Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

GCFW Practical Assignment
Version 1.5b

SANS Security 2001

New Orleans, LA

Mason Richardson

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Assignment 1 – Security Architecture 3
GIAC Network Diagram 4
Security principles 5
Diagram Explanatory Text 6
Perimeter router 6
Perimeter Firewall 6
Server Systems 7
GIAC Main Firewall 7
GIAC Network 8
GIAC Internal Firewall 8
Customer Access 8
Supplier Access 8
Partner Access 9
Assignment 2 – Security Policy 10
Border Router Policy 11
GIAC Perimeter Firewall Configuration 15
GIAC Firewall (Proxy) Configuration 18
HTTP Setup 19
FTP Setup 20
SMTP Setup 20
DNS Setup 20
Remote Management Setup 21
VPN configuration (supplier) 21
VPN configuration (partner) 23
Assignment 3 - Audit Your Security Architecture 26
Plan the assessment 27
Assignment 4 - Design Under Fire 32
Firewall Attack 34
If either of these attacks work you can get the passwords in the results file. 35
Denial-Of-Service Attack 35
Internal System Attack 35
References: 37

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Assignment 1 – Security Architecture

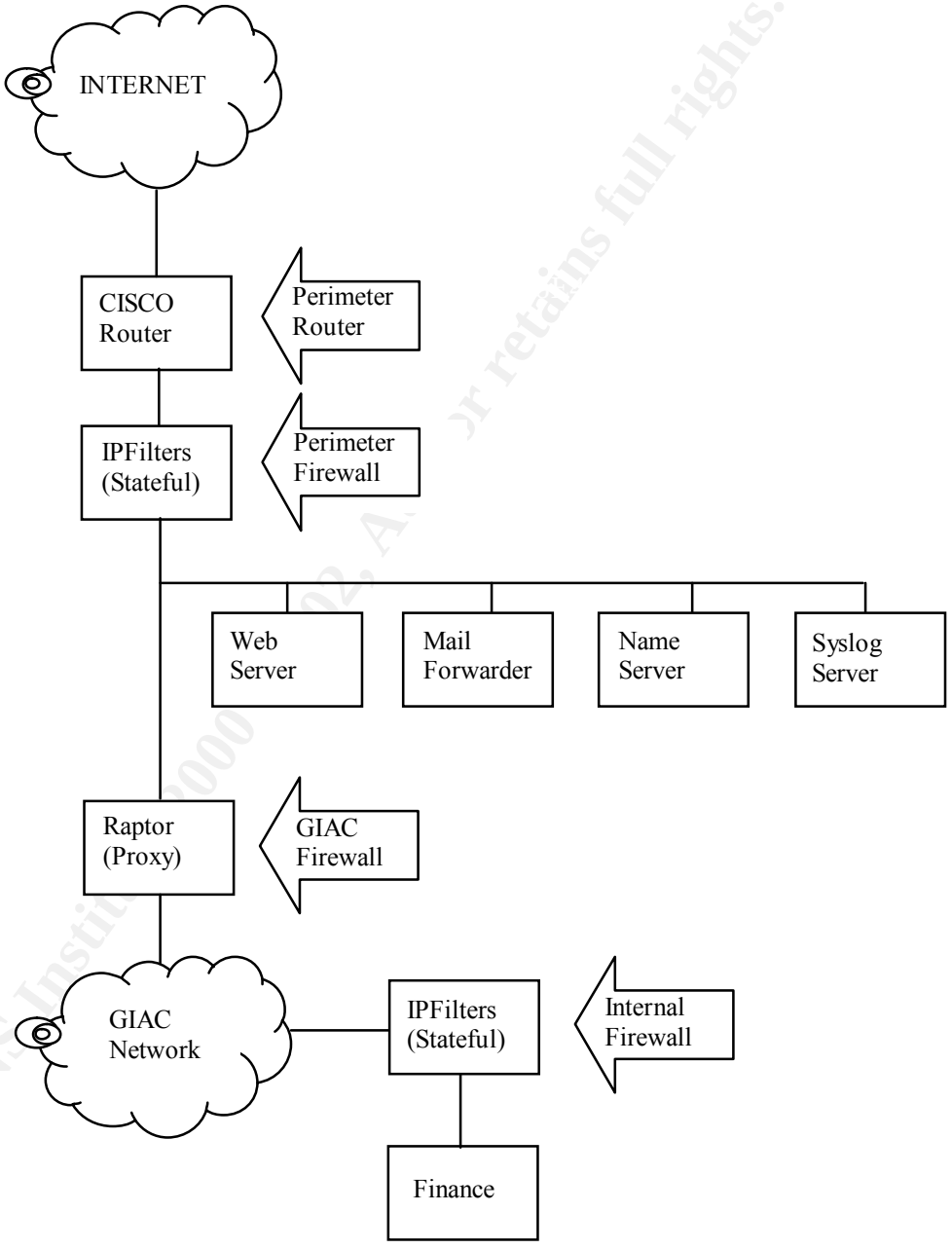
Define a security architecture for GIAC Enterprises, a growing Internet startup that expects to earn $200 million per year in online sales of fortune cookie sayings, and which has just completed a merger/acquisition. Your architecture must specify filtering routers, VPNs to partners, secure remote access, and internal firewalls. Be explicit about the brand and version of each perimeter defense component. Produce a diagram or set of diagrams with explanatory text that define how to use perimeter technologies to implement your security architecture.

You must consider and define access for:
Customers (the companies that purchase bulk online fortunes);
Suppliers (the authors of fortune cookie sayings that connect to supply fortunes);
Partners (the international partners that translate and resell fortunes).

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

GIAC Network Diagram



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Security principles

- All GIAC information security is driven by the GIAC corporate security policy. The above network security diagram is the implementation of the pertinent components of the policy which includes:
  - GIAC systems and information are strategic and vital assets. These assets require a degree of protection commensurate with their value.
  - Access to GIAC systems and information must be strictly controlled.
  - Risks to information resources must be managed. The expense of security safeguards must be appropriate to the value of the assets being protected.
  - The integrity of the data, its source, destination, and processing must be assured. The use, modification, and distribution of the data must be made only in authorized acceptable ways.
  - Administrative reviews of system logs must be made regularly and often to enable swift discovery and handling of mistakes, abuse, and intrusion attempts.
  - Physical access to all systems must be commensurate with the highest level of data residing on that system. [1]

- Security is employed in layers – also called "defense in depth". Similar to locking up your house, installing an alarm system, and a hungry pit bull, defense in depth emphasizes layers of security each having some type of logging and alerting to notify security personnel of a possible compromise of any layer.

- Keep It Simple & Straightforward (KISS) – The KISS principle is important to minimize complexity and possible confusion in security components. An example of this principle is minimizing interfaces in each of the firewalls. The author has seen firewall-rule-spaghetti in firewalls having four or more interfaces.

- A corollary of the previous principle is that each system should have only one function. This enables the communications to be limited to specific protocols and ports and allows the system to be hardened more effectively.

- The GIAC network systems will use private IP addresses (RFC 1918) and these addresses will be translated into Internet routable addresses at the firewall.

- Where possible the GIAC network will limit the information provided about systems, the network, and services. Examples of this include registering only required DNS hosts and dropping packets rather than responding that the service is not provided.

- New vulnerability announcements will be reviewed daily. Security patches, hotfixes, and service packs will be placed on Internet connected systems (service net and firewalls) as soon as reasonably possible to prevent compromise.

[1] Policy components extracted from Chris Brenton's "FUBAR's Computer User Policy"

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Diagram Explanatory Text

Perimeter router

System Configuration:

- Cisco 7204, running IOS 12.1

This router provides the initial screen for traffic coming into GIAC's external network. Although this router is blocking certain types of traffic the primary function of the router is still to route traffic. The light screening that is performed by this perimeter router reduces the load from the perimeter firewall by denying private Internet addresses, controlling ICMP traffic, and blocking protocols not used on GIAC's external network such as Netbios and Ident. In addition to decreasing the perimeter firewall processing, this screening also minimizes the entries in the firewall logs.

