Global Information Assurance Certification Paper

GIAC Enterprises Security Architecture, Policy and Audit.

Including

Design Under Fire

GIAC Level 2 - Firewalls, Perimeter Protection and VPN's

GCFW Practical Assignment For Sans London 2001

Author:	Mark Johnston
Date:	11 September 2001

Version:	1.5 e

TABLE OF CONTENTS

1. ASSIGNMENT 1 – Security Architecture

1.1 General Overview

GIAC Enterprises is a growing Internet Company that expects to earn $200 million per annum in online sales of fortune cookie sayings. GIAC has also recently completed a merger/acquisition with another company.

1.2 Purpose

Since GIAC has an Internet presence and that potential damage to their information/data could be accomplished because of this, the purpose of assignment one is to define a comprehensive security architecture that will enable GIAC Enterprises to operate securely on the Internet but without hindrance to essential operations.

1.3 Budget

Considering that this is a start-up Internet Company, a large portion of the first years income will be spent on the building up of the enterprise such as purchasing of office equipment, desktops and servers. However the following will be assumed with regards to the security architecture:

- Commercial products can be purchased where required and with justification.
- A dedicated security engineer and network administrator will be hired to administer GIAC's site. Thought should be given for trainee backup administrators in the event of one of the existing administrators falling ill or being unable to work.
- Budget has been allowed for user training on security.

1.4 Security Considerations

1.4.1 General

GIAC Enterprises has opted for a multi-platform environment consisting mainly of Unix, Microsoft and Cisco (with exception for the SunScreen Firewall). The security architecture will combine these platforms to give speed and processing power under Unix and Cisco combined with the worldwide support and ease of use with Microsoft.

1.4.2 Database

GIAC's livelihood is dependant on being able to supply cookie sayings to customers. The cookie sayings reside on a database within GIAC Enterprise's network and thus the database and its data are considered to be the core of GIAC's business. It is beyond the scope of this assignment to describe how to administer and maintain a database, but it is worthwhile to mention that adequate resources should be used to take care of the database. Some important resources would typically include competent administrators and an adequate backup strategy.

1.4.3 Access Requirements

According to GIAC's requirements there are 3 areas that access needs to be defined for which are partners, customers and suppliers respectively. However it is also important to touch on the internal Employee's access as according to a study conducted by the FBI and CSI, "60% of all attacks and malicious damage originate internally, normally caused by disgruntled employees." The notes that follow take a broader look at security considerations for each area:

1.4.3.1 Partners

It is known that GIAC has recently completed a merger/acquisition with another company and that the partner company provides services for translating and re-selling the cookie sayings. However nothing is known about the partners network and what security implementations they have implemented on their site. It would be a good idea, if possible for management to make an arrangement to have their partner's networks audited as the partners networks may contain Trojans or infected machines that may be used to compromise GIAC's network.

In order for partners to conduct their services it is assumed that they will only need access to the database where all the cookie sayings reside. (For the purpose of this assignment it will be assumed that the partners employees connecting to the database will have adequate skills to conduct their work and that GIAC's database administrators have set up the correct rights to prevent mis-usage.)

Access to the network will be provided via VPN to the primary firewall. Partners will make use of the Cisco VPN client to connect to GIAC's network and access to the database will be restricted on the Firewall once users have successfully authenticated.

1.4.3.2 Customers

Unfortunately not much is known about the customers and where they might connect from. However it is very important from a business perspective that customers know that the transactions they conduct are reliable and secure.

To conduct transactions customers will require access to GIAC's secure e-commerce website. (A separate web server will provide general company information) A digital certificate allowing 128-bit encryption, and SSL will be implemented on the e-commerce web server for transactions. (Note: Some international customers may have restrictions on the encryption that can be used thus GIAC should allow lower bit encryption.)

1.4.3.3 Suppliers

Similar to GIAC's partners, not much is known about the supplier's networks. Assuming that GIAC Enterprises has many suppliers it would be illogical to ask all of the suppliers to have their networks audited. Also considering that these types of industries tend to have weaker IT infrastructures, it would be unadvisable to let them connect to the database to upload/update data.

No access to GIAC's network will be granted other than to an external machine where the necessary data can be securely uploaded.

Suppliers will connect to the external upload machine [Public DMZ2] and use SCP (secure copy) with 2-factor authentication to transfer the necessary information. Once the information has been uploaded GIAC's allocated staff will perform the necessary steps to insert the information into the database. It should be insisted upon that the suppliers use fixed IP addresses in order to increase security and restrict access to the server.

1.4.3.4 Internal Users

As previously mentioned, according to statistics most attacks originate from the internal network. Thus GIAC has chosen to adopt a defense in depth strategy on the internal network to help curb attacks from all areas of the network.

Internal users will require defined access to certain file and print servers as well as a means for their local work to be backup up. Along with that GIAC has decided to grant unlimited web access to the Internet for an initial test period (where after a proxy server could be installed to limit Internet traffic and connections to "bad" sites as well as provide usage statistics). E-mail will also be required for internal and external communications.

Users on the internal network will be authenticated by means of a domain controller with the respective access rights. Granting local admin rights on machines should be avoided to prevent loading of unauthorised and potentially unlicensed "dangerous" software. The internal mail server will be loaded with a mail scanning and ant-virus package as well as all desktops.

1.4.4 Remote Access

Remote access will be required to GIAC's network typically for sales people that need documents when at a customer's site, users that need some information when working from home and at times for administrators that are not on company premises.

Access to the LAN will be provided via VPN for remote users and they will make use of Cisco's VPN client to connect. Access will be restricted on the Firewall after users have successfully authenticated.

