

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.

Table of Contents 1
Philip_Kemp_GCFW.doc 2

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

Firewalls, Perimeter Protection, and VPNs

SANS GCFW Practical Assignment

Version 1.5e

Philip Kemp

July 2001

© 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 (25 points)

Company Overview

GIAC Enterprises, a growing Internet startup company, expects to earn $200 million per year in online sales of fortune cookie sayings. The company has just completed a merger. GIAC Enterprises requires a secure network infrastructure that will allow electronic interaction with five groups in particular:

1. Customers—companies that purchase bulk online fortunes.
2. Suppliers—authors of fortune cookie sayings that connect to supply fortunes.
3. Partners—international partners that translate and resell fortunes.
4. Local users—network end users located on-site.
5. Remote users—employees needing remote VPN access.

GIAC Enterprises uses both UNIX and Windows NT/2000 operating systems. The company uses Windows NT for corporate desktops, including an internal Microsoft Exchange email server. Solaris 8 has been selected as the operating platform of choice for production and external services, due to its robustness, performance, and ability to be secured.

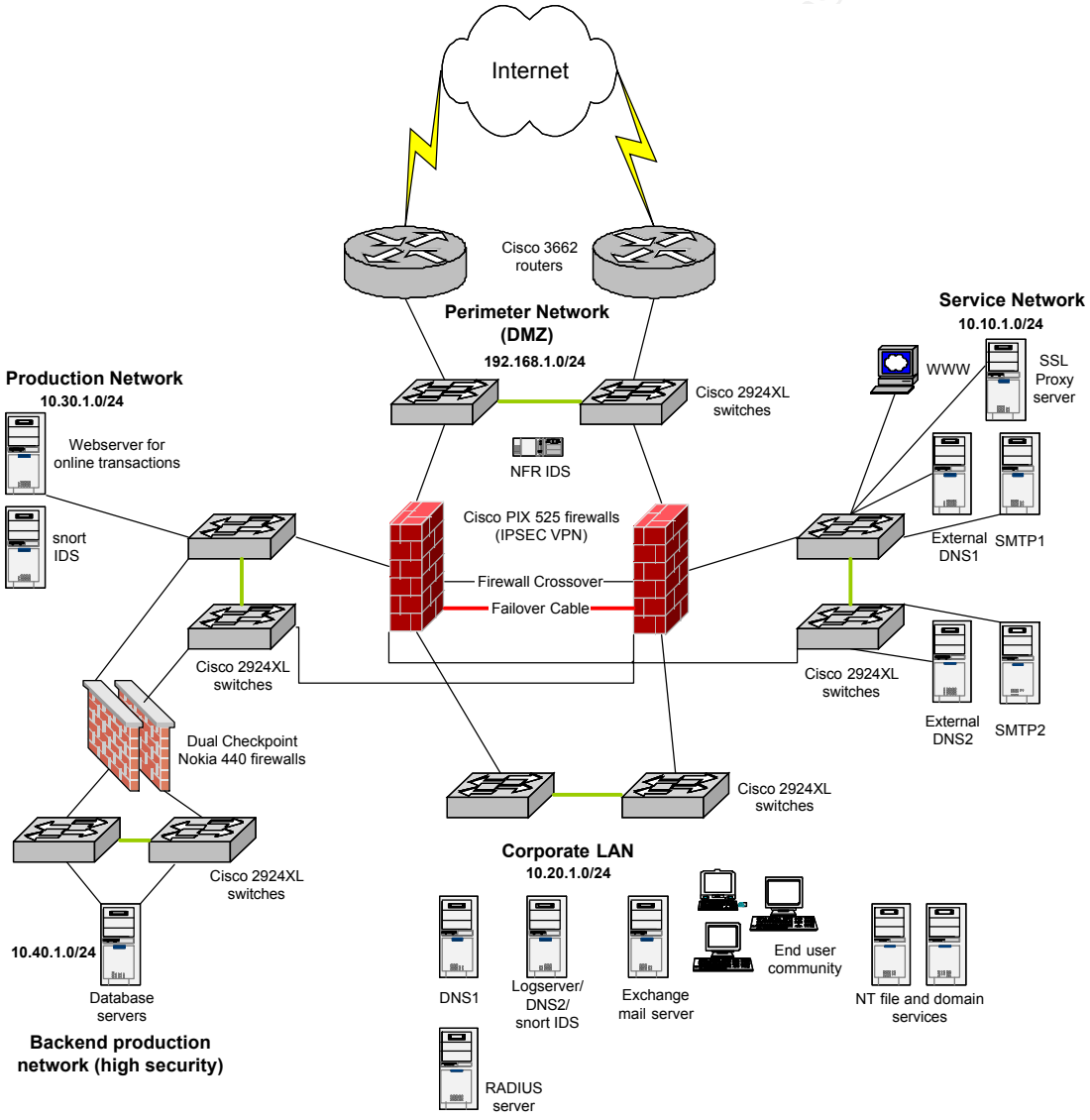
Security Design Considerations

One of the primary network design objectives that GIAC Enterprises must follow is to preserve scalability, particularly in the selection of the network infrastructure's hardware. In light of the success that GIAC Enterprises has already experienced, the possibility exists that network requirements one year from now may far exceed today's requirements. The capacity for growth must also be balanced by using hardware that is not too expensive for current budgetary allowances. Above and beyond these two guidelines, comes reliability, much of which can be gained by utilizing redundant hardware, i.e. dual firewalls and dual internet routers with multiple connections. Based on the earning estimates of GIAC Enterprises, I have designed a network with full redundancy in many areas; the additional associated costs seem reasonable and affordable, given projected profits. The cost of the network infrastructure's hardware can be reduced significantly, possibly by as much as half, though one must keep in mind that this will be at the expense of fault tolerance and security, in some cases. A scaled-down plan is almost

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

entirely the same logically, but may be a viable alternative since the exact financial details and goals of GIAC Enterprises are not known.

Network Diagram (fully redundant core and Internet access)



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

*Note—not all devices and connections are depicted, in order to provide a simple and more understandable network diagram.

Explanations of Network Diagram and Design

Network Divisions—Security Implications and Measures

The network design has provided for specific services, along with their applicable security risks and implications, to be divided into 5 distinct areas:

1. Perimeter Network—also known as the DMZ, this is the network between the border routers and the primary firewall. Because this area is not located behind the firewall (the border routers are the only defensive measure with which to block traffic), it is the most insecure network. All devices in this network use an IP address from the public 192.168.1.0/24 class C range. An NFR (Network Flight Recorder) intrusion detection system will be placed in this network to monitor all traffic, particular as a means of detecting the preliminary events prior to an attack. The NFR intrusion detection system can monitor abnormal behavior, known attacks, and violations of the corporate security policy. Its reporting features are good and it will be configured to send alerts to system administrators via email.
2. Service Network—services that will be publicly accessible from the Internet will be placed in this location. This includes SMTP relay servers, external DNS servers, public-information-only web servers, and proxy servers used to access the online product sales and storage systems. These servers will be running on Solaris 8, hardened in accordance with Lance Spitzner's "Armoring Solaris" document (http://www.enteract.com/~lspitz/armoring.html). The external DNS servers will be running bind version 9.1.3, continually being upgraded as new software is released to fix discovered bugs and vulnerabilities. These servers will not host any internal DNS zones; only registered IP addresses will be advertised. Extra security precautions will be undertaken such as only permitting recursive DNS lookups from private internal networks, and preventing the bind version number from being returned when queried. Care will also be taken to prohibit DNS transfers, except to the secondary host. The SMTP relay servers are running Postfix version 20010228-patchlevel 03. Postfix has been configured to prevent "spam" from being relayed—only mail from the internal networks or mail destined to the GIAC Enterprise domain is allowed. DNS has been configured with the MX record for each of the SMTP relay servers as the lowest priority, causing them to be used in a round-robin fashion while both are up and functioning. When one server is down, the other relays all mail. It is also possible to combine DNS and SMTP services on the same machine, in order to save hardware costs, but this is not the preferred solution. All systems in the service network are running only the services as designated by name, and SSH for remote management.

