Global Information Assurance Certification Paper

Firewalls, Perimeter Protection, and VPN's
SANS GCFW Practical Assignment
SANS 2002, Orlando, FL
Version 1.7
September 10, 2002

By
Barry Dowell

Assignment 1 – Security Architecture (15 points)

Introduction

GIAC Enterprises is engaged in the buying and selling of fortune cookie sayings via the Internet. GIAC has a network of suppliers who write fortunes, and periodically upload them to the GIAC database. In turn, GIAC will review and approve these fortunes and make them available to their customers and to their worldwide network of partners. GIAC had been doing business "the old fashioned way", sending samples of their fortunes via snail mail and taking orders over the telephone. It took an army of workers to process the orders, print and ship the fortunes and keep up with the accounting paper trail. Now, GIAC's web site can instantly show samples of their fortunes to anyone in the world, take orders for bulk fortunes, bill customer accounts, and make the orders available for immediate download. This instant communication has freed many workers to become more productive in other facets of their jobs and has increased production and profit tenfold. With this increase in communication and web presence comes a new security threat to the integrity of GIAC's data and reputation. We must design a secure network that will serve GIAC's immediate needs, but will have plenty of room for future expansion, and will stay within a reasonable budget. We will assume that GIAC has a small IT department and a small administrative staff located in the home office. Most of GIAC's employees are in the sales department and will be traveling extensively. GIAC's reputation is their most valuable asset and this is most visible in the quality and integrity displayed in their fortune cookie sayings, which reside in the database. Therefore, the database will be our main security concern. All components of the network will utilize the most recent software versions and the patches will be updated as part of a weekly maintenance schedule.

User Access

Customers will be able to purchase and download fortune cookie sayings and view account activity, order status, and account balances via https over the Internet. They will be able to view samples of different styles, such as; ancient Chinese phrases, modern English fortunes, Old English style quotes, etc. They can choose to have random "lucky" numbers printed with the fortune. And, they will be able to choose which language in which to have the fortunes printed. They will be required to

set up a customer account, including a user id and password with their initial purchase. This will allow GIAC to more closely monitor customer activity.

Suppliers, after completing an application process and contract, will be able to ftp files containing fortune cookie sayings using Secure FTP (http://security.sdsc.edu/software/secureftp/) via an SSL connection, directly to a receive server that will be on the service network, isolated from the internal network. While there, the data is scanned for viruses and content, then made available to the DB Server, which will poll for new sayings and perform an ftp 'GET', to add them to the database. Suppliers will also be able to log in to the web server to retrieve their account information via https.

Partners will be able to download sayings from our database via ftp through a VPN tunnel. They will be able to view and select the styles and languages of fortunes, as well as track their own account information. The database will have read only access, to eliminate the possibility of an attacker uploading malicious code or manipulating data.

Employees on the internal network will have job specific access to the database and internal servers. They will have normal Internet access for web browsing via http/https, email, and ftp file transfers, but will not be able to use instant messaging because of the inherent security risks. All internal hosts will have Norton Anti-virus 2003 (http://www.symantecstore.com/dr/sat2/ec_MAIN.Entry17c?CID=42122&SID=27674&SP=10007&PN=5&PID=426823&DSP=&CUR=840&PGRP=0&CACHE_ID=42122) enabled along with automated live update of the virus definition tables.

Mobile sales force and telecommuters will have the same privileges as internal employees and will connect to the internal network using the secure VPN. Due to the nature of their travel environment and inherent risk of a stolen laptop, they will use an RSA SecureID (http://www.rsasecurity.com/) authenticator for single sign-on passwords and will be required to use a personal firewall for added protection of the extended border of the GIAC network.

All employees, partners, and suppliers will be required to review and agree to the GIAC Network Usage Guidelines and Security Procedures, which outlines the rules for using the network and is intended to make all users aware of security threats to the network and their responsibilities in keeping it as secure as possible.

Network Architecture

The network design for GIAC Enterprises, shown in figure 1, consists of a service network and an internal network, separated from each other by a firewall, and further protected from the Internet by a border router. Customers, suppliers, and partners will interact exclusively with the service network, which will have tightly controlled access to the necessary resources on the internal network.

- The service network contains the network components that will be available to the Internet, including the Web server, external DNS/Mail server, and Receive server. The primary firewall and border router will filter traffic to and from this network.

- The internal network consists of a protected Database server, Log server, internal DNS/Mail server and workstations. The database is protected by a host-based firewall, and all servers will be limited to a select set of connections. The workstations allow employees to perform their jobs, including Internet access, database management, and network maintenance as required. And, this network is not accessible from outside of the border router.

Network Services

Web

The web server will be able to connect to the Internet and serve up content from the database server, including fortunes and account information. It will not be able to initiate connections to the Internet. Patches will be downloaded from an Administrator's box on the internal network.

DNS

A split DNS architecture will be employed. An external DNS will serve the World including the GIAC service network, and can be queried from any host on the Internet. The internal DNS will serve GIAC's internal servers and hosts and will be linked to the external DNS.

Mail

Mail will be split between an external mail relay accessible to the Internet and an internal mail server used by internal hosts. The external relay will perform virus scanning and forward mail to and from the internal hosts.

Syslog

Syslog will be sent from all hosts and network devices to a single secured Log server, located on the internal network.

User Authentication

Users will be authenticated by Sun One Directory Server 5.1, (formerly iPlanet) which will verify user ids, passwords, and permissions.

Note: All IP addresses relating to the actual network that this practical was based on have been changed to generic aaa.bbb.ccc. notations.

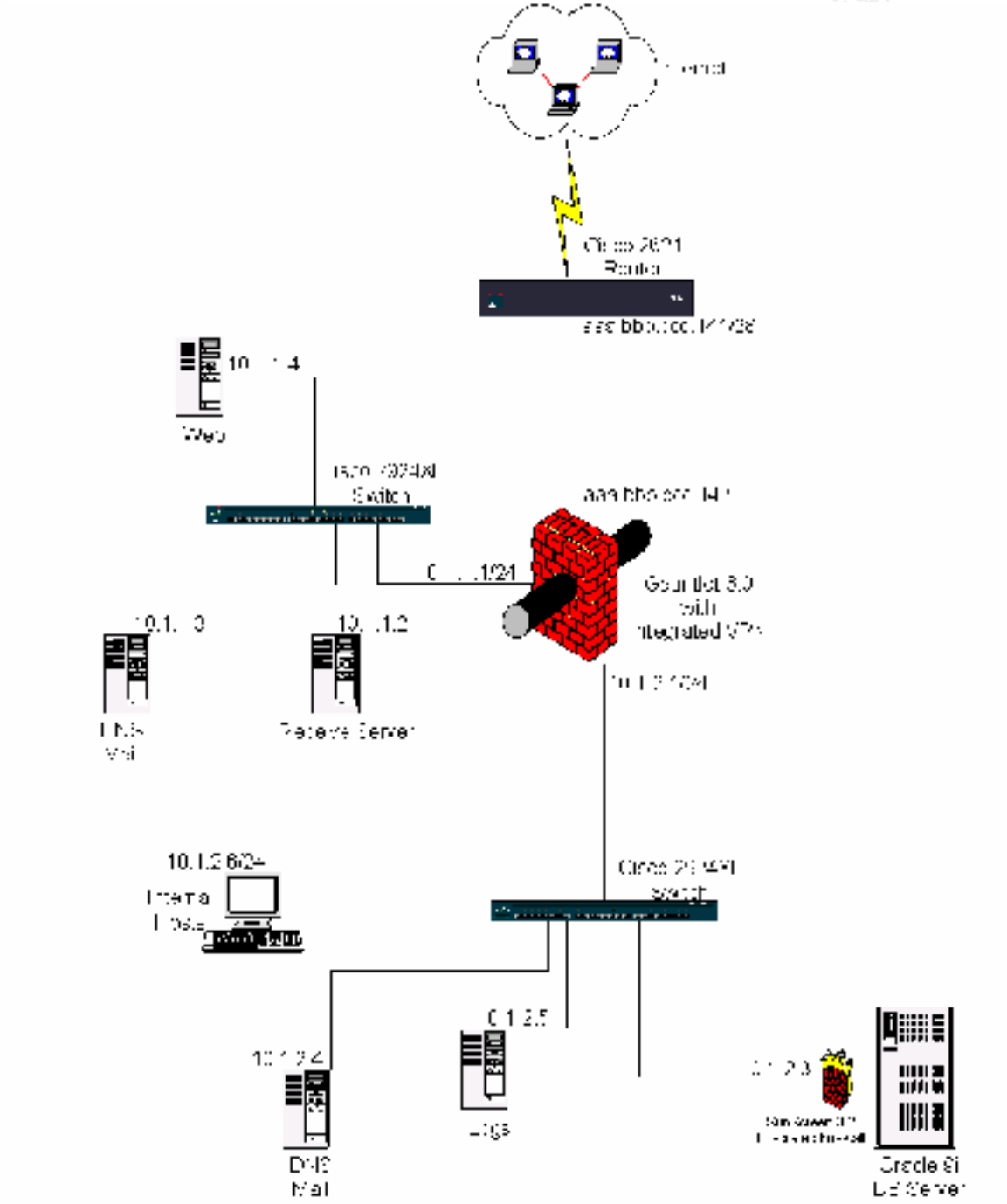

Figure 1. Network Architecture

Network Components

Border Router

The border router is a Cisco 2621, running Cisco IOS 12.2. It was chosen because of the familiarity that the security team has with it, and the reputation for reliability and support that Cisco has. This model was selected because it meets the current needs of GIAC Enterprises and has a relatively low cost. If more interfaces are needed in the future, adding a 4-port Ethernet card can expand this router.

Primary Firewall

The primary firewall will be a Secure Computing Gauntlet Firewall version 6.0 (http://www.pgp.com), running on a Sun Microsystems SunFire 280R. The 280R will have 2 X Ultrasparc II 450mhz processors, 1GB RAM, 2 X 17GB SCSI disks, and a QuadEthernet card. The OS is 64-bit Solaris 8 2/02, (Solaris 9 is not compatible with Gauntlet 6.0). Gauntlet was chosen because of the familiarity that the security team has with it, and its' excellent reputation. Gauntlet is a software based firewall that will allow us to use as much initial horsepower as deemed necessary by performance requirements and budget constraints, yet it will be easily upgradeable to meet future needs without having to buy a new box. It also has a high availability configuration option to handle failover to a backup system if needed.

VPN

We will be using Secure Computing Gauntlet 6.0 VPN (http://www.pgp.com). This VPN is integrated with the Gauntlet Firewall 6.0, insuring a seamless interface and ease of management. And, Gauntlet VPN can secure remote communications with no added cost.

Web Server

The web server will be running Apache version 2.0.39 (http://www.apache.org/) and will be located on the service network. Its IP address will be NATed by the firewall to hide it from the untrusted network. This will offer a small measure of added protection against script kiddies and other attackers looking for an easy target.

Receive Server

The receive server will be an ftp server configured to receive and verify the contents of files sent from GIAC's suppliers. After the files have been scanned and authenticated, they are made available to the DB Server, which will poll for and then download the new fortune cookie sayings.

External DNS/Mail Server

The external DNS server and mail relay will share the same box, to conserve space and available funds. The DNS server will run the latest version of BIND (http://www.isc.org), currently version 9.2.1. We will edit the /etc/named.conf file to hide the BIND version by changing the banner. This is done by opening named.conf with a text editor such as vi. Then search for "BIND". Now, edit the banner to give false information. You may change the listed BIND version to waste an attacker's time trying exploits that never affected your version of BIND, or you may change the banner to something completely off the wall, like, "All Your Base". Either way, a would be attacker will at least be temporarily sent down the wrong trail. The Mail server will employ the latest version of Sendmail (http://www.sendmail.org), currently 8.12.5.

Database Server

The Database will be Oracle 9i, running on a Sun Enterprise 250 with Solaris 9 OS. It will be further isolated from the rest of the network by SunScreen 3.2 integrated firewall, (included with Solaris 9 at no charge) configured to accept ftp data only from the receive server, in response to automated polling. We will also use Tripwire integrity checker (http://tripwire.org/) on this server to ensure data integrity.

Internal DNS/Mail Server

The internal DNS/Mail server will be configured similarly to the external DNS/Mail server, with the latest version of BIND and it will include the private address of the Web server, for use by internal hosts. The internal mail server will also use the latest version of Sendmail, and will route all messages to the external mail server on the service network.

Assignment 2 – Security Policy and Tutorial (35 points)

Security Policies

Border Router

ACLs act on the first match, starting with the first rule and moving down through the list. When a match is found, the packet is dropped or forwarded according to the rule, then the next packet is analyzed, etc. The order of the rules can be changed, but the rules in which more matches occur should be moved up in the list. This will cause more packets to be acted upon before traversing the entire ACL and will enhance performance. We will start our inbound ACL by denying certain source IP addresses and protocols. After these have been blocked, we will then have a single permit statement that will allow traffic addressed to

GIAC to be forwarded to our network. Finally, we will have a deny statement that will deny all other traffic. This is a safety measure to ensure that all traffic that has made it this far through the ACL will be dropped. We will use the NSA's Secure Configuration Guide for Cisco Routers, to help defend against known vulnerabilities. (http://nsa2.www.conxion.com/cisco/guides/) Then, we will have an outbound filter, to deny any traffic not coming from our network. (i.e. spoofed packets) We will use Cisco's extended ACLs. Extended ACLs (those with a number from 100-199) allow more granular control of our filters than standard ACLs, which only filter on source address. Extended ACLs enable one to filter on source and destination address, protocol, and protocol-specific options.