Perimeter Firewall

System Configuration:

- OpenBSD 2.8, Intel Pentium 3 800mghz, IPfilters ver 3.4.16

This perimeter firewall is used to filter traffic coming to the server network and to GIAC's main firewall. For example, only web traffic is permitted to go to the web server, mail to the mail forwarder, etc. This traffic filtering process protects the servers from attacks on ports other than the intended service port.

This firewall is a robust Intel based system with two network interfaces running OpenBSD as an operating system. OpenBSD is a freeware Unix operating system that was written with security as its primary goal.

This firewall is configured as a bridge so that it has no IP address. In fact it is invisible to people on the network which makes it very hard to attack. The downside of not having an IP address is that firewall configuration can only be done on the console.

The firewall function is performed by the firewall software IP Filters. IP Filters is also a freeware tool that not only serves as a packet filtering gateway device but also provides the ability to retain state information on communication sessions. For an example of how maintaining state information can help add security consider an internal system establishing a telnet session through this firewall. The first packet contains the SYN flag to start the session. The telnet server outside the firewall responds with a packet containing the SYN and the ACK flag. Because the firewall has an entry in its state tables for the initial connection request, it can allow a response to the request from the contacted host. At the same time a telnet request from the contacted host would be denied because no established session exists.

Besides being priced right, OpenBSD and IP Filters were both chosen for their performance providing higher speed connections to existing and potential customers.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Stateful packet filtering firewalls, while generally considered less secure than proxy firewalls, still provide good security at higher speeds.

Server Systems

System Configurations:

- Web Server: Sun Ultra 10, Solaris 2.7, Apache HTTP server version 1.3
- Mail Server: OpenBSD, Intel Pentium 3 800mghz, Sendmail version 8.11.3
- DNS Server: OpenBSD, Intel Pentium 3 800mghz, BIND Version 8.2.3
- Logging Server: OpenBSD, Intel Pentium 3 800mghz

As part of GIAC's defense in depth policy these server systems are configured very securely (hardened) even though they are protected by a firewall. Each system has one primary function and has all unnecessary services removed. All systems have a security software called tripwire running on them. The tripwire software takes a snapshot of system files by running a hashing algorithm against them. The resulting hash value from each system file is then mailed via the mail forwarder on the service network nightly to a system on GIACnet. This GIACnet system compares the nightly program hash values to baseline values. The hash comparison provides an indication as to whether any of the system files have been modified which could mean the system has been compromised. The Tripwire software is also used to detect and repair possible compromises on the Web server on an hourly basis. Tripwire is used to generate hashes of the GIAC static web pages. These hash values are compared to baseline values stored on read-only media. If the hashes are not identical, the baseline web pages are restored and an alert is sent to the administrator.

GIAC Main Firewall

System Configuration:

- Sun Ultra 60 with dual 400mghz CPUs, Solaris 2.7, Raptor version 6.5 with VPN

GIAC's main firewall, which protects their business network, is a proxy firewall. Proxy firewalls, in general, are considered more secure than either packet filtering firewalls or stateful firewalls. Proxy firewalls examine the source and destination IP addresses and ports like a packet filtering firewall. They also maintain information about the state of a communication session like a stateful firewall. A proxy firewall contains information about the application itself and provides an "air gap" between the two networks.[2] This means that a proxy firewall can detect different services running on well known ports like the newer internet tools that tunnel over port 80.

The Proxy firewall is also behind the stateful firewall. This provides an added layer of protection because vulnerabilities encountered in one type of firewall hopefully may not be found in another type.

[2] Spitzner, Lance (2001) Firewalls 101: Perimeter Protection with Firewalls, SANS, New Orleans, LA

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

A proxy firewall is not without drawbacks. Since the firewall actually performs the functions of the proxied services it is slower than other types of firewalls. Also, there are only a limited number of proxies that have been designed for a firewall. Communications on other than the well known services do not have proxies and therefore cannot be secured to the same level.

To make sure that the firewall does not become a bottleneck as it proxies the well known services GIAC has chosen a robust hardware platform. This powerful system is even more important because the firewall is also used as the VPN system for customers and suppliers. (VPN is discussed in more detail in assignment 2)

The Proxy firewall is also behind the stateful firewall. This provides an added layer of protection because vulnerabilities encountered in one type of firewall hopefully may not be found in another type.

GIAC Network

Security is not just for the perimeter devices. Systems on the GIAC network are also routinely scanned for vulnerabilities. GIAC users must either accept one of several company standard configurations that are maintained by the systems administrators or take responsibility for timely implementation of security patches that are recommended by the security staff.

GIAC Internal Firewall

System Configuration:

- OpenBSD 2.8, Intel Pentium 3 800mghz, IPfilters ver 3.4.16

GIAC also employs firewalls on the inside of its network. Recent statistics indicate that people within the company are responsible for many of the computer security incidents experienced at companies today.

The configuration of this system is similar to that of the GIAC perimeter firewall to leverage the company knowledge of the operating system and firewall software.

Customer Access

Customers that purchase bulk online fortunes do it by utilizing their desktops with Netscape web browsing software. These customers connect utilizing Secure Socket Layer with the largest key encryption allowed by the US export control laws.

Supplier Access

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Suppliers who author fortune cookie sayings connect to GIAC's main firewall using the Raptor Mobile VPN client. The Raptor Mobile client establishes an IPSec encrypted session to allow the suppliers to engineer life prognostication documents (fortunes).

Partner Access

Partners, those international associates who translate and resell fortunes, connect to GIAC utilizing Raptor's VPN connection. This VPN is configured with the largest key encryption allowed by U.S. encryption export laws.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Assignment 2 – Security Policy

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

- Border Router
- Primary Firewall
- VPN

You may also wish to include one of more internal firewalls used to implement defense in depth or to separate business functions.

By 'security policy' we mean the specific ACLs, firewall ruleset, IPSec policy, etc. (as appropriate) for the specific component used in your architecture. For each component, be sure to consider internal business operations, customers, suppliers and partners. Keep in mind you are an E-Business with customers, suppliers, and partners – you MAY NOT simply block everything!

(Special note VPNs: since IPSec VPNs are still a bit flaky when it comes to implementation, that component will be graded more loosely than the border router and primary firewall. However, be sure to define whether split-horizon is implemented, key exchange parameters, the choice of AH or ESP and why. PPP-based VPNs are also fully acceptable as long as they are well defined.)

For each security policy, write a tutorial on how to implement each ACL, rule, or policy measure on your specific component. Please use screen shots, network traffic traces, firewall log information, and/or URLs to find further information as appropriate. Be certain to include the following:

1. The service of protocol addressed by the ACL or rule, and the reason these services might be considered a vulnerability.
2. Any relevant information about the behavior of the service or protocol on the network.
3. The syntax of the ACL, filter, rule, etc.
4. A description of each of the parts of the filter.
5. An explanation of how to apply the filter.
6. If the filter is order-dependent, list any rules that should precede and/or follow this filter, and why this order is important. (Note: instead of explaining order dependencies for each individual rule, you may wish to create a separate section of your practical that describes the order in which All of the rules should be applied, and why.)
7. Explain how to test the ACL/filter/rule.

Be certain to point out any tips, tricks, or "gotchas".

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Border Router Policy

As stated above, the router function is to route or allow traffic. But it is still the best place to begin the perimeter defense. Access Control Lists are used to control traffic through the router. Here is the set of ACLs implemented on GIAC's perimeter router. I have included notes describing each ACL or group of ACLS before showing the actual ACL syntax. [3]

NOTES: This is the beginning section. I begin by showing the running configuration on the router (sho run). Here the version is documented. The "service timestamps" command configures the system to timestamp debugging and logging messages. The "service password-encryption" command specifies that the password will not be stored in clear text.

GIAC-rtr101#sho run
Building configuration...