1.4.5 Continuation of the Security process

An essential part of the any security architecture is keeping it up to date. The architecture might be valid at the time of writing but within a few days a new exploit could be developed rendering the design susceptible to attack. Subscribing to mailing lists such as bugtraq, keeping in contact with vendors for patches and fixes, applying the latest patches and fixes and staff training all aid in keeping the architecture secure and up to date.

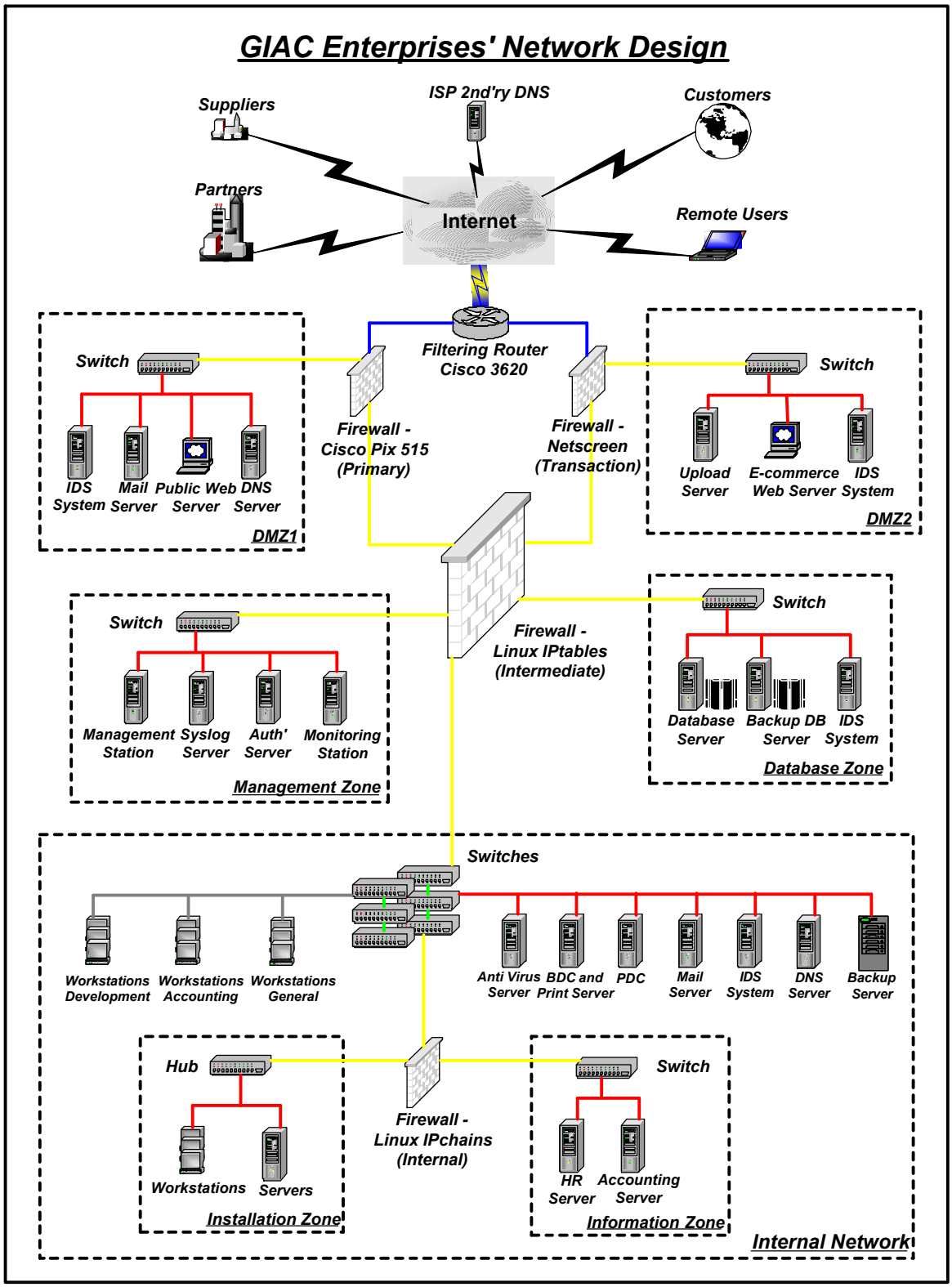
1.4.6 Internet Service Provider

It is essential that GIAC choose and have a good relationship with their Internet Service Provider. An effort should be made by management and security staff to meet a representative from the chosen ISP to set up a process in the event that their service is

urgently required.

1.5 The Network Design

The network has been segmented into 5 distinct zones being Public DMZ1, Public DMZ2, Management Zone, Database Zone and Internal network. The internal network has further been sub-divided into Installation Zone and Information Zone. The purpose of this segmentation is to keep as much as possible the relevant traffic in the relevant zones and for ease of management. The design utilizes defense in depth to protect against a single breach giving full access to the network.



1.5.1 Hardening of Servers

Before any of the applications are installed on the servers and before the servers are placed on the network, it is essential that the first be hardened (the process of removing all unwanted services and applications) and patched. All servers, devices and software mentioned below will be run through the hardening and patching process before being put into production.

However it is beyond the scope of this assignment to explain how to harden servers.

1.5.2 Border Router

The chosen border router is a Cisco 3640 running IOS version 12.1. The main purpose of the router is to connect GIAC with its Internet Service Provider (via a 2 meg pipe) and provide basic packet filtering with Access Control Lists (ACL's) for incoming and outgoing traffic. By selecting a slightly larger router that is actually required GIAC have the capability to upgrade any time in the future. The router will log to the central syslog server located on the management Zone.