Inbound Traffic

First we will block ICMP redirects and log any attempts. There is no reason to allow this traffic.

```
access-list 100 deny ICMP any any redirect log
```

We will not need SNMP on our network, so it will be denied and logged, to avoid its' recently discovered vulnerabilities. This also will disable RMON, remote monitoring, which uses SNMP. That's a good thing.

```
access-list 100 deny udp any any eq snmp log
access-list 100 deny udp any any eq snmptrap log
```

To stop "land" attacks on the router, those having the same source and destination addresses; we will add the following line.

```
access-list 100 deny ip host aaa.bbb.ccc.140 host
aaa.bbb.ccc.140 log
```

Now we want to deny any obviously spoofed packets coming from a private source address.

Internal network

```
access-list 100 deny aaa.bbb.ccc.0 0.0.0.127 any log
```

Local host

```
access-list 100 deny 127.0.0.0 0.255.255.255 any log
```

Documentation/test network

```
access-list 100 deny 192.0.2.0 0.0.0.255 any log
```

Reserved private addresses

```
access-list 100 deny 10.0.0.0 0.255.255.255 any log
access-list 100 deny 0.0.0.0 0.255.255.255 any log
access-list 100 deny 192.168.0.0 0.0.255.255 any log
```

```
access-list 100 deny 172.16.0.0 0.15.255.255 any log
access-list 100 deny 255.255.255.255 any log
```

Now, we will permit the traffic that is addressed to GIAC's network.
```
access-list 100 permit ip any aaa.bbb.ccc.0 0.0.0.127
```

Finally, we will deny all other packets that are not addressed to GIAC.
```
access-list 100 deny any any log
```

And, apply this ACL to our external interface from the "config-if" prompt.
```
interface eth0/0
ip address aaa.bbb.ccc.140 255.255.255.240
ip access-group 100 in
```

Outbound traffic
Only allow outbound traffic from GIAC's address space. This is to prevent spoofing by anyone within our network. (i.e. good neighbor policy)
```
access-list 101 permit ip aaa.bbb.ccc.0 0.0.0.127 any log
access-list 101 deny ip any any log
```

And, apply this ACL to our internal interface from the "config-if" prompt.
```
Interface eth0/1
ip address aaa.bbb.ccc.141 255.255.255.240
ip access-group 101 in
```

Firewall
Gauntlet Firewall 6.0 is administered by a GUI. Sources and destinations can be entered as IP addresses, network names or host names. We will configure the firewall to only forward necessary traffic, described in section 1. All other traffic will be logged and dropped. After Gauntlet has been properly installed according to the tutorial located at the end of this section, setting up the firewall rules is a simple matter of selecting source, destination, protocols, and actions from the drop down menus in the GUI. The following section describes traffic control requirements for the firewall.

From the Internet
- Allow HTTP and HTTPS to the Web Server
- Allow ftp to the Receive Server
- Allow SMTP and DNS to the external DNS/Mail Server
- Allow VPN traffic from GIAC partners and mobile employees

From the Web Server
- Allow HTTP, HTTPS, and ftp to the Internet
- Allow DNS to the external DNS server
- Allow Syslog to the Log Server

From the Receive Server

- Allow ftp to the Database Server
- Allow Syslog to the Log Server

From the external DNS/Mail Server

- Allow DNS and SMTP to the Internet
- Allow DNS and SMTP to the internal DNS/Mail Server
- Allow Syslog to the Log Server

From the internal hosts

- Allow HTTP, HTTPS, and ftp to the Internet
- Allow HTTP to the Web Server

From the internal DNS/Mail Server

- Allow DNS and SMTP to the external DNS/Mail Server

From the Database Server

- Allow ftp to the VPN
- Allow ftp to the Internet

From the Log Server

- Deny everything

Gauntlet denies all traffic by default, unless expressly permitted by the rules, but as an added measure of certainty, we will add a final rule to deny all traffic.

To start the Gauntlet GUI, from the command prompt, type <fwgui>.

1. Enter the hostname, administrator id and password used during the Gauntlet setup procedures.
2. Select <Rules> in the left frame. The Rules Table along with a list of default rules will appear in the right frame.
3. Delete all of the default rules by clicking on the rule to select it, then clicking **delete**.

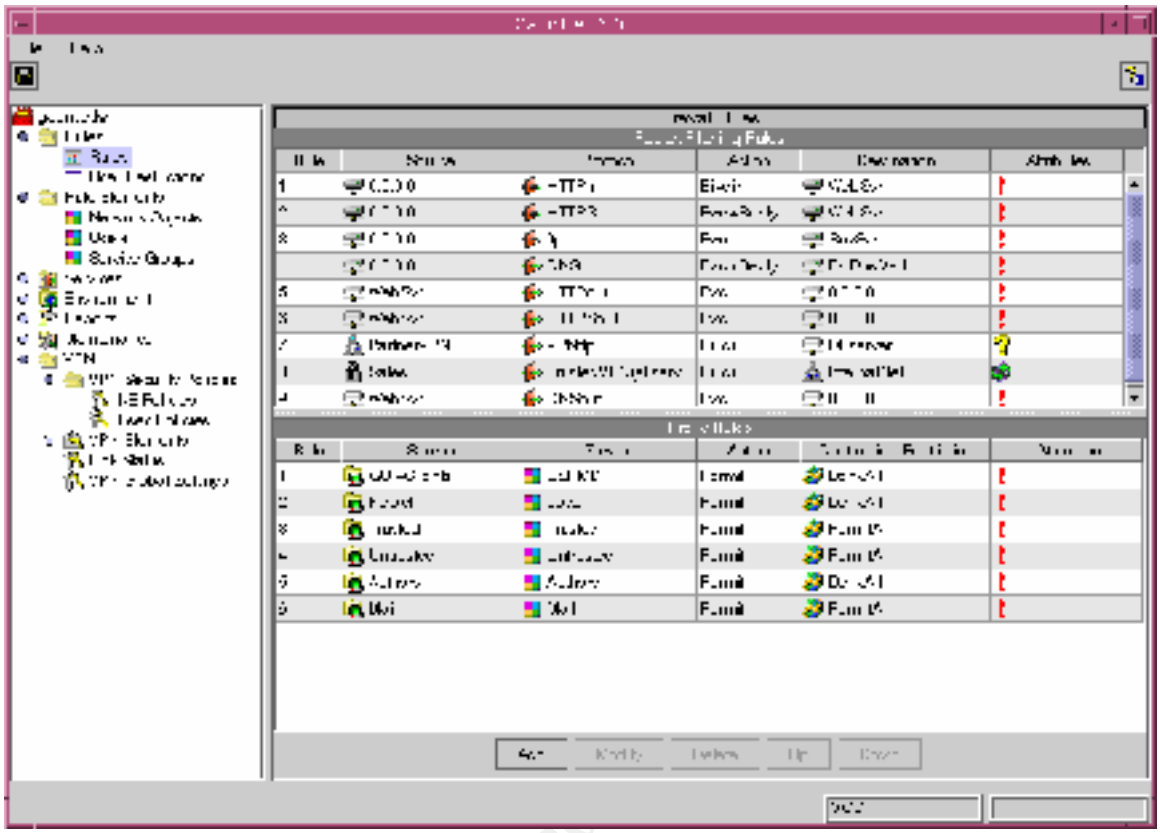

Figure 2. Gauntlet 6.0 Rules Table

Now we are ready to add the GIAC specific rules. The order of the rules is important. Like the router ACLs, the firewall rules are read top to bottom, and when a match is found, the packet is acted upon, and the next packet is brought into the filter. Rules should be rearranged by highlighting the rule and clicking the **Up** or **Down** button. Rules with the most matches should be moved near the top of the list. To save time, space, and an incredible amount of needless repetition, I will not repeat the rules definition process for each rule. Suffice it to say that the screens are very intuitive and each step reveals a drop down menu, which will include all of the necessary choices for each field. I will give the specifics for the first new rule, and then I will simply list each rule, along with the reasoning behind it. The tutorial at the end of this section will describe the necessary steps to setup Gauntlet Firewall 6.0 including the IP Addresses and Protocols referred to in the following rule add procedure.

The following rule is to allow HTTP traffic from the Internet to the GIAC Web Server.
From the Rules Table:

1. Click **Add**
2. Select **Packet Filter Rule**
3. Enter a *Rule Name* or leave it blank

4. Click **Next**

Enter the Source Information

5. Click **IP Address**
6. Select the name of the source from the drop down box. **0.0.0.0**
7. Click **Next**

Enter the protocol information

8. Select **HTTPin** from the drop down menu

This allows HTTP traffic from any high-order port to GIAC port 80

9. Click **Next**

Select the action to be performed on this traffic

10. Select **Bi-Dir**

This establishes a bi-directional HTTP connection between the GIAC Web Server and the source

11. Click **Next**

Enter the destination information

12. Click **IP Address**
13. Select the name of the destination from the drop down box. **WebSvr**
14. Click **Next**

Determine the desired Logging Level

15. Select **Alerts**

Save the new rule

16. Click **OK**

Continue adding rules in this manner, until all of the required traffic is being filtered properly. To save and apply the new rules, simply click on the diskette icon in the upper left hand corner.

Allow HTTPS from the Internet to the GIAC Web Server for secure web traffic.

Source	Protocol	Action	Destination	Logging
0.0.0.0	HTTPSin	Bi-Dir	WebSvr	Alerts

Allow FTP from the Internet to the Receive Server, so suppliers can upload their fortunes to GIAC.

Source	Protocol	Action	Destination	Logging
0.0.0.0	ftp	Fwd	RcvSvr	Alerts

Allow SMTP to the External GIAC Mail Server, for the delivery of email.

Source	Protocol	Action	Destination	Logging
0.0.0.0	SMTP	Fwd	ExtDnsMail	Alerts

Allow DNS to the External GIAC DNS Server, for name resolution.

Source	Protocol	Action	Destination	Logging
0.0.0.0	DNS	Fwd	ExtDnsMail	Alerts

Allow HTTP, HTTPS, and ftp from the Web Server to the Internet, for employees to browse and use the Internet.

Source	Protocol	Action	Destination	Logging
WebSvr	HTTPin	Fwd Reply	0.0.0.0	Alerts
WebSvr	HTTPSin	Fwd Reply	0.0.0.0	Alerts
WebSvr	ftp	Fwd Reply	0.0.0.0	Alerts

Allow DNS from the external DNS server to the internal DNS server to resolve names on the internal network.

Source	Protocol	Action	Destination	Logging
ExtDnsMail	DNS	FwdReply	IntDnsMail	Alerts

Allow Syslog to pass from the service network to the log server, for consolidated logs.

Source	Protocol	Action	Destination	Logging
ServiceGroup	Syslog	Fwd	LogSvr	Alerts

Allow the Database server to ftp new fortunes from the Receive server.

Source	Protocol	Action	Destination	Logging
DBserver	ftp	FwdReply	RcvSvr	Alerts

Allow DNS from the external DNS sever to the Internet for name resolution.

Source	Protocol	Action	Destination	Logging
ExtDnsMail	DNS	FwdReply	0.0.0.0	Alerts

Allow SMTP from the external mail relay to the Internet for email.

Source	Protocol	Action	Destination	Logging
ExtDnsMail	SMTP	Fwd	0.0.0.0	Alerts

Allow HTTP, HTTPS, and ftp for internal hosts connecting to the Internet and to the GIAC Web Server.

Source	Protocol	Action	Destination	Logging
InternalHosts	HTTPin	Fwd Reply	0.0.0.0	Alerts
InternalHosts	HTTPSin	Fwd Reply	0.0.0.0	Alerts
InternalHosts	ftp	Fwd Reply	0.0.0.0	Alerts
InternalHosts	HTTPin	Fwd Reply	WebSvr	Alerts
InternalHosts	HTTPSin	Fwd Reply	WebSvr	Alerts
InternalHosts	ftp	Fwd Reply	WebSvr	Alerts

Allow DNS from the internal DNS server to the external DNS server, for name resolution.

Source	Protocol	Action	Destination	Logging
IntDnsMail	DNS	FwdReply	ExtDnsMail	Alerts

Allow SMTP from the internal mail server to the external mail relay, for email delivery.

Source	Protocol	Action	Destination	Logging
IntDnsMail	SMTP	FwdReply	ExtDnsMail	Alerts

Finally, deny all other traffic through the firewall.

Source	Protocol	Action	Destination	Logging
Any	All	Deny	Any	Alerts

Secondary Firewall

For the purposes of this practical, detailed description of the secondary firewall is not required. Suffice it to say that SunScreen 3.2 has a "pretty GUI" (thanks, Chris Brenton) and it will be configured to proxy ftp traffic out to authorized customers and partners via the VPN, and will receive requested ftp from the Receive server on the service network.

VPN

Gauntlet VPN is configured using the same GUI as the firewall. The partner VPN will be setup as a VPN Network and the employee VPN will use VPN clients. The difference being static IP addresses for VPN networks and dynamic IP addresses used for mobile employee connections. We will use certificates for authentication. Shared secrets would be easier to use for the VPN networks, but are much less secure, and they cannot be used for the VPN clients.

IKE Policy

GIAC's IKE policy will use SHA-1 Hash Algorithm, Triple DES encryption, and 1536-bit Diffie Hellman crypto algorithm (recommended for Triple DES). The destination lifetime will be 480 minutes, to verify that the destination is valid every 8 hours.

IPsec Policy

GIAC's IPsec policy will use HMAC-SHA-1 Hash Algorithm and Triple DES encryption.

To give GIAC's partners ftp access to the database, we will add the following rule to our firewall rules.