Current configuration:
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
service password-encryption

NOTES: The hostname is specified. The next line is a very important line. The "enable secret" line means that the router will require a password to enter privileged mode. The number 5 indicates the type of encryption used for the password and the rest of the line is the encrypted password.

hostname GIAC-rtr101
enable secret 5 ?2?5faM?A($44xxxxxxxx/*

NOTES: The next configuration line turns off the ability to use subnet zero. This is used to remove the confusion in possibly having both a network and a subnet with the same IP addresses.

no ip subnet-zero

NOTES: Deny all source routed packets. This attack utilizes the ability to specify the route a packet will take rather than rely on the router to route the packet. Source routed packets are denied by the main firewall but it is good to stop them at the router also.

no ip source-route

NOTES: Disallow the ability to finger or query current connections on the router.

[3] Much of the router configuration and information was extracted from Cisco IOS Security Configuration Guide, Release 12.1. Retrieved March 27, 2001 from the World Wide Web: http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

no ip finger

NOTES: Define the domain name and the name server.

ip domain-name GIAC.com
ip name-server 12.33.247.9

NOTES: Disable unused services on the router. Disabling the http server stops a possible denial-of-service attack (Cisco bug ID CSCdr91706)[4] and the http management interface could allow a brute-force login attack. CDP (Cisco Discovery Protocol) allows devices to share basic configuration information so it should be turned off for security reasons.

no ip bootp server
no ip http server
no cdp run

NOTES: Send router alarms to the syslog server.

ip audit notify log

NOTES: Secure snmp with a community name other than public or private.

snmp-server community secret RO

NOTES: Specify the interface information including the type of connection, port number, IP address, filter list number (access-group), and duplex. Both the filter are on incoming traffic.

interface FastEthernet0/0
ip address 12.33.247.194 255.255.255.192
ip access-group 101 in
full-duplex

interface FastEthernet1/0
ip address 12.33.247.2 255.255.255.192
ip access-group 102 in
full-duplex

NOTES: Tell the router to forward packets that are destined for the subnets of directly connected networks.

ip classless

NOTES: Setup the default route.

ip route 0.0.0.0 0.0.0.0 <ISP Router IP>

NOTES: Send the router logs to our syslog server.

[4] Cisco IOS HTTP Server Query Vulnerability from Cisco October 25 2000. Retrieved March 27, 2001 from the World Wide Web: http://www.cisco.com/warp/public/707/ioshttpserverquery-pub.shtml

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

logging 12.33.247.10

NOTES: Here we begin our extended access list number 101. ACL 101 is applied to the interface that is attached to the Internet. First we must deny unwanted netbios traffic and also traffic from non-routable Internet IP addresses.

access-list 101 deny udp any any eq netbios-dgm log
access-list 101 deny udp any any eq netbios-ns log
access-list 101 deny udp any any eq netbios-ss log
access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
access-list 101 deny ip 192.168.0.0 0.0.255.255 any log
access-list 101 deny ip 172.16.0.0 0.15.255.255 any log
access-list 101 deny ip 12.33.247..0 0.0.0.63 any log
access-list 101 deny ip 12.33.247.64 0.0.0.63 any log
access-list 101 deny ip 12.33.247.128 0.0.0.63 any log

NOTES: Deny ICMP traffic (pings, traceroute, etc) from the Internet.

access-list 101 deny icmp any any

NOTES: If the traffic is not denied be the previous ACLs then we can allow it with the following.

access-list 101 permit ip any any

NOTES: This is the extended access list number 102. ACL 102 is applied to the interface connected to GIAC's server net. Allow any traffic from our service network. Deny any packets on our inside interface that aren't from our service network (spoofed addresses).

access-list 102 permit ip 12.33.247.0 0.0.0.63 any
access-list 102 deny ip any any log

NOTES: We need to add an intimidating banner for those who do get access.

banner motd ^C **********
*
* GIAC Perimeter Router. * * *
* Unauthorized Access is strictly prohibited *
*
* All access attempts are logged. Unauthorized access *
* is against the law and will be prosecuted. *
*
****
^C

NOTES: The next 4 lines allow the router to be managed from the console. A password is required. The "7" is the encryption type and the remainder of the line is the encrypted password. Because there aren't any additional lines here the router can only be managed from the console.

line con 0

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

password 7 037411A937E2D38170C4D
login
transport input none

end

There are several default ACLs not needed in version 12 of Cisco's IOS these include:
ip audit po max-events 100
no service udp-small-servers
no service tcp-small-servers

Good Web sites for help with Cisco router and security information.
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/index.htm for Cisco's security information.
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt3/scacls.htm for ACL help.
http://www.dtool.com/ccosec.html has a lot of Cisco security web pointers.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

GIAC Perimeter Firewall Configuration

My IP Filter firewall rule primer.

IP Filter is different from many firewalls in that it takes the last rule that satisfies the criteria for the packet and performs the desired operation.
IP Filter rules are implemented using key words. Here is a brief description of many of the IP Filter keywords:

block/pass – This is the first word in each rule. It describes the action to be taken on the packet that satisfies the rule criteria. "Block" is used to deny and "pass" is obviously used to allow a packet to proceed.
in/out/all – The next word describes what type of packet we are allowing or denying. "In" denotes a packet coming into the firewall, "out" denotes an outgoing packet, and "all" is both. ("in" and "out" are not interface specific)
on xl0 – This denotes the interface that the rule applies to. Our interfaces below are xl0 and xl1.
quick – The quick keyword is used to discontinue reading the rule base for applicable rules and perform the operation on the packet. This word cancels out the use-last-rule-that-applies structure of the firewall.
proto – IP Filters can filter all IP traffic. The "proto" keyword can indicate one of the common IP protocols (tcp, udp, or icmp).
from – The "from" keyword and the word that follows it enable the firewall to limit the packets by source. It can be a host or a network.
To – The "to" keyword like the "from" keyword causes the firewall to examine the destination of the packet.
log – The "log" keyword is used to specify logging of a packet that satisfies the rule (block or pass). Note: Logging is not automatic with IP Filters. You must run a tool to get the logs like "ipmon".
group – This keyword denotes the group that the rule is part of. It is used for flow control within the ruleset.
keep state – This enables the firewall to retain state information about a session.[5]

To configure a system to run IP Filters the following items must be accomplished:

- set ipfilter=YES in /etc/rc.conf
- make sure that the kernel has been compiled with option IPFILTER turned on
- set net.inet.ip.forwarding=1 in /etc/sysctl.conf

Then the rules in the file /etc/ipf.rules will be used to configure the firewall.

The rules outlined below are discussed by group according to interface and destination.

The firewall groups established are:

[5] Rules and rule format taken from IP Filter Based Firewalls HOWTO by Brendan Conoboy & Erik Fichtner March 10, 2001 Retrieved March 19, 2001 from the World Wide Web: http://www.obfuscation.org/ipf/ipf-howto.txt

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Group 10 – Incoming packets from the Internet (interface xl0) to GIACnet are examined.
Group 15 – Incoming packets from the Internet to our server network.
Group 20 – Incoming packets from the inside of the bridging firewall (interface xl1). Out going packets to the Internet are passed without examination. These packets are examined when entering the firewall. Again, outgoing packets on the inside interface of the firewall are also passed. Finally packets on the local host interface (lo) are allowed.[6]

This is my ruleset top level decision tree. Interface xl0 is the interface to our perimeter router and on to the Internet. Interface xl1 is our interface to the service network.