1.5.3 Primary Firewall

A Cisco PIX 515 running version 6.0 will be used as the Primary Firewall. The PIX was chosen, as it's capable of extremely high throughput, is able to handle VPN connections with 3DES encryption, supports NAT and Stateful Inspection. This firewall will pass traffic for DMZ1, the management zone and Internal Network. The firewall will log to the central syslog sever located in the management zone.

1.5.4 Transactions Firewall

A Sun Ultra10 server running Solaris 2.8 with Sunscreen Secure Net 3.1 will be used as the Transaction firewall. The main purpose of this Firewall is to serve as a protection to the transaction and upload servers. A different platform has been chosen to the Cisco PIX, as chances are that the different vendors wont have the same exploit at the same time. This Firewall will log to itself as well as the syslog server.

1.5.5 Intermediate Firewall

A box running Redhat 7.1 utilizing IPtables version 1.2.2 will be used for the intermediate firewall. IPtables provides probably about the best logging capabilities and handles stateful ICMP traffic much better than most available commercial firewalls. All logging will be kept locally on the machine as well as the syslog server. Once again using a different firewall negates the chances of using the same exploit twice.

1.5.6 Internal Firewall

A box running Redhat 7.1 utilizing IPtables version 1.2.2 will be used for the internal firewall. All logging will be kept locally on the machine as well as the syslog server. This firewall separates the information and installation zones from the internal network.

1.5.7 Switches

GIAC will make use of the Cisco Catalyst 2900 series switches. Switches are used because of their ability to reduce broadcast traffic and potentially increase network speed. Reducing broadcast traffic to nodes decreases the effectiveness of sniffers that might be unknowingly installed on the network.

1.5.8 Hubs

There is only one hub that will be used in this design and is located in the installation zone, as a switch is not necessary in this instance. A Cisco Fast Hub 400 will be used for this purpose.

1.5.9 IDS Systems

Snort version 1.8.1 will be used as the intrusion detection system installed on boxes running Redhat 7.1. The servers will be run with no IP address to prevent detection and all logging will be done locally as well as to the syslog server. Snort has been chosen over a commercial product as it is a very flexible tool and writing rules to detect new exploits is a simple task, whilst new updates from suppliers can take weeks. The snort servers will use a secondary interface to connect to the syslog server in the management zone.

1.5.10 Mail Servers

A box running Redhat 7.1 with qmail version 1.03 installed will be used for the external mail relay server. qmail is an extremely secure mail server created by D.J. Bernstein and is easy to configure and has an excellent ability to protect against relaying.

An NT4.0 server running exchange 5.5 and Mailsweeper for exchange will be used for the internal mail server. Mailsweeper has the ability to integrate with a third party antivirus applications to check mail for viruses, do content searches and remove attachments according to a defined set of policies.

1.5.11 Upload Server

A box running Redhat 7.1 with SSH2 server installed will be used for the upload server. The native IPtables will be used along with hosts-deny and hosts-allow to restrict access to the server. All logging will be kept locally on the machine as well as the syslog server.

1.5.12 Web Servers

An NT4.0 server running IIS 5.0 will be used for the e-commerce and public web server. The e-commerce server will communicate with the SQL server located in the database Zone.

1.5.13 Database Servers

A NT4.0 server with Microsoft SQL2000 has been chosen for the database. All cookie related information and data would be stored on this server, which the e-commerce web server communicates with.

1.5.14 Management Station

All the management tools such as for the CISCO PIX and Exchange will be run from a Windows 2000 workstation located in the management zone. The management zone is secured on the network as well as physically to only allow authorised persons to use the console.

1.5.15 Syslog Server

A box running Redhat 7.1 with large capacity disks and backup device will be used for the syslog server. There is going to be a wealth of information on this server, as all syslog-enabled devices will be logging here. To sift through the logs manually would take far to much time, thus a real-time log scanner such as swatch will be installed and configured on this server.

1.5.16 DNS Servers

A box running Redhat 7.1 will be used for both the internal and external DNS. BIND will be removed considering the numerous amounts of exploits that are available and djbdns (by D.J. Bernstein) version 1.05 used instead. The secondary external DNS server will be located at GIAC's Internet Service Provider. It is important to note that GIAC's external DNS server should not be recursive.

1.5.17 Authentication Server

A Windows 2000 server will be used as the Radius server. The Radius server will talk to the domain controller for authenticating requests.

1.5.18 Monitoring Station

A box running Redhat 7.1 with BigBrother version 1.8b3 will be used for the monitoring station. Big brother has a web interface that allows an administrator to visually see what's happening on the network as well as being able to send alerts via e-mail or pager. This station will log to the syslog server.

1.5.19 Domain Controller and Servers

NT4.0 servers will be used to run the PDC and BDC as well as file, print, DHCP and WINS services. No IIS will be run on these servers and a third party tool will be used to send event logs to the syslog server.

1.5.20 Anti-Virus Server

An NT4.0 server will be used to run the Sophos antivirus application. Sophos was chosen as it has the ability to be set up in such a manner the entire network can be controlled from a single management station. New installations, upgrades and updates can be conducted without the user even knowing about it.

1.5.21 Backup Server

An NT4.0 server running Omniback II version 4.0 will be used as the backup server. Omniback has the ability to control other backup devices from a central management point (Cell manager) and can backup multiple platforms. Omniback also supports open file backup.

1.5.22 Network Numbering and Colouring

To make network tracing easier in the event of an attack or for general maintenance and repairs the environment should be colour coded and labelled. Figure 1.0 shows the colour-coding scheme that was chosen for GIAC. Ethernet cables that connect servers should have the server name at either ends where plugged in and all the servers should have a label with a clearly indicated name.