Source	Protocol	Action	Destination	Logging
PartnerVPN	VPNftp	FwdReply	DBserver	Alerts

To give GIAC mobile employees the same accesses that home office employees have, we will add the following rule to our firewall rules.

Source	Protocol	Action	Destination	Logging
Sales	TrustedVPN(all services)	Bi-Dir	InternalNet	All

Gauntlet Firewall 6.0 Configuration Tutorial

Minimum system requirements for Gauntlet 6.0 with Solaris 8 are: any Ultra-based or Enterprise machine, 512MB of memory for the 64-bit installation, 4GB of disk, a quad Ethernet card, and a CD-ROM drive. The latest patches must be applied, and if you are planning to harden the firewall box with YASSP(http://www.yassp.org/), it must be done before Gauntlet is installed. Before you begin the installation into a production system, you should warn the users of a possible disruption of service. Mail and connections outside the firewall may be temporarily blocked. The firewall is installed following the instructions in the **Getting Started Guide,** supplied with the Gauntlet Firewall software. We have installed it as a standalone firewall using three of the five available interfaces.

Configure Interfaces

We begin the configuration by defining our interfaces as follows:
From the Gauntlet Firewall Manager (see figure 3), open **Environment->Interfaces.** Select and interface name from the drop-down list and proceed with the following choices:

- Interface name: **hme0**
  IP address: **aaa.bbb.ccc.143**
  Network mask: **255.255.255.240**
  Broadcast address: **aaa.bbb.ccc.143**
  Interface type: **outside**
  • Enable NAT
  • Enable Illegal NAT

- Interface name: **qfe0**
  IP address: **10.1.1.0**
  Network mask: **255.255.255.0**
  Broadcast address: **10.1.1.255**
  Interface type: **service**
  Ö Enable NAT
  • Enable Illegal NAT

- Interface name: **qfe1**
  IP address: **10.1.2.0**
  Network mask: **255.255.255.0**
  Broadcast address: **10.1.2.255**
  Interface type: **inside**
  Ö Enable NAT
  • Enable Illegal NAT

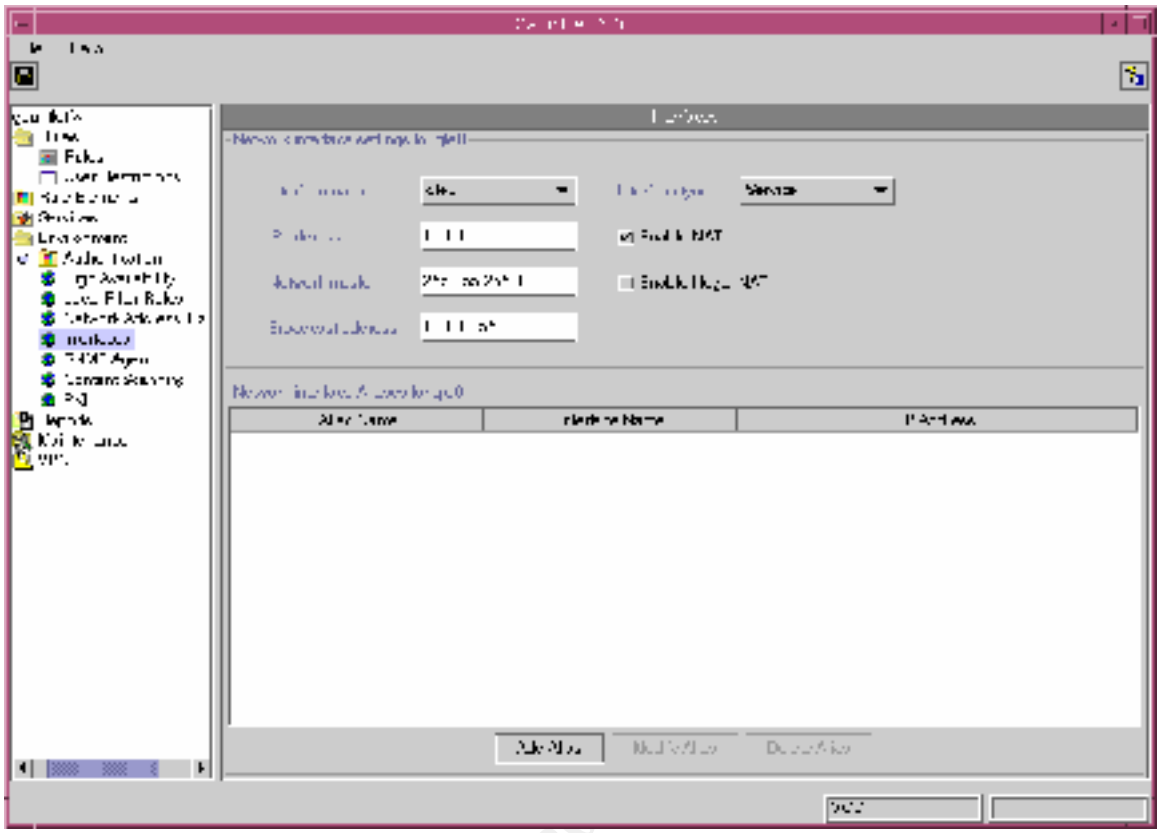

Figure 3. Gauntlet Interface Configuration

Create Network Objects

We must create network objects to be used in the rules defined in our ACLs. These network objects can be an IP address, an IP network, a group, or a host. To give GIAC the fine-grained control that is necessary to secure the network, we will create a network object for each of our hosts, networks and VPNs. The following is an example of how to create the network object that will represent our Web Server. From the Gauntlet Firewall Manager, open **Rule Elements->Network Objects.** (see figure 4) Click **Add** and select **IP address** from the drop-down menu. Fill in the blanks as follow:

Name: **WebSvr**

Description: **Web Server**

IP address: **10.1.1.2**

Click **OK** to save the information. Continue creating network objects in this manner, until all sources and destinations for GIAC's rules have been created.

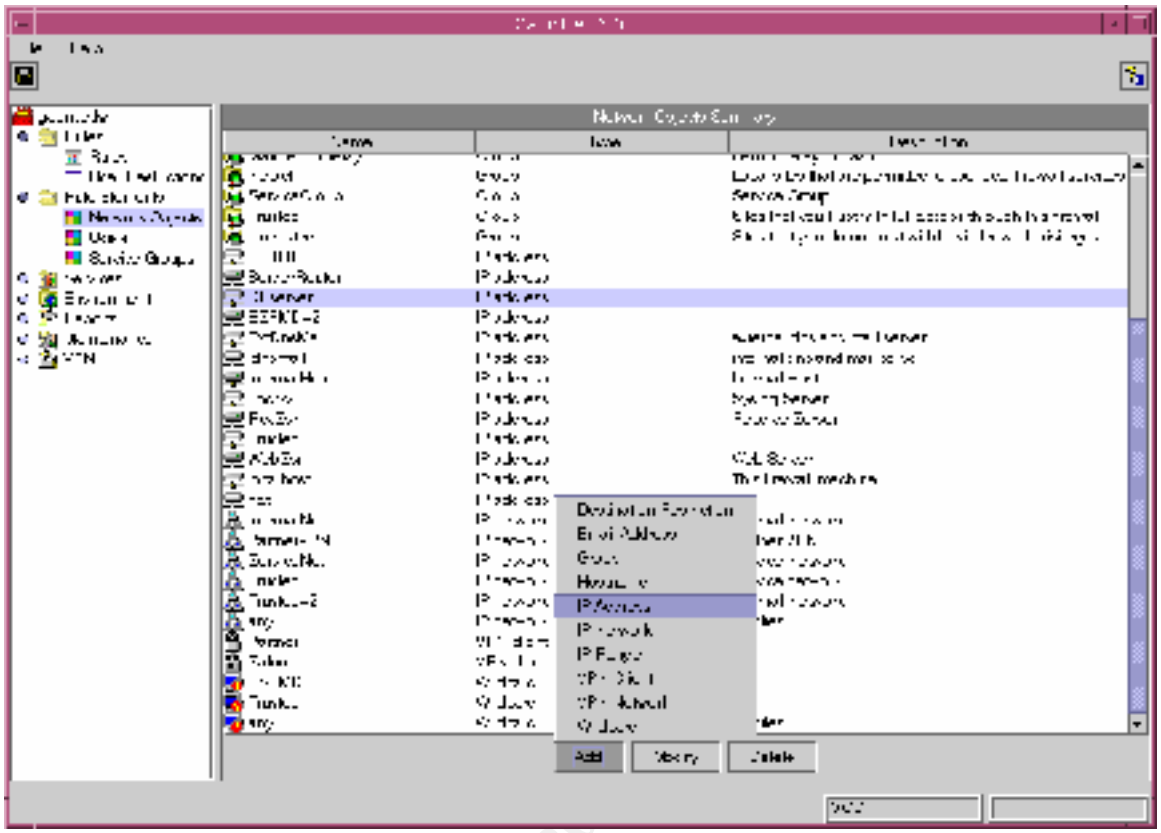

Figure 4. Gauntlet Network Object Configuration

Create Rules Table

The rules table will be constructed using the method described in the firewall ACL area at the beginning of this section. However, I will give details as to how the specific services or protocols can be defined for our rules. When entering the protocol information, we will select **Add**, and enter the information for our desired protocol. The following example is for **HTTPout**. This is the HTTP traffic that will be allowed out of our Web Server to the Internet. (see figure 5)

Name: **HTTPout**

Interface: **qfe0**

The source port is **UDP port 80** and the destination port range is **1024 to 65535.** Enter the necessary information and click **OK** to save. Each time a rule is created, you will have the option of using an existing protocol or creating a new one. Continue to create all necessary protocols as the rules are defined.

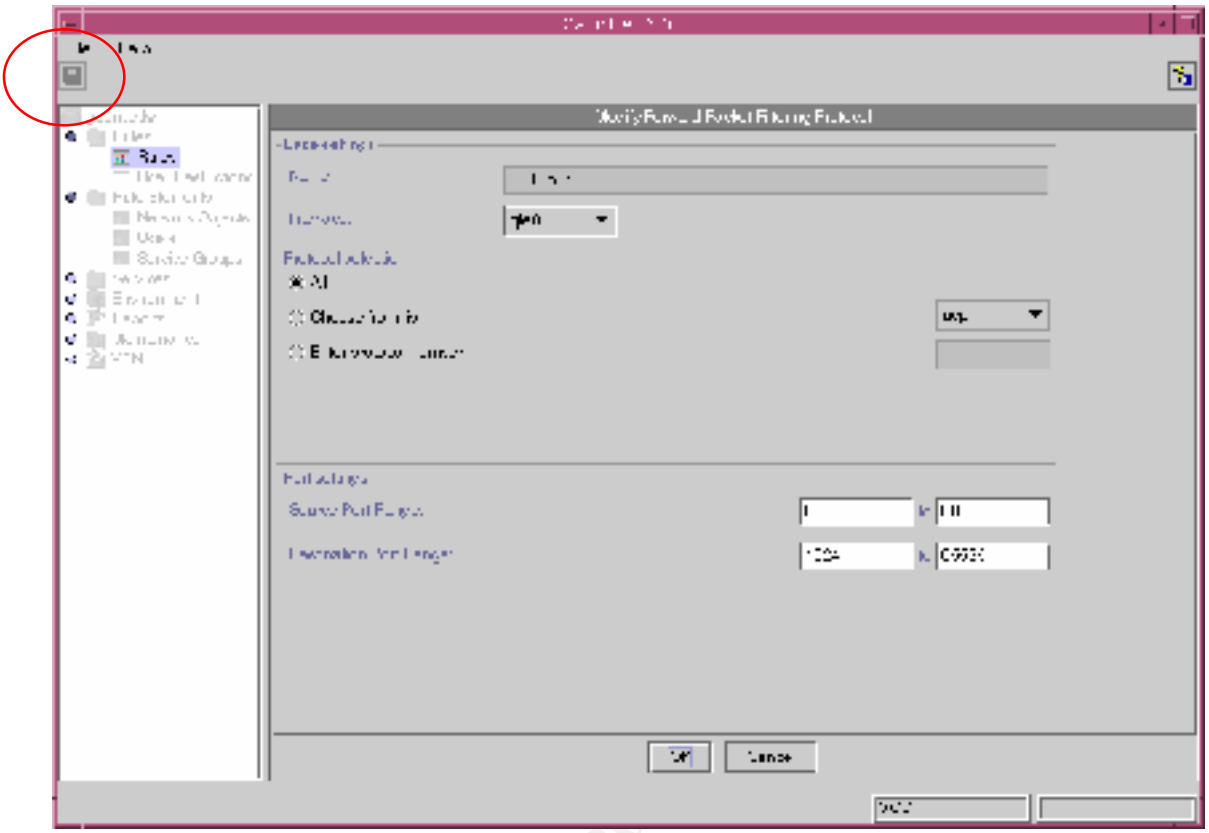

Figure 5. Gauntlet Protocol Definition

Save and apply the changes to the firewall by clicking the diskette icon, in the upper left corner.

NAT

We want to hide the internal private addresses of our networks from the outside world, so we will be using Network Address Translation. NAT will map an internal address to a legal address that is external to our network; therefore, attackers will have a harder time determining the internal address scheme of our network. To begin the NAT configuration from the Gauntlet Firewall Manager, select **Environment->Network Address Translation**. Click **Add** and select **NAT Rule** from the menu, then make the following selections:

Type: **Dynamic**
Local Addresses: **Any**
Global Addresses: **Any**
Interface: **qfe0**

Repeat the above steps for **qfe1**.