Block in log quick on xl0 from any to 12.33.247.0/24 all head 15
Block in log quick on xl0 all head 10
Pass in quick on xl1 all head 20
Pass out quick on xl0 all
Pass out quick on xl1 all
Pass in quick on l0 all

Rule Group 10
Notes: The following rules are part of group 10. These rules are the basic rules for watching traffic coming in from the Internet. The first two rules block all packets from the Internet with IP options set (first rule) and that are fragmented (second rule).

block in log quick all with ipopt group 10
block in log quick all with frag group 10

Notes: Deny any rules coming from the Internet with the IP addresses of our service network. (spoofed packets)

block in log quick from 12.33.247.0/24 to any group 10

Notes: Deny any other spoofed packets. Log these packets and watch the log closely because these packets should have been denied at the perimeter router.

block in log quick from 255.255.255.255/32 to any group 10
block in log quick from 0.0.0.0/32 to any group 10
block in log quick from 127.0.0.0/8 to any group 10
block in log quick from 10.0.0.0/8 to any group 10
block in log quick from 172.16.0.0/12 to any group 10
block in log quick from 192.168.0.0/16 to any group 10
block in log quick from any to 255.255.255.255/32 group 10
block in log quick from any to 0.0.0.0/32 group 10
block in log quick from any to 127.0.0.0/8 group 10
block in log quick from any to 10.0.0.0/8 group 10
block in log quick from any to 172.16.0.0/12 group 10

[6] Rule grouping for firewall efficiency taken from Maximum Security Configuration, Author unknown. Retrieved on March 19, 2001 from the World Wide Web: http://www.openlysecure.org/content/html/highestsec.html

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

block in log quick from any to 192.168.0.0/16 group 10

Rule Group 20
Notes: The following rules are part of the second group. These packets are coming in from the inside interface (from our service net). This rule allows communication attempts from inside GIACnet (come from the GIACnet proxy firewall). The "keep state" keyword means that only sessions initiated inside will be allowed to receive responses back.

pass in quick proto tcp port all flags S keep state group 20

Notes: UDP connections from DNS are also allowed.

pass in quick proto udp from any to any port = dns keep state group 20

Rule Group 15
Notes: Group 15 is for packets from the Internet coming to our server network. Here again we must be careful of the same items that we were concerned about in group 10. The following rules are duplicates from group 10.

block in log quick all with ipopt group 15
block in log quick all with frag group 15

block in log quick from 12.33.247.0/24 to any group 15

block in log quick from 255.255.255.255/32 to any group 15
block in log quick from 0.0.0.0/32 to any group 15
block in log quick from 127.0.0.0/8 to any group 15
block in log quick from 10.0.0.0/8 to any group 15
block in log quick from 172.16.0.0/12 to any group 15
block in log quick from 192.168.0.0/16 to any group 15
block in log quick from any to 255.255.255.255/32 group 15
block in log quick from any to 0.0.0.0/32 group 15
block in log quick from any to 127.0.0.0/8 group 15
block in log quick from any to 10.0.0.0/8 group 15
block in log quick from any to 172.16.0.0/12 group 15
block in log quick from any to 192.168.0.0/16 group 15

Note: Allow Internet requests to our server systems by port number.

pass in quick proto tcp from any to 1.2.3.6 port = http group 15
pass in quick proto tcp from any to 1.2.3.7 port = smtp group 15
pass in quick proto tcp from any to 1.2.3.2 port = ftp group 15

Note: Allow Internet requests to our firewall for VPN. Port 50 is used for Encapsulation Security Payloads (ESP).

pass in log quick proto udp from any to 1.2.3.2 port = 500 group 15
pass in log quick proto tcp from any to 1.2.3.2 port = 50 group 15

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Note: Allow UDP requests to our DNS server.

pass in log quick proto udp from any to 1.2.3.9 port = 53 group 15

Note: Requests to ports other than standard system service should be blocked and logged. (example: log http requests to our mail server) Here we are using the "flags" keyword to have the firewall examine the tcp/ip packet flags.

block in log level local0.warn quick proto tcp all flags S/SA group 15
block in log level local0.warn quick proto tcp all flags SA/SA group 15
block in log level local0.warn quick proto tcp all flags SAFRPU group 15

GIAC Firewall (Proxy) Configuration

The firewall that protects GIAC's own network is a Raptor proxy firewall. As mentioned above, the proxy firewall is very secure because it can filter the packets on source and destination ports and addresses, keep state information, and examine the application data at layer 7 of the ISO network model. The Raptor firewall being used to protect GIACnet is running the latest version of the Raptor software version 6.5. All authorization rules have the following elements:

Source – the originator of the packet (hopefully) and the interface it is to cross (called in via and out via)
Destination – where the packet is headed.
Action – such as permit or deny.
Services and protocols – there are 3 types of items for this element
- plain protocols
- protocols that you can select additional settings such as ftp
- protocols for which there is no pre-defined proxy

Optional rule elements include:
Scope – like rules for VPN tunnels
Time – to control connections by time or day of the week
User or User groups – for rules requiring authentication
Data scanning – specifying whether the application payload is examined
Thresholds – specifying a level at which an alert is generated[7]

Before creating rules in the Raptor firewall, you must first setup your network and user components. Examples of network components for Raptor include networks, subnets, specified hosts, and domains.

The Raptor firewall operates with the default mode of denying all connections except those that are specifically allowed. The rules are evaluated on a "best fit" basis for each

[7] Raptor Firewall and PowerVPN V6.5 Configuration Guide for Solaris. Axent Technologies, Inc. November 2000.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

connection attempt so the rule that best fits a packet is the one that is applied. The rule fit evaluation criterion is most specific rules first then the more general rules. If there is a tie between rules Raptor will first go with a deny rule if one exists. If not, Raptor will use the most restrictive rule.

An example of the Raptor rule ranking process is the ranking done first by service and next by source and destination. The ranking of source and destination is performed first by hosts, then by subnets, and finally by interface. The interface parameter is new on Raptor version 6.5.

For the purposes of clarity the following labels will be used in the ruleset description process.

GIAC-net - all the systems in GIAC's 192.168 internal network.
Universe – a Raptor provided label for all network entities.
Service-Net – for the systems on the service network
GIAC-Int – the inside interface to the firewall.
Out-Int- the outside interface to the service net and Internet
Serv-mail – the service net mail system
GIAC-mail – GIAC's internal mail server
GIAC-DNS – internal DNS server
Serv-DNS – the service net DNS system

The following table will be used to present the GIAC proxy firewall rules. It is similar to Raptor's rule maintenance window. There are only a couple of rules needed because of the special way that Raptor handles mail and DNS.

TYPE	INVIA	SOURCE	DESTINATION	OUTVIA

HTTP Setup

The first rule we will create is to allow GIAC employees to use the world wide web.

TYPE	INVIA	SOURCE	DESTINATION	OUTVIA
Allow	GIAC-Int	GIAC-Net	Universe	Out-Int

This rule is for service HTTP. When we specify this protocol we are prompted for extra information. Here we can choose to also allow HTTPS and choose the ports. We choose the standard ports (443 & 563). We can also select other application-type choices like:

- allow FTP protocol conversion
- allow Gopher Protocol conversion
- allow DCOM over HTTP

We can also choose whether we want to restrict certain URLs or filename extensions. Restricting HTTP traffic by either URL or filename extension is not recommended because you must then maintain a table of allowed URLs or filename extensions.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

FTP Setup

The next rule we will create is to allow GIAC employees to FTP out to the Internet.

TYPE	INVIA	SOURCE	DESTINATION	OUTVIA
Allow	GIAC-Int	GIAC-Net	Universe	Out-Int

This rule is for service FTP. Here we can further specify whether to allow FTP Puts and/or Gets. GIAC employees are allowed to do both.

SMTP Setup

Next we will configure mail on our Firewall. Raptor has an SMTP server application proxy. The server supports transparent addressing and checks all traffic entering and leaving your domain for known sendmail attacks. To set up our mail proxy we must use the "configure mail menu" option. The resulting window requests the IP address of the GIAC internal mail server. Here we will not select the button to "allow all internal hosts out". This means the Raptor mail proxy will only allow the GIAC internal mail server to talk to the service net mail server and vice versa. We will not utilize Raptor's anti-spam measures since the mail servers disallow SMTP forwarding. The resulting mail rules looks like this.

