Global Information Assurance Certification Paper

SANS GIAC
Certified Firewall Analyst (GCFW)
Practical Assignment
Version 1.8 (revised September 10, 2002)

Don't Let Your Cookies Crumble

James Carlson
April 12, 2003

Table of Contents

GIAC Enterprises Background

GIAC Enterprises (GE) is an e-business that sells fortune cookie sayings online. The president of the company wants to upgrade the security posture of the network. The plan calls for designing secure, inexpensive, expandable and maintainable network architecture.

A "defense in depth" strategy will be deployed to protect the confidentiality, integrity and availability of all data that resides on the GE network. Fortune cookie sayings must be protected from competitors "prying eyes". Therefore all proprietary data crossing the Internet must be encrypted. In addition, customer's information must be safeguarded. Security protocols such as IPsec, SSL and SSH will be deployed to heighten the security of the GIAC Network. Also, security technologies such as a packet-filtering router, proxy-based firewall, and two encrypted Virtual Private Networks (VPNs) will protect GE's network resources. Logging and monitoring systems provide an additional layer of protection.

Part 1 – Security Architecture

Before we define the security architecture for GE we need to understand the business operations and how each of the following groups interacts with the company's network.

Customers

GE's customers purchase bulk online fortunes. The customer requires access to the GE Website. The confidentiality of the fortune cookie sayings and customer information must be protected in transit. Web browsers with 128-bit encryption are required for access. The Web Site will utilize the Public Key Infrastructure (PKI) and Secure Socket Layers (SSL). Service ports opened will be TCP 80 and TCP 443 on the web site. These are HTTP and HTTPS respectively. SSL is a public key-based security protocol that is used by Internet services and clients to authenticate each other and to establish message integrity and confidentiality. SSL uses certificates for authentication, and it uses encryption for message integrity and confidentiality. For business purposes, the customers will not have to authenticate. They will be sent an e-mail confirming their order. After that they will be allowed to download their sayings from the website.

Suppliers

This group of network users will supply GIAC Enterprises with fortune cookie sayings. The suppliers will upload the sayings to a GIAC Secured Shell (SSH) Server residing on the GIAC Internal Network. Similar to GE customers

their access will be limited to one system. They require access to service port TCP 22 on the SSH Server. Only authenticated users will be allowed SSH access. To further restrict access GE Network Administrators will know the IP Address space of the supplier's systems.

International Business Partners

Business Partners need to download sayings for later resell. International Business Partners need limited secure access to GE's Internal Network. A network-to-network VPN will be set up with each Business Partner. The VPN endpoints consist of the International Partner's Firewall and GE's Firewall. GE has chosen to deploy a Gauntlet 6.0 Firewall. This firewall provides built-in support for Client and Network VPNs. A Public Key Infrastructure (PKI) setup authenticates the VPN connection and IPsec encrypts it. This group needs access to web services and e-mail on GIAC's Internal Network.

GIAC Enterprise Employees

GIAC employees must manage the business of selling fortune cookie sayings. The Internal GE Network consists of network administrators, program developers and accounting personnel. The network admins are responsible for the security and maintenance of the network. The programmers maintain and update the web and database servers. The accounting department needs to ensure that the customers, suppliers and business partner's activities are tracked. Employees need web and e-mail access to the outside world. In addition, administrators and developers need secure access to GE's systems residing on their Service Network. Gauntlet firewall services provide web, ssh, and smtp proxies for employees to access the "outside".

GIAC Enterprise Mobile Sales Force

The mobile sales force requires client to network vpn access to GE's Internal Network. Authentication requires a PKI certificate or pre-shared secrets. GIAC's firewall controls access and logs each vpn connection. These workers will need access to e-mail, file shares and GE Internal Website.

Network Architecture Components

Filtering Router

A Cisco 3640 running Cisco IOS 12.2 equipped with two fast ethernet interfaces provides the first line of defense for our network. The main purpose of the router is to route packets into and out of our network. However, an important security function of a border router is to filter packets coming into or out of the network. Our router uses static packet filtering to drop unwanted packets and

permit allowed packets. Our filtering router will not maintain the "state" of the connection or do payload inspection. The primary purpose of the router's access control list (ACL) is to block spoofed ip attacks, prevent other unwanted ip source addresses such as unallocated address space, and to provide access control for necessary services on the GE network.

Firewall

The workhorse of GE's network, a rackable Sun Fire V120 Server manages Secure Computing Corporation's Gauntlet 6.0 Firewall Application. The server contains a 650 MHz processor, 1 GB of ram, support for 3 10/100 Mbps ethernet ports and 2 38GB hard drives. Gauntlet Firewall 6.0 runs on a "hardened" version of Solaris 8 64 bit operating environment. The main role of the firewall is to implement GE's corporate security policy. The firewall will enable access to the Internet for GE's employees while protecting the Internal Network from unauthorized access. In addition to stateful packet filtering, Gauntlet 6.0 Firewall includes built-in support for application proxies, VPN's, McAfee anti-virus software, and file integrity checking.

VPN's

The purpose of the VPNs is to allow authenticated users encrypted access to GIAC's internal resources. The GE's VPN will establish a secure tunnel across the Internet by encrypting the data using the IPsec protocol and authenticating the user using PKI certificates or pre-shared secrets.

GE's supports two types of VPN's. A client-to-network VPN allows the mobile sales force and teleworkers to connect to GE's Internal Network. The second type, a network-to-network VPN establishes an authenticated encrypted connection between GE's international business partners and its Internal Network. Both VPN's connect to GE's firewall allowing access to be controlled and logged. Gauntlet 6.0 interoperates with other vendor's products as long as the Internet Key Exchange (IKE) and IPsec standards are followed.

IP Addressing Scheme

For the purposes of this practical Private IP Addresses are used. IP Addresses in the 192.168.0.0 space have been variably sub netted into two networks. The firewall divides the address space. One interface connects to the Service Network while the other connects to the internal network. The following table lists the overall IP addressing scheme for GE.

Cisco 3640 Router External Interface	10.0.0.1
Cisco 3640 Router Internal Interface	192.168.100.1 255.255.255.252
Gauntlet 6.0 Firewall External Interface	192.168.100.2 255.255.255.252
Gauntlet 6.0 Firewall Internal Interface	192.168.0.1 255.255.255.224
Gauntlet 6.0 Firewall Service Interface	192.168.0.33 3255.255.255.224

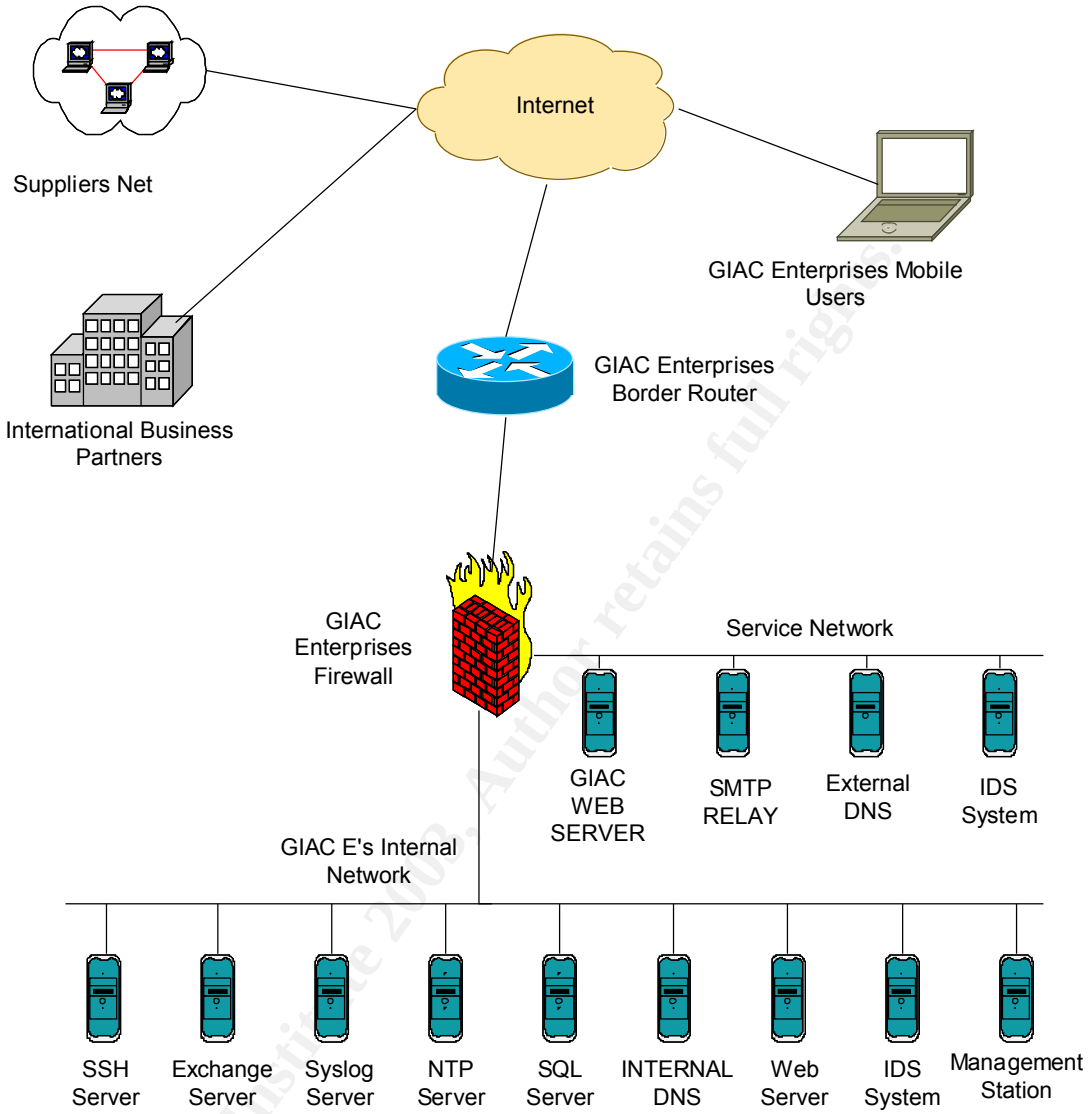
The following table shows the Service Network IP Addresses:

GE's Service Network	NETID: 192.168.0.33	MASK: 255.255.255.224
GE's Customer Web Site	192.168.0.34	
External SMTP Server	192.168.0.35	
External DNS Server	192.168.0.36	
IDS System	192.168.0.37	

The following table lists the IP Address for the Internal Network:

GE's Internal Network	NETID: 192.168.0.0	MASK: 255.255.255.224
SQL Server	192.168.0.2	
Internal Web Server	192.168.0.4	
Exchange Server	192.168.0.5	
Internal DNS Server	192.168.0.6	
Time Server	192.168.0.7	
SSH Server	192.168.0.8	
Syslog Server	192.168.0.20	
Management Station	192.168.0.21	
IDS System	192.168.0.22	

Network Architecture Diagram



Part 2 – Security Policy and Tutorial

The Security Policy for the CISCO 3640 Border/Filtering Router

The main role of GE'S border router is to route packets to and from the Internal Network and Service Network. Static Routes route packets more securely than other routing protocols such as RIP or OSPF.