Colour	Representation
	Switch Links
	Connections to servers
	Connections to firewalls
	Connections to routers
	Connections to workstations

Figure 1.0

2. ASSIGNMENT 2 – Security Policy

Assignment 2 takes a closer look at the actual implementation of the rules on the relevant selected devices. We are going to take a look at how to write ACL's and firewall rules and what the written ACL's and firewall rules actually mean. Included will also be a look at some of the issues that affect the ACL's and firewall rules when implemented.

2.1 Address Scheme

Figure 2.0 shows the layout of the address scheme that GIAC Enterprises will use for their network. GIAC have been lucky enough to be assigned a full class C address by their ISP for the external network and have chosen to use private ranges for internal use. The internal addresses will be NAT'ed or PAT'ed where required.

Location	IP Addresses
External Network	196.230.43.0/24
DMZ1	192.168.1.0/24
DMZ2	192.168.2.0/24
Management Zone	192.168.3.0/24
Database Zone	192.168.4.0/24
Information Zone	192.168.5.0/24
Internal Network	192.168.10.0/24
Installation Zone	Same as Internal

Figure 2.0

Figure 2.1 shows a list of the important servers that are relevant to the security policy. The internal and external IP addresses have been shown were applicable.

Server	IP Address (Int)	IP Address (Ext)
PIX Outside	196.230.43.1	N/A
PIX Dmz1	192.168.1.1	N/A
PIX Inside	192.168.100.1	N/A
Mail Server	192.168.1.10	196.230.43.10
Web Server	192.168.1.11	196.230.43.11
DNS Server (ext)	192.168.1.12	196.230.43.12
GW Router	196.230.43.3	N/A
Syslog Server	N/A	192.168.3.10
Auth Server	N/A	192.168.3.11
DNS Server (Int)	N/A	192.168.10.20
WINS Server	N/A	192.168.10.21
Database Server	N/A	192.168.3.20

Figure 2.1

2.2 Border Router

Although the border routers man function is to route packets from GIAC's network to the Internet, the security features of Cisco IOS should not be ignored. The border router is going to be used as the first layer of defense to protect GIAC's network by filtering out most unwanted packets before even reaching the respective firewalls. These type of packets typically included spoofed addresses and unwanted services.

2.2.1 General Border Router Command Usage

The first step is to log into the router, and there are 2 possible options for this using either telnet or console access. When connected normally you would see a prompt as shown below:

router>

This indicates that you are in EXEC mode. There are only a limited number of options that an administrator can use when in this mode. To have access to all available commands one must enter the "Privileged EXEC" mode. Typing ***"enable"*** and entering the correct password allows this. Once that's completed there should be a prompt as indicated below:

router#

From here to enter specific configuration modes, such as that for interfaces, you have to enter

the global configuration first. Issuing the command ***"configure terminal"*** does this and the prompt should be the same as below:

router(config)#
Entering ***"interface <interface_name>"*** will bring you to a prompt where you can change the specific interface details:

router(config-if)#

At any stage one can enter ***"exit"*** or ***"Ctrl z"*** to exit that particular configuration mode into the previous mode.

2.2.2 ACL Command Usage

There are three types of Access Control Lists (ACL's) related to IP within the Cisco IOS software as shown in the Figure 2.2

ACL Type	Description
Standard	Based only on Source IP address
Extended	Based on Source, Destination, Protocol and Ports
Reflexive	Based on the above with state connections

Figure 2.2

Since we are only going to be using Extended ACL's on the router, we'll take at its syntax structure.

1)Access-list 2)number 3)action 4)type 5)source 6)options 7)destination 8)options 9)log

1) A specific number for Extended ACL's, must be between 100-199
2) Action to what must happen to the packet (either permit or deny)
3) Name or number of the protocol
4) The source IP address
5) Related to protocol like port number or ICMP number
6) The destination IP address
7) Related to protocol like port number or ICMP number
8) Log this information (if required)

2.2.3 Securing the Router

The first and most important step in securing a router is to shut down all unwanted services, much like when installing a new server. Once that has been completed the access lists can be created and applied to the respective interfaces.

2.2.4 Stopping Unwanted Services

Figure 2.3 shows a table of the services and servers that should be shut down on the router.

Command	Description
service password-encryption	Encrypt clear text passwords in configuration
line vty 0 4	Configure login access
access-class 10	Configure login access
Login	Configure login access
no service tcp-small-servers	Stop unwanted server
no service udp-small-servers	Stop unwanted server
no service finger	Stop unwanted server
no ip bootp server	Stop unwanted server
no ip http server	Stop unwanted server
no snmp	Stop unwanted server
no ip unreachables	Stop unwanted services
no ip direct-broadcast	Stop unwanted services
no ip source-route	Stop unwanted services
no cdp run	Stop unwanted services
Banner	Insert a banner for users to see when logged in (used for security reasons)

Figure 2.3

2.2.5 Setting Up Logging

It is vital to enable logging on the border router. This helps gives some idea as to what's actually happening on the router and what attackers are trying to accomplish. Figure 2.4 shows a table of the commands used to set up logging on the router.

Command	Description
logging on	Enables logging
logging <host>	Specify the log host were logs are to be sent
logging trap debugging	Set the level of information that you would like to see in the logs

Figure 2.4

2.2.6 Creating the Access Control Lists

Below is a list of the ACL's with descriptions that will be implemented on GIAC's router. For packets incoming on the external interface an "allow all except that which is explicitly denied" policy will be implemented, and for packets incoming from the internal interfaces a "Deny all except that which is explicitly allowed" policy will be enforced.