TYPE	INVIA	SOURCE	DESTINATION	OUTVIA
Allow	<ANY>	Universe	GIAC-mail	<ANY>
Allow	<ANY>	GIAC-mail	Universe	<ANY>

Since we are using an external forwarding mail system we will further refine this rule to authorize only communications between our external and internal mail servers. The new rules look like this:

TYPE	INVIA	SOURCE	DESTINATION	OUTVIA
Allow	Out-Int	Serv-mail	GIAC-mail	GIAC-Int
Allow	GIAC-Int	GIAC-mail	Serv-mail	Out-Int

DNS Setup

Next we will configure DNS. Raptor provides what appears to be a fairly strong DNS proxy solution in the firewall itself. The problem with this solution is that it will violate the GIAC principle of one primary service on one system. Raptor does not use BIND for DNS on the firewall but it still may have similar vulnerabilities. For this reason and because the firewall system is of critical importance in protecting GIACnet we will utilize a system on the service network for DNS.

TYPE	INVIA	SOURCE	DESTINATION	OUTVIA
Allow	GIAC-Int	GIAC-DNS	Serv-DNS	Out-Int

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Allow	Out-Int	Serv-DNS	GIAC-DNS	GIAC-Int

These rules allow the GIAC internal DNS server to pass unknown requests to the service network DNS server. The service network DNS server can then respond back to the GIACnet DNS system. To configure this communication we will use a Generic Service Passer (GSP) on Raptor. Our GSP will be a UDP protocol and will have the standard port number for DNS, 53.

Remote Management Setup

Finally, we can configure the firewall to be managed from systems other than the console. Care must be taken to minimize the number of administrators who can manage the firewall because only one person can have read/write access to the firewall at a time. A message is given to the second administrator to attempt to manage the firewall. If that administrator chooses to over-ride the first administrator, then all previous work of the first administrator will be lost.

Raptor's remote management console (RMC) communicates to the firewall using triple DES for domestic use or DES for international use. A RMC configured for domestic use can manage an international firewall but a RMC configured for international use cannot manage a domestic firewall.

The RMC talks to the Raptor firewall on ports 416, 418, and 481. We have installed filters on our firewall so that it does not listen for connections on these ports from the outside interface. This was done for security reasons, the fewer ways to talk to the firewall from outside the fewer ways to try and find a vulnerability. All firewall management must be done from GIACnet or on the console.

To setup remote management you run two commands on the firewall console.

- rempass – sets the remote password for management.
- setremote – tells the firewall to allow management access from a specific remote system.

Raptor provides remote management client software for both Solaris systems and Windows NT systems. In Raptor version 6.5 the remote management client software is free with the purchase of the firewall software.

VPN configuration (supplier)

First I will discuss the configuration used in the Raptor Mobile client VPN. This Raptor Mobile allows individuals to utilize an encryption client on a desktop or laptop system to establish a VPN over the Internet. This type of connection works well for the talented individuals who walk in Confucius' footsteps and author the fortunes for GIAC (suppliers).

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The steps required to establish a Raptor Mobile secure tunnel include:

- defining network entities – systems and subnets that the VPN will access
- defining the local gateway entity – firewall's outside interface and security parameters
- defining the VPN policy – what type of encapsulation, what encryption algorithm, what data integrity algorithm, etc.
- defining the secure tunnel
- configuring the Raptor Mobile client

Our configuration:
Network entities – Here we setup a single system on GIACnet inside the firewall to receive the supplied fortunes. Because name resolution can be an issue with the mobile clients, we configure only one place for the supplied fortunes to be maintained. The firewall will be the local VPN endpoint and we have chosen IPSec/IKE as our VPN policy. Also, because GIACnet utilizes non-routable IP addresses, we will utilize address translation for our VPN.

Here is an example of the firewall rules for this VPN.

TYPE	**INVIA**	**SOURCE**	**DESTINATION**	**OUTVIA**
Allow	Out-Int	Universe	Supplier-host	GIAC-Int
Allow	GIAC-Int	GIAC-Net	Universe	Out-Int

The user entity setup on the firewall requires:

- phase 1 ID – a value for first level key negotiations (the user will be prompted for a password)
- a shared secret (optional) that is entered both on the firewall and in the Raptor Mobile client
- a user certificate – an authentication device bound to identifying information called a distinguished name as defined by the X.509 standard

The phase 1 ID is a unique name provided to each supplier by GIAC administrators. For simplicity, GIAC uses a shared secret and not a certificate. For greater security all suppliers are assigned a SecureID card to use with Raptor's extended authentication.

We will use ike_default_crypto_strong one of the 5 pre-configured VPN policies that come with Raptor. This policy uses the IPSec/IKE encapsulation protocol. Because we are translating the IP address we will pass the traffic through the Raptor proxies. For our data integrity algorithm we have chosen SHA1 since it is believed to be more secure. And finally, we select triple DES for our primary encryption preference followed by regular DES.

These same configuration parameters are placed in the Raptor Mobile client configuration and includes the phase 1 ID and the shared secret.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

VPN configuration (partner)

Many of the configuration entries used for the Raptor Mobile are also used for the VPN connection to GIAC's partners. Here we configure Raptor's VPN to work with a Cisco VPN device. I have been assured by a very reputable person (my Raptor training instructor) that this Raptor-to-Cisco VPN has been made to work in production environments.

Steps to configuring a VPN tunnel on the Raptor

- Setup the network entities
- Setup up the security gateways
- Setup the filters
- Determine and setup VPN policies

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

I have been told several times that the first step in setting up a VPN is drawing a picture – so here it is.

Our network entities are the Private supplier system, and our internal subnet (part of GIACnet).
Next we configure our security gateways:

Cisco Router	Raptor
IP = ipaddr2	IP=ipaddr3
Shared secret = n/a	Shared secret = n/a
Remote = Raptor	Remote = cisco
IP = ipaddr3	IP = ipaddr2
Shared secret = "will this #$?@! work"	Shared secret = "will this #$?@! work"

With the gateway information configured we can now configure our tunnel. Here is where we have to choose our VPN policy. We cannot choose to use a predefined policy so we will build one ourselves. Our policy settings include:

- MD5 for data integrity with no second or third preference
- DES with no second or third preference
- No data compression

We can also use a predefined IKE policy. The IKE policy settings will be:

- Data integrity preferences: first – MD5; second – none
- Encryption preferences: first – Des; second – none
- Encapsulating header chosen will be "encryption header" and not "authentication header"
- Time expiration 1080 seconds to establish a connection

Now we can configure the tunnel on the Raptor firewall. Because we are translating the addresses of the GIACnet systems we select the "past traffic through proxies" checkbox. Using the dropdown menu boxes we choose the VPN and IKE policy settings outlined above. The "Perfect Forward Secrecy" is the default option so that each key is generated without any reference to the previous key. This prevents attackers from guessing successive keys.

Now we must help configure the Cisco router to talk to our Raptor. The Cisco configuration should look something like this:[8]

First we will set up an ACL for the VPN endpoints. The local endpoint is always placed first in the ACL.

[8] Firetower, (2000) Raptor-to-Cisco IPSEC VPN Static Keys using Raptor Eagle v5.0 Cisco Instructions

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Access-list 105 permit ip Ipaddr2 0.0.255.255 Ipaddr3 0.0.0.255

Next we will configure the ISAKMP or IKE policy. We specify on the router the pre-shared key. It must be identical to the key configured on the Raptor firewall. The key lifetime stated here corresponds to the 1080 minute key lifetime default on the Raptor firewall.

Crypto isakmp policy 10
Authentication pre-share
Lifetime 64800
Crypto isakmp key "will this #$?@! work" address Ipaddr3 (raptor address)

We must create a Cisco transform-set to apply to the VPN tunnel. We have named our transform set "RaptorVPN" and chosen DES encryption and MD5 integrity.

Crypto ipsec transform-set RaptorVPN esp-des esp-md5-hmac

Now we create the VPN tunnel map. Raptormap is the name of our map and the number 10 is an arbitrary number.

Crypto map Raptormap 10 ipsec-isakmp
Set peer Ipaddr3
Set transform-set RaptorVPN

The following configuration sets the Perfect Forward Secrecy option as set on the Raptor firewall.

Set PFS group1

Finally we configure the router to use the ACL defined above.