In addition to routing, the security policy covers the following areas:

1) Physical Security
2) Remote and Local Access Policy
3) Permitted and Disallowed Network Services

4) Tutorial on Logging and Access Control Lists

Physical Security:

Physical Security is vital because anyone with physical access to the router can connect to the console port and become administrators with full privileges. The GE's border router will be located in a limited access area. Only people with administrative responsibilities for the router will be granted access. The room will be monitored for access. Another area of concern is the operating environment. The temperature and humidity of the area must be controlled and monitored. The area must be free of electrostatic and magnetic interference. In addition, the router will be connected to an Uninterruptible Power Supply (UPS) to prevent damage and network outages.

Remote and Local Access Policy:

Setup enable and user accounts with password encryption.

Use the following command to prevent passwords from being displayed in clear-text in the router configuration file.

```
GIAC#config t
Enter configuration commands, one per line.  End with CNTL/Z.
GIAC(config)#service password-encryption
GIAC(config)#end
```

Setup and protect the privileged EXEC level password. Use the enable secret password command and disable the enable password. Enable secret password uses a MD5 Hash to encrypt the password instead of the weaker Cisco hash algorithm. The password chosen should conform to GE's password policy.

```
GIAC#config t
Enter configuration commands, one per line.  End with CNTL/Z.
GIAC(config)#enable secret q2#Y0gh3
GIAC(config)#no enable password
GIAC(config)#end
```

Setup user accounts. For accounting purposes all users must have their own accounts. Users start with privilege level 1. Users that require a higher level of access will use the enable secret password after logging on. The following commands set up a user logon account.

```
GIAC#config t
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
GIAC(config)#username joesmith privilege 1 password q2#Y0gh3
GIAC(config)#end
```

Setup a login banner for local and remote connections. The banner should include a legal notice. Don't include any information that should not be shared with the general public. Here are the commands for setting up a login banner.

```
GIAC#config t
GIAC(config)#banner motd ;
Enter TEXT message.  End with the character ';'.
You have logged into a GIAC Enterprises System. The information in this system
is the sole property of GIAC Enterprises. This system may be used for authorize
business purposes only. Any unauthorized use may be subject to prosecution.
;
```

Configure the console port to enforce user logon and timeout. This will protect administrators who forget to logout and walk away from the console. Note: You must create a user account first; otherwise you will be locked out of the console. The following commands enforce user logon and set the timeout to 5 minutes.

```
GIAC#config t
Enter configuration commands, one per line.  End with CNTL/Z.
GIAC(config)#line con 0
GIAC(config-line)#transport input none
GIAC(config-line)#login local
GIAC(config-line)#exec-timeout 5 0
GIAC(config-line)#end
```

Disable the auxiliary port. The auxiliary port is used for a modem connection. To prevent a war-dialing attack, disable the modem/aux port. The following commands disable the aux port.

```
GIAC#config t
Enter configuration commands, one per line.  End with CNTL/Z.
GIAC(config)#line aux 0
GIAC(config-line)#transport input none
GIAC(config-line)#login local
GIAC(config-line)#exec time-out 0 1
GIAC(config-line)#no exec
GIAC(config-line)#exit
GIAC(config)#exit
```

Setup Secure Shell remote access. Console access is the most secure way to configure the router. The security policy for GE's allows an encrypted connection

from an Internal Network host to access the router. The following commands permit one internal host 192.168.0.15 to connect to the router via Secured Shell (SSH).

```
GIAC#config t
Enter configuration commands, one per line.  End with CNTL/Z.
GIAC(config)#access-list 8 permit host 192.168.0.15
GIAC(config)#line vty 0 4
GIAC(config-line)#access-class 8 in
GIAC(config-line)#login local
GIAC(config-line)#transport input ssh
GIAC(config-line)#exit
```

Generate an RSA key pair.

```
GIAC#config t
Enter configuration commands, one per line.  End with CNTL/Z.
GIAC(config)#crypto key generate rsa
How many bits in the modulus [512] 2048
[OK]
```

When an RSA key pair exists SSH service is present on the router.

Disable and Secure Router Services.

A default router configuration enables insecure services. The following section describes which network services to disable and how to disable them.

Disable the Cisco Discovery Protocol. It allows Cisco routers to identify each other. It is useful for troubleshooting but not needed in a production environment.

```
GIAC#config t
Enter configuration commands, one per line.  End with CNTL/Z.
GIAC(config)#no cdp run
GIAC(config)#exit
```

Test to see if cdp is disabled

```
GIAC#show cdp
% CDP is not enabled
```

Disable TCP and UDP small servers. This will prevent some trivial denial of service attacks.

```
GIAC#config t
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
GIAC(config)#no service udp-small-servers
GIAC(config)#no service tcp-small-servers
GIAC(config)#exit
```

Test: Connect to character generator port

```
GIAC#connect 10.0.0.1 chargen
Trying 10.0.0.1, 19 ...
% Connection refused by remote host
```

Disable HTTP remote administration. The Security Policy doesn't allow web-based administration of the routers. The router is less vulnerable to attack by closing port 80. Here are the commands for disabling the HTTP Server.

```
GIAC#config t
Enter configuration commands, one per line.  End with CNTL/Z.
GIAC(config)#no ip http server
GIAC(config)#exit
```

Test: Connect to HTTP Server Port.

```
GIAC#connect 10.0.0.1 www
Trying 10.0.0.1, 80 ...
% Connection refused by remote host
```

Disable Bootp Server. Bootp used by hosts to load their operating systems over the network. GE's will not be using this service. An attacker could download a copy of the router's operating system.

```
GIAC#config t
Enter configuration commands, one per line.  End with CNTL/Z.
GIAC(config)#no ip bootp server
GIAC(config)#exit
```

Disable the finger service. The finger service shows the logged in users. This information should not be freely available. The following commands shuts down the finger service and test to see if it is open.

```
GIAC#config t
Enter configuration commands, one per line.  End with CNTL/Z.
GIAC(config)#no ip finger
GIAC(config)#no service finger
GIAC(config)#exit
```

Test: Connect to Finger Server Port.

```
GIAC#connect 10.0.0.1 finger
Trying 10.0.0.1, 79 ...
% Connection refused by remote host
```

Disable Auto-Loading. Cisco routers can load their startup configurations from the network. It is not secure to keep configurations on the network without proper access controls. Disable this service with the following commands:

```
GIAC#config t
Enter configuration commands, one per line.  End with CNTL/Z.
GIAC(config)#no boot network
GIAC(config)#no service config
GIAC(config)#exit
```

Configure the Network Time Protocol (NTP) Service. Auditing depends on synchronization of all device clocks in the network. Configure the NTP Service to receive updates from the Internal NTP Server only.

Disable NTP Updates to the external router interface:

```
GIAC#config t
Enter configuration commands, one per line.  End with CNTL/Z.
GIAC(config)#interface fastethernet1/0
GIAC(config-if)#ntp disable
GIAC(config-if)#exit
GIAC(config)#exit
```

Set up NTP on the Internal Interface.

```
GIAC#config t
Enter configuration commands, one per line.  End with CNTL/Z.
GIAC(config)#interface fastethernet1/1
GIAC(config-if)#no ntp disable
GIAC(config-if)#exit
GIAC(config)#ntp server 192.168.0.15 source fastethernet1/1
GIAC(config)#exit
```

Next set up Access Control List for the Network Time Protocol (NTP) Server.

```
GIAC#config t
Enter configuration commands, one per line.  End with CNTL/Z.
GIAC(config)#ntp server 192.168.0.15 source fastethernet1/1
GIAC(config)#access-list 15 permit host 192.168.0.15
GIAC(config)#access-list 15 deny any log
GIAC(config)#ntp access group peer 15
GIAC(config)#exit
```

Check to see if NTP is configured:

```
GIAC#show ntp associations

     address         ref clock     st  when  poll reach  delay  offset    disp
 ~192.168.0.15     0.0.0.0         16    25    64    0     0.0    0.00  16000.
 * master (synced), # master (unsynced), + selected, - candidate, ~ configured
```

Protecting against ICMP and other Protocol Attacks

Now that unnecessary services are disabled and necessary security services are configured. The router needs to be protected from malicious use of ICMP and other protocols The following commands play an important role in protecting the network against mapping and routing attacks.

