, so it will be discontinued in the next major product release (see "Discontinuation of Fast Mode" below)." See http://www.checkpoint.com/techsupport/alerts/fastmode.html for further information.

4) RDP Communication Vulnerability

"Check Point uses a proprietary protocol called RDP (UDP/259) for some internal communication between software components (this is not the same RDP as IP protocol 27). By default, VPN-1/FireWall-1 allows RDP packets to traverse firewall gateways in order to simplify encryption setup. Under some conditions, packets with RDP headers could be constructed which would be allowed across a VPN-1/FireWall-1 gateway without being explicitly allowed by the rule base. In the 4.1 SP4 hotfix and all future service packs and releases, this default behavior is changed and RDP communication is blocked unless a specific access rule is written." See http://www.checkpoint.com/techsupport/alerts/rdp.html for further information.

CheckPoint Firewall-1 was reviewed for each of the vulnerabilities listed above. When conducting research on vulnerabilities, any vulnerabilities that are identified should be patched immediately.

Analysis

Due to the limited resources available, a complete actual test of the environment cannot be analyzed. However, assuming the security architecture assessment was successful and no security issues or flaws were identified. There are some additional key points that GIAC Enterprises should consider implementing.

1) There are multiple points in the architecture that are single points of failure. GIAC Enterprises should consider implementing redundancy at these points in the architecture.
2) GIAC Enterprises should consider using digital certificates.
3) GIAC Enterprises should require password protecting screen savers for all employees when they are not at their desk to further prevent unauthorized access. Additionally, the screen savers should be automatically activated after a reasonable time period of inactivity, such as five minutes.
4) Continual audits and risk assessments of the environment should be conducted every four to six months. These activities should be done by employees as well as outside consultants to ensure the systems are as secure as possible.
5) Security should be a continual process. There should be a security awareness program implemented, and security should be a part of everyone's daily job.

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

Design Under Fire

Requirements

The purpose of this exercise is to help you think about threats to your network and therefore develop a more robust design. Keep in mind that the next certification group will be attacking your architecture!

Select a network design from any previously posted GCFW practical (http://www.sans.org/giactc/gcfw.htm) and paste the graphic into your submission. Be certain to list the URL of the practical you are using. Design the following three attacks against the architecture:

1. An attack against the firewall itself. Research vulnerabilities that have been found for the type of firewall chosen for the design. Choose an attack and explain the results of running that attack against the firewall.

2. A denial of service attack. Subject the design to a theoretical attack from 50 compromised cable modem/DSL systems using TCP SYN, UDP, or ICMP floods. Describe the countermeasures that can be put into place to mitigate the attack that you chose.

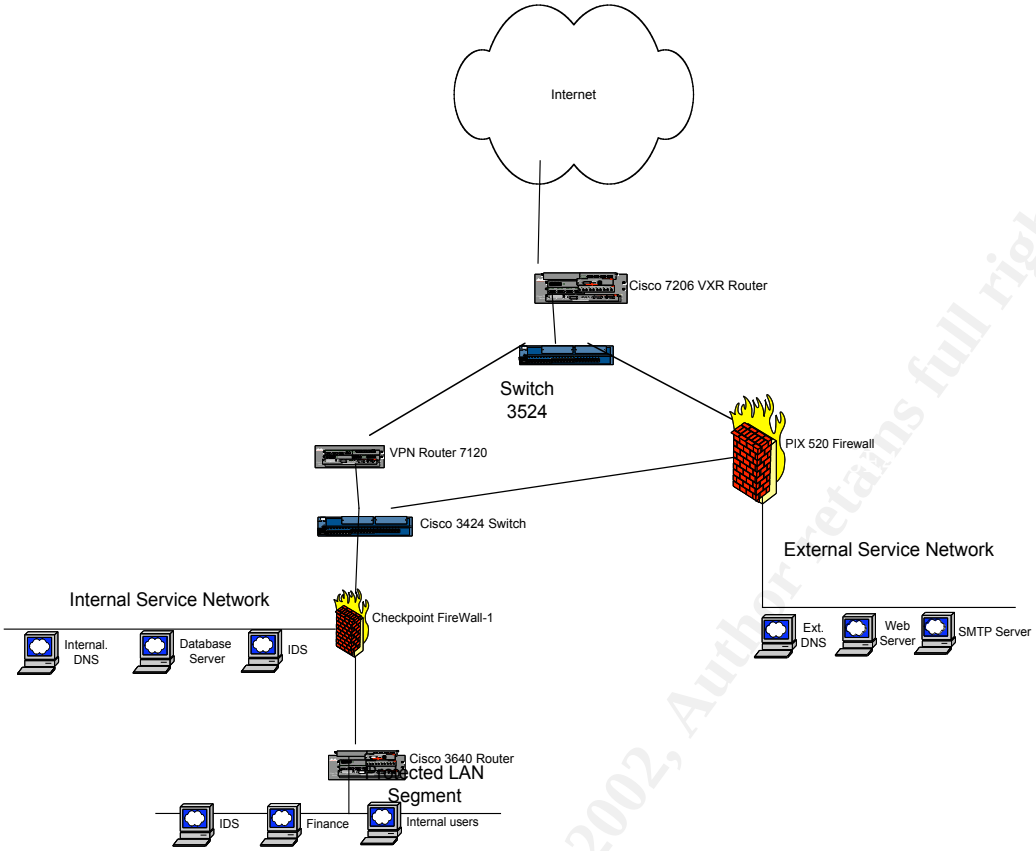
3. An attack plan to compromise an internal system through the perimeter system. Select a target, explain your reasons for choosing that target, and describe the process to compromise the target.