Match address 105

© SANS Institute 2000 - 2002, Author Retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Assignment 3 - Audit Your Security Architecture

You have been assigned to provide technical support for a comprehensive information systems audit for GIAC Enterprises. You are required to audit the Primary Firewall described in Assignments 1 and 2. Your assignment is to:

1. Plan the assessment. Describe the technical approach you recommend to assess your perimeter. Be certain to include considerations such as what shift or day you would do the assessment. Estimate costs and level of effort. Identify risks and considerations.
2. Implement the assessment. Validate that the Primary Firewall is actually implementing the security policy. Be certain to state exactly how you do this, including the tools and commands used. Include screen shots in your report if possible.
3. Conduct a perimeter analysis. Based on your assessment (and referring to data from your assessment), analyze the perimeter defense and make recommendations for improvements or alternate architectures.

Diagrams are strongly recommended for this part of the assignment.

Note: DO NOT simply submit the output of nmap or a similar tool here. It is fine to use any assessment tool you choose, but annotate the output.

© SANS Institute 2000 - 2002 Author Retains Full Rights

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Plan the assessment

Before assessing GIAC's security we must revisit the GIAC corporate security policy document. Just as this document has driven the way we have architected the perimeter security, it will also dictate each and every test to be implemented. What is allowed to enter the service network? What is allowed to enter GIACnet? What type of encryption is valid? What risks are considered acceptable and what are not?

My approach for assessing the security of the GIAC perimeter is both multi-leveled and comprehensive. Since we are utilizing a defense-in-depth strategy, we need to make sure that our security at each level is as strong as if it were the only security level. To do this we will establish a node outside of each level and verify that the level does indeed control the communications as expected. Also, we need to confirm that alerts are generated when network traffic indicates a previous level of security has been breached. Again, take a look at our network security diagram (page 4).

The locations we will test our security include:

- From the Internet. At this location we will verify the perimeter router does disallow private Internet address, control ICMP traffic, and block protocols like Netbios.
- From inside the perimeter router. Here we will test our perimeter firewall.
- From inside our perimeter firewall. This is the location that we test the hardness of our server net systems. Each system must be configured to be as secure as if the system were directly placed on the Internet.
- From inside our perimeter router we will test the security of GIAC's main firewall. Here again we must assume that all previous safeguards of the system have been compromised.
- The security of the systems on GIACnet. Both the individual systems and the internal firewalls should be tested. Most of the recent statistics indicate the threat from being attacked by an insider is significant. Checking for poorly protected modems is essential here (war dialing). The strongest network perimeter can be thwarted by one individual who leaves his laptop plugged into both the telephone jack and the network jack at the same time.

For a one-time security evaluation these tests will probably be adequate, but only for about 10 minutes. Because of the ever changing nature of information technology and the human propensity to play and explore, we must continuously monitor the security of our systems and networks.

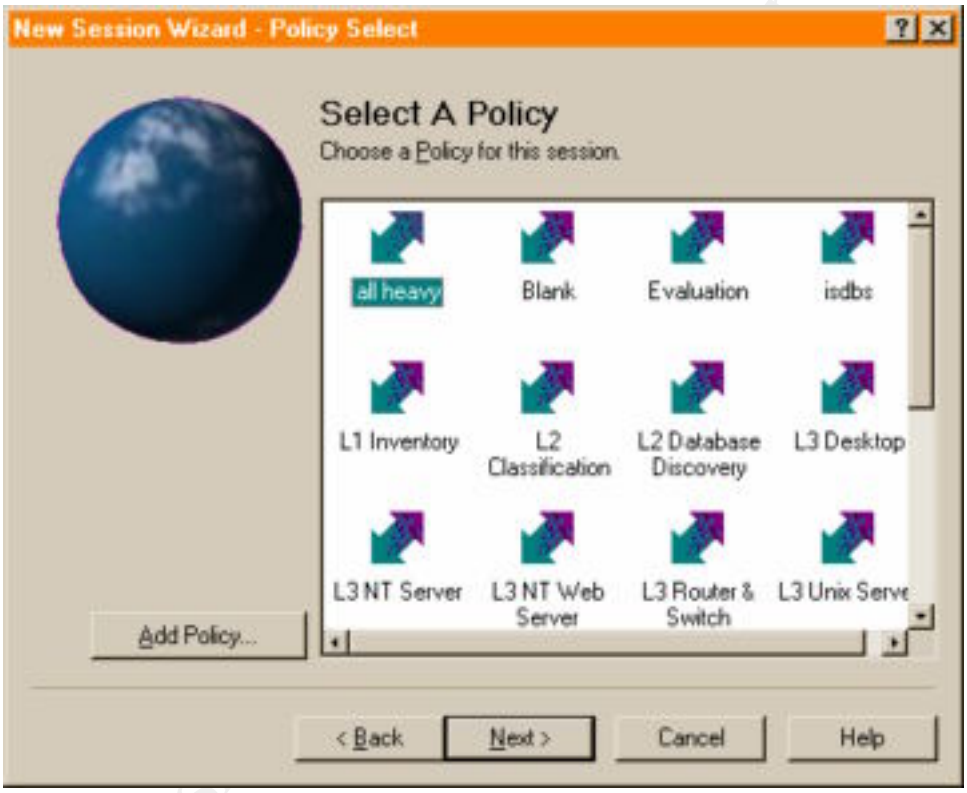
Because our perimeter must provide strong security 24 hours a day, 7 days a week, I don't think it matters much what time or day you perform the assessment. Of course, there may be a greater opportunity to exploit a man-in-the-middle type of attack at a time when there are more sessions present.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Although no single software tool can come close to doing all the security tests that are required to verify each level of our perimeter, our task in this assignment is to audit the primary firewall. For this task my tool of choice is the ISS Internet Scanner product. This product incidentally scored the highest in the SANS vulnerability scanning product comparison. The latest version is version 6.1 with express update 4.6.

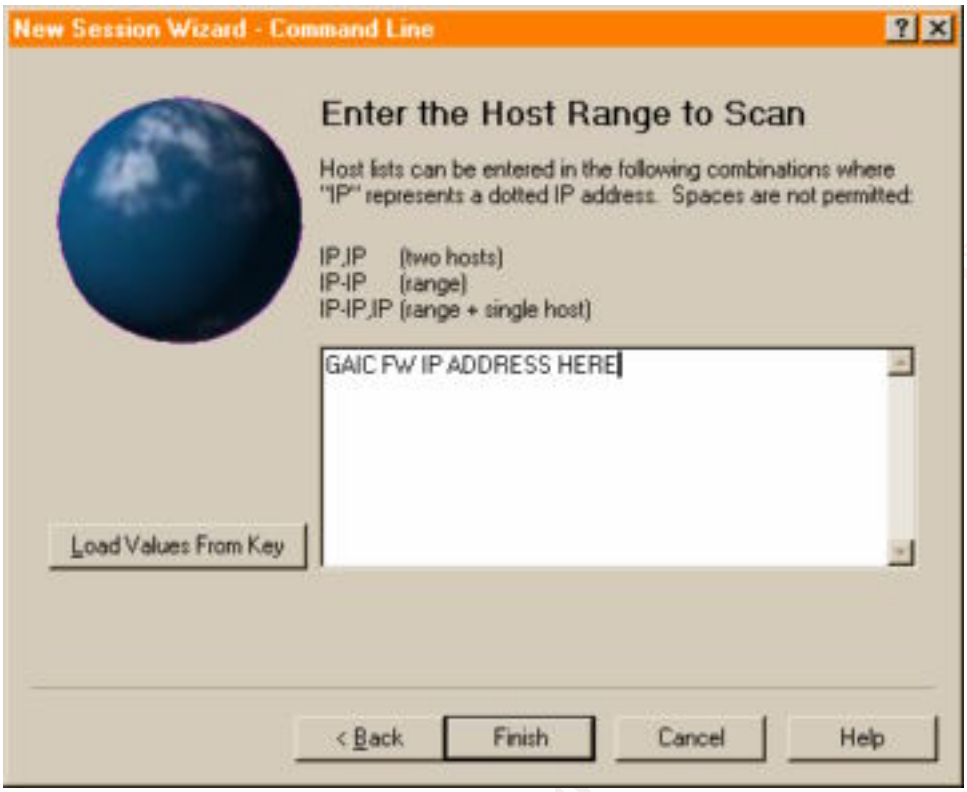
Since we are using this tool to scan both the perimeter systems and the internal systems a 500 system license will be adequate while still allowing a little room for growth. The cost for this size license will vary but is estimated at $30,000.