Block the RFC 1918 networks from coming into GIAC's network and 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 10.0.0.0 0.255.255.255 any log
```

Deny packets with localhost, broadcast and multicast addresses and log

```
access-list 101 deny   ip 127.0.0.0 0.255.255.255 any log
access-list 101 deny   ip 255.0.0.0 0.255.255.255 any log
access-list 101 deny   ip 224.0.0.0 7.255.255.255 any log
access-list 101 deny   ip 255.255.255.255 0.0.0.0 any log
```

Deny packets without ip address and log

```
access-list 101 deny   ip host 0.0.0.0 any log
```

Deny Services that should not be entering the network from external

Most of the ports listed below are services that should not originate from the external network, for example the netbios protocol should not be seen on the net, however there are quite a few misconfigured firewalls on the net that might let it in/out. If that where to happen, much information could be obtained from that system as well as been able to be quite easily hacked.

```
access-list 101 deny  udp any any eq 111              Block SunRPC
access-list 101 deny  tcp  any any eq 111             Block SunRPC
access-list 101 deny  tcp  any any range 139 139      Block Netbios
access-list 101 deny  udp  any any range 139 139      Block Netbios
access-list 101 deny  tcp  any any range 512 514      Block "r" commands
access-list 101 deny  udp any any eq 2049             Block NFS
access-list 101 deny  tcp any any eq 2049             Block NFS
access-list 101 deny  udp any any eq 4045             Block Lockd
access-list 101 deny  udp any any eq 4045             Block Lockd
access-list 101 deny  tcp any any range 6000 6100     Block X
access-list 101 deny  udp any any eq 389              Block Ldap
access-list 101 deny  tcp any any eq  389             Block Ldap
access-list 101 deny  udp any any eq 69               Block Tftp
access-list 101 deny  tcp  any any eq 79              Block Finger
access-list 101 deny  udp any any eq 514              Block Syslog
access-list 101 deny  tcp  any any eq 515             Block LPD
```

Allow all other packets through but don't log