The following commands prevent ICMP messages from providing information about the network to an attacker on the external interface.

```
GIAC#config t
Enter configuration commands, one per line.  End with CNTL/Z.
GIAC(config)#interface fastethernet1/0
GIAC(config-if)#no ip unreachable
GIAC(config-if)#no ip redirect
GIAC(config-if)#no ip mask-reply
GIAC(config-if)#end
```

The following commands prevent packets from specifying their own routes (no ip source-route) and rejects packets to a subnet with no default gateway (no ip classless). Both commands prevent some denial of service attacks and are not needed for operational purposes.

```
GIAC#config t
Enter configuration commands, one per line.  End with CNTL/Z.
GIAC(config)#no ip classless
GIAC(config)#no ip source-route
GIAC(config)#exit
```

The security policy for GE's border router prevents the Internal Network from the communicating with the external network at layer 2. We need to disable directed broadcast and proxy arp on all interfaces.

```
GIAC#config t
Enter configuration commands, one per line.  End with CNTL/Z.
GIAC(config)#interface fastethernet1/0
GIAC(config-if)#no ip proxy-arp
GIAC(config-if)#no ip directed-broadcast
GIAC(config-if)#end
```

```
GIAC(config)#interface fastethernet1/1
GIAC(config-if)#no ip proxy-arp
GIAC(config-if)#no ip directed-broadcast
GIAC(config-if)#end
```

Tutorial on CISCO Access Control Lists and Logging

The CISCO IOS 12.2 supports logging to the Console, Terminal Line, Memory Buffer, Syslog Server and to a SNMP Trap Manager. The preferred method is logging to a Syslog Server. These logs can be protected and off loaded to a long-term storage device. Logging to the Console is useful only if a user is logged on, but the logs are not persistent. Buffered Logging resets the logs when the system reboots. Another form of logging, Terminal Line Logging is useful when a remote user is logged on. SNMP Trap Logging is used in an SNMP based network management network. GE's Security Policy requires SNMP to be disabled. The following commands disable SNMP on the border router.

```
GIAC#config t
Enter configuration commands, one per line. End with CNTL/Z.
GIAC(config)#no snmp-server
GIAC(config)#exit
```

Understanding the severity level of log message is key to setting up logging on a Cisco router. The following table shows the severity levels and gives an example at each level. The table is from the "Router Security Configuration Guide Ver. 1.1"

LEVEL	NAME	EXAMPLE
0	Emergencies	IOS not loaded
1	Alerts	Temperature too High
2	Critical	Unable to allocate memory
3	Errors	Invalid Memory Size
4	Warnings	Crypto operation failed
5	Notifications	Interface state change
6	Informational	Access list denial
7	Debugging	Debug Info

It is important to note that logging at a specific severity level will capture all levels below it. For example, we will log messages to the console at level 5 (Notifications). In addition to level 5, levels 0 through 4 also get logged. The key to successful logging is knowing what messages to log. Logging too much information fills up the logs with useless information. GE's security policy calls for Console, Buffered and Syslog logging. The following commands set up console logging at severity level 5 (Notifications).

```
GIAC#config t
Enter configuration commands, one per line.  End with CNTL/Z.
GIAC(config)#logging console notifications
GIAC(config)#logging on
GIAC(config)#exit
```

The buffer size can be adjusted. It should be based on the amount of memory in the router. The following commands set up a 16Kbytes buffer log with date and time stamps:

```
GIAC#config t
Enter configuration commands, one per line.  End with CNTL/Z.
GIAC(config)#logging buffered 16000 information
GIAC(config)#service timestamps log date msec local show-timezone
GIAC(config)#exit
```

Setting Up a Syslog Client on the Router:

The following commands will use the internal interface to log informational messages and above to GE's Syslog Server using local 6 as the facility. The facility on a Syslog Server is a storage area for messages. Syslog Servers typically support local0 through Local7 facility for routers. Logging informational messages ensures that packets denied by our access control list get logged.

```
GIAC#config t
Enter configuration commands, one per line.  End with CNTL/Z.
GIAC(config)#logging trap information
GIAC(config)#logging 192.168.0.20
GIAC(config)#logging facility local6
GIAC(config)#logging source-interface fastethernet1/1
GIAC(config)#exit
```

The following command verifies whether logging is set up correctly.

```
GIAC#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited, 0
flushes,
 0 overruns)
    Console logging: level notifications, 36 messages logged
    Monitor logging: level debugging, 0 messages logged
    Buffer logging: level informational, 36 messages logged
    Logging Exception size (4096 bytes)
    Trap logging: level informational, 40 message lines logged
        Logging to 192.168.0.20, 40 message lines logged
```

Log Buffer (16000 bytes):

Once the console is secured, unnecessary router services have been disabled, logging and time services setup; the next thing to do is create Access Control Lists (ACL). ACL's filter traffic by determining whether a packet is permitted to pass through a specific router interface. An ACL is made up of one are more rules. The rules are processed in sequential order. One of the most common causes of ACL's malfunctioning is putting the rules in the wrong order. Once a packet is matched to a rule processing stops and the action permit or deny for that packet is performed. Cisco supports standard, extended, named and reflexive ACL's. The general syntax for a Cisco ACL is shown below.

access-list *list-number* { deny | permit } *condition*

The list-number specifies whether it is a standard or extended ACL. Standard lists only allow matching on the source ip address. Extended lists can permit or deny packets based on their protocols, source or destination addresses or service ports. A standard ACL can be numbered 1 to 99. An extended ACL can be in the range 100 to 199. Named ACL's offer a more user friendly way to create ACL's. The final type of Cisco ACL, Reflexive offers stateful packet filtering. Due to performance issues stateful packet filtering will not be used on GE's filtering router.

An important rule to remember is an ACL can only be applied to one interface in one direction. It is possible for the same interface to have one outbound ACL and another inbound ACL, but the ACL number must be different.

The syntax for an extended ACL is shown below.

access-list *list-number* { deny | permit } *protocol source source-wildcard source-qualifiers destination destination-wildcard destination-qualifiers* { log | log-input }

list-number: A number from 100 to 199.
deny: Denies packet if condition is matched.
permit: Permits packet if condition is matched.
protocol: A name or number describing a specific IP-related protocol.
source: Source IP address of the packet.
source-wildcard: Wildcard bits applied to source address.
source-qualifiers: Other protocol specific information like port numbers.
destination: Destination IP address of the packet.
destination-wildcard: Wildcard bits applied to destination address.
destination-qualifiers: Other protocol specific information like port numbers.
log: A message is logged if the rule is matched.
log-input: A message is logged if the rule is matched and includes the interface.

The keyword **any** can be used in place of *source, destination. source-wildcard or destination-wildcard*. The protocol can be one of the following keywords: eigrp, gre, icmp, igmp, ip, ipinip, nos, ospf, tcp or udp. It can also be a number from 0 to 255.

Implementing GE's Security Policy for Inbound Traffic

The border router is the first line of defense in the network. The border router reduces the load on the firewall. Packets are not allowed unless the security policy states so.

GE's security policy requires filtering out the following network traffic on the Ingress (inbound) side of our Cisco 3640 router.

1) Source Address of GE's Internal Networks. To prevent spoofing attacks.
2) Unallocated Address space. See www.iana.org/assignments/ipv4-address-space.
3) Private Address Space. The private addresses are listed in RFC 1918.
4) Loop back and Broadcast Address. This can prevent some denial of service attacks and prevents your network from being used as a SMURF Amplifier.
5) Multicast Addresses. The network does not need multicast traffic.

In addition, GE's Security Policy is to permit only the following services into the Internal Networks.

Source	Destination	Destination IP	Service	Port
Any	GIAC Web	192.168.0.34	HTTP HTTPS	TCP 80 TCP 443
Suppliers	SSH Server	192.168.0.8	SSH	TCP 22
Any	Ext. DNS Server	192.168.0.36	DNS	TCP 53 UDP 53
Any	Mail Relay	192.168.0.35	SMTP	TCP 25
Any	VPN	192.168.100.2	IKE IPsec (esp)	UDP 500

Extended access list 150 was created with a text editor. Then cut and paste into the Cisco 3640 command line interface. This is a necessary step when editing an existing ACL because from the console one cannot add a line to the middle of the list. It also provides a means to comment and store the ACL.

!Deny Internal Addresses as source addresses
access-list 150 deny ip 192.168.0.0 0.0.255.255 any log

!Deny loopback address as source addresses
access-list 150 deny   ip 127.0.0.0 0.255.255.255 any log

!Deny Broadcast Addresses as source addresses
access-list 150 deny   ip host 255.255.255.255 any log

!Deny access to Internal Broadcast Addresses as destination addreses
access-list 150 deny ip any host 192.168.0.0 log
access-list 150 deny ip any host 192.168.0.31 log
access-list 150 deny ip any host 192.168.0.32 log
access-list 150 deny ip any host 192.168.0.63 log

!Deny Private Ip's as source addresses
access-list 150 deny   ip 10.0.0.0 0.255.255.255 any log
access-list 150 deny   ip 172.16.0.0 0.15.255.255 any log

!Deny unasigned IP's as source addresses
access-list 150 deny   ip 0.0.0.0 255.255.255.255 any log
access-list 150 deny   ip 1.0.0.0 255.255.255.255 any log
access-list 150 deny   ip 2.0.0.0 255.255.255.255 any log
! much more unallocated ip space to deny.

!Deny Multicast Traffic as source addresses
access-list 150 deny ip 224.0.0.0 0.255.255.255 any log

!Permit Acceptable Traffic
access-list 150 permit tcp any host 192.168.0.34 eq 80
access-list 150 permit tcp any host 192.168.0.34 eq 443
access-list 150 permit tcp any host 192.168.0.8 eq 22
access-list 150 permit tcp any host 192.168.0.36 eq 53
access-list 150 permit udp any host 192.168.0.36 eq 53
access-list 150 permit tcp any host 192.168.0.35 eq 25

!Allow VPN/IPSec Traffic to External Firewall Interface
access-list 150 permit 50 any host 192.168.100.2
access-list 150 permit 51 any host 192.168.100.2
access-list 150 permit udp any host 192.168.100.2 eq 500

The following three rules must be placed last otherwise no rule after these three would be processed. Log all traffic that is not acceptable according to policy. In addition, monitor the Sans Internet Storm Center http://isc.sans.org/ for current hacker activity. Add the blocked list to your ingress filter.

!Block and Log all other traffic
access-list 150 deny tcp any range 0 65535 any range 0 65535 log

```
access-list 150 deny udp any range 0 65535 any range 0 65535 log
access-list 150 deny ip any any log
```

The ordering of rules is important in ACL's. More specific rules need to be place before more general rules. Rules need to be monitored so that the most processed rules are near the top of the ACL. Doing so helps the performance of the network. In addition, logging is an issue when setting up ACL's. The administrator needs to examine the logs daily and adjust the ACL accordingly. Too much logging can make the administrator's job a nightmare.

Egress (Outbound) rules:

The important thing here is to not allow any IP's going out of your network that is not part of the Internal Network address space. This blocks outbound spoofing attempts. In addition, block unneeded services too. A hacker can use outbound services such as ftp to his advantage.