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

All other services have been disabled in the run control scripts and /etc/inetd.conf file. The SMTP relay servers are running Trend Micro virus scanner for detecting viruses.

3. Corporate LAN—general employees will log into desktop machines that are located in this network. GIAC Enterprises trusts its employees and will allow almost any type of traffic to be sent to the Internet from the corporate LAN. Microsoft Windows NT/2000 is the predominant operating system for end users and will also fulfill their authentication and file system needs. A central Microsoft Exchange server will be used for email, though mail will not be allowed to this machine directly from the Internet. Mail will be relayed via SMTP from the relay servers in the service network.
4. Production Network—machines that provide the online front end for fortune cookie sales and transactions can be found in this network. The main machine that is located here provides HTTPS connections to those users from the Internet that can successfully authenticate. This particular system has a certificate that is signed by VeriSign and can be viewed or verified by the customer. Direct access to this system from the Internet is not allowed; traffic is proxied by an SSL-capable proxy server located in the services network.
5. Backend Production Network—this network is guarded by dual Checkpoint firewalls, running on Nokia 440's, in addition to being behind the Cisco PIX's, the primary firewalls. Because this network contains the databases for the fortune cookie sayings themselves and data from financial transactions, (such as credit card numbers), it is necessary to provide a very high measure of security. A Checkpoint firewall was chosen in order to protect important data from any vulnerabilities that might be discovered on the Cisco PIX's by attackers. It is unlikely that the different firewalls would have the exact same problems. This additional layer of defense also helps to protect the backend network from any misconfigurations that might allow undesired access. Very limited traffic will be allowed into this network.

Border Routers

The border routers are the boundary between GIAC Enterprises' network and the Internet. This design uses two Cisco 3662 routers, running IOS software version 12.0.7T, each connected to a different ISP. Preferably, the ISP's would be using different local loops. Two routers and separate ISP's brings a measure of fault tolerance to the network's internet connectivity. Should one connection be down or under attack, the other connection is available for internet communication. These particular routers allow for exponential growth. Each router has the capacity for multiple T1 circuits (approximately 1.5 Mb/s of data capacity) and multiple DS3 circuits (approximately 45 Mb/s) if needed in the future; 6 slots are available for expansion cards. Within each router itself is a measure of redundancy—each has two power supplies. Should one power supply fail the router will continue to function perfectly. The routers are configured with HSRP (hot standby routing protocol), which allows all traffic to funnel through one router if the other router's links are down. It is also possible to run IOS Firewall software on these routers—while still limited in comparison to the functionality of the core firewalls, this provides a measure of security above and beyond that of the typical router.

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

Primary Firewalls

I have selected dual Cisco PIX 525 firewalls, running software version 5.2(5), as the core firewalls for GIAC Enterprises' network. In part, this selection has been made because of my familiarity with the product, and the performance value for the associated cost. That aside, my experience has shown that the Cisco PIX is a very capable firewall. Two 525's are being used for redundancy, should one firewall cease to function properly as in the case when an interface or another component fails. This redundancy allows for high availability connections between all of the company's networks and the Internet. The firewalls each have six interfaces, 5 of which are currently in use. This allows a 6th interface for future growth—future versions of code promise the capacity of 8 interfaces per firewall. Stateful failover is configured on the firewalls. This capability allows state information concerning details about the current connections to be transferred to the standby firewall, preserving connections in the case of failover. This feature requires the use of one network interface. In order to preserve registered IP address space and to mask the IP addresses of internal systems, NAT (network address translation) is used. This functionality essentially rewrites the IP address of a transmitting internal machine with an IP address from the 192.168.1.0/24 network that has been temporarily assigned; the reverse operation is preformed on IP packets traveling into the network from the Internet. Support for 3DES encryption has been enabled for VPN usage. Besides being an exterior firewall, this also functions as an interior firewall, separating the major network divisions.

VPN

GIAC Enterprises' business plan requires network connectivity with not only its business partners and suppliers, but also remote employees, such as traveling salespersons. For security measures all partners and remote users are required to use GIAC's VPN solution. In my design I have chosen to use an IPSEC VPN solution using dual PIX 525 firewalls, the core firewalls of the network infrastructure. Remote users will use the Cisco VPN Client, while partners and suppliers are required to implement an IPSEC device on their end, in order to create an IPSEC tunnel. Partners and suppliers will only be allowed to perform their needed tasks through the IPSEC tunnel, as specified by the network device configurations and security policies. Remote users will be able to authenticate to the corporate NT network by means of a RADIUS server, providing all capabilities of a local user. As a general rule, triple DES has been selected as the encryption algorithm, in tandem with SHA-1 for authentication, except where law prohibits this strong of encryption, such as foreign communications. In some situations it may be permissible to allow SSH from certain locations to specific machines, for use in remote system administration.

Switches

I have selected Cisco 2924xl switches, running software version 12.0(5.1)XW, to provide connectivity on each network. These switches are relatively inexpensive, yet are quite adequate for projected network traffic patterns. Each switch that connects to a firewall is cross-connected

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

to another switch that connects to that firewall's redundant host. This measure allows the firewalls to communicate with each other at each interface, (necessary for failover capability), and also allow for redundancy, should one of the switches fail. In a situation where there exists both a primary and a secondary server for a particular service, as is the case with the external DNS servers, each server is connected to a different switch, assuring that at least on server will be available in the event of a failed switch. Switches are being used, as opposed to hubs, for their performance advantages (reducing collisions and boosting throughput), and increased security. Should a machine be compromised, it is unlikely that all network traffic could be sniffed. This traffic could likely contain sensitive information, such as passwords, that could be used to attack yet another system. In the case of the intrusion detection systems that have been deployed for security, logging, and troubleshooting, (namely Snort and NFR), port forwarding will be used to forward all traffic from all ports to the port into which the intrusion detections system is connected.

Defense in Depth

GIAC's network design is based around the principle of defense in depth. This is evident in a couple of ways.

- The network design limits access by means of multiple levels of defense, each level performing some of the same functionality as the previous. An example of this is that the Internet routers block certain types of traffic from entering the network, the core firewalls also prevent certain traffic from getting past them, and the highly secure backend production network is guarded by yet another firewall. This final firewall, which protects the company's prime intellectual property and financial transaction data, has been purposely chosen to be of a different make and model than the core firewall. This limits exposure to potential vulnerabilities that may adversely affect another part of the network. To further increase the level of security on the production backend network the packet-filtering Checkpoint firewalls could be replaced with a firewall that dramatically differs from the Cisco PIX, possibly a proxy firewall (Raptor, for example).
- Different tools are being used to secure the network. Firewalls, intrusion detection systems, logging servers, and proxy servers all complement each other in their ability to protect the company's infrastructure from harm.