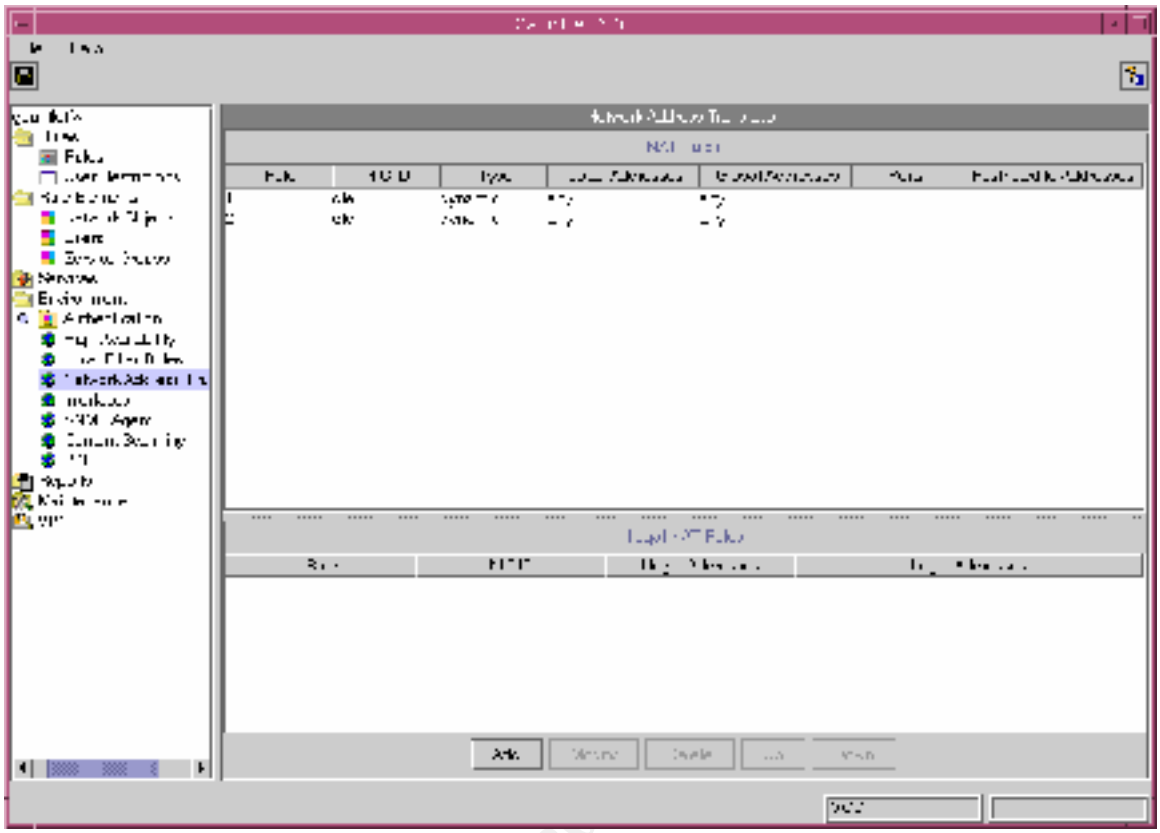

Figure 6. Gauntlet NAT Rules

Save and apply the rules, and Gauntlet Firewall 6.0 is ready for some simple testing.

Ping test

To make sure that all of your hosts and interfaces can 'talk' to each other, we will temporarily add a rule to permit **ICMP** from any source to any destination. Once the rule has been saved and applied, we will attempt to ping through the firewall from all interfaces to all other interfaces. Then we will take a random sample of pings from several hosts on each interface to several hosts on the other interfaces. The router is configured to drop ICMP, so we will not be able to ping the router. After this is successfully completed, we will remove the new ICMP rule and save.

Assignment 3 – Verify the Firewall Policy (25 points)

Although Gauntlet Firewall defaults to drop all traffic, and we have added rules to only allow desired packets to pass through the firewall, it is always necessary to fully test a new firewall installation to verify the ACLs that we have in place are functioning as expected.

The Plan

This is an audit of the firewall only. We will not be conducting a much needed vulnerability assessment of our entire network. We will choose a time when the network is least likely to be busy, such as a weekend in the middle of a fiscal quarter. Before continuing we will obtain written approval from Management. Most of the testing should be completely harmless, but if something does fail, such as a server crash, etc., we want to make sure that the fewest number of users will be affected. We will warn the users that the system will be temporarily unavailable for a 48-hour period. We will use a laptop loaded with Nessus to scan for open ports and look for vulnerabilities in Gauntlet and Solaris. At the same time, we will verify the ability of desired traffic to flow to its' intended destination. The laptop will be connected to each of our firewall's interfaces and will scan all ports from each of the different servers' IP addresses.

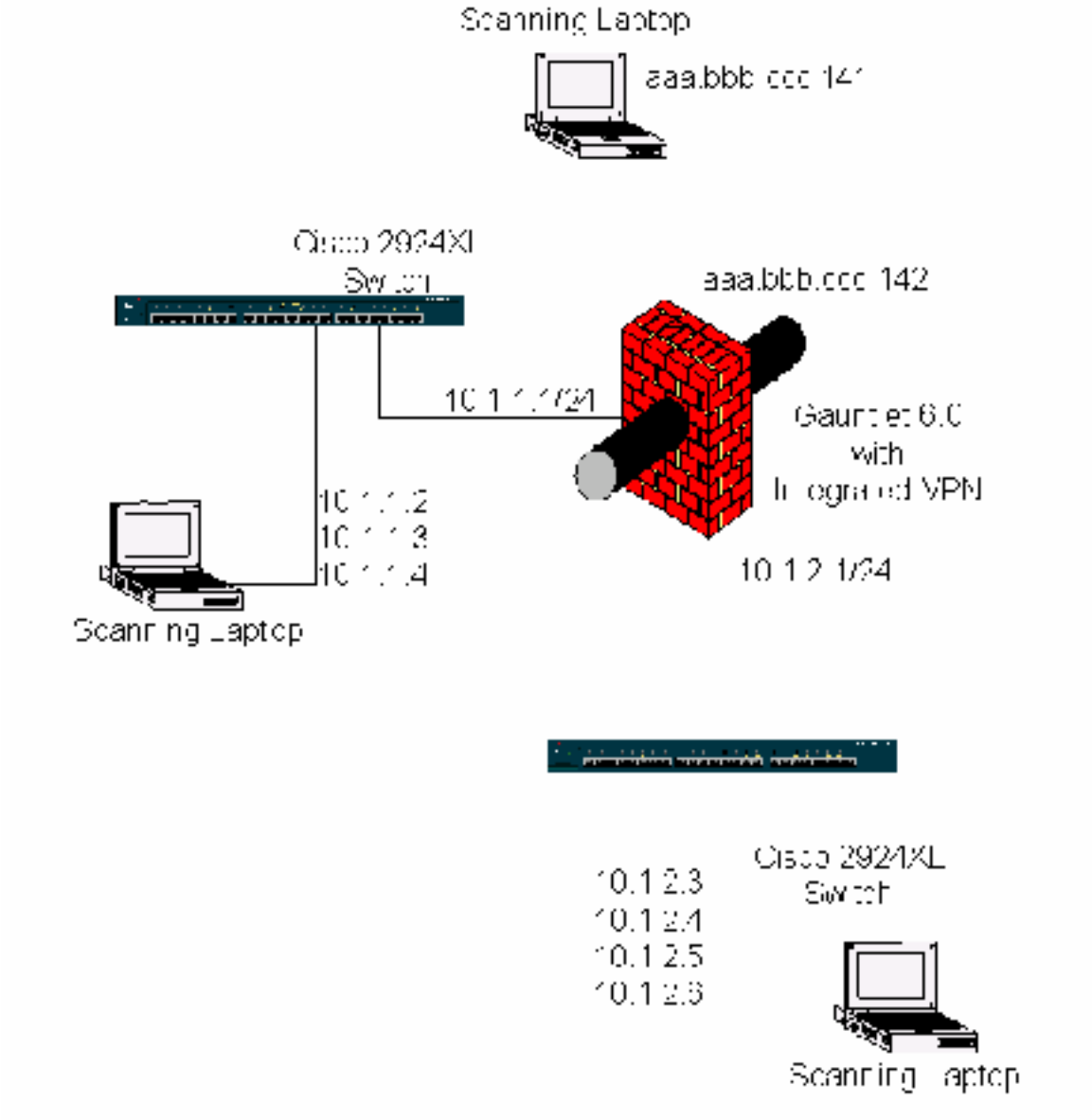

Figure 7. Scan and Audit Network Diagram

Finally, we will analyze our findings and prepare a report replete with suggestions for improving the firewall security and performance. See table 1 for a breakdown of our cost estimate.

Table 1. Estimated Cost

Plan the Audit	8 hours	$800
Port Scans	4 hours X 3 interfaces	$1200
Vulnerability Scans	8 hours	$800
Analysis and Reports	8 hours	$800
Total	**36 hours**	**$3600**

The Audit

We begin by checking CERT advisories for know vulnerabilities Solaris 8 and Gauntlet Firewall and VPN 6.0. The following advisories were found at www.cert.org. These warnings referring to Solaris are for earlier versions of Solaris and BIND, so GIAC is not affected by these.

```
CERT Advisory CA-2001-02 describes four vulnerabilities in
certain versions of BIND.  The four vulnerabilities are
listed below along with the affected versions of Solaris
and the version of BIND shipped with each version of
Solaris.

VU#196945 - ISC BIND 8 contains buffer overflow in
transaction signature (TSIG)

handling code

Solaris 8 04/01* (BIND 8.2.2-p5)
Solaris 8 Maintenance Update 4* (BIND 8.2.2-p5)
VU#572183 - ISC BIND 4 contains buffer overflow in
nslookupComplain()
Solaris 2.6 (BIND 4.9.4-P1)
Solaris 2.5.1** (BIND 4.9.3)

VU#868916 - ISC BIND 4 contains input validation error in
nslookupComplain()
Solaris 2.6 (BIND 4.9.4-P1)
Solaris 2.5.1** (BIND 4.9.3)

VU#325431 - Queries to ISC BIND servers may disclose
environment variables

Solaris 2.4, 2.5 (BIND 4.8.3)
Solaris 2.5.1** (BIND 4.9.3 and BIND 4.8.3)
Solaris 2.6 (BIND 4.9.4-P1)
Solaris 7 and 8 (BIND 8.1.2)

•    To determine if one is running Solaris 8 04/01 or
Solaris 8 Maintenance

Update 4, check the contents of the /etc/release file.

** Solaris 2.5.1 ships with BIND 4.8.3 but patch 103663-01
for SPARC and 103664-01 for x86 upgrades BIND to 4.9.3,
current revision for each patch is -17.
```

List of Patches

The following patches are available in relation to the above problems.

OS Version	Patch ID
SunOS 5.8	109326-04
SunOS 5.8_x86	109327-04
SunOS 5.7	107018-03
SunOS 5.7_x86	107019-03
SunOS 5.6	105755-10
SunOS 5.6_x86	105756-10
SunOS 5.5.1	103663-16
SunOS 5.5.1_x86	103664-16
SunOS 5.5	103667-12
SunOS 5.5_x86	103668-12
SunOS 5.4	102479-14
SunOS 5.4_x86	102480-12

The following advisory was found for Gauntlet 6.0 http://www.cert.org/advisories/CA-2001-25.html. It would affect an unpatched version of the firewall, however the GIAC IT department is required by the corporate security policy to keep all software patched with the most current patches available from the vendors. This advisory describes a vulnerability to a buffer overflow. A buffer overflow is an attack involving code that sends more data than a buffer is expecting or able to handle. The "extra" data can be processed as executable code and compromise the integrity of the system.

Network Associates CSMAP and smap/smapd vulnerable to buffer overflow thereby allowing arbitrary command execution

Overview

A remotely exploitable buffer overflow exists in the Gauntlet Firewall.

I. Description

The buffer overflow occurs in the smap/smapd and CSMAP daemons. According to PGP Security, these daemons are responsible for handling email transactions for both inbound and outbound e-mail.

```
This vulnerability occurs in smap/smapd on the following
products:

Gauntlet for Unix versions 5.x
PGP e-ppliance 300 series version 1.0
McAfee e-ppliance 100 and 120 series

This vulnerability occurs in CSMAP on the following
products:
Gauntlet for Unix version 6.0
PGP e-ppliance 300 series versions 1.5, 2.0
PGP e-ppliance 1000 series versions 1.5, 2.0
McAfee WebShield for Solaris v4.1

II. Impact

An intruder can execute arbitrary code with the privileges
of the corresponding daemon.

III. Solution

Patchs for this vulnerability are available from the vendor
at ftp://ftp.nai.com/pub/security/ and
http://www.pgp.com/naicommon/download/upgrade/upgrades-
patch.asp.
```

(The above link is no longer valid. Gauntlet patches can be found at http://www.securecomputing.com/index.cfm?sKey=987

For vulnerability testing we have chosen Nessus security scanner version 1.2.5 (nessus.org). Nessus begins by running an Nmap scan, and then it proceeds to check for possible exploits that bad guys may use to attack your system. A laptop loaded with Nessus was connected to the untrusted external interface of the Gauntlet Firewall 6.0 with the IP address of the border router, and a port scan and attack assessment was conducted against this interface. After starting Nessus and logging in as the client, we select our target, which is the external firewall interface, enable all scans, and start the scan. After this procedure has run, it will give us a report of possible vulnerabilities and suggestions of how to negate the threat. See Appendix A for the Nessus output of a scan conducted against an unsecured host on GIAC's internal network. It was scanned from inside the firewall and is simply a reference point to compare with the scan of our external firewall interface. Note the large amount of open ports and dangerous services running on this host. We

will not discuss closing the security holes on this box, as the intent of this audit is to evaluate our firewall.