Extended ACL 125 prevents and logs IP spoofing attempts and prevents access to unneeded outbound services.

```
! Allow Internal Hosts Web Browsing
access-list 125 permit tcp 192.168.0.0 0.0.0.31   any eq 80
access-list 125 permit tcp 192.168.0.0 0.0.0.31   any eq 443

! Allow External DNS Server through the router
access-list 125 permit tcp  host 192.168.0.36 any eq 53
access-list 125 permit udp host 192.168.0.36 any  eq 53

! Allow External Mail Server through
access-list 125 permit tcp host 192.168.0.35 any  eq 25

!Allow Management Station SSH access to the Router.
Access-list 125 permit tcp host 192.168.0.21 host 192.168.100.1 eq 22

!Allow access to network time server
Access-list 125 permit tcp host 192.168.0.7 host 192.168.100.1 eq 123
Access-list 125 permit udp host 192.168.0.7 host 192.168.100.1 eq 123

!Block and Log all Other Traffic from Internal Network
access-list 125 deny tcp any range 0 65535 any range 0 65535 log
access-list 125 deny udp any range 0 65535 any range 0 65535 log
!Log any spoofed IP Addreses
access-list 125 deny ip any any log
```

The next step is applying the access list to a router interface. An access list can be applied as an outbound or inbound filter on an interface. We apply access list 150 as an inbound filter. This stops denied packets before entering the routing process. This saves valuable router CPU cycles. The following commands show how to apply Extended Access List 150 to the routers external interface fastethernet1/0.

```
GIAC#config t
Enter configuration commands, one per line.  End with CNTL/Z.
GIAC(config)#interface fastethernet1/0
GIAC(config-if)#ip access-group 150 in
GIAC(config-if)#exit
```

Next, Extended Access List 125 is applied on the inbound Fastethernet1/0 interface. Here again, this prevents dropped packets from entering the routing process. The following commands show how to apply this ACL.

```
GIAC#config t
Enter configuration commands, one per line.  End with CNTL/Z.
GIAC(config)#interface fastethernet1/1
GIAC(config-if)#ip access-group 125 in
GIAC(config-if)#exit
```

Access Lists should be monitored to determine configuration problems or to make adjustments to an ACL. Cisco provides some useful commands for monitoring the ACL's. The following commands display Access list 125 with the number of matches for each filter/rule.

```
GIAC#sh ip access-list 125
Extended IP access list 125
    permit tcp 192.168.0.0 0.0.0.31 any eq www
    permit tcp 192.168.0.0 0.0.0.31 any eq 443
    permit tcp host 192.168.0.36 any eq domain
    permit udp host 192.168.0.36 any eq domain
    permit tcp host 192.168.0.35 any eq smtp
    permit tcp host 192.168.0.21 host 192.168.100.1 eq 22
    permit tcp host 192.168.0.7 host 192.168.100.1 eq 123
    permit udp host 192.168.0.7 host 192.168.100.1 eq ntp
    deny tcp any range 0 65535 any range 0 65535 log (1 match)
    deny udp any range 0 65535 any range 0 65535 log
    deny ip any any log (1 match)
```

Use the following command to clear the above counters.

```
GIAC#clear access-list counters
```

Another form of monitoring ACL's is configuring each interface to create a database of all packets that have been denied by any access list on that interface. The following commands create this database.

```
GIAC#config t
Enter configuration commands, one per line.  End with CNTL/Z.
GIAC(config)#interface fastethernet1/1
GIAC(config-if)#ip accounting access-violations
GIAC(config-if)#exit
```

The following command displays the access violations database.

```
GIAC#show ip accounting access-violations
  Source          Destination          Packets            Bytes   ACL
 192.168.0.20     10.0.0.5                 1               28   125

Accounting data age is 14
```

The following command clears the IP accounting database.

```
GIAC#clear ip accounting
```

Firewall Policy

Gauntlet 6.0 Firewall provides packet filtering rules and proxy rules to implement the security policy. The ordering of the rules is important. Packet-filtering rules are processed first. Proxy rules can provide inspection at the application layer. Therefore, proxy rules are considered more secure and should be used when performance is not an issue. The proxy prevents applications on the outside of the network from communicating directly with applications on the inside and visa versa. Gauntlet provides application proxies for many types of services. A generic TCP plug proxy can do stateful packet inspection. If a proxy is not provided for a service, that type of traffic will not pass through the firewall. Gauntlet also protects the firewall interfaces with built-in anti-spoofing rules.

GE's firewall policy is based on the access needs of the various groups that support GE. The firewall policy considers business operations as a basis for implementing the Corporate Security Policy on the firewall.

The most used policies are placed near the top of the list to increase performance. In addition, Gauntlet provides adaptive proxies, which can be configured to allow a proxy connection to do routine packet filtering thereby improving performance. If performance becomes an issue a third-party proxy such as squid can be used to off-load traffic from the firewall. Squid is a dedicated HTTP proxy that is optimized for handling HTTP traffic.

The following table lists the rules/policies for GE's Gauntlet 6.0 Firewall.

Proxy Rules				
Rule	Source	Service	Action	Destination Restriction
1	Customers	WebServices	Permit	GIACWEBSITE
2	any	Mail	Permit	ExternalMail
3	SuppliersNetwork	SSHSERVERPLUG	Permit	SSHSERVER
4	ExternalMail	Mail	Permit	PermitAll
5	InternalNet	WebServices	Permit	PermitAll
6	External-DNS-Server	DNS	Permit	PermitAll
7	Internal-Mail-server	Mail	Permit	ExternalMail
8	InternalDNSServer	DNS	Permit	ExternalDNS
9	Customer-WebSite	SQLServer	Permit	SQL-Server
10	Router-in	SYSLOG	Permit	SyslogServer
11	SeviceNet	SYSLOG	Permit	SyslogServer
12	InternalNet	SSHPLUG	Permit	ServiceNET
13	OutsideTrusted	NTP	Permit	NTP-Server
14	ESPMD	ESPMD	Permit	DenyAll

Rule #1: Allow GE's Customers access to the GE's Customer Web Site. The source Customers is a group that includes any IP address. The service WebServices includes the pre-defined Gauntlet proxy services HTTP and SSL. The HTTP application proxy scans for virus, denies activeX controls and denies scripting languages. The SSL proxy is a TCP plug proxy that only monitors the state of the connection at the transport layer. The action permit allows the connection to the GIAC Web Site only.

Rule #2: Allows any Network to connect to the External Mail Server. The Service Mail enables the application proxy for SMTP traffic to scan for virus, configure Anti-Spam rules and supply Anti-Relay information. The only destination allowed is the External Mail Server.

Rule #3: Allows the Suppliers Network to connect to the Internal SSH Server to upload fortunes. The SSH Plug Proxy maintains the state of the connection. Suppliers are required to authenticate to the SSH Server.

Rule #4: Allows the External Mail Server to connect to any other mail server using the SMTP proxy described in rule #2.

Rule#5: Permits GE's employees to access the World Wide Web using the HTTP and SSL application proxies described in rule #1.

Rule #6: Allows the External DNS Server to do DNS queries to outside DNS Servers. The DNS plug proxy provides additional logging capabilities over packet-filtering rules. However, in terms of performance a packet filtering is faster.

Rule #7: Allow the Internal Mail Server to exchange e-mail with the External Mail Server. The SMTP proxy provides application level content scanning for virus. In addition the proxy provides the other elements described in rule #2.

Rule #8: Allow the Internal DNS Server to send DNS updates to the External DNS Server. This is done on UDP Port 53 using the UDP Plug Proxy. A plug proxy passes all traffic to the destination without inspection at the application layer. In addition, since the traffic is UDP state is not maintained.

Rule #9: Allow the Customer Web Site to query or update the Internal SQL Database. The SQL Server proxy is an application level proxy that can be configured for access control, authentication and logging.

Rule #10: Allow Systems on the Service Network access to the Syslog Server. Syslog messages will pass through the Firewall using Gauntlet's UDP Plug Proxy. Again, this proxy is not application aware.

Rule #11: Allows the Border Router's Internal Interface to send Syslog messages to the Syslog Server on the Internal Network using the UDP Plug Proxy. The rule allows a one-way connection with a handoff port of UDP 514.

Rule #12: Allows the Internal Network to manage servers on the Service Network using SSH. The SSH proxy is a TCP Plug proxy. The SSH Server requires authentication.

Rule #13 Allows the Service Network and Inside Router Interface to access the Network Time Server located on the Internal Network. A group called Outside-Trusted is configured with the network address of the Service Network and the Router's internal IP address. The NTP Plug Proxy passes ntp traffic on port UDP 123 through the firewall to and from the NTP Server.

Rule #14 Allows Firewall Managers to access the Firewall using Gauntlet's graphical user interface (GUI).

Gauntlet 6.0 is a Proxy Based Firewall. The main advantage of using proxies is increased security. However, proxies are not without their problems. The main problem is proxy firewalls are slower than packet filtering firewalls.

Load balancing or off loading to a dedicated proxy helps increase performance. Another concern with firewall proxies is each proxy opens a listening port on the firewall, leaving a potential entryway for an attacker.

VPN Security Policy

GE's will deploy two VPNs. A network-to-network VPN for International Business Partners and a client-to-network VPN for Mobile Users. The VPNs leverage the firewall for authentication and access control.

GE establishes an encrypted tunnel to its International Business Partner's Networks through a network-to-network VPN. The connection encrypts traffic from the GE firewall to its partners firewall. GE transmits it fortune cookie sayings to its partners for translation. The VPN connection allows for data origin authentication, data integrity checking and confidentiality through IPsec's Encapsulating Security Payload (ESP).

To set up a VPN connection using the Gauntlet 6.0 Firewall GUI a VPN Network Object is created. This object includes the source address of the Partner's external firewall interface and any networks behind it needing access to GE internal network. In addition, the IKE and IPSec policies, and the authentication method is established in the Network Object. The partner's access is limited by destination restrictions imposed by the firewall to the Internal SQL Server and Mail Server. Once inside the firewall the same firewall proxies used by GIAC Internal Employees provide access to Internet. A packet-filtering rule is created with the VPN Network Object as the source. This allows the remote network to access internal resources.