Assignment 2 – Security Policy (25 points)

Overview of GIAC Enterprises Security Policy

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

GIAC Enterprises' security policy is based on implicitly denying all traffic. In other words, the only traffic that is allowed to enter into the network is that which is necessary for the business to function and has been explicitly allowed.

In this section I have provided some of the more important parts of the configurations for the border router, the primary firewall, and VPN functionality (which is handled by the primary firewall). Commands are shown in `Courier New` font, followed by explanations in Times New Roman type, the font that has been used throughout the bulk of this document. The explanations will be given as C-style comments, bounded within /* and */, to add clarity for the reader.

Because I have only designated IP address ranges for each network, not addresses for individual machines, I will use a notation in configuration rulesets that incorporates the network ID and the name or function of a machine for the host ID. For example, 10.20.1.dns2 would represent the secondary DNS server on the corporate LAN (10.20.1.0/24). For devices that require static network address mappings to a registered IP address, names only are used (corresponding to the names used in the related static NAT commands) that is representative of an address on the 192.168.1.0/24 address space.

Border Router Configuration and Instructional Comments

/* This configuration is for one of the border routers. The other router would have a similar configuration. */

```
service password-encryption
enable secret ####################
username user1 privilege 15 password 7 ####################
username user2 privilege 15 password 7 ####################
username user3 privilege 15 password 7 ####################
username user4 privilege  2  password 7 ####################
```

/* For an extra measure of security, the passwords stored in the configuration have been encrypted to the operator's view. Separate accounts have been set up for each operator, allowing configuration changes to be attributed to a particular user. */

```
no service finger
```

/* The finger service is disabled. /*

```
no ip source-route
```

/* This blocks source-routed traffic. /*

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

```
no service tcp-small-servers
no service udp-small-servers
```

/* The above two commands eliminate unneeded services from the network, some of which are Echo, Discard, Chargen, and the Daytime services. /*

```
interface FastEthernet0/0
 description fa0/0 connected to GIACEXDMZSW1 port fa 0/1
 ip address 192.168.1.2 255.255.255.0
 ip access-group 109 in
 no ip redirects
 no ip directed-broadcast
 speed 100
 full-duplex
 arp timeout 1800
 standby track Serial1/0
 standby track Serial1/1
 standby 1 priority 110 preempt
 standby 1 ip 192.168.1.1
```

/* HSRP (hot standby routing protocol) is configured on the Ethernet port on the perimeter network. The other router has a default priority of 100. /*

```
interface Serial1/0
 description GIACISP Internet Circuit full T1 circuit
 ip address 172.16.1.90 255.255.255.252
 ip access-group 105 in
 no ip directed-broadcast
 ip accounting output-packets
 no ip mroute-cache
 service-module t1 timeslots 1-24
 no cdp enable
```

/* CDP is disabled on the serial interface. Access list 105 is enabled to prevent specific traffic from entering into GIAC Enterprises network/*

```
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.1.3 90
ip route 0.0.0.0 0.0.0.0 172.16.1.89 190
no ip http server
```

/* Set up the default route, including a route for use with HSRP. Be sure to disable the http management interface, often known for its security vulnerabilities. /*

```
access-list 102 permit ip 10.20.1.0 0.0.0.255 any eq 23 log
```


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

/* Having been assigned to the virtual terminal, this access list permits telnet connections only from the corporate LAN. All connections are logged. */

/*Access list syntax for Cisco 12.x IOS software (modifiers in square brackets are optional):
access-list *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**log | log-input**]

In the above syntax there are optional command modifiers that can be used. The keyword "host," for example, signifies a particular machine and does not require the use of a wildcard mask (or subnet mask in the case of a Cisco firewall) to identify the network. A wildcard mask is used to match particular hosts for the given network ID, similar in concept to a subnet mask, except that binary bits are "turned on," beginning with the low order bits. "source_addr" is representative of the originating host of the IP traffic and "desination_addr" represents the final destination of the traffic. If the "protocol" selected is either TCP or UDP, one may further define traffic that matches the access list by also requiring it to match a specific port number. These port numbers are usually characteristic of a particular type of traffic. Access lists for the PIX firewall (included in the firewall configuration later in this document) are similar in nature to those of a router. When an IP packet reaches the router it is compared to each successive statement in the access list for the interface on which the traffic arrived, until a match is found and the specified action taken. Although unlisted, the final implication is that traffic that has not matched a previous statement is denied.

A useful tip is to use a word processor to create all access lists, and to cut-and-paste the commands into the router. ***Note—deleting an access list, with a statement such as "no access-list 105" will remove all commands for that access list. */

```
access-list 105 permit icmp any 192.168.1.0 echo-reply log
access-list 105 permit icmp any 192.168.1.0 host-unreachable log
access-list 105 permit icmp any 192.168.1.0 time-exceeded log
access-list 105 deny   icmp any any log
```

/* Allow, but log, certain ICMP replies and error messages—useful for troubleshooting. Some companies may choose to block all ICMP. Inbound ICMP requests are blocked. /*

```
access-list 105 deny ip 192.168.1.0 0.0.0.255 any log
access-list 105 deny ip 10.0.0.0 0.255.255.255 any log
access-list 105 deny ip 127.0.0.0 0.255.255.255 any log
access-list 105 deny ip 172.16.0.0 0.15.255.255 any log
access-list 105 deny ip host 0.0.0.0 any log
```

/* Inbound traffic—the above access list blocks non-routable traffic entering GIAC Enterprises' network from the Internet, protecting against "spoofed" packets that could not legitimately originate outside the border router. This is known as ingress filtering. The public IP address range of GIAC Enterprises is included. /*

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

```
access-list 105 permit ip any any
```

/* Allow all other IP traffic through; the firewall will deal with it. In some circumstances it is desirable to fully duplicate the primary firewall ruleset. This would protect against any misconfigurations and further streamlines traffic before it even reaches the firewall, improving firewall performance.

An example of such a ruleset for the border routers is as follows:

access-list 105 permit tcp any any established
access-list 105 permit udp any host 192.168.1.ext_dns_1 eq 53
access-list 105 permit udp any host 192.168.1.ext_dns_2 eq 53
access-list 105 permit tcp any host 192.168.1.ext_web eq 80
access-list 105 permit tcp any host 192.168.1.ext_web_proxy eq 443
*/

```
access-list 109 deny ip 10.0.0.0 0.255.255.255 any log
access-list 109 deny ip 127.0.0.0 0.255.255.255 any log
access-list 109 deny ip 172.16.0.0 0.15.255.255 any log
access-list 109 deny ip host 0.0.0.0 any log
access-list 109 permit ip any any
```

/* Outbound traffic—the above access list blocks non-routable traffic to the Internet. All other traffic is allowed outbound. This is known as egress filtering and makes GIAC Enterprises a "good Internet neighbor." */

```
line con 0
 login local
 transport input none
line aux 0
line vty 0 4
 access-class 102 in
 login local
```

/* Access list 102 permits telnet connections from the corporate LAN only. */

Primary Firewall and Remote VPN Configurations and Instructional Comments

/* Note—the PIX 525 firewall also performs GIAC Enterprise's VPN services. */

```
PIX Version 5.2(5)
```


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

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 service security20
nameif ethernet3 production security80
nameif ethernet4 unused4 security30
nameif ethernet5 failover security35
enable password *************** encrypted
passwd **************** encrypted
```

/* Each interface is given a logical name. */

```
hostname giacfw
domain-name giacenterprises.com
```

/* Hostname and domain-name assignments are required to generate RSA keys for SSH, an encrypted protocol, similar in usage to telnet. These commands are also needed for VPN configuration. */