Firewall

Compare the output in Appendix A to the following report that Nessus generated after scanning the external interface of our firewall.

timestamps|||scan_start|Thu Aug 29 05:45:05 2002|

timestamps||aaa.bbb.ccc.142|host_start|Thu Aug 29 05:45:15 2002|

results|aaa.bbb.ccc|aaa.bbb.ccc.142|general/tcp|10336|Security Note|"Default scan" set. nmap will ignore the user specified port range and scan only the 1024 first ports and those declared in nmap-services

results|aaa.bbb.ccc|aaa.bbb.ccc.142|ftp (21/tcp)
results|aaa.bbb.ccc|aaa.bbb.ccc.142|smtp (25/tcp)
results|aaa.bbb.ccc|aaa.bbb.ccc.142|http (80/tcp)
results|aaa.bbb.ccc|aaa.bbb.ccc.142|ident (113/tcp)
results|aaa.bbb.ccc|aaa.bbb.ccc.142|https (443/tcp)

results|aaa.bbb.ccc|aaa.bbb.ccc.142|general/tcp|10336|Security Note|Nmap found that this host is running Sun Solaris 8 early access beta through actual release\n

results|aaa.bbb.ccc|aaa.bbb.ccc.142|ftp (21/tcp)|10330|Security Note|a FTP server is running on this port.\nHere is its banner : \n220 gauntletfw.gcfw.com FTP proxy (Version V6.0) ready.\r

results|aaa.bbb.ccc|aaa.bbb.ccc.142|smtp (25/tcp)|10330|Security Note|a SMTP server is running on this port\nHere is its banner : \n220 gauntletfw.gcfw.com SMTP/smap Ready.\r

results|aaa.bbb.ccc|aaa.bbb.ccc.142|http (80/tcp)|10330|Security Note|a web server is running on this port

results|aaa.bbb.ccc|aaa.bbb.ccc.142|ftp (21/tcp)|10092|Security Note|Remote FTP server banner :\n gauntletfw.gcfw.com FTP proxy (Version V6.0) ready.\r

results|aaa.bbb.ccc|aaa.bbb.ccc.142|smtp (25/tcp)|10249|**Security Warning**|The remote SMTP server\nanswers to the EXPN and/or VRFY commands.\n\nThe EXPN command can be used to find \nthe delivery address of mail aliases, or \neven the full name of the recipients, and \nthe VRFY command may be used to check the \nvalidity of an account.\n\n\nYour mailer should not allow remote users to\nuse any of these commands, because it gives\nthem too much information.\n\n\nSolution : if you are using Sendmail, add the \noption\n O PrivacyOptions=goaway\nin /etc/sendmail.cf.\n\nRisk factor : Low\nCVE : CAN-1999-0531\n
results|aaa.bbb.ccc|aaa.bbb.ccc.142|smtp (25/tcp)|10262|**Security Warning**|The remote SMTP server allows the relaying. This means that\nit allows spammers to use your mail server to send their mails to\nthe world, thus wasting your network bandwidth.\n\nRisk factor :

```
Low/Medium\n\nSolution : configure your SMTP server so that it can't be
used as a relay\n           any more.\nCVE : CAN-1999-0512\n
results|aaa.bbb.ccc|aaa.bbb.ccc.142|smtp (25/tcp)|10263|Security
Note|Remote SMTP server banner :\ngauntletfw.gcfw.com SMTP/smap
Ready.\n214-Commands214-HELO    MAIL    RCPT    DATA    RSET\r\n214
NOOP    QUIT    HELP    VRFY    EXPN\r\n
results|aaa.bbb.ccc|aaa.bbb.ccc.142|smtp (25/tcp)|10250|Security
Warning|\nThe remote SMTP server is vulnerable to a
redirection\nattack. That is, if a mail is sent to :\n\n
      user@hostname1@victim\n       \nThen the remote SMTP server
(victim) will happily send the\nmail to :\n          user@hostname1\n
      \nUsing this flaw, an attacker may route a message\nthrough your
firewall, in order to exploit other\nSMTP servers that can not be
reached from the\noutside.\n\n*** THIS WARNING MAY BE A FALSE POSITIVE,
SINCE\n    SOME SMTP SERVERS LIKE POSTFIX WILL NOT\n    COMPLAIN BUT
DROP THIS MESSAGE ***\n    \n    \nSolution : if you are using
sendmail, then at the top\nof ruleset 98, in /etc/sendmail.cf, insert
:\nR$*@$*@$*       $#error $@ 5.7.1 $: '551 Sorry, no
redirections.'\n\nRisk factor : Low
results|aaa.bbb.ccc|aaa.bbb.ccc.142|general/udp|10287|Security Note|For
your information, here is the traceroute to aaa.bbb.ccc.142 :
\naaa.bbb.ccc.142\n
timestamps||aaa.bbb.ccc.142|host_end|Thu Aug 29 05:53:40 2002|
timestamps|||scan_end|Thu Aug 29 05:53:41 2002|
```

Just by the shear volume of output, one can tell that there are far fewer problems on our firewall box. Breaking it down, we see the open ports that are necessary for the services GIAC's network needs. There are several security notes that state what servers were found: ftp, SMTP, and a web server. These are necessary and relatively harmless. This traffic is filtered by the firewall and directed to the specific server. There are a few security warnings coming from our mail server. Sendmail has some inherent vulnerabilities and Nessus has given us some suggestions for changing our configuration to eliminate these. We will verify that we have the latest version and patches for Sendmail, make the changes to the configuration, and rerun the Nessus scan. One glaring problem is having port 113 open. Having this port listening, could open our network to reverse ident-scanning (http://www.insecure.org/nmap/nmap_doc.html - ident). This could allow an attacker to connect to our web server and use identd to find the identity of the owners of any TCP connected process running. We need to add a local rule to the firewall to deny any traffic on port 113. Also, the production firewall box must have some obscure name such as "giacXXX" or test box was poorly named "gauntletfw". We would never want to advertise the name of the firewall or give any hints as to what the intended use of this box is.

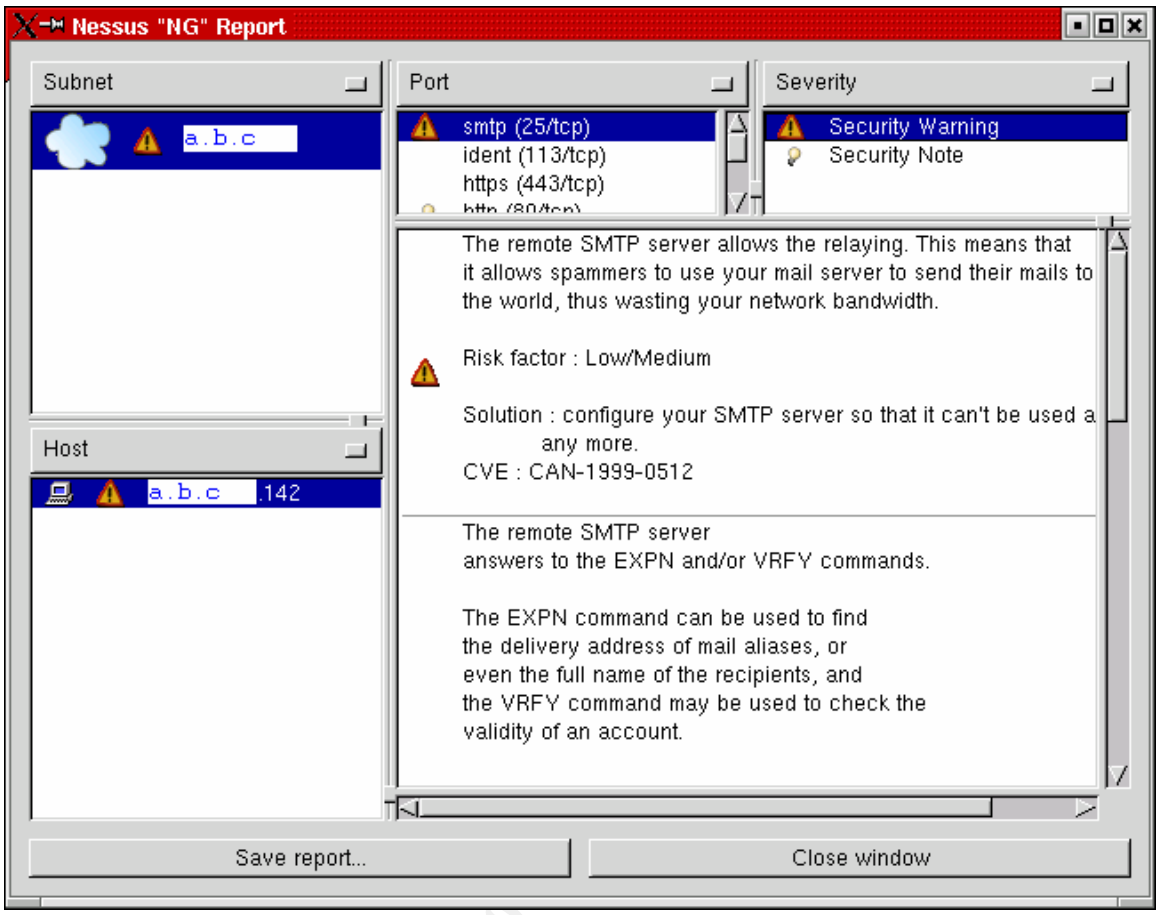

Figure 8. Nessus Report of an SMTP Configuration Error

One other step that could be taken to harden our firewall box is to install YASSP. (Yet Another Solaris Security Product) YASSP takes an inverse approach to the default settings one would observe when installing Solaris 8. It uses **fix-modes** set file permissions on core and startup files and **SEClean** to configure secure default settings in listening daemons and startup files. Solaris turns on many unneeded services initially and they must be disabled manually to harden the OS. With YASSP, most services are disabled by default, and the administrator must specifically enable the services deemed necessary by the network. YASSP hardens the OS so well, that it is almost unusable in its' initial state.

Note: When installing YASSP on a Solaris box intended to run Gauntlet Firewall 6.0, YASSP must be installed and configured before installing the firewall software.

Our architecture for the GIAC Network does not include an Network Intrusion Detection System (NIDS), however, this could be added in front of the firewall and to each of the internal subnets, to help determine what attacks are being tried against our network. We decided to leave NIDS

out of the initial design because of increased cost of equipment and the increased workload on the system administrators to monitor and maintain the NIDS.
Due to the hypothetical nature of GIAC's network and lack of "real" traffic flowing through the firewall, it is difficult to determine the true performance of our firewall, however there are several things that could be done to enhance performance of the firewall. Currently we are running NAT on the firewall. This could be done on the router, to relieve some of the burden placed on the firewall. We could increase the memory on the Sunfire 280R. We could also move some of the filters pertaining to our database server from the primary firewall to the secondary SunScreen firewall on the DB server, although that may overwork the database server during large ftp file transfers.

Note: During our initial rules testing of the Gauntlet firewall, Nessus issued a warning that our firewall was receiving and replying to ICMP timestamp requests. This may allow an attacker to defeat any time-based protocols that GIAC is using. Had we conducted our scanning from outside of the border router, the ICMP would have been dropped, and never reached our firewall. However, to stay within the concept of defense-in-depth, we added a local rule to Gauntlet, to deny ICMP on port 13 (timestamp request) and port 14 (timestamp reply). The warning did not appear on subsequent scans.