Once authentication using pre-shared secrets occurs. The Internet Key Exchange (IKE) Protocol establishes the IPSec Security Associations (SAs). IKE policies negotiate the hash, cipher, and Diffie-Hellman key size used to generate a secret key. The GE security policy requires a Message-Digest Algorithm (MD5) hash to authenticate the source. The encryption algorithm used must be 3DES and the Diffie-Hellman key size 1536 bit. Once both sides of the VPN agree on the negotiation parameters, the IPSec SA is created. Next, an agreement on IPSec Policies must be established between the two nodes. Policy requires the encapsulating Security Payload (ESP) be used. ESP provides data integrity and encryption. The one-way hash algorithm HMAC MD5 is required for data integrity and 3DES encryption strength must be used. The IPSec packet can now be securely transported using tunnel mode since security gateways are involved. ESP used in tunnel mode will hide the real source and destination IP's, although no protection is provided for the outer IP header.

To successfully establish a VPN connection both sides of the VPN must agree on IKE and IPSec policies. Multiple IPSec policies can be negotiated for a VPN connection. Multiple policies can cause a less secure policy to negotiated. To avoid this situation, GE Security policy only allows for strong encryption to be

used. In addition, all intermediary routers must allow UDP port 500 (IKE) and protocol 50 (ESP).

Part 3 – Verify the Firewall Policy

Planning the Audit

GE will perform an audit to verify the integrity of its firewall. After installing a firewall, or any other major changes to the network it is necessary to perform an audit to ensure enforcement of the corporate security policy. Auditing can spot vulnerabilities in our system before an attacker strikes. However, the goal of auditing is not stopping an attack, but minimizing damage if an attack occurs. Besides minimizing damage an audit can help show the normal behavior of the network.

The cost of an audit can vary greatly. If an outside contractor performs the audit the costs go up. It is generally a good idea to have an impartial third party perform the audit, however due to the high cost GE will perform the audit. The cost will be minimal. Two employees conduct the 6-hour audit. Freely available tools such as NMAP, WINDUMP and RAFALE X will be used. NMAP port scans hosts to determine what services are listening. RAFALE can craft packets and simulate attacks such as SYN floods. WINDUMP sniffs packets from the network. Additionally, an audit is not without risks. Firewall performance may suffer, a firewall crash could occur or an actual attacker may try to penetrate the network. To mitigate these risks, we will perform the audit during non-peak traffic hours, pay more attention to the firewall logs and have our disaster recovery plan at the ready. In addition, written permission from GE CEO will be needed to perform the audit.

The first step of a good audit is documenting the procedure. Our goal is to document specific procedures for the following areas:

1) Verify open ports on the firewall.
2) Verify legitimate traffic is passed
3) Verify unwanted traffic is blocked
4) Verify File System Integrity

Conducting the Audit

1. Verify Open Ports on the Firewall.

Open ports on our firewall are potentially exploitable communication channels. Since, Gauntlet is a proxy-based firewall, the proxy ports must be opened. GE Security Policy calls for the following tcp proxy ports to be opened: SSH TCP 22, SMTP TCP 25, HTTP TCP PORT 80, TCP 8004 for remote management.

To verify the open tcp ports we use the NMAP Command:

nmap -sS -P0 -p 1-65535 -O -v -T 3 -oN nmapsyn.txt 192.168.100.2

from an external network host of 10.0.0.5. This command scans the external firewall interface using SYN packets. If a SYN/ACK is received nmap knows that the port is listening. In addition, the –PO option prevents pings going to the firewall. This option is can be used against firewalls that block ICMP. However in our case the firewall is up so we don't need to ping it. The –p option is used to determine which ports to scan. The –O option does operating system detection using TCP/IP fingerprinting. The –T 3 option provides normal timing for the scan. The –oN stores the results into an output file called nmapsyn.txt.

Here are the results of the scan:

```
nmap (V. 3.00) scan initiated Sat Mar 22 06:51:12 2003 as: nmap -sS -P0 -p 1-65535 -O
-v -T 3 -oN nmapsyn.txt 192.168.100.2
Interesting ports on  (192.168.100.2):
(The 65528 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
22/tcp     open        ssh
25/tcp     open        smtp
80/tcp     open        http
111/tcp    open        sunrpc
113/tcp    open        auth
8004/tcp   open        unknown
Remote operating system guess: Solaris 8 early access beta through actual release
Uptime 3.966 days (since Tue Mar 18 08:17:38 2003)
```

The results show two additional ports 111/tcp and 113/tcp that are not defined in the security policy. We must disable these ports using Gauntlet's local filtering rules.

The following log statement is from /var/log/messages on the firewall host:

Mar 22 23:02:49 sunfire.fw.sienoc.spawar.navy.smil.mil gfw: [ID 702911 kern.info] securityalert: tcp if=dmfe0 from 10.0.0.5:58833 to 192.168.100.5 on unserved port 7967

This statement shows the source IP of the nmap scanner system is being logged. It also provides evidence that our firewall is alerting when a packet tries to access an unopened port on the firewall.

The following packet was captured using Windump –Xx during the above Nmap Syn Scan, This option turns on the hex and ASCII packet display options.

```
07:04:05.067993 192.168.0.1.32788 > 192.168.0.20.514:  udp 132 (DF)
0x0000          4500 00a0 0ef0 4000 ff11 eaf6 c0a8 0001      E.....@.........
0x0010          c0a8 0014 8014 0202 008c 0cfb 3c36 3e4d      ............<6>M
0x0020          6172 2032 3220 3232 3a35 343a 3338 2067      ar.22.22:54:38.g
0x0030          6677 3a20 5b49 4420 3730 3239 3131 206b      fw:.[ID.702911.k
0x0040          6572 6e2e 696e 666f 5d20 7365 6375 7269      ern.info].securi
0x0050          7479                                         ty
```

The above capture verifies that udp traffic from 192.168.0.1 (Firewall Internal Interface) is being sent to 192.168.0.20 (Syslog Server) on port 514 (Syslog). The ASCII text indicates a security message.

The following nmap command verifies the state of our firewall's UDP ports:

nmap –sU –PO –p 1-65535 -v –T 3 –oN "c:\nmap.txt" 192.168.100.2

This command relies on receiving an ICMP unreachable message to determine the state of the port. The port is closed if an ICMP Unreachable message is received otherwise it is reported as open. The –v option shows output in verbose mode. The other options are the same as the TCP Syn scan above. O.S. detection is not performed this time.

Here are the results of the UDP Port Scan:

```
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Host  (192.168.100.2) appears to be up ... good.
Initiating UDP Scan against  (192.168.100.2)
Too many drops ... increasing senddelay to 50000
The UDP Scan took 6608 seconds to scan 65535 ports.
Adding open port 111/udp
Adding open port 514/udp
Adding open port 123/udp
Adding open port 53/udp
Adding open port 32788/udp
Adding open port 32775/udp
Interesting ports on  (192.168.100.5):
(The 65529 ports scanned but not shown below are in state: closed)
Port       State       Service
53/udp     open        domain
```

```
111/udp    open       sunrpc
123/udp    open       ntp
514/udp    open       syslog
32775/udp  open       sometimes-rpc14
32788/udp  open       unknown
Nmap run completed -- 1 IP address (1 host up) scanned
```

The results show UDP 53, 123 and 514 are open services. These ports are acceptable to GE security policy, however ports 111, 32775 and 32788 are not acceptable. These ports must be investigated and shut off on the firewall.

The following log is taken from /var/log/messages on the firewall. It shows one log entry indicating that the firewall is alerting when an external source tries to access a closed port In fact, there were thousands of such entries. This indicates Nmap UDP Scan is easily detected by our firewall.

Mar 23 00:02:04 sunfire.fw.sienoc.spawar.navy.smil.mil gfw: [ID 702911 kern.info] securityalert: udp if=dmfe0 from 10.0.0.5:57960 to 192.168.100.5 on unserved port 42906

The following packet was captured from the firewall host using the snoop command. Snoop is used to capture packets on a Solaris System.

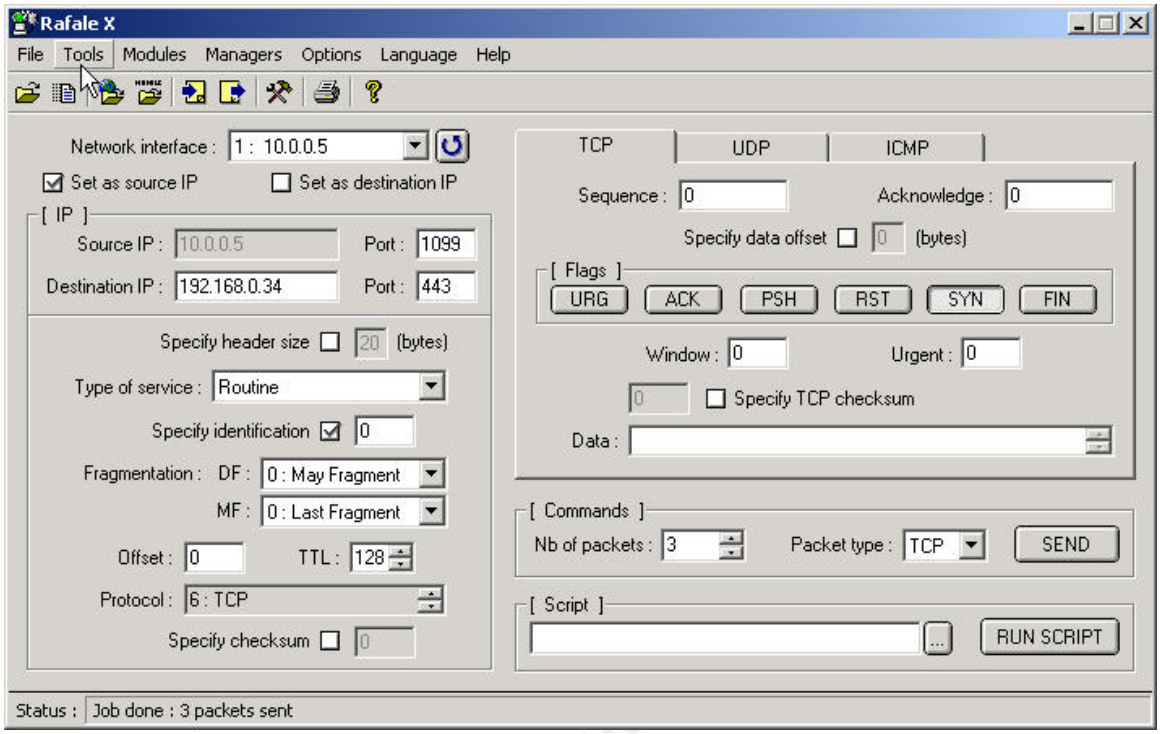
10.0.0.5 -> sunfire UDP D=51908 S=57960 LEN=8
sunfire -> 10.0.0.5 ICMP Destination unreachable (UDP port 51908 unreachable)

This packet shows the ICMP Destination Unreachable Message generated by Nmap to determine which UDP Ports are opened. GE Security Policy prohibits these types of packets at the border router. This helps prevent others from mapping our network using tools such as Nmap.