```
access-list 101 permit   ip any any
```

The 101 access lists are going to be applied to the incoming external interface of the router.

Allow GIAC's ip's to get out, but block all other and log

access-list 110 permit ip 196.230.43.0 0.0.0.255 any
access-list 110 deny ip any any log

The 110 access lists are going to be applied to the incoming internal interfaces of the router.

2.2.7 Gotcha's and General information

When applying access control lists on the router keep in mind that the router reads the ACL's from the top down, i.e. "Top Down Processing". This means that the router will check the packet against the first ACL and if it doesn't match the next one below it until a rule matches or it reaches the end of the ACL list. Because the router operates in this manner it is advisable to put most frequently hit rules at the top of the list.
Another thing to be careful of is blocking access on the router, one can inadvertently cut ones own connection.

After a while with the logs gathered from the border router GIAC could set up a general networking trends graph. For example lets say that the router blocks approximately 5000 netbios packets a week. Lets say then one week GIAC notices that there is an increase to 10 000 packets. This could mean that there is a potential new netbios attack on the Internet, so administrators could check for any news related to this.

2.3 Cisco PIX Firewall

The Cisco PIX is the primary firewall for GIAC enterprises and allows access to essential services as well dealing with all VPN connections. As mentioned previously the PIX was chosen for its high throughput capability, ability to do NAT and stateful inspection.

2.3.1 General Command Usage

Out of the box one isn't able to telnet or ssh to the PIX box, thus the initial configuration of the firewall needs to completed via console cable. When logged in the first prompt that should be seen is shown below assuming that the firewalls host name is firewall. (Note -There is much similarity between the router and firewall commands)

firewall>

From this prompt there are 3 possible commands that can be used. To view the commands that are available under each mode, the ***"?"*** can be used. If typed in at this prompt one should see the following:

enable Enter privileged mode or change privileged mode password
pager Control page length for pagination
quit Disable, end configuration or logout
firewall>

Typing in enable and the correct password will get one into a privileged mode and will be seen as below:

firewall#

From here the administrator has full access to the firewall. Typing in ***"conf t"*** will change mode into global configuration, all configuration is done in this mode. The prompt displayed will be shown as below:

firewall(config)#

A helpful hint is to use the ***"?"*** whenever one is unsure of a command syntax. For example if you are unsure on how to use the access-list command, type in ***"access-list"*** followed by a ***"?"*** (access-list ?) and the syntax will be displayed. To exit out of the mode into the previous mode the command ***"quit"*** can be used.

2.3.2 Cisco PIX Information

The PIX doesn't quite function the same as most other firewalls. Instead the PIX segregates the interfaces into separate zones with a security rating. By default the outside interface is given a rating of 0 (the lowest) and inside 100 (the highest). The PIX by default allows traffic to flow from a higher security zone to a lower (i.e. from internal to external) but will not allow it from a lower to a higher (i.e. from external to internal) unless adequate rules are configured.

For access from a higher to a lower zone there are 2 commands that are used which are ***"nat"*** and ***"global"***. From a lower to a higher zone one has to make use of the ***"static"*** and ***"access-list"*** commands.

2.3.3 ACL Command Usage

Below shows the syntax for the access-list command used on the Cisco PIX. There are a few other commands related to access-lists that will also be looked at. (The access-list command can only be used when in configuration mode.)

1) access-list 2) acl_ID 3) [deny|permit] 4) protocol 5) [source address|local address] 6) [source mask|local mask] 7) operator 8) port 9) [destination address|remote address] 10) [destination mask|remote mask] 11) operator 12) port

1) The actual command
2) The ACL description (can be a name or number)
3) Allow or deny the packet to traverse the PIX firewall
4) The protocol type (e.g ICMP, TCP or UDP)
5) Address or network from where the packet is being sent
6) The subnet mask of the network or host from where the packet is being sent
7) The syntax used with port can be one of the following
   - lt = Less than
   - gt = Greater than
   - range = Port range

eq = Equal to
neq = Not equal to

8) The port number or name
9) Address or network of the to where the packets is going
10) The subnet mask of the network or host to where the packet is going
11) See number 7
12) See number 8

Show access-list – Show all the existing access-lists in the configuration
No access-list – Remove a specific ACL from the configuration
Clear access-list – Remove all the access-list in the configuration

2.3.4 Standard Configuration

Figure 2.5 below shows the standard configuration commands that will be used to set up the PIX to allow necessary services through to the respective servers. All these commands are entered under the configure terminal prompt "firewall(config)#"

Number	PIX Command
1	hostname firewall
2	Domain-name giac.com
3	nameif ethernet0 outside security0
4	nameif ethernet1 inside security100
5	nameif ethernet2 dmz1 security50
6	interface ethernet0 100basetx
7	interface ethernet1 100basetx
8	interface ethernet2 100basetx
9	Mtu outside 1500
10	Mtu inside 1500
11	Mtu dmz1 1500
12	ip address outside 196.230.43.1 255.255.255.0
13	ip address inside 192.168.100.1 255.255.255.0
14	ip address dmz1 192.168.1.1 255.255.255.0
15	static (dmz1,outside) 196.230.43.10 192.168.1.10 netmask 255.255.255.255 0 0
16	static (dmz1,outside) 196.230.43.11 192.168.1.11 netmask 255.255.255.255 0 0
17	static (dmz1,outside) 196.230.43.12 192.168.1.12 netmask 255.255.255.255 0 0
18	access-list outside permit tcp any host 196.230.43.11 eq www
19	access-list outside permit tcp any host 196.230.43.11 eq ssl
20	access-list outside permit tcp any host 196.230.43.10 eq smtp