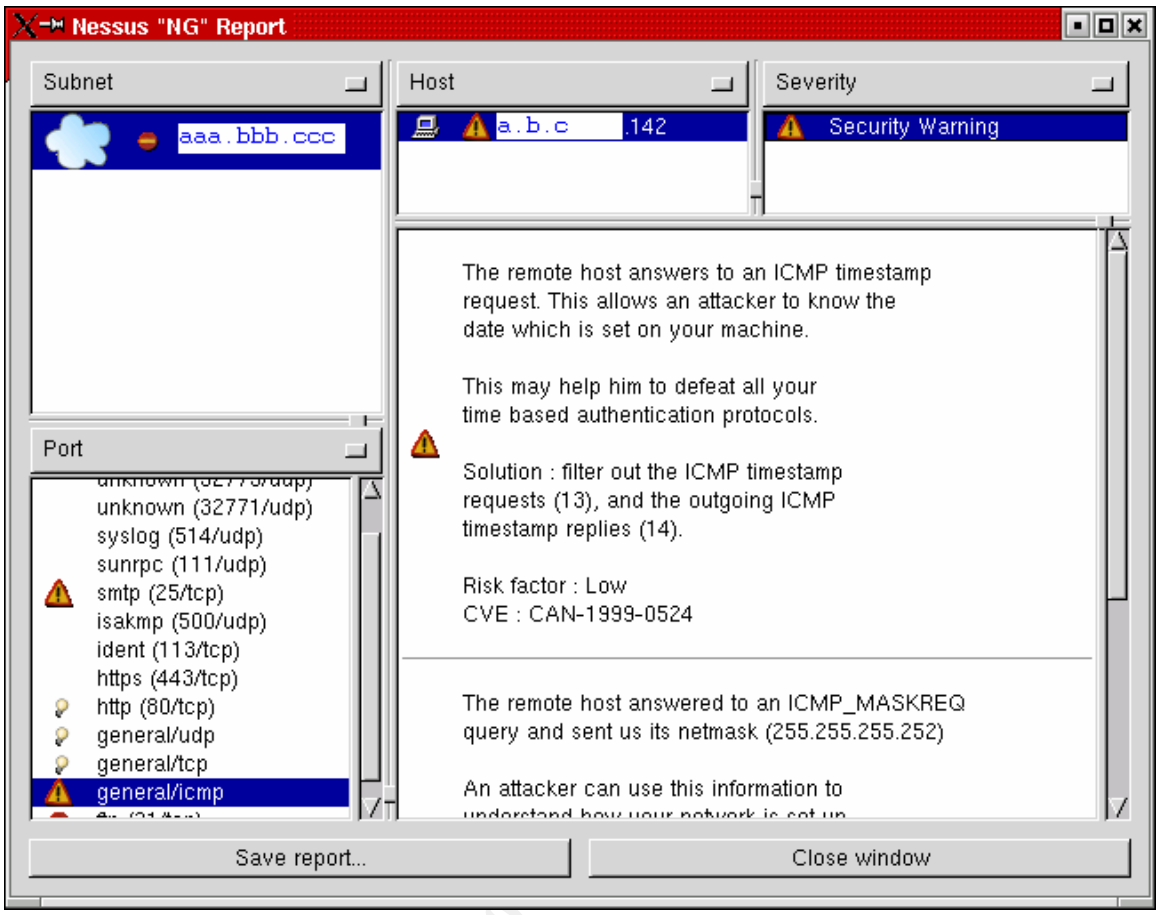

Figure 9. ICMP Timestamp Warning from Nessus

Assignment 4 – Design Under Fire (25 points)

The concluding section of this practical assignment involves researching and designing an attack on the GCFW practical assignment of Matthew Briddell. Matthew's practical can be found at http://www.giac.org/practical/Matt_Briddell_GCFW.zip. This will include three different attack scenarios. First, we will research and design an attack against the firewall itself, then a denial of service attack using 50 compromised systems with cable modems, and then an attack against any internal system through the perimeter. Matthew's network diagram, utilizing Checkpoint Firewall-1 is below in figure 10.

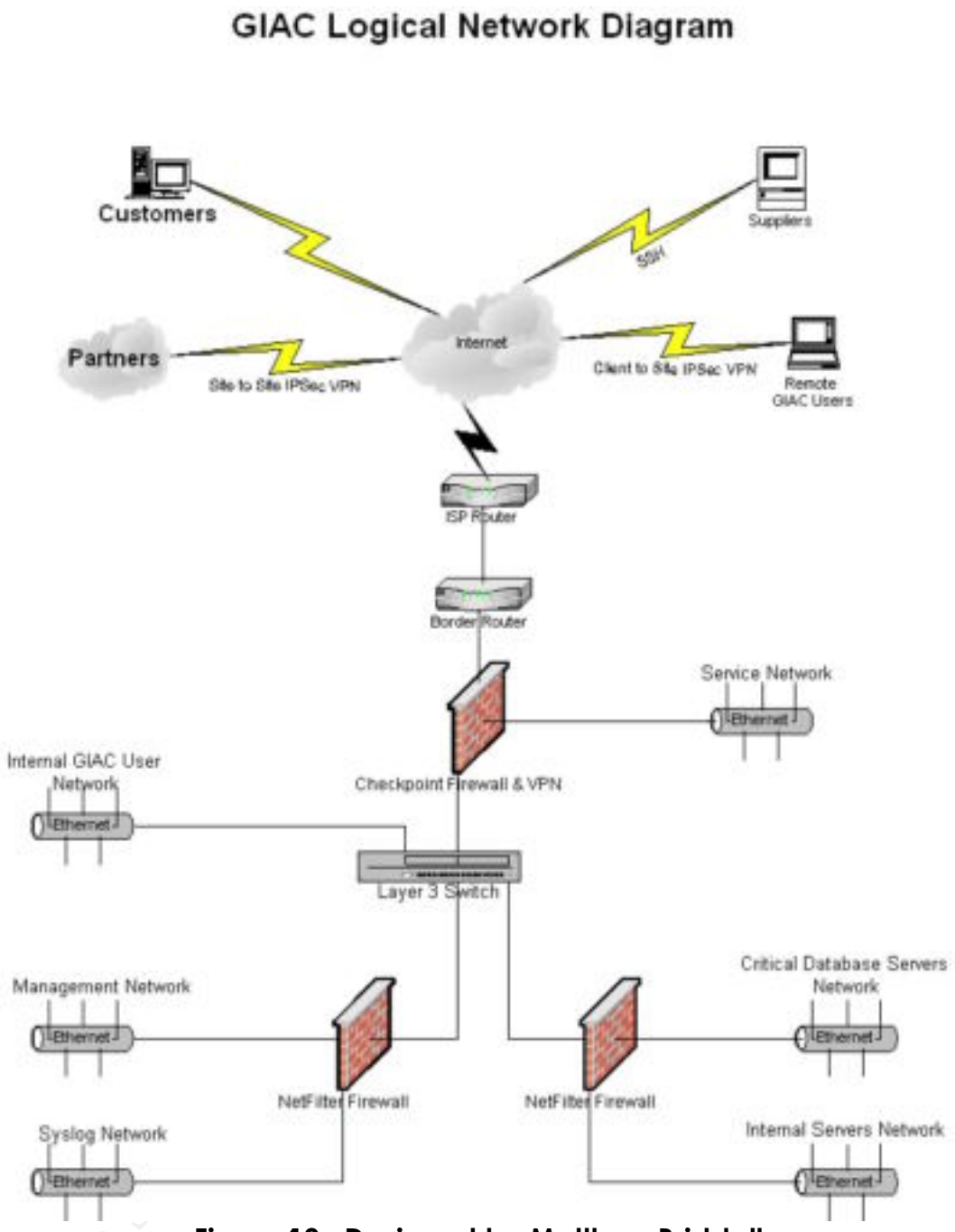

Figure 10. Designed by Matthew Briddell

Attack the Firewall

Matthew is using Check Point Firewall-1 Next Generation with Feature Pack 1 installed on a Linux RedHat 7.2 box with kernel 2.4.9-13. We begin our search for a suitable exploit at the source, the Check Point alerts page at http://www.checkpoint.com/techsupport/alerts/. The following vulnerability was noted:

Ike Aggressive Mode

In the vulnerability claim document, two issues were presented:

1.usernames are passed in cleartext using IKE Aggressive Mode

2.usernames are susceptible to brute-force guessing when using IKE Aggressive Mode

Firewall-1 versions 4.0 SP 7, 4.1 SP2, 4.1 SP6, NG Base, NG FP1 and NG FP2 allow username guessing using IKE aggressive mode. According to Security Focus at http://online.securityfocus.com/archive/1/290202/2002-09-01/2002-09-07/0, When presented with a username in an appropriately formatted IKE aggressive mode packet, the Firewall will respond differently depending on whether the username is valid or not. This allows usernames to be guessed using a dictionary attack. Versions up to NG base also provide additional information about accounts that exist but are not valid for IKE for some reason; NG FP1 and FP2 do not provide this extra information although they still indicate if the user is valid or not.

The Attack

We begin our attack by sending a properly formatted IKE aggressive mode packet with the following payload:

1. ISAKMP Header
2. SA - Containing one proposal with four transforms
3. Key Exchange - DH Group 2
4. Nonce
5. Identification - Type ID_USER_FQDN, Value is SecuRemote username

Security Focus gives the following output of an ike user guessing script, which can be run against the firewall, including an example of the firewall's response:

```
rsh@radon [502]% fw1-ike-userguess—file=testusers.txt—
sport=0 192.168.124.150
testuser        Notification code 14
test-ike-3des   USER EXISTS
testing123      Notification code 14
test-ike-des    USER EXISTS
guest   Notification code 14
test-expired    Notification code 14
rsh@radon [503]% exit
Script done on Tue Aug 20 17:28:08 2002
```

In this example, users "test-ike-3des" and "test-ike-des" exist and have valid IKE configurations with shared secret auth; the users "testuser", "testing123" and "guest" don't exist; and the user "test-expired" exists but has expired. With NG FP2, the Firewall does confirm if the user is valid or not, but it doesn't give additional information about why a user is not valid, but instead responds with notification code 14 which is defined in RFC 2408 section 3.14.1 as "NO-PROPOSAL-CHOSEN". However, the basic issue remains.

Check Point gives the following solution to the problem:

```
By default, Aggressive Mode is not enabled in NG. In 4.1,
the recommended configuration is to disable Aggressive Mode
and use Hybrid Mode instead (which involves no change to
the user experience).
```

If we were to run this attack against Mr. Briddell's Check Point Firewall installation, we would not be successful. Check Point Firewall NG defaults to disable IKE Aggressive Mode, and according to screen shots and the configuration instructions in Matthew's practical, he has not enabled this.

Denial of Service Attack

A distributed denial of service (Ddos) attack is one in which a master (attacker's system) and a number of agents (systems infected with a daemon listening for the master's command) conduct a coordinated attack involving a flood of assorted packets at a target, the result of which is an overwhelmed target that is no longer able to respond to any request sent to it. We will attack the network using 50 compromised systems, connected to the Internet via cable modem. Our target will be the web server running on port 80. We will use Tribal Flood Network 2000 (TFN2K) to coordinate our 50 agents to overwhelm the target with SYN packets sent from random IP addresses. TFN2K can be downloaded freely from http://1337.txn.org, but be prepared to be bombarded by porn pop-ups when connecting. TFN2K has two components: a client on the master, and a daemon operating on an agent. The master instructs its agents to attack the designated target. The agents respond by flooding the target with a barrage of packets. Multiple agents, coordinated by the master, can work in tandem during this attack to disrupt access to the target. Both master-to-agent communications and the attacks themselves can be sent via randomized TCP, UDP, and ICMP packets. Additionally, the master can spoof its IP address. These facts significantly complicate development of effective and efficient countermeasures for TFN2K.

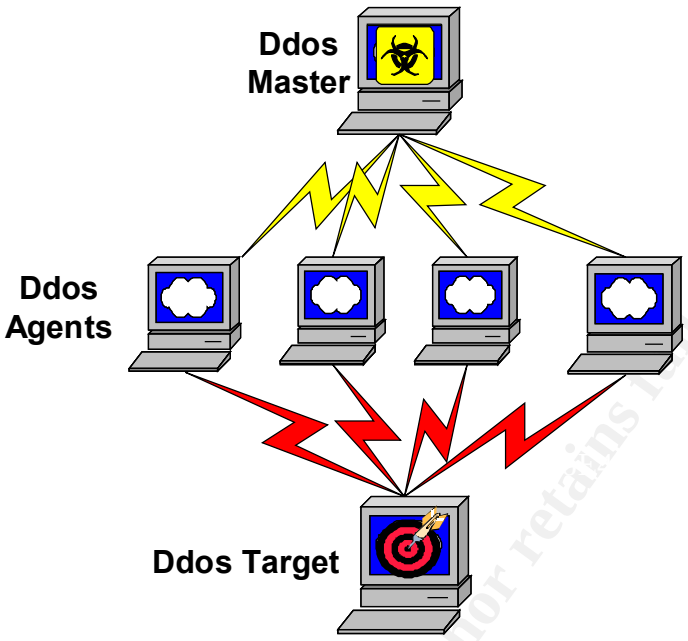

Figure 11. Diagram of a Distributed Denial of Service Attack

We execute TFN2K using the **–f <agentfile>** argument to read in a file containing the hostnames of our agents, the **–c 5** command to signify a TCP/SYN flood, the **<target ip>,** and port number **–p 80**. The agents then respond by bombarding the target (giac.com) with SYN packets directed at the web server on port 80. Matthew has configured Firewall NG's SYNDefender to use SYN relay, which completes the three-way-handshake before forwarding our SYN packets to the web server. This may initially thwart our attempts to crash the web server, but if enough traffic is hitting the firewall, performance will begin to degrade as the firewall attempts to complete or reset all of the connection attempts. Eventually, the SYNDefender will be overwhelmed and will start forwarding packets to the web server. Matthew does a good job trying to alleviate the problem, by reducing the timeout value to 3 seconds. As stated in his paper, "this will allow enough time for slow connections to succeed, but should keep the SYNDefender connection table from reaching its maximum."

Ddos attacks are very difficult to mitigate. Depending on the processing power of the firewall, it is only a matter of having enough agents attacking the box, before it will succumb to the SYN flood and forward the packets. With that said, I believe that the firewall configuration outlined by Matthew Briddell is about as close to a secure defense against the SYN flood Ddos attack as possible. Using SYNDefender and insulating his web

servers with a Squid proxy-caching cluster, it is unlikely that this attack will be successful.

Attack an Internal System

We begin by performing an **NMAP** (http://www.insecure.org/nmap/) port scan of the GIAC network, and discover that udp port 53 (dns) is open, as expected. After executing **NSLOOKUP** for giac.com, we find that the IP address for the Domain Name Server is 222.222.222.14. Now, armed with this information we use **NESSUS** to scan the DNS server for vulnerabilities, and we discover that it may be running BIND version 8.3.1. We soon discover that there are very few posted vulnerabilities for this version of BIND, but we will attempt to exploit a buffer overflow in the DNS resolver library found at http://www.cert.org/advisories/CA-2002-19.html.