2) Verify Legitimate Traffic is Passed

Rafale X can be used to verify the firewall policy. By crafting packets that match our policies, we can verify where the traffic goes. In addition, WINDUMP displays the crafted packet at the destination host. The firewall logs can be checked also. The following procedure checks firewall Rule #1 which is to allow GE's Customers access to the GE's Customer Web Site.

First, enter the information in the Rafale X GUI:



The firewall policy states the source can by any host. The source address is the machine executing RAFALE, an external network address. We enter the destination IP 192.168.0.14 (Web Server) and port 443 (SSL). We set the syn bit in the flags field of the TCP Header. Then the packet is sent on its way. The following firewall entry in /var/log/messages shows the firewall allowed the packet to pass through to port 443 on 192.168.0.34.

Mar 26 01:52:28 sunfire gfw: [ID 702911 kern.info] permit-forward (40 bytes): TCP(2) if=dmfe0 srcaddr=10.0.0.5 srcport=1099 dstaddr=192.168.0.34 dstport=443

The following WINDUMP Output shows the syn packet arriving at the GE Web Server on PORT 443. In addition, line 2 indicates the acknowledgement of the packet.

10:01:41.111459 10.0.0.5.1099 > 192.168.0.34.443: S 0:0(0) win 0
10:01:41.111590 192.168.0.34.443 > 10.0.0.5.1099: S 4035168858:4035168858(0) ack 1 win 16616 <mss 1460> (DF)

The complete firewall rule set should be verified using the above procedure.

3) Verify Unwanted Traffic is Blocked

Gauntlet 6.0 claims to provide built-in protection against IP Spoofing Attacks. We test this claim using Rafale X. This windows application allows the user to build custom TCP, UDP and ICMP packets. It allows modification of the source IP of an external host to check the firewall for IP Spoofing Attacks. First we test the external interface of the firewall (192.168.100.2) with a spoofed IP Address 0f 192.168.0.15.

windump –xX displays the Rafale X crafted source IP packet . The Source IP of an external system is set to internal IP 192.168..0.15. The source and destination ports are set to 22 in the crafted packet. Port 22 (SSH) is used as the destination port because our firewall has an active SSH Proxy. The packet is directed to the external firewall interface. Here is the windump output of that packet on the "attacker" system.

```
12:02:04.414102 IP 192.168.0.15.22 > 192.168.100.2.22: .    win 0
0x0000          4500 0028 1b7a 0000 8006 39f1 c0a8 000f     E..(.z....9.....
0x0010          c0a8 6405 0016 0016 0000 0000 0000 0000     ..d.............
0x0020          5000 0000 ca53 0000                          P....S..
```

The spoofed packet generated the following firewall log entry:
Mar 23 03:51:31 sunfire gfw: [ID 702911 kern.info] securityalert: source not allowed on interface: TCP(0) if=dmfe0 srcaddr=192.168.0.15 srcport=22 dstaddr=192.168.100.2 dstport=22

This backs up Gauntlet's claim. The packet was blocked and an alert established. The Internal and Service Network interface should be verified using the above procedure.

Another kind of prohibited traffic is ICMP. We need to verify that external hosts cannot send ICMP echo requests through the firewall.

External host sends ICMP Echo Request Packets to an Internal Host. The following is a Windump capture on the external host.

```
13:26:26.765252 IP 10.0.0.5 > 192.168.0.15: icmp 40: echo request seq 51456
13:26:26.765309 IP 10.0.0.5 > 192.168.0.15: icmp 40: echo request seq 51456
13:26:27.894726 IP 10.0.0.5 > 192.168.0.15: icmp 40: echo request seq 51712
13:26:27.894789 IP 10.0.0.5 > 192.168.0.15: icmp 40: echo request seq 51712
13:26:28.896035 IP 10.0.0.5 > 192.168.0.15: icmp 40: echo request seq 51968
13:26:28.896105 IP 10.0.0.5 > 192.168.0.15: icmp 40: echo request seq 51968
```

Notice no echo replies packets received by the external host. The following firewall log confirms that ICMP packets are blocked by the firewall.

Mar 26 05:16:01 sunfire gfw: [ID 702911 kern.info] securityalert: packet denied by forward screen: ICMP(8/0) if=dmfe0 srcaddr=10.0.0.5 dstaddr=192.168.0.15

Due to budget and time constraints a limited number of packet combinations were checked.

4) Verify File System Integrity

After verifying the firewall policy, checking the file system for tampering provides an extra level of protection. Gauntlet 6.0 provides built-in facilities for verifying the integrity of the file system. The first step is creating a database of encrypted checksums for most system files. This database is the baseline. It is compared to future versions to determine if files have been modified. The security policy dictates how often an integrity check should be performed. GE performs an integrity check every audit or when the firewall displays abnormal behavior. The following file on the firewall (/usr/local/etc/checksums/localize.sum) shows any file changes since our last database update.

#version local (Thu Mar 27 08:12:39 2003)
#origin X the unknown@sunfire
#created 1048723959

f 0 0 100644 F6DB735722DB1A677B639BEDDCBCC2FD
/usr/local/etc/checksums/gauntlet.sum
f 0 0 100644 092E60539E734489B96A5B4239E936D0
/usr/local/etc/mgmt/gauntlet.saved
f 0 1 100644 092E60539E734489B96A5B4239E936D0 /usr/local/etc/mgmt/gauntlet.conf
f 0 0 100644 3CB83CF3FC8D0E79F8CAE3122C492D38 /usr/local/etc/mgmt/gcsaved.0
f 0 0 100644 2E7681B443D7CE42164000B6D8EF6C1E /usr/local/etc/mgmt/gcsaved.1
f 0 0 100644 282209297491406EBF3EE0C81E2E6A2F /usr/local/etc/mgmt/gcsaved.2
f 0 0 100644 7853173A213A239A27385D609D6F7AA3 /usr/local/etc/mgmt/gcsaved.3
f 0 0 100644 4997DDCE99219B084B3197AF80E26491 /usr/local/etc/mgmt/gcsaved.28
f 0 0 100644 BE97479B3C40F84FF5E9B364578FC41F /usr/local/etc/mgmt/gcsaved.4
f 0 0 100644 307A21EC564329ABEEDD38C9FC98FD01 /usr/local/etc/mgmt/gcsaved.5
f 0 0 100644 A4D155093CED8AE61FCB7D6C3A3835D0
/usr/local/etc/mgmt/gcsaved.6
f 0 0 100644 04F55D68BF821E6D92954A301D97937D /usr/local/etc/mgmt/gcsaved.7
f 0 0 100644 8E81D6CC8E9CF422328C50B216401049 /usr/local/etc/mgmt/gcsaved.8
f 0 0 100644 61974A09EA46C3D1EB383D95E7AF880E /usr/local/etc/mgmt/gcsaved.9
f 0 0 100644 D16CDCD375ADA8D65946A09F6F2476A4
/usr/local/etc/mgmt/gcsaved.10
f 0 0 100644 1B8C88A1A1F645347119418B3DF32623 /usr/local/etc/mgmt/gcsaved.11

f 0 0 100644 9DD2F4AE38120BBD26040FD716589D8A
/usr/local/etc/mgmt/gcsaved.12
f 0 0 100644 CD47D3BC3E76E9EA5AA35985F9C175F3
/usr/local/etc/mgmt/gcsaved.13
f 0 0 100644 E0E10712B0DAC38B28EC06717373B5D7 /usr/local/etc/mgmt/gcsaved.14
f 0 0 100644 585EA893D99E7394708DC6D7280680F5 /usr/local/etc/mgmt/gcsaved.15
f 0 0 100644 30AF061A2E6FE0EEFAE72CE754976899 /usr/local/etc/mgmt/gcsaved.16
f 0 0 100644 BAE849E67ED089A78D00F6C5DA5E8C55
/usr/local/etc/mgmt/gcsaved.17
f 0 0 100644 443689A57F4D44D463EF753E728CEFAE /usr/local/etc/mgmt/gcsaved.18
f 0 0 100644 72E26EF993A7512F2BFCB98E4F69ED4F /usr/local/etc/mgmt/gcsaved.19
f 0 0 100644 6349F5B4CB4E765CD2FBC369F6DE67E8
/usr/local/etc/mgmt/gcsaved.20
f 0 0 100644 56B4DFE574AFEE7D7DD08F1B38DD134F
/usr/local/etc/mgmt/gcsaved.21
f 0 0 100644 BDE369301303E82EA7E7C58FA7FBE30E
/usr/local/etc/mgmt/gcsaved.22
f 0 0 100644 02902CE05C223F87AFD2A747F578434C /usr/local/etc/mgmt/gcsaved.23
f 0 0 100644 E8FDEF176270555A686322011DE575CD /usr/local/etc/mgmt/gcsaved.24
f 0 1 100644 8F3760920F389CC051622EA38C553833 /usr/local/etc/mgmt/gcsaved.25
f 0 1 100644 6C14516951F3B094814BC093CD3ACC2A /usr/local/etc/mgmt/gcsaved.26
f 0 1 100644 7CE46E123EFAE235A3845194C93661C5 /usr/local/etc/mgmt/gcsaved.27
f 0 0 100644 9A2E70F193730E014494E651A0691524 /usr/local/etc/mgmt/gcsaved.29
f 0 0 100644 461F98AE11691803DF46BB71E95237F0 /usr/local/etc/mgmt/gcsaved.30
f 0 1 100600 21D14CE4FEC0F58330C995D9318112C5 /usr/local/etc/fw-authdb.db