The effort for running the tool is minimal (approximately 6 – 8 hours). This estimate includes scanning all 65355 ports and printing several reports.



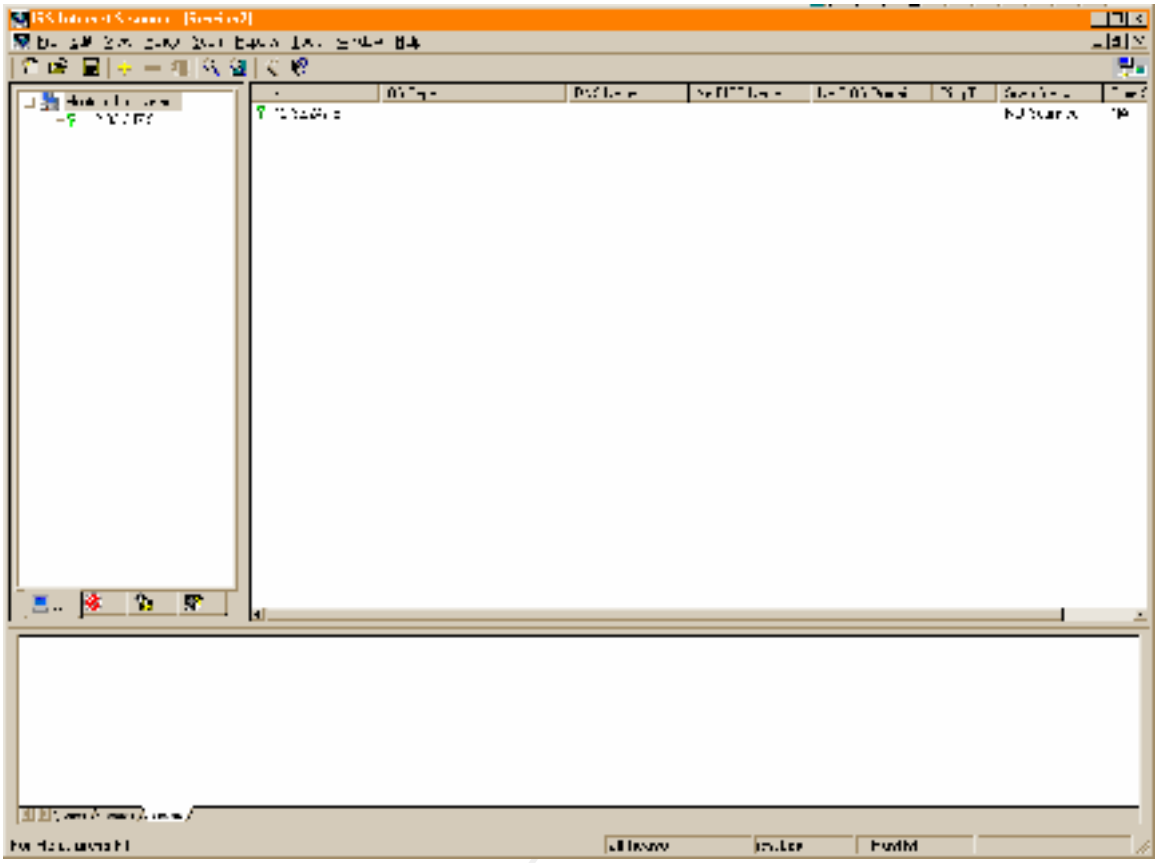
I have created a custom policy from the templates provided and called it "all heavy". My new policy incorporates all of the denial-of-service attacks as well as both Unix and NT vulnerability tests. Next I enter the IP address of the firewall and click on the finish button.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



Now we are presented with the main vulnerability scanning window of Internet Scanner.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



On this screen select the "Scan" pull-down menu and click on "Start".

The vulnerability scanner will begin testing for hundreds of vulnerabilities. The scanner can produce a great variety of reports. This is an example of a vulnerability report sorted by severity of the vulnerability.

Network Vulnerability Assessment Report

Sorted by Vulnerability Severity and Name Wednesday, April 04, 2001

Report Description:

This report displays the organization's susceptibility to attack in relation to its policy and vulnerability conditions. Specifically, this report identifies network vulnerabilities and suggested corrective action. Vulnerabilities are classified as high, medium and low. High risk vulnerabilities are those which provide unauthorized access to the host, and possibly, the network. Medium risk vulnerabilities are those that provide access to sensitive network data that may lead to the exploitation of higher risk vulnerabilities. Low risk vulnerabilities are those which provide access to sensitive, yet non-lethal, network data. It is recommended that all high risk vulnerabilities be corrected as soon as possible.

Session Name:	Session1	**Session ID:**	1
Comment:		**Template:**	Heavy Scan
File Name:	Session1_000930	**Termination Status:**	Finished
Scan Summary Information			
Hosts Scanned:	1	**Scan Start:**	2001/04/04 12:00:20

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Hosts Active:	1	**Scan End:**	2001/04/04 12:49:09
Hosts InActive:	0	**Elapsed:**	00:49:11

Vulnerability Name:
Severity:

Description:

Fix:

IP Address	DNS Name	Associated Info	More Info	Session ID

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Assignment 4 - Design Under Fire

The purpose of this exercise is to help you think about threats to your network and therefore develop a more robust design. Keep in mind that the next certification group will be attacking your architecture!

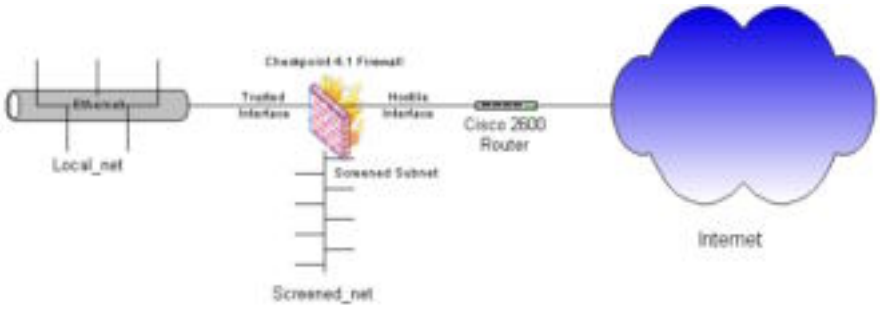
Select a network design from any previously posted GCFW practical (http://www.sans.org/giactc/gcfw.htm) and paste the graphic into your submission. Be certain to list the URL of the practical you are using. Design the following three attacks against the architecture:

1. An attack against the firewall itself. Research vulnerabilities that have been found for the type of firewall chosen for the design. Choose an attack and explain the results of running that attack against the firewall.
2. A denial of service attack. Subject the design to a theoretical attack from 50 compromised cable modem/DSL systems using TCP SYN, UDP, or ICMP floods. Describe the countermeasures that can be put into place to mitigate the attack that you chose.
3. An attack plan to compromise an internal system through the perimeter system. Select a target, explain your reasons for choosing that target, and describe the process to compromise the target.

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

My diagram that I will attack comes from Rick Dreger at
http://www.sans.org/y2k/practical/Rick_Dreger.doc



Assumptions: I have a diagram of the perimeter defenses for this network.

Before I planned any type of attack I would first go about the business of getting information about the target. This doesn't have to be dumpster diving, although that is a pretty good way to get information. Just reviewing the company web site or reading their quarterly financial report can provide lots of information that could be used to assist an attack. Other places to look include the company's DNS records. What is the address of their mail system and their DNS system? Did the company use common names for common systems like gateway for their firewall? The questions that you are trying to answer include:

What systems are within reach?
What type of systems are they?
Contact names and numbers?
Domain information?