CERT® Advisory CA-2002-19 Buffer Overflows in Multiple DNS Resolver Libraries
Original release date: June 28, 2002
Last revised: August 28, 2002
Source: CERT/CC

Description

The DNS protocol provides name, address, and other information about Internet Protocol (IP) networks and devices. To access DNS information, a network application uses the resolver to perform DNS queries on its behalf. Resolver functionality is commonly implemented in libraries that are included with operating systems. Multiple implementations of DNS resolver libraries contain remotely exploitable buffer overflow vulnerabilities in the code used to handle DNS responses. Both BSD (libc) and ISC BIND (libbind) resolver libraries share a common code base and are vulnerable to this problem; any DNS resolver implementation that derives code from either of these libraries may also be vulnerable. Network applications that use vulnerable resolver libraries are likely to be affected, therefore this problem is not limited to DNS or BIND servers. Two sets of responses could trigger buffer overflows in vulnerable DNS resolver libraries: responses for host names or addresses, and responses for network names or addresses. The GNU glibc resolver addressed the vulnerability in handling responses for host resolution in version 2.1.3. However, versions of glibc prior to and including 2.2.5 are vulnerable to responses for network resolution, as explained below in the GNU glibc vendor statement. BSD (libc) and ISC BIND (libbind) resolvers are vulnerable to both types of responses.

pkgsrc prior to bind-8.3.3 are vulnerable. Upgrade to bind-8.3.3

.

Impact
An attacker who is able to send malicious DNS responses could remotely exploit these vulnerabilities to execute arbitrary code or cause a denial of service on vulnerable systems. Any code executed by the attacker would run with the privileges of the process that calls the vulnerable resolver function.

Note that an attacker could cause one of the victim's network services to make a DNS request to a DNS server under the attacker's control. This would permit the attacker to remotely exploit these vulnerabilities.

Exploit
Many websites noted the presence of this weakness in BIND 8.3.1, however, I was unable to locate any exploit code for this vulnerability, and so I have decided to move on to another approach.

Second Attempt
I begin this attack with a little social engineering by posing as a troubleshooter for some obscure, but high tech, company. I explain to the receptionist (in a slightly perturbed voice) that "I was in the middle of a conversation with one of her IT administrators, trying to solve the problem that is causing the computer network slowdown, when the telephone suddenly went dead. I didn't catch the man's name. Maybe Bob, or Bill…?"

She replies, "I'm sorry, we don't have a Bob or Bill in IT. Could it have been Mike, John or Ron?

"I guess it had to be one of them. What are their last names?

"Mike Jones, John Smith, and Ron Jettson"

"Jettson sounds right. Would you reconnect me to Ron? Thank you."

Now, I hang up and go to the phone book to find Ron's home phone and address. That evening, after blocking the feature to send caller id information from my phone, I make a bogus telemarketing call to Ron, during dinner. I tell him he has been chosen to receive a "special deal" from AT&T on a cable modem and 6 months of broadband service. Ron explains that he is already an AT&T broadband customer. Lucky for him, he qualifies for half-price service, just for answering a few questions about his home Internet experience. I soon find out that Ron is running Windows 2000 and uses Outlook Express for email, and his email address is dumbRon@attbi.com. I tell him to expect a confirmation email from me,

detailing his discount etc., in the next 24 hours. Now, I send Ron a congratulatory email from a false attbi.com account, (remember, I work for AT&T) that executes a script to install Spector Pro (http://www.spectorsoft.com/) monitoring software. Spector will run in stealth mode to monitor keystrokes and email. When it recognizes a key word, such as GIAC, it will email a report to me that will include Ron's user id and passwords etc. From there, it's a fairly simple matter of spoofing Ron's IP address and tunneling through the VPN with his authorized administrator's id and password, to have my way with the GIAC network.

Prevention

A scheme such as this would only work on the newest, most gullible administrator. It is highly unlikely that a person trusted to administer the system from home, would give out any information about his home system, and be naïve enough to unknowingly download an executable. However, anything is possible. The corporate policy must dictate that all users, especially home users, attend security awareness classes that emphasize the importance of keeping private information private. Also, personal firewalls and anti-virus protection must be made available to all employees, and its use must be mandatory for those who must connect to the corporate intranet from remote locations.

Conclusion

As we have seen, defense-in-depth really is a code to live or die by. Information protection requires security at many different levels, and the best firewall or router on the market is not a be-all, end-all solution to securing ones network. The hardware must be properly configured to keep out the bad guys, while giving access to the good guys. A combination of physical security, user awareness, and a secure network configuration is necessary to truly secure ones precious information, and even then, constant vigilance is required to maintain a secure perimeter.

References

Information gleaned from the SANS 2002 conference in Orlando, FL, including the following course literature:

The SANS Institute, TCP/IP for Firewalls, SANS Firewalls Track 2.1

The SANS Institute, Firewalls 101: Perimeter Protection with Firewalls, SANS Firewalls Track 2.2

The SANS Institute, Firewalls 102: Perimeter Protection Defense In-Depth, SANS Firewalls Track 2.3

The SANS Institute, VPNs and Remote Access, SANS Firewalls Track 2.4

The SANS Institute, Network Design and Performance, SANS Firewalls Track 2.5

Norton Antivirus 2003
http://www.symantecstore.com/dr/sat2/ec_MAIN.Entry17c?CID=42122&SID=27674&SP=10007&PN=5&PID=426823&DSP=&CUR=840&PGRP=0&CACHE_ID=42122

RSA Secure ID
http://rsasecurity.com/products/securid/index.html

Gauntlet Firewall 6.0
http://www.securecomputing.com/index.cfm?sKey=979

Apache Webserver
http://www.apache.org/

Bind
http://www.isc.org

SendMail
http://www.sendmail.org

NSA Router Configuration Guide
http://nsa2.www.conxion.com/cisco/guides/

How to Install Solaris and have a good Host Security by Jean Chouanard
http://www.yassp.org/

Computer Emergency Response Team
www.cert.org

Nessus vulnerability scanner
nessus.org

GCFW Practical by Matthew Briddell
http://www.giac.org/practical/Matt_Briddell_GCFW.zip

Checkpoint Firewall Next Generation Alerts
http://www.checkpoint.com/techsupport/alerts/

Bugtraq regarding SecuRemote usernames can be guessed or sniffed using IKE exchange
http://online.securityfocus.com/archive/1/290202/2002-09-01/2002-09-07/0

Tribal Flood Network 2000. Distributed Denial of Attack tool
http://1337.txn.org

CERT® Advisory CA-2002-19 Buffer Overflows in Multiple DNS Resolver Libraries
http://www.cert.org/advisories/CA-2002-19.html

Spector Soft, Internet Monitoring and Surveillance
http://www.spectorsoft.com/

CERT® Advisory CA-2001-25 Buffer Overflow in Gauntlet Firewall allows intruders to execute arbitrary code
http://www.cert.org/advisories/CA-2001-25.html

Tripwire open source integrity checker
http://tripwire.org/

Nmap Port Scanner
http://www.insecure.org/nmap/

Secure FTP, San Diego Super Computer Center
http://security.sdsc.edu/software/secureftp/

The Art of Port Scanning, by Fyodor
http://www.insecure.org/nmap/nmap_doc.html - ident

Appendix A

Nessus Output of an Unsecured Host inside the Firewall

timestamps|||scan_start|Sat Aug 24 10:35:57 2002|
timestamps||10.1.2.6|host_start|Sat Aug 24 10:36:08 2002|
results|10.1.2|10.1.2.6|echo (7/tcp)
results|10.1.2|10.1.2.6|discard (9/tcp)
results|10.1.2|10.1.2.6|daytime (13/tcp)
results|10.1.2|10.1.2.6|chargen (19/tcp)
results|10.1.2|10.1.2.6|ftp (21/tcp)
results|10.1.2|10.1.2.6|telnet (23/tcp)
results|10.1.2|10.1.2.6|smtp (25/tcp)
results|10.1.2|10.1.2.6|time (37/tcp)
results|10.1.2|10.1.2.6|finger (79/tcp)
results|10.1.2|10.1.2.6|sunrpc (111/tcp)
results|10.1.2|10.1.2.6|exec (512/tcp)
results|10.1.2|10.1.2.6|login (513/tcp)
results|10.1.2|10.1.2.6|shell (514/tcp)
results|10.1.2|10.1.2.6|printer (515/tcp)
results|10.1.2|10.1.2.6|ibm-db2 (523/tcp)
results|10.1.2|10.1.2.6|uucp (540/tcp)
results|10.1.2|10.1.2.6|submission (587/tcp)
results|10.1.2|10.1.2.6|sun-dr (665/tcp)
results|10.1.2|10.1.2.6|unknown (898/tcp)
results|10.1.2|10.1.2.6|unknown (4045/tcp)
results|10.1.2|10.1.2.6|wbem-rmi (5987/tcp)
results|10.1.2|10.1.2.6|unknown (6000/tcp)
results|10.1.2|10.1.2.6|dtspcd (6112/tcp)
results|10.1.2|10.1.2.6|font-service (7100/tcp)

results|10.1.2|10.1.2.6|ddi-tcp-1 (8888/tcp)

results|10.1.2|10.1.2.6|general/tcp|10336|Security Note|Nmap found that this host is running Sun Solaris 8 early access beta through actual release\n

results|10.1.2|10.1.2.6|general/tcp|10336|Security Note|Nmap only scanned 15000 TCP ports out of 65535.Nmap did not do a UDP scan, I guess.

results|10.1.2|10.1.2.6|echo (7/tcp)|10330|Security Note|an echo server is running on this port

results|10.1.2|10.1.2.6|chargen (19/tcp)|10330|Security Note|Chargen is running on this port

results|10.1.2|10.1.2.6|telnet (23/tcp)|10330|Security Note|a telnet server seems to be running on this port

results|10.1.2|10.1.2.6|submission (587/tcp)|10330|Security Note|a SMTP server is running on this port\nHere is its banner : \n220 appserver ESMTP Sendmail 8.11.6+Sun/8.11.6; Fri, 23 Aug 2002 10:36:32 -0500 (CDT)\r

results|10.1.2|10.1.2.6|ddi-tcp-1 (8888/tcp)|10330|Security Note|a web server is running on this port

results|10.1.2|10.1.2.6|snmp (161/udp)|10264|**Security Hole**|;;SNMP Agent responded as expected with community name: public\nCVE : CAN-1999-0517\n

results|10.1.2|10.1.2.6|ftp (21/tcp)|10092|Security Note|Remote FTP server banner :\n appserver FTP server (SunOS 5.8) ready.\r\n

results|10.1.2|10.1.2.6|snmp (161/udp)|10800|Security Note|Using SNMP, we could determine that the remote operating system is :\nSun SNMP Agent, Ultra-5_10

results|10.1.2|10.1.2.6|smtp (25/tcp)|10249|**Security Warning**|The remote SMTP server\nanswers to the EXPN and/or VRFY commands.\n\nThe EXPN command can be used to find \nthe delivery address of mail aliases, or \neven the full name of the recipients, and \nthe VRFY command may be used to check the \nvalidity of an account.\n\n\nYour mailer should not allow remote users to\nuse any of these commands, because it gives\nthem too much information.\n\n\nSolution : if you are using Sendmail, add the \noption\n O PrivacyOptions=goaway\nin /etc/sendmail.cf.\n\nRisk factor : Low\nCVE : CAN-1999-0531\n

results|10.1.2|10.1.2.6|ddi-tcp-1 (8888/tcp)|10107|Security Note|The remote web server type is :\n\ndwhttpd/4.2a7 (Inso; sun5)\r\n\nWe recommend that you configure your web server to return\nbogus versions in order to not leak information\n

results|10.1.2|10.1.2.6|finger (79/tcp)|10068|**Security Warning**|The 'finger' service provides useful information\nto attackers, since it allow them to gain usernames, check if a machine\nis being used, and so on... \n\nRisk factor : Low\n\nSolution : comment out the 'finger' line in /etc/inetd.conf\nCVE : CVE-1999-0612\n

results|10.1.2|10.1.2.6|shell (514/tcp)|10245|**Security Warning**|The rsh service is running.\nThis service is dangerous in the sense that\nit is not ciphered - that is, everyone can sniff\nthe data that passes between the rsh client\nand the rsh server. This includes logins\nand passwords.\n\nYou should disable this service and use ssh instead.\n\nSolution : Comment out the 'rsh' line in /etc/inetd.conf.\n\nRisk factor : Low\nCVE : CAN-1999-0651\n

```
results|10.1.2|10.1.2.6|submission (587/tcp)|10263|Security Note|Remote
SMTP server banner :\nappserver ESMTP Sendmail 8.11.6+Sun/8.11.6; Fri,
23 Aug 2002 10:39:32 -0500 (CDT)\n214-2.0.0 This is sendmail version
8.11.6+Sun214-2.0.0 Topics:\r\n214-2.0.0  HELO  EHLO  MAIL  RCPT
      DATA\r\n214-2.0.0       RSET  NOOP  QUIT  HELP  VRFY\r\n214-2.0.0
      EXPN  VERB  ETRN  DSN\r\n214-2.0.0 For more info use "HELP
<topic>".\r\n214-2.0.0 To report bugs in the implementation contact Sun
Microsystems\r\n214-2.0.0 Technical Support.\r\n214-2.0.0 For local
information send email to Postmaster at your site.\r\n214 2.0.0 End of
HELP info\r\n
results|10.1.2|10.1.2.6|ddi-tcp-1 (8888/tcp)|10662|Security Note|For
your information, here is the list of CGIs\nthat are used by the remote
host, as well as their arguments : \n\nSyntax: cginame (arguments
```