```
fixup protocol ftp 21
fixup protocol h323 1720
fixup protocol http 80
fixup protocol smtp 25
```

/* The above commands enable various application protocol features in the firewall, allowing the firewall to observe the respective protocols at the application level. In some cases, such as with "fixup protocol smtp 25," there is a security benefit—only certain smtp commands are allowed, and version information of the mailserver is masked. In other cases, as is the case with "fixup protocol ftp 21," it allows more functionality—active FTP, as opposed to passive FTP, is supported through the firewall. */

```
access-list acl_outside permit tcp any host ext_web_sever eq www
access-list acl_outside permit tcp any host ext_web_proxy eq 443
access-list acl_outside permit udp any host ext_dns1 eq domain
access-list acl_outside permit udp any host ext_dns2 eq domain
access-list acl_outside permit tcp any host ext_smtp1 eq smtp
access-list acl_outside permit tcp any host ext_smtp2 eq smtp
```

/* Access list syntax for Cisco PIX firewall software version 5.2(5):
access-list *acl_ID* [**deny** | **permit**] *protocol* {*source_addr* | *local_addr*} {*source_mask* | *local_mask*} *operator port* {*destination_addr* | *remote_addr*} {*destination_mask* | *remote_mask*} *operator port* */

/* When an IP packet reaches the firewall it is compared to each successive statement in the access list for the interface on which the traffic arrived, until a match is found and the specified action taken. Although unlisted, the final implication is that traffic that has not matched a

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

previous statement is denied. For the above access list ruleset, necessary traffic is permitted from the Internet to servers on the service network. The service network is the only network that can be accessed directly from the Internet. Services on the production network are accessed indirectly, i.e. the webserver for online transactions is accessed via the web proxy server on the service network over SSL. */

```
access-list acl_outside permit icmp any any echo-reply
access-list acl_outside permit icmp any any unreachable
access-list acl_outside permit icmp any any time-exceeded
```

/* Allow certain ICMP replies and error messages—useful for troubleshooting. Some companies may choose to block all ICMP. Inbound ICMP requests are not permitted. /*

```
access-list acl_service permit tcp host 10.10.1.web_proxy host
10.30.1.https_web_server eq 443
```

/* The HTTPS proxy server is allowed to access the webserver for online transactions, located on the production network. Only HTTPS connections are permitted. */

```
access-list acl_service permit tcp host 10.10.1.smtp1 host
10.20.1.exchange eq smtp
access-list acl_service permit tcp host 10.10.1.smtp2 host
10.20.1.exchange eq smtp
```

/* Allow mail to be relayed from the service network to the Microsoft Exchange server on the corporate LAN. */

```
access-list acl_service permit udp host 10.10.1.smtp1 host
10.20.1.logserver eq syslog
access-list acl_service permit udp host 10.10.1.smtp2 host
10.20.1.logserver eq syslog
access-list acl_service permit udp host 10.10.1.dns1 host
10.20.1.logserver eq syslog
access-list acl_service permit udp host 10.10.1.dns2 host
10.20.1.logserver eq syslog
access-list acl_service permit udp host 10.10.1.web_proxy host
10.20.1.logserver eq syslog
access-list acl_service permit udp host 10.10.1.web_server host
10.20.1.logserver eq syslog
access-list acl_production permit udp host
10.30.1.https_web_server host 10.20.1.logserver eq syslog
```

/* Syslog messages are allowed to pass through the firewall to be collected by a central logging server on the corporate LAN. Should one of these machines be compromised and have its

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

logging information changed or removed, there will be a second copy on the central logging server. The logfiles of this logging server are continually monitored with Logcheck scripts—if a message of importance is found the system administrators will be alerted. */

```
access-list acl_service permit udp host 10.10.1.smtp1 any eq smtp
access-list acl_service permit udp host 10.10.1.smtp2 any eq smtp
access-list acl_service permit udp host 10.10.1.dns1 any eq dns
access-list acl_service permit udp host 10.10.1.dns2 any eq dns
access-list acl_service permit tcp host 10.10.1.dns1 any eq dns
access-list acl_service permit tcp host 10.10.1.dns2 any eq dns
```

/* Allow the external mail servers to relay mail to the Internet. The DNS servers can perform recursive queries, but are configured to do so on behalf of the mail relay servers only. */

```
access-list acl_service deny ip any any
```

/* All other traffic originating on the service network is blocked. */

```
access-list 110 permit ip 10.20.0.0 255.255.0.0 172.50.1.0
255.255.255.0
```

/* The above command is related to the firewall's VPN configuration for remote users. Any user that negotiates an IPSEC tunnel, authenticates, and is successfully assigned an IP address in the 172.50.1.0/24 network, will be permitted to access the corporate LAN. */

```
logging on
logging timestamp
no logging standby
no logging console
no logging monitor
logging buffered errors
logging trap notifications
no logging history
logging facility 20
logging queue 512
logging host inside 10.20.1logserver
```

/* The firewall is configured to send syslog messages to the central logging server on the corporate LAN where important messages will trigger an alert for system administrators. */

```
icmp deny any echo-reply outside
icmp deny any echo-reply production
icmp deny any echo-reply service
```

/* The above commands prohibit specific firewall interfaces from responding to ICMP requests.

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

Systems on the corporate LAN are permitted to "ping" the firewall. */

```
ip address outside 192.168.1.11 255.255.255.0
ip address inside 10.20.1.1 255.255.255.0
ip address service 10.10.1.1 255.255.255.0
ip address production 10.30.1.1 255.255.255.0
ip address unused4 10.254.1.1 255.255.255.0
ip address failover 10.100.100.1 255.255.255.0
```

/* Interfaces for the primary firewall have been assigned IP addresses. */

```
ip local pool vpn 172.50.1.1-172.50.1.25
```

/* Remote VPN users will be assigned IP addresses from the 172.50.1.1-25 range. */

```
failover
failover timeout 0:00:00
failover poll 6
failover ip address outside 192.168.1.12
failover ip address inside 10.20.1.2
failover ip address service 10.10.1.2
failover ip address production 10.30.1.2
failover ip address unused4 10.254.1.2
failover ip address failover 10.100.100.2
failover link failover
```

/* Stateful failover has been activated by the previous block of commands, incuding assigning IP addresses to the standby firewall. */

```
global (outside) 1 192.168.1.176-192.168.1.250 netmask
255.255.255.0
global (outside) 1 192.168.1.175 netmask 255.255.255.0
```

/* Outbound traffic will be translated to an address in the 192.168.1.175-250 range, unless a static mapping has been created. */

```
nat (inside) 0 access-list 110
nat (inside) 1 10.20.1.0 255.255.255.0 0 0
nat (service) 1 10.10.1.0 255.255.255.0 0 0
nat (production) 1 10.30.1.0 255.255.255.0 0 0
nat (production) 1 10.40.1.0 255.255.0.0 0 0
```

/* VPN traffic from remote users is exempted from network address translation and systems on all networks will use NAT for outbound traffic if the traffic is not denied by an access list. */