Once you have obtained all of the easily available information then you begin to find out what you can learn by probing the company's systems. Now we are looking for:

What ports are open?
What type of operating system?
Does the company have active defense systems?
Does the company have a honeypot?

Hopefully by now there has turned up some interesting information you can use to plan an attack.

From the diagram above we know that Checkpoint's Firewall-1 version 4.0 is being used to secure the corporate network as well as the DMZ systems. Firewall-1 is known to be a very secure firewall, but around 8 months ago new information about several vulnerabilities was released about this firewall. Because of these recent vulnerabilities and the lack of mention of service packs in the document this security design may be susceptible to attack.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Firewall Attack

A tool to attack Checkpoint's Firewall-1 version 4.1 pre-service pack 2 was written by Gregory Duchemin. This tool is called FWSA, which is short for Firewall-1 session Authentication. The comments in this hacker program boasts that it is the Swiss Army knife for firewall-1. FWSA is a bash shell script that runs on Linux operating system. It can be obtained at http://cks.wox.org/hack/os/hardware/firewalls/firewall-1/fwsa.sh. FWSA runs in several modes:

1. Password recovery mode – it will attempt to obtain a login/password for the firewall.
2. Denial of Service 1 – (called stupid DOS) – the script will open a connection and block other connections.
3. Denial of Service 2 – (called dangerous DOS) – the script will inter an infinite loop sending random characters to the firewall.
4. Brute force password attack – the script will guess users passwords on the firewall.[9]

So, after downloading FWSA and placing it on a linux system, the next step is to run this program against the firewall. The script does rely on port 261 being open for Firewall-1's session authentication.

Because we are attempting to compromise the firewall the first run will be in mode 1 or password recovery mode.

[root@localhost /root]# ./fwsa fwipfile.txt 1

****
Launching dangerous DOS attack against <fw1-ipaddr>
****

Done. (see resultfile to read stolen informations)

If FWSA mode 1 (password recovery) doesn't work the next step would be to try the brute force attack against the session authentication. You may want to edit the script to increase the chances of getting a password hit on the firewall. Lines in the script allow you to determine how many characters and what characters will be used in the password guessing.

[root@localhost /root]# ./fwsa fwipfile.txt 4

****

[9] FWSA – Gegory Duchemin Retrieved on March 29, 2001 from the World Wide Web: http://cks.wox.org/hack/os/hardware/firewalls/firewall-1/fwsa.sh

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Launching dangerous DOS attack against <fw1-ipaddr>
****

Done. (see resultfile to read stolen informations)

If either of these attacks work you can get the passwords in the results file.

Denial-Of-Service Attack

There are several denial-of-service tools that target firewall-1. One particular tool, CPD.C will crash a firewall-1 system that does not have anti-spoofing turned on.

For this attack however, we will use the 50 compromised cable modems all sending thousands of TCP SYN packets at the firewall. Each TCP SYN packet tells the firewall that a connection is being requested. The firewall allocates memory and responds with SYN/ACK acknowledging the request. It is important to know what ports the firewall is listening on to target the denial-of-service.

If you have synchronized your compromised cable modem systems well once you start the attack the firewall should be flooded with requests and run out of memory after a short time.

For our GIAC company that does all of its business on-line this denial-of-service could cost them a lot of money. Assuming their sales are roughly constant through out the day and year (no peak times) they would be loosing at least 380 dollars for every minute their connection to their customers is down.

Countermeasures to mitigate the denial-of-service attack include:

- Minimize the time the firewall waits for the next packet after the SYN/ACK is sent in response. This will mean fewer open connections during the flood and require more systems to enable a successful attack.
- Establish greater capacity with load balancing. If your business depends on the network then it may be cost effective to implement redundant routers and firewalls.
- Establish an active perimeter defense. When an intrusion detection system (IDS) recognizes a SYN flood (a certain number of packets in a given amount of time) the IDS can send an SNMP command to the perimeter router to deny any further packets from the offending hosts. Caution must be used when implementing such a defense. Intelligent hackers if aware of this can use it against you by spoofing addresses and causing you to deny connections from key customers.

Internal System Attack

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Since the description of this attack is somewhat vague I am going to design an attack a little outside the box. My attack is targeted at the GAIC company. Within the company I would target GIAC's desktop systems. It is a pretty safe bet that GIAC utilizes Microsoft operating systems on their desktop platform.

My attack would attempt to exploit the most vulnerable part of every computer …the nut in front of the keyboard (my computer more so than many).

I would design "FCN2001", Fortune Cookie Newsreader 2001, a news browser that would provide up to the minute information on the fast paced fortune cookie industry (new trends, latest predicted lottery numbers, …). This program would do more than provide information and entertainment to the various administrative, operational, and executive employees at GIAC International. FCN2001 would turn the computers that run this program into stealthy sniffers that would covertly observe network traffic and pluck passwords from the telnet and ftp packets. FCN2001 would weekly send a zipped and encrypted file to a couple of Hotmail, Yahoo, and/or Juno accounts.

To plant this program only in the GIAC company and keep from getting flooded by all the other fortune cookie companies I would spam as many of the GIAC employees as possible with an e-mail telling them where they could get FCN2001(the beta version while it is still free). When the employees came to my web site to get more information I would send those visitors from GIAC IP addresses to the "trojaned" download site and all others to the legitimate download site.

One of the issues with pulling this off is to make sure FCN2001 can obtain GIAC's internal mail system address from MS Explorer or Netscape.

Countermeasures for mitigating an attack like this:

- Scan systems regularly for network interface cards in promiscuous mode. Except for the Security and Network staff there should never be systems listening to traffic (in promiscuous mode) on the network.
- Utilize VPN inside of GIAC. Encrypted traffic would keep any passwords from going across the network in clear text. FCN2001 would have to be changed to a type of keystroke logger.
- Utilize switches to minimize the number of sessions that could be sniffed.
- Routinely review a report of mail source and destinations. Of course this may be seen as an invasion of privacy so at least review the destinations.
- Limit employee downloads to programs that have been analyzed in a laboratory environment.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

References:

The SANS Institute, Brenton, Chris & Spitzner, Lance (2001, January) Track 2 training manuals.

Brenton, Chris (2001) FUBAR's Computer User Policy, Received via e-mail February 2001

Cisco IOS Security Configuration Guide, Release 12.1. Retrieved March 27, 2001 from the World Wide Web:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/

Cisco IOS HTTP Server Query Vulnerability from Cisco(2000, October) Retrieved March 27, 2001 from the World Wide Web:
http://www.cisco.com/warp/public/707/ioshttpserverquery-pub.shtml

Conoboy, Brendan & Fichtner, Erik (2001, March)IP Filter Based Firewalls: HOWTO March 10, 2001 Retrieved March 19, 2001 from the World Wide Web:
http://www.obfuscation.org/ipf/ipf-howto.txt

Author Unknown (2001, March) Maximum Security Configuration, Retrieved on March 19, 2001 from the World Wide Web: http://www.openlysecure.org/content/html/highestsec.html

Axent Technologies, Inc., (2000, November) Raptor Firewall and PowerVPN V6.5 Configuration Guide for Solaris.

Duchemin, Gegory (date unknown) FWSA –Retrieved on March 29, 2001 from the World Wide Web: http://cks.wox.org/hack/os/hardware/firewalls/firewall-1/fwsa.sh

Firetower, (2000) Raptor-to-Cisco IPSEC VPN Static Keys using Raptor Eagle v5.0 Cisco Instructions Retrieved on March 21, 2001 from the World Wide Web:
http://www.firetower.com/faqs/vpn/ciscovpn-static-ciscoside.html

SANS GCFW Papers:
Rick Dreger
Pat Malone
Jeff Horne
Chris Robertson
Clay Maney
Graham Bennett
James McMahon
Alan Moe
Jeremy Browns
Carrie Chalmers

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.