[default value])\n\n/@Ab2LibSearch (_AB2_SearchAllColl DwebQuery Search [Search]
results|10.1.2|10.1.2.6|general/tcp|10794|Security Note|The plugin PC_anywhere_tcp.nasl was too slow to finish - the server killed it\n
results|10.1.2|10.1.2.6|unknown (32775/tcp)|10951|**Security Warning**|\nThe cachefsd RPC service is running. \nSome versions of this server allow an attacker to gain\nroot access remotely, by consuming the resources of the \nremote host then sending a specially formed packet with\nformat strings to this host.\n\nSolaris 2.5.1, 2.6, 7 and 8 are vulnerable to this\nissue. Other operating systems might be affected as well.\n\n*** Nessus did not check for this vulnerability, \n*** so this might be a false positive\n\nSolution : Deactivate this service - there is no patch at this time\n
/etc/init.d/cachefs.daemon stop\nRisk factor : High\nCVE : CAN-2002-0084\n
results|10.1.2|10.1.2.6|chargen (19/tcp)|10043|**Security Warning**|The chargen service is running.\nThe 'chargen' service should only be enabled when testing the machine. \n\nWhen contacted, chargen responds with some random (something like all \nthe characters in the alphabet in row). When contacted via UDP, it \nwill respond with a single UDP packet. When contacted via TCP, it will \ncontinue spewing characters until the client closes the connection. \n\nAn easy attack is 'pingpong' which IP spoofs a packet between two machines\nrunning chargen. They will commence spewing characters at each other, slowing\nthe machines down and saturating the network. \n
\nSolution : disable this service in
/etc/inetd.conf.\n\nRisk factor : Low\nCVE : CVE-1999-0103\n
results|10.1.2|10.1.2.6|daytime (13/tcp)|10052|**Security Warning**|The daytime service is running.\nThe date format issued by this service\nmay sometimes help an attacker to guess\nthe operating system type. \n\nIn addition to that, when the UDP version of\ndaytime is running, an attacker may link it \nto the echo port using spoofing, thus creating\na possible denial of service.\n\nSolution : disable this service in /etc/inetd.conf.\n\nRisk factor : Low\nCVE : CVE-1999-0103\n

results|10.1.2|10.1.2.6|daytime (13/udp)|10052|**Security Warning**|The daytime service is running.\nThe date format issued by this service\nmay sometimes help an attacker to guess\nthe operating system type. \n\nIn addition to that, when the UDP version of\ndaytime is running, an attacker may link it \nto the echo port using spoofing, thus creating\na possible denial of service.\n\nSolution : disable this service in /etc/inetd.conf.\n\nRisk factor : Low\nCVE : CVE-1999-0103\n

results|10.1.2|10.1.2.6|echo (7/tcp)|10061|**Security Warning**|The 'echo' port is open. This port is\nnot of any use nowadays, and may be a source of problems, \nsince it can be used along with other ports to perform a denial\nof service. You should really disable this service.\n\nRisk factor : Low\n\nSolution : comment out 'echo' in /etc/inetd.conf\nCVE : CVE-1999-0103\n

results|10.1.2|10.1.2.6|dtspcd (6112/tcp)|10833|**Security Hole**|\nThe 'dtspcd' service is running.\n\nSome versions of this daemon are vulnerable to\na buffer overflow attack which allows an attacker\nto gain root privileges\n\n*** This warning might be a false positive,\n*** as no real overflow was performed\n\nSolution : See http://www.cert.org/advisories/CA-2001-31.html\nto determine if you are vulnerable or

deactivate\nthis service (comment out the line ‘dtspc’ in /etc/inetd.conf)\n\nRisk factor : High\nCVE : CVE-2001-0803\n

results|10.1.2|10.1.2.6|echo (7/udp)|10061|**Security Warning**|The ‘echo’ port is open. This port is\nnot of any use nowadays, and may be a source of problems, \nsince it can be used along with other ports to perform a denial\nof service. You should really disable this service.\n\nRisk factor : Low\n\nSolution : comment out ‘echo’ in /etc/inetd.conf\nCVE : CVE-1999-0103\n

results|10.1.2|10.1.2.6|finger (79/tcp)|10073|**Security Warning**|The remote finger daemon accepts\nto redirect requests. That is, users can perform\nrequests like :\n
finger user@host@victim\n\nThis allows an attacker to use your computer\nas a relay to gather information on another\nnetwork, making the other network think you\nare making the requests.\n\nSolution: disable your finger daemon (comment out\nthe finger line in /etc/inetd.conf) or \ninstall a more secure one.\n\nRisk factor : Low\nCVE : CAN-1999-0105\n

results|10.1.2|10.1.2.6|general/icmp|10113|**Security Warning**|\nThe remote host answered to an ICMP_MASKREQ\nquery and sent us its netmask (255.255.255.0)\n\nAn attacker can use this information to\nunderstand how your network is set up\nand how the routing is done. This may\nhelp him to bypass your filters.\n\nSolution : reconfigure the remote host so\nthat it does not answer to those requests.\nSet up filters that deny ICMP packets of\ntype 17.\n\nRisk factor : Low\nCVE : CAN-1999-0524\n

results|10.1.2|10.1.2.6|general/icmp|10114|**Security Warning**|\nThe remote host answers to an ICMP timestamp\nrequest. This allows an attacker to know the\ndate which is set on your machine. \n\nThis may help him to defeat all your \ntime based authentication protocols.\n\nSolution : filter out the ICMP timestamp\nrequests (13), and the outgoing ICMP \ntimestamp replies (14).\n\nRisk factor : Low\nCVE : CAN-1999-0524\n

results|10.1.2|10.1.2.6|exec (512/tcp)|10203|**Security Warning**|\nThe rexecd service is open. \nBecause rexecd does not provide any good\nmeans of authentication, it can be\nused by an attacker to scan a third party\nhost, giving you troubles or bypassing\nyour firewall.\n\nSolution : comment out the ‘exec’ line \nin /etc/inetd.conf.\n\nRisk factor : Medium\nCVE : CAN-1999-0618\n

results|10.1.2|10.1.2.6|login (513/tcp)|10205|**Security Warning**|The rlogin service is running.\nThis service is dangerous in the sense that\nit is not ciphered - that is, everyone can sniff\nthe data that passes between the rlogin client\nand the rlogin server. This includes logins\nand passwords.\n\nYou should disable this service and use openssh instead\n(www.openssh.com)\n\nSolution : Comment out the ‘rlogin’ line in /etc/inetd.conf.\n\nRisk factor : Low\nCVE : CAN-1999-0651\n

results|10.1.2|10.1.2.6|submission (587/tcp)|10167|**Security Warning**|There is a problem in NTMail3, which allows anyone to\nuse it as a mail relay, provided that the source address is set to ‘<>’. \nThis problem allows any spammer to use your mail server to spam the\nworld, thus blacklisting your mailserver, and using your network\nresources.\n\nRisk factor : Medium\n\nSolution : There are no solution

provided by the author of NTMail,\nso you might want to change mail servers\nCVE : CVE-1999-0819\n

results|10.1.2|10.1.2.6|unknown (32779/udp)|10213|**Security Hole**|\nThe cmsd RPC service is running. \nThis service has a long history of \nsecurity holes, so you should really\nknow what you are doing if you decide\nto let it run.\n\n* NO SECURITY HOLE REGARDING THIS\n PROGRAM HAS BEEN TESTED, SO\n THIS MIGHT BE A FALSE POSITIVE *\n\nWe suggest you to disable this\nservice.\n\n\nRisk factor : High\nCVE : CVE-1999-0320\n

results|10.1.2|10.1.2.6|unknown (4045/udp)|10220|**Security Warning**|\nThe nlockmgr RPC service is running. \nIf you do not use this service, then\ndisable it as it may become a security\nthreat in the future, if a vulnerability\nis discovered.\n\nRisk factor : Low\nCVE : CVE-2000-0508\n

results|10.1.2|10.1.2.6|unknown (32777/udp)|10227|**Security Warning**|\nThe rstatd RPC service is running. \nIt provides an attacker interesting\ninformation such as :\n\n - the CPU usage\n - the system uptime\n - its network usage\n - and more\n \nIt usually not a good idea to let this\nservice open\n\n\nRisk factor : Low\nCVE : CAN-1999-0624\n

results|10.1.2|10.1.2.6|unknown (32773/udp)|10226|**Security Warning**|\nThe rquotad RPC service is running. \nIf you do not use this service, then\ndisable it as it may become a security\nthreat in the future, if a vulnerability\nis discovered.\n\nRisk factor : Low\nCVE : CAN-1999-0625\n

results|10.1.2|10.1.2.6|unknown (32774/udp)|10228|**Security Warning**|\nThe rusersd RPC service is running. \nIt provides an attacker interesting\ninformation such as how often the\nsystem is being used, the names of\nthe users, and so on.\n \nIt usually not a good idea to leave this\nservice open.\n\n\nRisk factor : Low\nCVE : CVE-1999-0626\n

results|10.1.2|10.1.2.6|unknown (32772/udp)|10229|**Security Hole**|\nThe sadmin RPC service is running. \nThere is a bug in Solaris versions of\nthis service that allow an intruder to\nexecute arbitrary commands on your system.\n\nSolution : disable this service\nRisk factor : High\nCVE : CVE-1999-0977\n

results|10.1.2|10.1.2.6|unknown (32775/udp)|10234|**Security Warning**|\nThe sprayd RPC service is running. \nIf you do not use this service, then\ndisable it as it may become a security\nthreat in the future, if a vulnerability\nis discovered.\n\nRisk factor : Low\nCVE : CAN-1999-0613\n

results|10.1.2|10.1.2.6|unknown (32778/udp)|10235|**Security Warning**|\nThe statd RPC service is running. \nThis service has a long history of \nsecurity holes, so you should really\nknow what you are doing if you decide\nto let it run.\n\n* NO SECURITY HOLE REGARDING THIS\n PROGRAM HAVE BEEN TESTED, SO\n THIS MIGHT BE A FALSE POSITIVE *\n\nWe suggest you to disable this\nservice.\n\n\nRisk factor : High\nCVE : CVE-1999-0018\n

results|10.1.2|10.1.2.6|unknown (32773/tcp)|10787|**Security Hole**|\nThe tooltalk RPC service is running.\n\nThere is a format string bug in many versions\nof this service, which allow an attacker to gain\nroot remotely.\n\n*** This warning may be a false

positive since the presence\n*** of the bug was not verified locally.\n \nSolution : Disable this service or patch it\nSee also : CERT Advisory CA-2001-27\n\nRisk factor : High

results|10.1.2|10.1.2.6|unknown (32776/udp)|10240|**Security Warning**|\nThe walld RPC service is running. \nIt is usually used by the administrator\nto tell something to the users of a\nnetwork by making a message appear\non their screen.\n\nSince this service lacks any kind\nof authentication, an attacker\nmay use it to trick users into\ndoing something (change their password,\nleave the console, or worse), by sending\na message which would appear to be\nwritten by the administrator.\n\nIt can also be used as a denial of service\nattack, by continually sending garbage\nto the users screens, preventing them\nfrom working properly.\n\nSolution : Deactivate this service.\n\nRisk factor : Medium\nCVE : CVE-1999-0181\n

results|10.1.2|10.1.2.6|unknown (32776/udp)|10950|**Security Warning**|\nThe rpc.walld RPC service is running. \nSome versions of this server allow an attacker to gain\nroot access remotely, by consuming the resources of the \nremote host then sending a specially formed packet with\nformat strings to this host.\n\nSolaris 2.5.1, 2.6, 7 and 8 are vulnerable to this\nissue. Other operating systems might be affected as well.\n\n*** Nessus did not check for this vulnerability, \n*** so this might be a false positive\n\nSolution : Deactivate this service.\nRisk factor : High

results|10.1.2|10.1.2.6|general/udp|10287|Security Note|For your information, here is the traceroute to 10.1.2.6 : \n10.1.2.6\n

results|10.1.2|10.1.2.6|unknown (6000/tcp)|10407|**Security Warning**|This X server does **not** accept clients to connect to it\nhowever it is recommended that you filter incoming connections\nto this port as attacker may send garbage data and slow down\nyour X session or even kill the server\nHere is the message we received : \n\n Client is not authorized to connect to Server\n\nSolution : filter incoming connections to ports 6000-6009\nRisk factor : Low\nCVE : CVE-1999-0526\n

results|10.1.2|10.1.2.6|general/tcp|10879|Security Note|The plugin port_shell_execution.nasl was too slow to finish - the server killed it\n

results|10.1.2|10.1.2.6|general/tcp|10672|Security Note|The plugin torturecgis.nasl was too slow to finish - the server killed it\n

results|10.1.2|10.1.2.6|unknown (32796/tcp)|10659|**Security Hole**| \nThe remote RPC service 100249 (snmpXdmid) may be vulnerable\nto a heap overflow which allows any user to obtain a root\nshell on this host.\n\n*** Nessus reports this vulnerability using only\n*** information that was gathered. Use caution\n*** when testing without safe checks enabled.\n\nSolution : disable this service (/etc/init.d/init.dmi stop) if you don't use\nit, or contact Sun for a patch\nRisk factor : High\nCVE : CVE-2001-0236\n

results|10.1.2|10.1.2.6|unknown (32778/udp)|10544|**Security Hole**|\nThe remote statd service may be vulnerable\nto a format string attack.\n\nThis means that an attacker may execute arbitrary\ncode thanks to a bug in this daemon.\n\n*** Nessus reports this vulnerability using only\n*** information that was gathered. Use caution\n*** when testing without safe checks enabled.\n\nSolution : upgrade to the latest version of rpc.statd\nRisk factor : High\nCVE : CVE-2000-0666\n

timestamps||10.1.2.6|host_end|Sat Aug 24 10:58:50 2002|

timestamps|||scan_end|Sat Aug 24 10:58:51 2002|