```
static (service,outside) 192.168.1.smtp1 10.10.1.smtp1 netmask
```


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

255.255.255.255 0 0
static (service,outside) 192.168.1.smtp2 10.10.1.smtp1 netmask 255.255.255.255 0 0
static (service,outside) 192.168.1.dns1 10.10.1.dns1 netmask 255.255.255.255 0 0
static (service,outside) 192.168.1.dns2 10.10.1.dns2 netmask 255.255.255.255 0 0
static (service,outside) 192.168.1.www 10.10.1.www netmask
255.255.255.255 0 0
static (service,outside) 192.168.1.web_proxy 10.10.1.web_proxy
netmask 255.255.255.255 0 0
static (inside,service) 10.20.1.0 10.20.1.0 netmask 255.255.255.0
0 0
static (inside,production) 10.20.1.0 10.20.1.0 netmask
255.255.255.0 0 0
static (production,service) 10.30.1.0 10.30.1.0 netmask
255.255.255.0 0 0

/* Static network address translations have been set up for systems in the services network. Internal networks will not use NAT for communication with other internal networks. */

access-group acl_outside in interface outside
access-group acl_service in interface service
access-group acl_production in interface production

/* Previously defined access lists are now enabled. */

route outside 0.0.0.0 0.0.0.0 192.168.1.1 1
route production 10.40.1.0 255.255.255.0 Checkpoint_fw 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00
h323 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute

/* Network routes have been set up and timeouts for address translations and certain types of connections have been established. */

aaa-server RADIUS protocol radius
aaa-server steel_belted (inside) host 10.20.1.radius
********** timeout 10
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set myset esp-3des esp-sha-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap client configuration address initiate
crypto map mymap client configuration address respond
crypto map mymap interface outside
isakmp enable outside

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

```
isakmp key ********** address 0.0.0.0 netmask 0.0.0.0
isakmp identity hostname
isakmp client configuration address-pool local vpn outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash sha
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400
```

/* The above block of commands sets up the crypto maps and transform sets to enable VPN for remote users. Users can authenticate to the corporate Windows NT network through the RADIUS server. In the case of this particular configuration, remote users can authenticate from any location, as will be the case with traveling salespersons. The Cisco VPN client installed on each remote computer must be configured with the same pre-shared key value as given in the firewall configuration. Given the fact that there are few remote users, using a pre-shared key requires less effort than using digital certificates. As the company grows, dynamic key exchange will make administration simpler. For maximum encryption security, all remote users must use the Triple DES encryption algorithm for ESP and SHA-1 for AH. These have been selected because they are the strongest IPSEC algorithms supported by the PIX firewall. There is slightly more overhead as compared to weaker algorithms, but the difference is negligible on systems with fast processors. Single DES for international remote users will be implemented if required by law. */

```
ssh 10.20.1.sysadmin 255.255.255.0 inside
ssh timeout 20
```

/* The firewall virtual console can be accessed remotely via SSH from the system administrator's machine. */

Testing Access Lists

One of the best tools that I have found for testing firewall and router filtering rulesets is Nmap. This free security scanning tool, created by Fyodor, is available for download at www.insecure.org/nmap. It is simple to use, yet is a very effective tool. Nmap is designed to connect to a particular host or hosts on a specified port or ports. This can be done with UDP or TCP with a variety of different types of scans. If Nmap is able to make a connection the port is accessible from that location. If the port is not accessible, it is either being filtered by a router or firewall, or the service is not running. Because of the way that connections are way, it is usually possible to tell if the service is not active or if access to the port is being blocked.

The results of a typical Nmap scan are shown below:

> nmap -P0 -p 1-65535 192.168.1.ext_smtp1

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

```
Starting nmap V. 2.54BETA7 ( www.insecure.org/nmap/ )
Interesting ports on smtp1.giacenterprises.com (192.168.1.ext_smtp1):
(The 65535 ports scanned but not shown below are in state: closed)
Port       State       Service
25/tcp     open        smtp