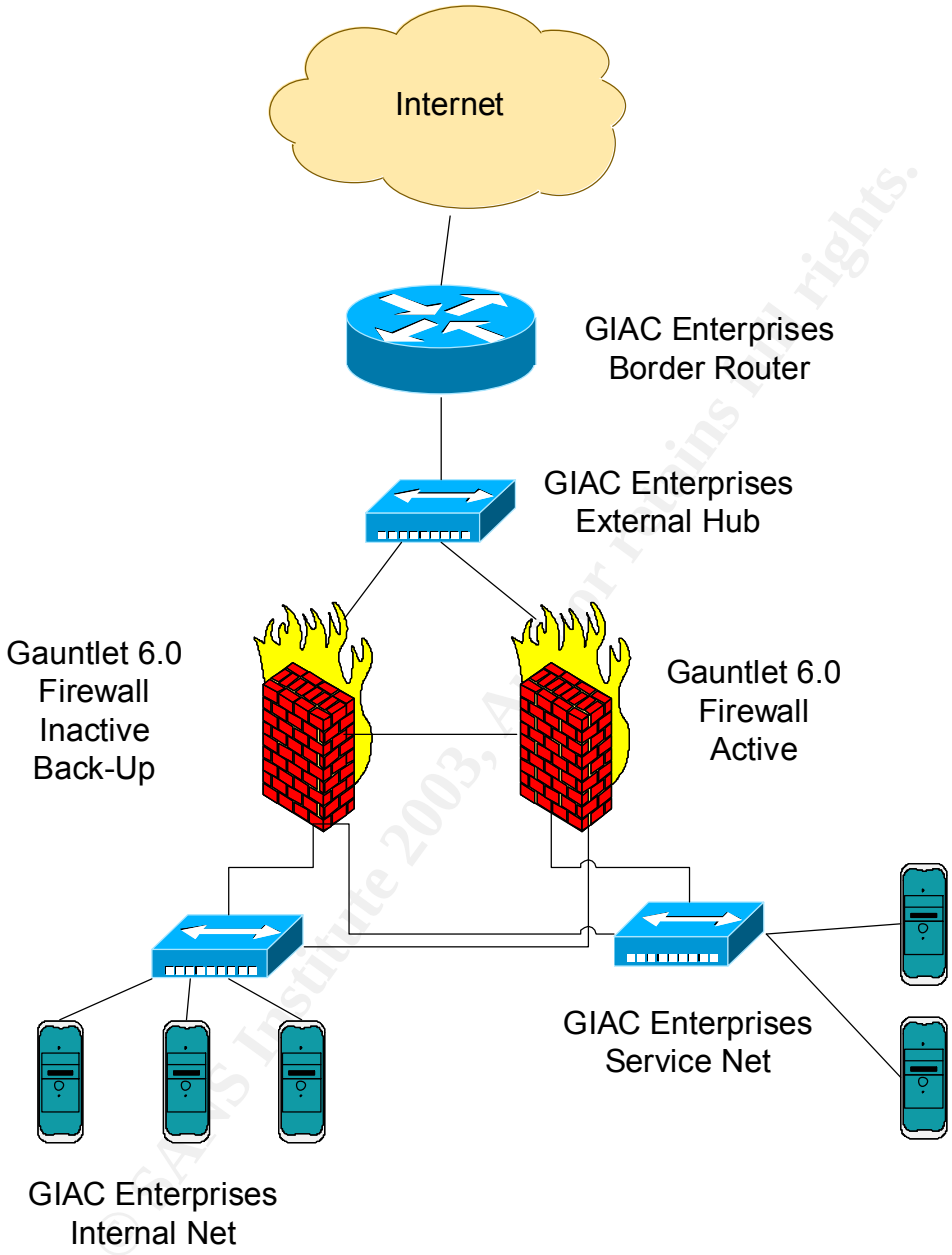
The file shows the cryptographic hash of all files that have changed since the last audit. Investigation shows no critical system files were modified.

Results of the Audit

Before presenting the results of the audit, GE ensures all signs of auditing are removed from the network, including auditing tools such as Nmap. The results were favorable. However, port scanning revealed open ports that need to be examined and closed if not needed. An investigation to determine if this was caused by an attack is already underway. Normal traffic behavior seems to pass through the firewall properly. Unwanted traffic, such as ICMP is being blocked. No critical system files were compromised.

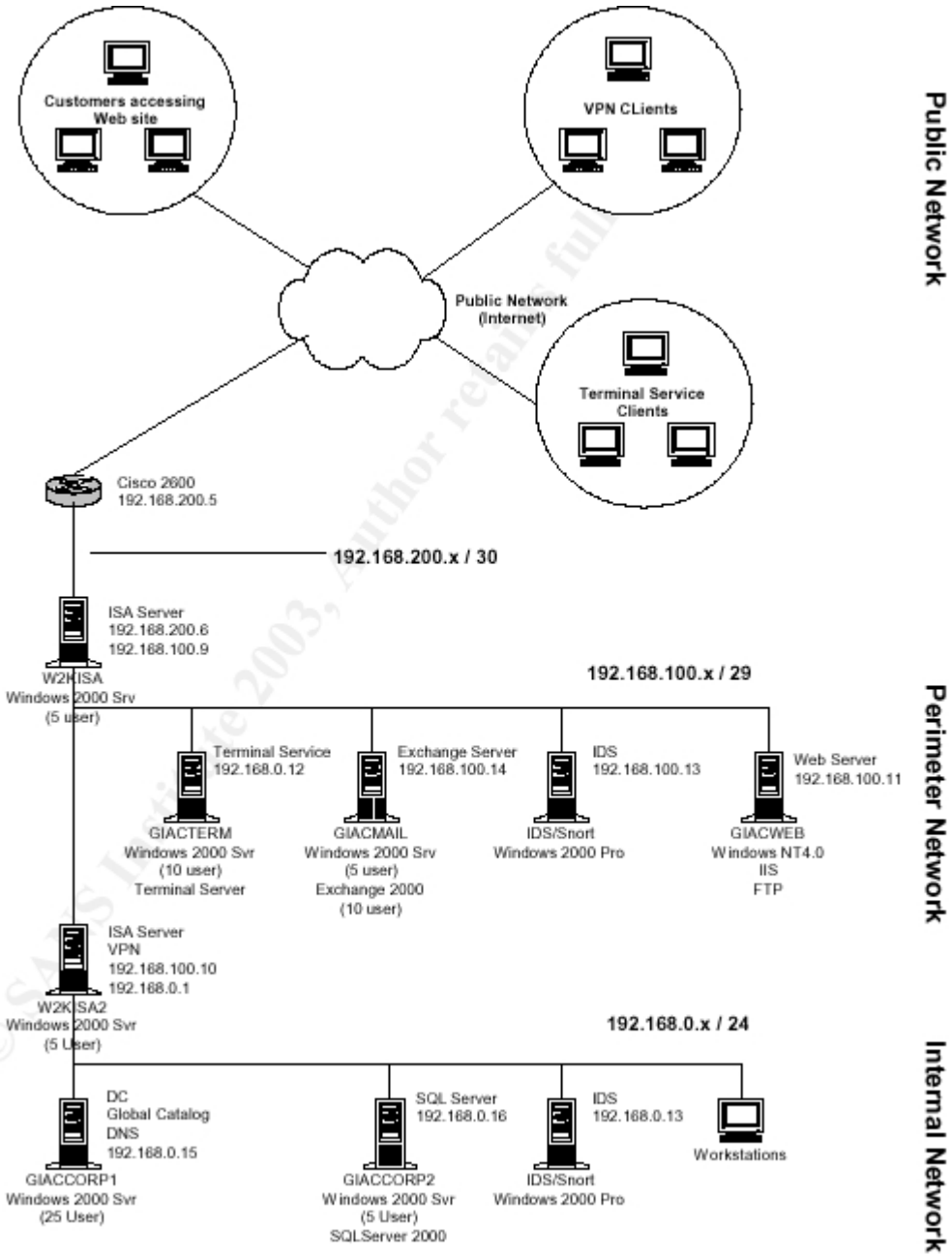
Although favorable, the audit exposed weaknesses in our network. The main weakness is the Internet Service Provider (ISP) Link, Border Router and Firewall represent a single point of failure in GE Network. A Denial of Service Attack (DOS) against any of the above would put GE out of business until the attack stops. Therefore, it is recommended to purchase as much bandwidth as possible

from the ISP. Also, Gauntlet provides the option to configure a “fail over” firewall. If the active firewall goes down, the back up automatically comes on-line. The following diagram illustrates this recommended configuration.



Part 4 – Design Under Fire

Robert Alley, analyst number 0360 posted the following network diagram at http://www.giac.org/practical/GCFW/Robert_Alley_GCFW.pdf.



This section presents an attack against the firewall, a distributed denial of service attack and an attack against an internal host from the above network architecture diagram. In addition, this section presents countermeasures against such attacks.

An Attack against the Firewall

The first step is to gather information about GIAC Enterprises. The Internic Domain Registration site located at http://www-whois.internic.net/whois.html reveals publicly available information about GIAC.ORG. This information is useful for deploying a social engineering attack. In addition, the host names of organization's domain servers are listed. This information used with the O.S. command "nslookup" reveals the IP addresses for the domain name servers for GE. Another website, http://www.arin.net/whois can be used to obtain a range of IP's for a particular organization. This information along with the O.S. tool traceroute can determine the IP's of the external router and firewall. Once the IP is known, Nmap can be used for port scanning and O.S. fingerprinting. Nmap sees that port 53 (DNS) is open and the operating system is windows 2000. Checking other ports from the Nmap Scan reveals that this system is running Internet Security and Acceleration (ISA) Server. ISA Server inspects, blocks, redirects or modifies data as it passes through the firewall. A search of Microsoft's Tech Net Site finds Microsoft Security Bulletin MS03-009 at http://www.microsoft.com/security/security_bulletins/ms03-009.asp . The bulletin states that a flaw In ISA Server DNS Intrusion Detection Filter Can Cause Denial Of Service. The following technical description from Microsoft is located at http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS03-009.asp.

Technical description:

"Microsoft Internet Security and Acceleration (ISA) Server 2000 contains the ability to apply application filters to incoming traffic. Application filters allow ISA Server to analyze a data stream for a particular application and provide application-specific processing including inspecting, screening or blocking, redirecting, or modifying the data as it passes through the firewall. This mechanism is used to protect against invalid URLs which may indicate attempted attacks as well as attacks against internal Domain Name Service (DNS) Servers.