Note: this is the second time this assignment has been used. The first time, a number of students came up with magical "hand-waving" attacks. You must supply documentation (preferably a URL) for any vulnerability you use in your attack, and the exploit code that you use to accomplish the attack. The purpose of this exercise is for the student to clearly demonstrate they understand that firewall and perimeter systems are not magic "silver bullets" immune to all attacks.

Firewall Vulnerabilities

I have chosen to review Daniel Bachrach's architecture. First, let me congratulate Daniel on implementing defense in depth by utilizing multiple technologies within his environment. One of the reasons I have chosen his architecture is because he has implemented a Cisco Pix 520, Version 5.1(1). I have also implemented a Cisco PIX in my architecture and I would like to understand the specific vulnerabilities. Daniel's paper can be located at www.sans.org/giactc/gcfw/Daniel_Bachrach_GCFW.doc. The diagram of his architecture is attached below.

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



During my research for Cisco PIX vulnerabilities, I discovered the following vulnerabilities and attacks. I have chosen to outline the TCP Reset vulnerability and the FTP vulnerabilities.

1) TCP Reset vulnerability
This vulnerability stems from the fact that the Cisco PIX firewall cannot distinguish between a forged TCP Reset packet and a genuine TCP Reset packet. An attack can terminate a current connection if the connection can be uniquely determined. The reset packet is evaluated based on data contained in the TCP packet header, including source IP, source port, destination IP and destination port. It these values match the values stored in the stateful inspection table, the connection will be reset. This vulnerability is identified by Cisco as Cisco bug ID CSCdr11711. More information about this vulnerability can be found at http://www.cisco.com/warp/public/707/pixtcpreset-pub.shtml. To address this vulnerability, an upgrade to version 5.1(2) should be completed.

2) FTP Vulnerabilities
There are two FTP vulnerabilities that were identified on June 27, 2001. The first vulnerability documented as Cisco Bug ID CSCdp86352, allows a separate connection to be opened through the firewall. This is accomplished when a firewall receives an error message sent by an internal FTP server that contains an encapsulated comment. The firewall may interpret this command as a distinct command. The second vulnerability documented as Cisco Bug ID CSCdr09226, also allows a separate connection to be opened through the firewall. This is accomplished when the firewall interprets a client browsing from inside the firewall to an external server selecting a link,

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

as two or more FTP commands. The regular FTP session, which is expected, is started and at the same time an unexpected connection is created. More information about these vulnerabilities can be found at http://www.cisco.com/warp/public/707/pixftp-pub.shtml. To address the second vulnerability, which affects Daniel's architecture, an upgrade to version 5.1(2) should be completed.

Denial of Service attack

The first item I would like to point out about Daniel Bachrach's architecture is that his border router is configured with the "no ip directed-broadcast". This is an important step to ensure that his site is not utilized as an amplification site for distributed denial of service attacks against other sites.

To address an attack against Daniel's architecture, I will conduct a bandwidth consumption attack. A bandwidth consumption attack results from the attacker being able to flood the bandwidth in a network which in turn will cause a denial of service attack. This attack can be amplified by multiple sites conducting this attack at the same time. In this instance, the ICMP protocol could be utilized to conduct a bandwidth consumption attack. An attack that fits this profile would be the Smurf attack. A Smurf attack involves using machines from multiple sites. By utilizing the 50 compromised cable modem/DSL systems mentioned above to send packets to amplifying networks, the attacker will be able to overload the connection to GIAC's network. The attacker will send a spoofed ICMP ECHO packet to the amplifying networks that will respond to the spoofed packet. The spoofed packet will contain the IP address of the victim's machine. Since the ICMP ECHO packet will be sent to the broadcast address, each machine on that network will reply to the spoofed address of the victim's machine. Although the size of the pipe entering Daniel's architecture was not defined, it is highly unlikely that such an attack could be avoided. More information about Smurf attacks can be found at http://www.cert.org/advisories/CA-1998-01.html.