Nmap run completed -- 1 IP address (1 host up) scanned in 35 seconds
```

The above command issued a typical TCP scan on host 192.168.1.ext_smtp1, GIAC Enterprises primary SMTP relay server. The scan was done on all ports numbered 1-65535, was issued from the Internet through the primary firewall, and was done without first pinging the host, -P0 (often it is not possible to ping the host if a firewall is blocking ICMP). Because only TCP port 25, the port for SMTP email communication, is shown as being open, we can be relatively confident that our firewall is blocking traffic to the other 65534 ports. This is the result that we were hoping to get based on the firewall ruleset for this host as discussed previously.

To thoroughly test our firewall and router access lists we should perform a similar scan from the Internet for the entire GIAC Enterprises public IP address range. We should follow up with a UDP scan of the same ports and hosts, using the –sU option. If the results are not what we had anticipated, i.e. either more or less ports are accessible than are rulesets allow access to, we must investigate the problems that are discovered.

It is also possible to use Nmap to test filtering rules that prevent spoofing of non-routable IP addresses. This can be done with the command line "nmap –sS –p 1-65535 –D 10.10.10.1 192.168.1.ext_smtp". –D denotes a decoy address (10.10.10.1). It is not possible to use the default scan type to use decoys; -sS, a half-open TCP SYN scan will work with decoys—so will other options. In order to see if the spoofed IP traffic passed through the access lists it is necessary to snoop traffic on the destination side of the firewall, with a traffic capturing application such as Tcpdump. Tcpdump is a handy tool for examining network traffic off of the wire; it is available free from http://www.tcpdump.org/. VPN traffic can be sniffed with Tcpdump to check packet payloads for readable data that should be encrypted. A similar tool, Windump, is available to run on Windows operating systems. Port scanning tools, such as SuperScan 3.0 (http://www.foundstone.com/rdlabs/tools.php), are also available for the Windows platform. Other tools can be used to spoof traffic, including Hping2, one of the more popular spoofing applications (http://www.kyuzz.org/antirez/hping.html).

Assignment 3 – Audit Your Security Architecture (25 Points)

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

The primary goal of auditing GIAC Enterprises' network infrastructure is to verify that the mandated security policy is still being followed and that its rules and regulations actually create a secure environment. Testing will be done on a semi-annual basis, unless further testing is deemed appropriate at any future time. For a security audit to have any worthwhile effect, it must be possible to make changes to the network that correlate to the security policy, if changes need to be made. The authority to enforce the security policy must exist, or else the policy is nothing more than hopes and dreams. In some circumstances, the beginning step toward a security audit is to actually come up with a documented security policy, which can sometimes be a long series of battles, especially if the policy is not backed by somebody from the ranks of management (upper management preferably).

Planning the Assessment

Much of the time spent in a security audit will be in the planning stage. Care must be used to make sure exactly what tests should be run, why they should be run, and how they should be run. An overlooked area is potentially an overlooked vulnerability.

Security auditing is to be done by GIAC Enterprises' staff members or a third party company if desired. Tests are to be performed on the perimeter network from the Internet and on internal networks; the exact tests will be dictated by the security policy—test everywhere that access is restricted in one form or another. All testing is to take place during off-peak hours, preferably Friday evening. If possible, tests should occur on the eve of a three-day weekend. The off-peak time following the testing will be very important should something go wrong and require extensive effort to either repair any services, or to make appropriate changes if a serious problem arises. Minor testing may be done during evening hours during the normal workweek.

The audit will strictly involve searching for vulnerabilities and determining if the corporate security policy is actually in effect. There should be no DOS (denial of service) testing or exploitation of destructive vulnerabilities on production equipment.

It is difficult to project the cost of a security audit, particularly if there is uncertainty concerning the security policy, and if there is disagreement regarding its guidelines. Planning may require numerous meetings with practically every department if authority is spread thin throughout the company. For the sake of this assignment we will assume that the security policy is followed rather diligently by the IT staff, and that it is supported by upper management. In this scenario estimated costs would likely be along the following lines:

- 3 hours—review of security policy.
- 3 hours—discussions of security policy and planning meetings for security audit agenda. (This is likely to involve a number of staff members and the IT manager.)
- 12 hours—Verify configurations of important hosts. It is anticipated that different people

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

will perform different tasks, but the total man-hours will be 12.

- 6 hours—extensive testing of all packet filtering rulesets, in accordance with filter testing methodology described in assignment 2.
- 6 hours—Document results and produce report.
- 8 hours—work to resolve any discovered issues (this may take longer if serious and complex problems are found).
- Total—38 hours, essentially 1 full workweek.

Implementing the Assessment

One of the most important auditing tasks is to audit GIAC Enterprises primary firewall, dual Cisco PIX 525's running software version 5.2(5). A major focus of this task involves using a port scanning tool, such as nmap, to verify that the firewall access lists are functioning as originally intended. The conclusion will determine who can and can't use certain network services of GIAC Enterprises that are located behind the firewall.

Since the use of nmap and a packet sniffer to test packet-filtering rulesets has been outlined in assignment 2, I will not go into detail about how to perform these tests, nor extensively show all of the tests involved, but will present a summary of the basic procedures and commands.

In order to determine which tests should be ran, one must determine the restrictions that the security policy places upon each network and its respective services. Then, the firewall ruleset should be analyzed to see if it is in compliance. Following this, the expected results of a portscan to a particular network or host should be determined and compared to the actual results. All data should be documented.

One might decide to start the scans be determining which services on which hosts are available from the Internet by scanning GIAC Enterprises' entire registered class C network as follows:

> nmap -sS -P0 -p 1-65535 192.168.1.1-254

For non-existent hosts or those that should not be accessible at all, the results should be similar to the following:

All 65535 scanned ports on (192.168.1.1) are: filtered

Those hosts that should be accessible should only be accessible by the ports that are specified in the firewall ruleset, as in the result below:

Interesting ports on ext_dns2.giacenterprises.com (192.168.1.ext_dns2):
(The 65535 ports scanned but not shown below are in state: closed) Port

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

State Service 53/tcp
open domain

As shown above, only traffic on TCP port 53 (typical DNS queries) can reach the external secondary DNS server. Likewise port TCP 80 (HTTP) is open for the webserver, TCP port 25 for the SMTP mail relays, and TCP port 443 for the HTTPS proxy server.

Similar testing with Nmap should be done against all networks and hosts according any restrictions that should be in place specified by the security policy. Besides scanning for open TCP ports, scanning for open UDP ports will also be necessary to determine other available services.

An intensive Nmap TCP port scan performed on the corporate LAN from the service network reveals that TCP port 25 (SMTP) is open to the Exchange server from the mail relay servers only and that UDP port 514 (syslog) is open to the central logging server from all servers. Additionally, TCP port 443 (HTTPS) is open on the production network's online web transaction server from the HTTPS proxy server. No other traffic is allowed to be initiated to any other network, including the Internet. This is also the case for the production network.

Nmap scans from the corporate LAN show that all UDP and TCP ports are open to the service network, the production network, and the Internet. Originally, it was thought that this configuration was fine, since all employees are trusted under the current security policy. This may pose a serious problem, particularly if GIAC Enterprises ever employs a malicious person. Even worms and viruses downloaded by end users may cause problems attempting to exploit vulnerabilities on machines.

One important fact to note is that during the assessment attempts were made to penetrate the firewall with various types of ICMP traffic. Although ICMP echo requests were not allowed to pass into the network from the Internet, certain types of ICMP messages could be crafted that could bypass access lists. For example, one could send unsolicited ICMP echo replies into the network. This could possibly be exploited in an ICMP DOS attack or be used as a covert communication channel, such as Loki.

Besides scanning the firewall for misconfigurations, it is also necessary to continually be aware of software bugs on all systems and to upgrade the software when stable patches become available. Production machines should be compared to a baseline that was gathered before initial deployment to see if performance or anything else has since changed. It is helpful to use a software package such as tripwire that will periodically monitor selected files and alert system administrators of changes—sometimes these changes are the result of a machine being compromised. For the sake of this exercise it has been determined that all systems are intact, fully functioning, and that there are no known vulnerabilities or issues with their operating processes and servers.

Perimeter Analysis and recommendations

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

Based on the previously conducted assessment it has been determined that the network infrastructure is solid, as viewed externally from the Internet. All systems are fully operating and can handle the current load.

However, it is evident that some changes to the firewall ruleset must be made, in order to protect production machines from users and systems on the internal corporate LAN, especially should a malicious person ever be employed. Other problems could arise from worms and viruses that may exploit vulnerabilities on production systems; end users could also install modems to their desktop PC's that may lead to compromises. From the corporate LAN all hosts and services on the service network and production network are accessible. The high-security backend production network, where financial and intellectual property databases are kept, is protected from the corporate LAN with a Checkpoint firewall, but if that firewall is ever misconfigured its protected network may become open as well. In particular, since it is not necessary for internal employees to have unrestricted access to these networks in order to complete their jobs, this added protection will not be counterproductive. Some exceptions must be made—for example, system administrators use SSH for remote management of production machines.

To solve the potential problems mentioned above, the following access list rules will be applied to traffic entering the firewall on the inside interface, the interface located on the corporate LAN:

```
access-list acl_inside permit tcp 10.20.1.0 255.255.255.0 host
10.10.1.web_sever eq www                                    access-
list acl_inside permit tcp 10.20.1.0 255.255.255.0 host
10.10.1.web_proxy eq 443
access-list acl_inside permit tcp host 10.20.1.exchange host
10.10.1.smtp1 eq smtp
access-list acl_inside permit tcp host 10.20.1.exchange host
10.10.1.smtp2 eq smtp
access-list acl_inside permit tcp host 10.20.1.sys_admin
10.10.1.all_machines eq 22
access-list acl_inside permit tcp host 10.20.1.sys_admin
10.30.1.all_machines eq 22
access-list acl_inside deny ip any 10.10.1.0 255.255.255.0 access-
list acl_inside deny ip any 10.30.1.0 255.255.255.0
access-list acl_inside deny ip any 10.40.1.0 255.255.255.0
access-list acl_inside permit ip 10.20.1.0 255.255.255.0 any
```

Additionally, the following ICMP access list rules will be removed from the outside interface, in order to block all ICMP traffic:

```
access-list acl_outside permit icmp any any echo-reply
access-list acl_outside permit icmp any any unreachable
access-list acl_outside permit icmp any any time-exceeded
```


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

Conclusion

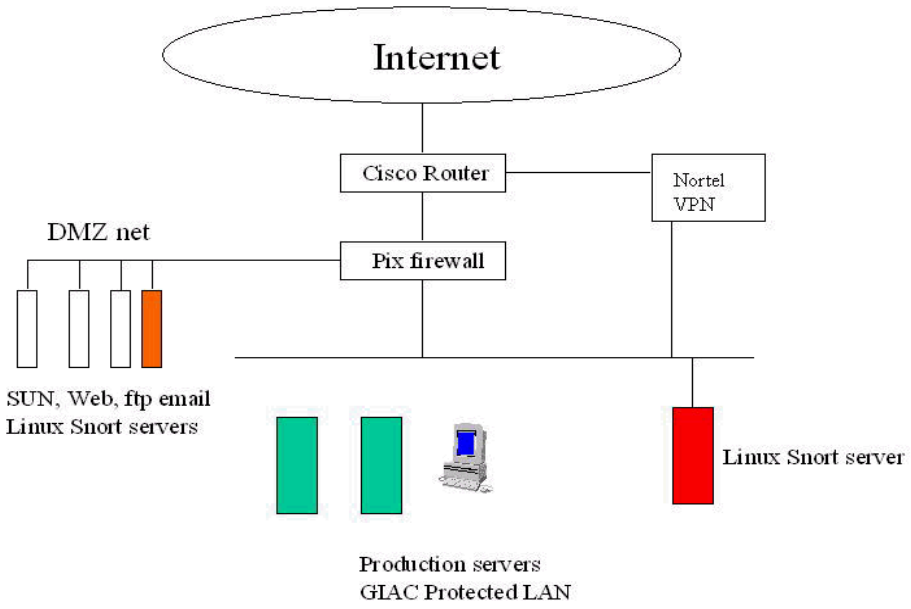
Auditing GIAC Enterprises' network infrastructure proved to be an effective task. Certain problems that were not considered during the design phase were eliminated, the IT staff more fully understood the network and many of its potential weaknesses, and confidence was gained. The security policy was modified to counteract all discovered vulnerabilities and device configurations were changed to be in compliance to the new security policy.

Assignment 4 – Design Under Fire (25 points)

For this assignment I have chosen to attack the network designed by Chap Wong, 11/20/2000. This network design, submitted as part of a practical can be found at:

http://www.sans.org/y2k/practical/chap_wong_GCFW.doc

A diagram of the victim network is shown below:



Attacking the Primary Firewall

I intend to exploit a vulnerability with the Cisco PIX firewall's ability to handle FTP, Cisco bug

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

ID CSCdp86352. This bug is documented on numerous websites, including Cisco's own http://www.cisco.com/warp/public/707/pixftp-pub.shtml. Further explanation of this exploit is given at http://oliver.efri.hr/~crv/security/bugs/Others/cisco26.html. There are a number of ways to perform this exploit, one of which is the public exploit ftp-ozone, written by Dug Song (this can also be used against certain versions of Checkpoint FW-1). Source code for ftp-ozone can be found at http://packetstormsecurity.org/0002-exploits/ftp-ozone.c.txt.

The victim network meets all 3 qualifications of this FTP vulnerability:

- The PIX firewall is running software version 5.0(3), one of the affected versions
- The command "fixup protocol ftp 21" is enabled
- There is an FTP server behind the firewall, accessible from the Internet. This is evident in the command "conduit permit tcp host 2.2.2.3 eq ftp any"

This vulnerability is due to the fact that the PIX can be fooled into opening up ports for inbound connections to an FTP server if the FTP server can be triggered into sending, according to Cisco, "a valid command, encapsulated within an error message, and causes the firewall to read the encapsulated partial command as a valid command." This command appears to be a valid 227(xxx,xxx,xxx,xx,prt,prt) response. The problem with the PIX is "that the 'fixup protocol ftp' component does not provide sufficient enough checks to verify PASV connections before creating a dynamic hole through the firewall." Exploiting this vulnerability, any port on the FTP server can be accessed.

Simply opening up a connection to an FTP server on a port of choice does not cause any harm in itself. Harm may come when an attacker opens up a port to an insecure service, possibly compromises the machine, and uses that machine as a springboard from which to attack other systems. Therefore, the firewall ruleset is not able to do the job that was originally intended.

One may argue that it is not fair game to select this particular network, designed prior to current versions of PIX firewall software—that this is too easy of a scenario under future conditions, and that the software would have been upgraded by now. My argument is that, although this network design was submitted 8 months ago, this particular vulnerability was made public a number of months prior to submittal. Additionally, it is quite common to find insecure and unpatched network systems in production, despite all the warnings and alerts that are given.

Updating the PIX software to a non-affected version would resolve the problem, if the victim network still wants to provide FTP service and allow outbound active FTP sessions.

Denial of Service Attack

We will now subject the same victim network configuration and design to a theoretical attack from 50 compromised cable modem/DSL systems.

Looking at the configuration of the Cisco border router, it is apparent that a number of privileged ports (and a few upper port numbers as well) are blocked. But, most of the 65,535 available UDP

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

and TCP ports are open to the perimeter network. All ICMP traffic is blocked by the implicit "deny" statement that is examined as the final rule of the Internet access list. There is no ingress filtering, so we have the option of using spoofed IP addresses if desired.

The PIX firewall is locked down for the most part. Ports to various servers are open, such as SMTP, FTP, DNS, HTTP, and a couple of ports for the Citrix ICA protocol. Standard UDP DNS queries are not accessible, but TCP port 53 is. With this in mind, it is quite possible that the DNS servers are not restricted in zone transfer requests. This may prove to be useful during the reconnaissance phase. Instead of reviewing the configuration, it would be possible to determine these open ports with a port scanning tool such as nmap.

After reviewing our options, and scoping out the victim network, it appears that using a DDOS tool such as TFN2K (Tribal Flood Network 2000) will be one of the easiest ways to use all 50 zombie machines to create a formidable attack. Zipped source code for TFN2K can be found at ftp://ftp.ntua.gr/pub/security/technotronic/denial/. It is very likely that most of these 50 machines under our control are Windows PC's; this is fine, because TFN2K runs on Windows. Using TFN2K, we will have one master computer that controls 50 attacking agents. Communications between the master and agents may be encrypted; the master can spoof its source IP address so that it cannot be identified as the master if it is detected. Agents can attack using a variety of packet types: TCP SYN flood, UDP flood, ICMP flood, or a Smurf attack. Since the victim network has only a single connection to the Internet, we will try a DOS attack to use up all of its bandwidth, not just to prevent access to one host. Our attack will target a host on the inside of the firewall, such as the mail server. This will use the router's processing resources as it enters the outside interface and as it is passed by the inside interface. The firewall will spend CPU time dealing with the packets as well, where most of the traffic will be blocked, never actually reaching the mail server. It is expected that we can effectively accomplish this with 50 hosts using TFN2K.

For the attack, we will spoof the source address of the master, in order to hide our identity. We will communicate to the majority of the agents to perform a MIX attack, an option that interchanges UDP, TCP, and ICMP traffic in a 1:1:1 ratio. This is specifically designed to wreak havoc on packet filtering devices. We will also increase the packet size to 1500 bytes, which will use up dramatically more of the victims precious bandwidth and processing power. A small group of our zombies will carry out a TARGA3 attack, sending random packets with bogus IP based values, hoping that this will cause the IP stack implementation to crash, fail, or show other undefined behavior, the main purpose behind TARGA3. There should be no bandwidth left for traffic to exit the victim's network, nor should useful traffic be able to enter. Our backup plan is to issue a Smurf attack against the network, having previously created a huge list of broadcast amplifiers, potentially more devastating than the primary planned attack.

It is very difficult to defend against this type of attack, especially if the victim network has only one connection to the Internet. A second connection would be one of the most effective methods of defense, particularly if one of the router's outside interfaces is the target destination. Just disconnect the one interface that is under attack. Of course, attackers use the same mentality—if 50 zombies are good, 100, or even 1,000 are even better (especially if they have

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

DSL or cable modem connections). One method of precaution that would fully remove pressure from the victim's network is to have the victim's ISP (who probably has lots of bandwidth) block the traffic from even getting to the victim. This may be difficult if the source IP's are being spoofed and ports and traffic types are random and/or mixed. Good access lists help, but they can't solve the problem fully.

Another very simple DOS attack with certain results would be to exploit a bug involving the Cisco 4500 router and its 11.2 IOS revision. This would only apply if the command "no ip http server" is not in effect on the router, implying that the web interface is available. Nothing is mentioned to indicate whether or not this is enabled in the router configuration. But, if the web interface is enabled, since HTTP traffic is allowed to the outside and inside interfaces of the victim router, a simple command would boost CPU utilization to 100%, rendering the router useless, causing it to reboot shortly. From an HTTP browser window, the command "http://router.victim.com/%%" would crash the router. A script could be written to have each zombie host issue the command repeatedly if desired. Since we are targeting the outside interface of the router, the victim's intrusion detection systems will be useless. The victim may just think that their router is failing (after this lockup occurs repeatedly). I have personally tested this vulnerability on a Cisco 4500 with 11.2 IOS software and have verified the exact results described above. This exploit can easily be prevented by disabling the web interface with the command "no ip http server." A description of Cisco bug ID CSCdr36952, can be found on Cisco's website at: http://www.cisco.com/warp/public/707/ioshttpserver-pub.shtml.

Internal System Compromise

The network designer did not mention the specific operating systems that each service would run on, although it is clear that there are both Unix and Windows NT machines. Reconnaissance will hopefully shed some light on the matter.

Initially I would target the webserver, since they are often poorly secured. In addition, because the victim company performs online e-commerce, this may get us closer to stealing valuable information—credit card data, for example. It is also possible that the webserver is running Microsoft IIS. There have been quite a few serious vulnerabilities discovered during the past few months, some that are very likely to give an attacker administrator privileges. With all of the IIS server patches that have been released, finding a server that is not up to date would not be too surprising. A couple of quick commands provide us with some important system information:

```
>telnet webserver.victim.com 80

get /http/1.0
```

The above commands bring back the following text, abbreviated for pertinence:

HTTP/1.1 401 Access Denied
Server: Microsoft-IIS/5.0

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

```
Date: Fri, 20 Jul 2001 02:51:43 GMT
WWW-Authenticate: Negotiate
WWW-Authenticate: NTLM
WWW-Authenticate: Basic realm="inside.webserver.address"
Content-Length: 3643
Content-Type: text/html
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html dir=ltr>
<head>
<style>
a:link              {font:8pt/11pt verdana; color:FF0000}
a:visited           {font:8pt/11pt verdana; color:#4e4e4e}
</style>
<META NAME="ROBOTS" CONTENT="NOINDEX">
<title>You are not authorized to view this page</title>
<META HTTP-EQUIV="Content-Type" Content="text-html; charset=Windows-1252">
</head>
……..
```

We now know that the server is in fact a Windows 2000 system, running IIS 5.0. Additionally, we have even discovered its internal IP address, if the victim network is using network address translation. (An explanation of how to protect this internal address is given at http://support.microsoft.com/support/kb/articles/Q218/1/80.ASP).

Now we will try to use one of IIS's vulnerabilities to our advantage. We will cause a buffer overflow and install a backdoor application. The source code for our exploit, iis-injector, is found at http://www.phreak.org/archives/exploits/microsoft/iis-injector.c. This allows us to deliver and execute a payload of our choice, stored in a binary file. The payload will be a back door program, such as BO2k. BO2k can be obtained from http://sourceforge.net/projects/bo2k/. After we have created the bo2k server package, we will compile the exploit source code and attempt to use it. If the IIS 5.0 server is unpatched and vulnerable, we will install the BO2k server as root—then we will take control of the webserver. This will be a good place from which we can attack other systems.

After unsuccessfully attempting the exploit, we find that the server has indeed been patched and is not susceptible. Maybe we can get to the webserver another way.

Now we will try an attack on the FTP server, another system that may prove to be an easy target. Telneting to the FTP server produces the following banner:

```
>ftp ftp.victim.com
Connected to ftp.victim.com.
220 ftp server Microsoft FTP Service (Version 5.0).
User (ftp.victim.com:(none)):
```


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

The FTP server is also running IIS 5.0. Today might be our lucky day! Since the HTTP service on the FTP server is not configured to be accessible from the Internet, it is possible that the administrators have been more lackadaisical in its patching and upkeep. Using the PIX FTP vulnerability, previously discussed as a firewall attack, will allow us to connect to any port on that system, including TCP port 80. This approach confirms that the IIS HTTP server is in fact running. We can try the same exploit as we did with the webserver. We may also want to try other exploits as well if necessary, especially since we are free to access any TCP port that we choose. Using the standard Windows netBIOS commands (i.e. nbtstat –A host.victim.com) may produce some important clues to further aid our efforts. Upon executing the buffer overflow exploit we find that the FTP server is indeed vulnerable—BO2k is now installed and has given us full control of the system! (If these two servers are not actually running IIS and are not Windows machines we would have to search for vulnerabilities after determining the relevant system details).

The next step is to install some useful tools onto our compromised machine; a packet sniffer (it is not indicated whether or not the network is switched) and other exploit tools would be helpful. We will also obtain the SAM file and decrypt the passwords that it contains. It doesn't take long for us to figure out that the webserver has the same accounts and passwords as the FTP server—the webserver has now been compromised!

Further attempts warrant investigation of the DNS servers. Considering the fact that the firewall is not configured correctly to allow UDP queries on port 53, the administrator may not fully understand how to support and configure DNS. The machine may be running an older version of Bind that can be used to gain root access. The possibilities are limitless. If we hadn't had success yet, the Citrix server and mail servers would be next.

Eventually, we will attempt to progressively work our way to the customer and product databases. After obtaining all of the information we desired it will be helpful to cause some problems to make the victim's investigation efforts much more difficult. After all evidence of our activities has been erased, (removing/editing logfiles), we will execute the DDOS attack that was previously described.

Conclusion

It is very critical to never underestimate the importance of keeping a system up to date, and configured properly. Services that aren't needed should be disabled—they will only use up resources and give attackers more options to use when trying to compromise the system.

References

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

Zwicky, Elizabeth, Simon Cooper, D. Brent Chapman. Building Internet Firewalls. 2nd ed. Sebastopol: O' Reilly & Associates, Inc., 2000

Northcut, Stephen, Judy Novak. Network Intrusion Detection, an Analyst's Handbook. 2nd ed. Indianapolis: New Riders Publishing, 2001

Spitzner, Lance. "Armoring Solaris." 22 October 2000. URL: http://www.enteract.com/~lspitz/armoring.html (17 July 2001).

Cisco Systems, Inc. "Configuration Guide for the Cisco Secure PIX firewall Version 5.2." 2000

Northcutt, Stephen, Gary Kessler, Hal Pomeranz. "TCP/IP for Firewalls and Intrusion Detection." The SANS Institute, 2001

Brenton, Chris. "Firewalls 101: Perimeter Protection with Firewalls." The SANS Institute, 2001

Brenton, Chris, Lance Spitzner, S. Winters, Stephen Northcutt. "Firewalls 102: Perimeter Protections and Defense, In-Depth." The SANS Institute, 2001

Brenton, Chris. "VPNs and Remote Access." The SANS Institute, 2001

Brenton, Chris. "Network Design and Performance." The SANS Institute, 2001

Scambray, Joel, Stuart McClure, George Kurtz. Hacking Exposed. 2nd Ed. Berkely: Mcgraw-Hill, 2001

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

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