A flaw exists in the ISA Server DNS intrusion detection application filter, and results because the filter does not properly handle a specific type of request when scanning incoming DNS requests.

An attacker could exploit the vulnerability by sending a specially formed request to an ISA Server computer that is publishing a DNS server, which could then result in a denial of service to the published DNS server. DNS requests arriving at the ISA Server would be stopped at the firewall, and not passed through to the internal DNS server. All other ISA Server functionality would be unaffected."

In other words the ISA Intrusion Detection System causes a denial of service attack under "certain specific circumstances". This may be a good time to point out it may be better to install a security solution from a company that specializes in security rather than a large multi-product corporation. No exploits have been published at this time. However, the flaw causes the DNS Intrusion Detection Filters to stop responding to DNS Requests. The Denial of Service Attack ends when the ISA Server is rebooted. The exploit for this specific DNS attack requires that the attacker send a crafted packet to an internal DNS Server. The firewall intercepts this malicious packet and performs inspection at the application layer. The malformed data in the application layer causes the Intrusion Detection System to malfunction, thus causing the denial of service attack. The countermeasure for this attack is to installed the patch located at http://www.microsoft.com/downloads/details.aspx?FamilyID=f62127c5-51e3-4b34-a6d3-b9cf840358bd&DisplayLang=en.

Distributed Denial of Service Attack (DDOS)

The next attack involves the compromise of 50 cable/DSL modem systems by installing Tribal Flood Network 2000 (TFN2K) daemon. TFN2K allows a master system to communicate with multiple daemon systems to direct a DDOS attack at a specific target. An analysis for TFN2K is posted at http://www.securiteam.com/securitynews/5YP0G000FS.html

Nmap reconnaissance with O.S detection provides a listing of active hosts vulnerable port open to a specific type of attack. To make the job easier, those systems that reveal the greatest number of vulnerabilities will be used as TFN2K agents. Once our 50-cable/DSL systems are compromised with the TFN2K daemon. The compromised systems will act as "zombies" awaiting instructions from the TFN2K master. On the TFN2K master the following command executes the TFN2K DDOS attack against GE network.

```
#. /tfn –f hostlist –c8 –l 192.168.200.6
```

The hostlist contains the list of TFN2K agents. The –c8 indicates a mixed UDP, TCP/SYN and ICMP/PING flood attack by the agents. Another type of flood attack TFN2K can use is ICMP/SMURF. The target network needs to protect against the above 4 types of attacks plus protect itself against being used as a TFN2K agent site.

The TFN2K master uses unidirectional, random and encrypted TCP, UDP and ICMP packets to communicate with the agents. Unsolicited Echo Reply packets could be blocked at the border router. However, 2/3's of the communication to the agents still makes it through. The best practice is not allowing your network to be compromised in the first place.

To prevent becoming a TFN2K agent or victim site the following procedures are recommended.

1) Install the latest security related patches to the O.S. and applications.
2) Block IP Spoofing at the ingress filter. Prevent spoofed traffic from exiting your network.
3) Block unwanted services and protocols from leaving your network. Don't let an attacker use ftp to get his tools.
4) Provide multiple connections to the Internet in case traffic needs to be re-routed. Increase Bandwidth.
5) Install Intrusion Detection Systems.
6) Have your ISP Block Attacking IP Addresses.
7) Use Scanning Tools. The following tool "**find_ddos 4.2-1"** can be used to determine if TFN2K is on your system.

Attack against an Internal System through the Perimeter System.

Our target is the GIAC Web Server. It was chosen because it is easily accessible from the Internet and always online.

First Nmap with O.S. Detection is executed.

```
# nmap (V. 3.00) scan initiated Fri Apr 04 15:52:31 2003 as: nmap -sS -PT -PI -O
-T 3 -oN C:\webnmap.log 192.168.100.11
Interesting ports on otht.nosc.mil (128.49.28.40):
(The 1591 ports scanned but not shown below are in state: closed)
Port       State       Service
80/tcp     open        http
443/tcp    open        https
445/tcp    open        microsoft-ds
1025/tcp   open        NFS-or-IIS
Remote operating system guess: Windows Millennium Edition (Me), Win 2000, or
WinXP
```

The above Nmap Scan tells us the Operating System is Windows and web services are running. The most common type of web server for Windows is Internet Information Server (IIS) 5.0. Instead of scanning all TCP ports, a SYN Stealth Scan using Port 80 only is less likely to set off alarms.

To confirm that the web server is running IIS the following command is performed.

telnet www.giac.org 80
and issue GET / HTTP\1.1 and hit enter

The following output reveals the Web Server is IIS 5.0.

```
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Content-Type: text/html
Content-Length: 87
<html><head><title>Error</title></head><body>The parameter is incorrect.
</body>
</html>
Connection to host lost.
```

This information cannot be completely trusted because the administrator can alter it.

A quick search of the Microsoft Web Site indicates numerous vulnerabilities for IIS 5.0. In addition, http://www.guninski.com/iisasp.html lists exploit code for a Microsoft Patch. That's right, if IIS 5.0 patch Q277873 is installed it is possible to execute arbitrary programs on the Web Server. This is the reason all patches should be tested before put into production. An e-mail spoofing attack is used to increase the odds that this patch is installed. However, a bit of social engineering is needed first to determine the e-mail address of the Web Administrator and the boss. We can call, visit or view the company's website to acquire this information.

To start the e-mail spoofing attack telnet to a mail server on port 25 and enter the following commands:

```
220 MailServer.org ESMTP service (Netscape Messaging Service 4.15 Patch 2
(Built May 30 2000))
mail from: yourboss@GIAC.org
250 Sender <yourboss@GIAC.ORG>
rcpt to: webadmin@GIAC.org
250 Recipient webadmin@GIAC.ORG
data
354 OK Send data ending with <CRLF>.<CRLF>
Install the following patch from Microsoft Q277873. Keep up the good work! Your
Boss.
250 Message received: HCW79J00.8WS
```

Most newer e-mail programs validate that the recipient's domain is in the same domain as the mail server. This prevents the above email-relaying spoofing attack.

Once the vulnerable patch is installed, exploitation takes place through the attacker's web browser.

The following URL typed in the browser provides a directory listing of files from the C drive.

http://www.giac.org/scripts/georgi.bat/..%C1%9C..%C1%9C..%C1%9Cwinnt/system32/cmd.exe?/c%20dir%20C:\

This attack occurs because of the way unpatched versions of IIS decode special characters. To minimize the risks, the following can be done.

1) Removing virtual directories in the Internet Services Manager.
2) Installing the web application on a separate partition.
3) Restricting permissions on cmd.exe.
4) Install the following Microsoft IIS cumulative patch for IIS 5.0: http://www.microsoft.com/windows2000/downloads/critical/q293826/default.asp.

In addition, Microsoft has removed Patch Q277873 from its website.

Best practices posted on Microsoft IIS Website if followed can prevent this type of attack. The following link is a security checklist for IIS. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/iis/tips/iis5chk.asp.

References:

Sans Institute. Track 2 –Firewalls, Perimeter Protection and VPNs 2.1 TCP/IP for Firewalls. 2002.

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

Sans Institute. Track 2 –Firewalls, Perimeter Protection and VPNs 2.3 Firewalls 102: Perimeter Protection and Defense In-Depth. 2002.

Sans Institute. Track 2 –Firewalls, Perimeter Protection and VPNs 2.4 VPNs and Remote Access. 2002.

Sans Institute. Track 2 –Firewalls, Perimeter Protection and VPNs 2.5 Network Design and Performance. 2002.

Howard, Michael. Designing Secure Web-Based Applications. Redmond: Microsoft Press, 2000.

Scambray, Joel. Hacking Exposed Second Edition. Berkeley: Osborne/McGraw-Hill, 2001.

Network Associates. Gauntlet Firewall Administrators Guide. Santa Clara: Networks Associates Technology, Inc., 2001

Network Associates. Gauntlet Firewall Services Guide. Santa Clara: Networks Associates Technology, Inc., 2001

Cole, Eric. Hackers Beware. Indianapolis: New Riders, 2001.

Numerous Authors. "Router Security Configuration Guide Ver. 1.1". Sept. 27, 2002 URL:http://acs1.conxion.com/cisco/download.htm (10 Feb. 2003).

Guninski, Georgi. "Security Advisory #30". Nov. 27, 2000. URL: http://www.guninski.com/iisasp.html . (March 17, 2003).

Barlow, Jason. "TFN2K-An Analysis." February 10, 2000. URL:http://security-archive.merton.ox.ac.uk/bugtraq-200002/0191.html (March 15, 2003).

Microsoft Technet. "Microsoft Security Bulletin MS03-009 – flaw in ISA Server DNS Intrusion Detection Filter Can Cause Denial of Service. (331065)." March 19, 2003. URL:http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-009.asp (March 23, 2003).

"WinDump Manual" March 14, 2002. URL: http://windump.polito.it/docs/manual.htm (21 Feb. 2002).
Wolfgang, Mark. "Host Discovery with nmap" November 2002. URL: http://moonpie.org/writings/discovery.pdf (5 March, 2003).

CERT/CC, "CERT Advisory CA-1999-17 Denial of Service" March 3, 2000. URL: HTTP: http://www.cert.org/advisories/CA-1999-17.html (March 7, 2003).

Graesser, Dana. "Cisco Router Hardening Step-by-Step" July 25, 2001. URL:http://rr.sans.org/firewall/router2.php. (Feb 22, 2003).

"Nmap network security scanner man page" URL: http://www.insecure.org/nmap/data/nmap_manpage.html (Feb. 6, 2003).

"Rafale X / Help." URL:http://packx.net/packx/html/en/rafalex/help.htm (Feb, 4, 2003).

Secure Computing. "White Paper: Distributed Denial of Service Attacks: Analysis and Partial Solutions". March 2000. URL: http://www.securecomputing.com/pdf/ddos_wp.pdf. (March 3, 2003).

Secure Computing. "White Paper: An Overview of Virtual Private Networks (VPNs)". March 2000. URL: http://www.securecomputing.com/pdf/wp_vpn.pdf. (Feb 4, 2003).