The first step in being sure you cannot be utilized as an amplification network is to apply the "no ip directed-broadcast" command on Cisco routers. This will ensure that you are not utilized to attack other networks.

On Solaris systems, the "ndd –set /dev/ip ip_respond_to_echo_broadcast 0" line can be added to /etc/rc2.d/S69inet to discard the broadcast packets.

For Linux systems, the commands "ipfwadm –I –a deny –P icmp –D X.Y.Z.0 –S 0/0 0 8" and "ipfwadm –I –a deny –P icmp –D X.Y.Z.255 –S 0/0 0 8" can be utilized to ignore broadcast ECHO requests. Kernel firewalling must be enabled to complete this process.

A countermeasure that could be utilized on the Cisco routers would be to enable the committed access rate (CAR) functionality on the Cisco router. This will allow ICMP traffic to a reasonable number of packets.

Attack plan

The system I will be outlining an attack against is for the web server. This is a focal point for GIAC Enterprises and the server the customers and GIAC Enterprise use to transact sales. It is foundational for the e-commerce business they conduct. If the web server is compromised, it is the first step in gaining access to the database server which contains some of the most valuable company assets. Many times company web servers are not as protected, since they run on a port, such as 80, which are allowed through the firewall in order to conduct business over the Internet. Below are some steps that can be taken to compromise the web server.

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

1) A vulnerability scanner such as whisker can be utilized to identify weaknesses in the web server. If vulnerabilities are identified, these vulnerabilities can then be exploited. Additionally, many scripts have been written that can identify or exploit vulnerabilities in a web server. These scripts can be utilized to attempt to gain access to the server.

2) A review of the website source code can also be conducted. Items such as comments, vulnerabilities in the code, and design issues can assist in identifying vulnerabilities that can be exploited.

3) Since the HTTP protocol does not maintain state, administrators may have their application maintain state through the use of such items as URL session tracking, hidden form elements and/or cookies in order to conduct e-commerce transactions. Each of these items can be modified. If an attacker can modify the values to match those of another session, they will, in effect, become the user of the other session. This session can be utilized to obtain valuable information about the machine. To defend web applications from these kind of attacks, sensitive data in URLs, cookies or hidden form elements should obtain a timestamp within the variables, digitally sign or hash the state information, encrypt the information in the cookie or hidden variable and/or make sure the session Ids are long enough to prevent accidental collision.

It may take some time to exploit web vulnerabilities, as well as requiring a level of knowledge about CGI, Javascript and/or Perl. However, with some diligence, an attacker could be able to identify and exploit a web server vulnerability.

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

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

Bibliography

Bilby, Darren. "SANS GIAC Level 2: GCFW – Firewalls, Perimeter Protection, and VPNs Practical Assignment". Available at http://www.sans.org/y2k/practical/Darren_Bilby_GCFW.doc.

Brenton, Chris. "Mastering Network Security." Alameda, CA: Sybex Inc., 1999.

Brenton, Chris, Lance Spitzner, and Stephen Northcutt. "The SANS Institute: Track 2-Firewalls, Perimeter Protection, and Virtual Private Networks." Volumes 2.1-2.5. Presented at Lone Star Dallas II on 3 June 2001 by Chris Brenton.

Cole, Eric and Ed Skoudis. "Computer and Network Hacker Exploits – Part 8 Application Level Attacks." Available be taking the SANS GCIH course located at http://www.sans.org/giactc.htm.

Farnsworth, William. "What Do I Put in a Security Policy?". Available at http://secinf.net/info/policy/policy.htm. August 10, 2000.

Fyodor. "Nmap network security scanner man page" Available at http://www.insecure.org/nmap/nmap_manpage.html.

Kelly, Brian. "SANS GIAC Level 2: GCFW – Firewalls, Perimeter Protection, and VPNs Practical Assignment". Available at http://www.sans.org/y2k/practical/Brian_Kelly_GCFW.doc.

Martin, Daniel. "SANS GIAC Level 2: GCFW – Firewall, Perimeter Protection, and VPNs Practical Assignment". Available at http://www.sans.org/y2k/practical/Daniel_Martin_GCFW.doc.

Orebaugh, Angela. "SANS GIAC Level 2: GCFW – Firewalls, Perimeter Protection, and VPNs Practical Assignment". Available at http://www.sans.org/y2k/practical/Angela_Orebaugh_GCFW.zip.

Stevens, W. Richard. "TCP/IP Illustrated, Volume 1: The Protocols." Boston, MA: Addison-Wesley, 1994.

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