21	access-list outside permit udp any host 196.230.43.12 eq dns
22	Logging on
23	Logging monitor critical
24	Logging buffered alerts
25	Logging trap warnings
26	Logging host inside 192.168.3.10
27	global (outside) 1 196.230.43.101-196.230.43.120

28	global (outside) 1 196.230.43.100
29	nat (inside) 1 0.0.0.0 0.0.0.0 0 0
30	access-group outside in interface outside

Figure 2.5

2.3.5 Description of the Commands

Figure 2.6 gives the descriptions of the commands used from the table above.

Number	Description
1	Set the firewall name to "firewall"
2	Set the firewall domain name to "giac.com"
3	Set the security for the outside interface to 0
4	Set the security for the inside interface to 100
5	Set the security for the DMZ1 interface to 50
6	Set the interface speed for outside
7	Set the interface speed for inside
8	Set the interface speed for DMZ1
9	Set the Maximum transfer unit size to 1500 for outside
10	Set the Maximum transfer unit size to 1500 for inside
11	Set the Maximum transfer unit size to 1500 for dmz1
12	Set the ip address for the outside interface
13	Set the ip address for the inside interface
14	Set the ip address for the dmz1 interface
15	Map the mail server to an external ip address
16	Map the web server to an external ip address
17	Map the DNS server to an external ip address
18	Allow web (port 80) through to the web server
19	Allow ssl (port 443) through to the web server
20	Allow smtp (port 25) through to the mail server
21	Allow dns (port 53) through to the dns server
22	Turn logging on
23	Log critical alerts when logged in via telnet console
24	Log alert alerts to the PIX console
25	Log warning alerts to the syslog server
26	Specify the IP address of the syslog server for the PIX logs
27	Set up a range of IP's that the pix will use before PAT'ing
28	Set up the PAT address when static address are all used up
29	Grant that traffic from inside may flow to a lower security zone
30	Apply the access lists outside to the outside interface

Figure 2.6

2.4 Setup the VPN

The VPN will be used for two functions. The first function is to enable remote users (GIAC

employee's only) to connect to the internal network and the second function is to allow partner sites to connect to the Database for translation and re-selling abilities of cookies.

Figure 2.7 shows the commands used to set up the VPN components on the PIX firewall version 6.0 with the VPN 300 clients.

Number	Command
1	aaa-server radius protocol radius
2	aaa-server partnerauth protocol radius
3	aaa-server partnerauth (inside) host 192.168.3.11 <radkey> timeout 5
4	isakmp enable outside
5	isakmp policy 8 encr 3des
6	isakmp policy 8 hash md5
7	isakmp policy authentication pre-share
8	isakmp key <isakey> address 0.0.0.0 netmask 0.0.0.0
9	isakmp policy 8 group 2
10	access-list 80 permit ip 192.168.100.0 255.255.255.0 192.168.101.0 255.255.255.0
11	nat (inside) 0 access-list 80
12	access-list remoteacl permit ip any any
13	access-list patneracl permit tcp 192.168.101.0 255.255.255.0 192.168.3.20 eq 1433
14	access-list partneracl permit tcp 192.168.101.0 255.255.255.0 192.168.3.20 eq 22
15	crypto ipsec transform-set strond-des esp-3des esp-sha-hmac
16	crypto dynamic-map cisco 4 set transform-set strong-des
17	crypto map partner map 20 ipsec-isakmp dynamic cisco
18	crypto map partner-map interface outside
19	crypto map partner-map client authentication partnerauth
20	ip local pool remote 192.168.101.1-192.168.101.150
21	ip local pool partner 192.168.101.151-192.168.101.254
22	vpngroup partneruser address-pool partner
23	vpngroup partneruser default-domain giac.com
24	vpngroup partneruser idle-time 1800
25	vpngroup remoteuser address-pool remote
26	vpngroup remoteuser dns-server 192.168.10.20
27	vpngroup remoteuser wins-server 192.168.10.21
28	vpngroup remoteuser default-domain giac.com
29	vpngroup remoteuser idle-time 1800
30	sysopt connection permit-ipsec

Figure 2.7

Figure 2.8 shows the description of the commands from the table above.

Number	Description
1	Set up the AAA related parameters
2	Use the radius protocol and tag name "partnerauth"
3	Select the host for Radius Authentication and key
4	ISAKMP Policies using 3Des, and md5 hash on outside interface
5	ISAKMP Policies using 3Des, and md5 hash on outside interface
6	ISAKMP Policies using 3Des, and md5 hash on outside interface
7	ISAKMP Policies using 3Des, and md5 hash on outside interface
8	Configure a wildcard pre-share key
9	Use Dife Hilman group 2
10	Define an access list for Ipsec networks
11	Configure NAT 0
12	Access control lists for VPN users
13	Access control lists for VPN users
14	Access control lists for VPN users
15	Create transform for 3Des, ESP, SHA and HMAC
16	Create dynamic crypto map
17	Define crypto map to enable ISAKMP policy
18	Apply crypto map to outside interface
19	Enable extended authentication
20	Create the pool for remote users
21	Create the pool for partner users
22	Configure VPN 3000 client polices
23	Configure VPN 3000 client polices
24	Configure VPN 3000 client polices
25	Configure VPN 3000 client polices
26	Configure VPN 3000 client polices
27	Configure VPN 3000 client polices
28	Configure VPN 3000 client polices
29	Configure VPN 3000 client polices
30	Permit Ipsec connections through the PIX firewall

Figure 2.8

2.5 Testing ACL's

Lets take the PIX firewall example of only letting through smtp to server 196.230.43.10. For the test we are going to make use of a free tool called nmap. Nmap has the ability to scan systems with a multiple range of options and this tool is considered amongst one of the best in its field.

What we are going to do is tell nmap that we what to scan the host 196.230.43.10 using a stealth scan (-sS), verbose output (-v) and no name lookups (-n)

Nmap –v –n –sS 196.230.43.10

This is the output from the above command:

Starting nmap V. 2.53 by fyodor@insecure.org (www.insecure.org/nmap/)
Host (194.230.43.10) appears to be up ... good.
Initiating SYN half-open stealth scan against (194.230.43.10)
Adding TCP port 25 (state open).
The SYN scan took 183 seconds to scan 1523 ports.
Interesting ports on (194.230.43.10):
(The 1522 ports scanned but not shown below are in state: filtered)
Port State Service
25/tcp open smtp

Nmap run completed -- 1 IP address (1 host up) scanned in 183 seconds

This proves that the firewall is doing is job by blocking all ports besides 25. The other servers can be tested in the same manner. One can also use the –sU to scan the UDP ports.

3. ASSIGNMENT 3 – Audit of the Security Architecture

The purpose of assignment 3 is to complete a comprehensive security audit on GIAC Enterprise's primary firewall, with the end goal being to check whether the device and is fulfilling its role as well as to give recommendations for further improvements where applicable. The audit will be broken into 3 stages. Stage one will cover the planning, stage two the actual implementation and testing and stage three feedback and reports.

3.1 Stage One – Planning and Requirements

3.1.1 Authorisation and Times

The first stage in getting started with any security audit is to get full authorisation from management. It should be a signed document stating the purpose and agreements for the tasks that need to be completed. Some of the agreements required are for access to certain severs to view logs and configurations and access to network diagrams. Second would be arranging times when the tasks could be conducted. Assuming that most of the companies that GIAC deals with close at 5:00pm Monday to Friday and that traffic is at its lowest at that time, most of the tests etc will be conducted from 7:00pm till 4:00am the next morning and on weekends if necessary.

3.1.2 Tools

We are going to require some tools in order to complete the testing and it has been chosen to use 2 laptops running Redhat 7.1 (fully hardened and patched) with numerous freely available scanning tools as well as a few hubs. To save time and be professional the security tools (Figure 3.0) can be pre-installed before arriving at GIAC's site.

Tool Name	Description	Where it's found
Nmap	Port scanning tool	http://www.insecure.org
Nessus	Vulnerability scanner	http://www.nessus.org
Tcpdump	Unix packet capture tool	http://www.packetstorm.org
Ethereal	Graphical packet capture display	http://www.packetstorm.org
Netcat	Network debugging tool	http://www.atstake.com/research/tools/
hping2	Packet Constructor	http://sourceforge.net/projects/hping2/
Nemesis	Packet crafting tool	http://www.packetstormsecurity.com

Figure 3.0

3.1.3 Hours and Cost

Two highly skilled security persons will be required for the job at a cost of around 250 CHF per hour after hours each. An initial period of the time will be used to review the security policy and actual PIX setup before the testing is started. Figure 3.1 shows a break down of the tasks and costs.

Task to be completed	Persons	Hours	Unit Cost	Cost
Review of company policy and diagrams	2	4	CHF 250.00	CHF 2,000.00
Patch and vulnerability check of the PIX	2	3	CHF 250.00	CHF 1,500.00
Rule-base testing	2	9	CHF 250.00	CHF 4,500.00
Data analysis	2	4	CHF 250.00	CHF 2,000.00
Reporting and recommendations	2	4	CHF 250.00	CHF 2,000.00
User awareness and feedback	1	2	CHF 250.00	CHF 500.00
			TOTAL	***CHF 12,500.00***

Figure 3.1

3.2 Stage Two – Testing

As mentioned above, before testing is started but after the security policy is read the PIX primary firewall will be checked to see if it has the latest patches and hot-fixes applied. The local administrators will be shown how this is conducted and where the latest patches and versions can be found. It must be stated however that through the PIX versions some of the command syntax's have changed so it is not always advisable to change versions straight

away and local administrators should be made aware of this.

The next stage is to test the firewall rule-base and firewall robustness and after reading the policy we have a good idea as to what sort of traffic is to be expected in the various zones. We are going to make use of 4 tools here namely nmap, tcpdump, ethereal and Nemesis. Nmap is going to be used first to test the open ports through the firewall against the servers in the DMZ1 and internal network. One of the Linux laptops will be installed outside the firewall with a legal address and the probes will be started from there. The other laptop will be placed in the DMZ1 (when testing this area) and tcpdump run to capture any packets in that zone. Afterwards ethereal will be used to convert the tcpdump captures into a graphical representation. We are not going to look at every test conducted but rather an overview of the most important. Below shows some of the commands used.

To test all (-p 1-65535) TCP ports (-sT) of a server using no name lookups (-n) and verbose output (-v) also don't ping host (-P0)

Nmap –v –n –P0 –sT –p 1-65535 <host IP address>

To test all (-p 1-65535) UDP ports (-sU) of a server using no name lookups (-n) and verbose output (-v) also don't ping host (-P0)

Nmap –v –n –P0 –sU –p 1-65535 <host IP address>

Using the above two commands on all the servers in the DMZ1 we would be ale to see what ports were let through the firewall. We should expect something similar to below for an smtp server.

Starting nmap V. 2.53 by fyodor@insecure.org (www.insecure.org/nmap/)
Initiating TCP scan against (194.230.43.10)
Adding TCP port 25 (state open).
The TCP scan took 2341 seconds to scan 65535 ports.
Interesting ports on (194.230.43.10):
(The 65534 ports scanned but not shown below are in state: filtered)
Port State Service
25/tcp open smtp

Nmap run completed -- 1 IP address (1 host up) scanned in 2341 seconds

The VPN connections and restrictions is another important stage of testing. We will use the same client that partners and remote people use. Will then connect to the firewall and run nmap once again to check the restrictions on the servers.

3.3 Stage Three – Reports and Recommendations

The results from nmap, tcpdump and the various logs show that all is functioning according to the security policy and we are happy with the architecture design. However looking at the entire security architecture there are a few improvements that can be made. If the primary firewall were to fail most of GIAC's public services would be lost. To compensate for this it is

recommended that a fail-over unit be installed with the existing PIX firewall as shown in

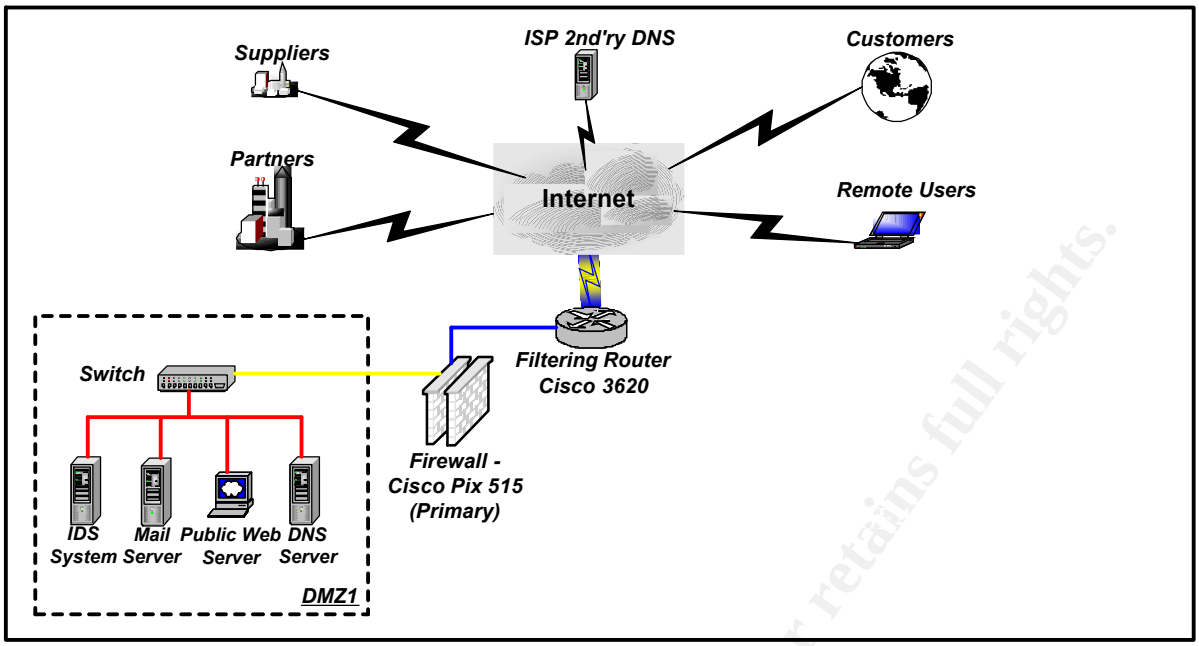


figure 3.2.

Figure 3.2

All of the above tests and reports will be presented to management and security administrators. Being an active part of the security community we would show the administrators our methodology so that they could help keep their site more efficient and secure.

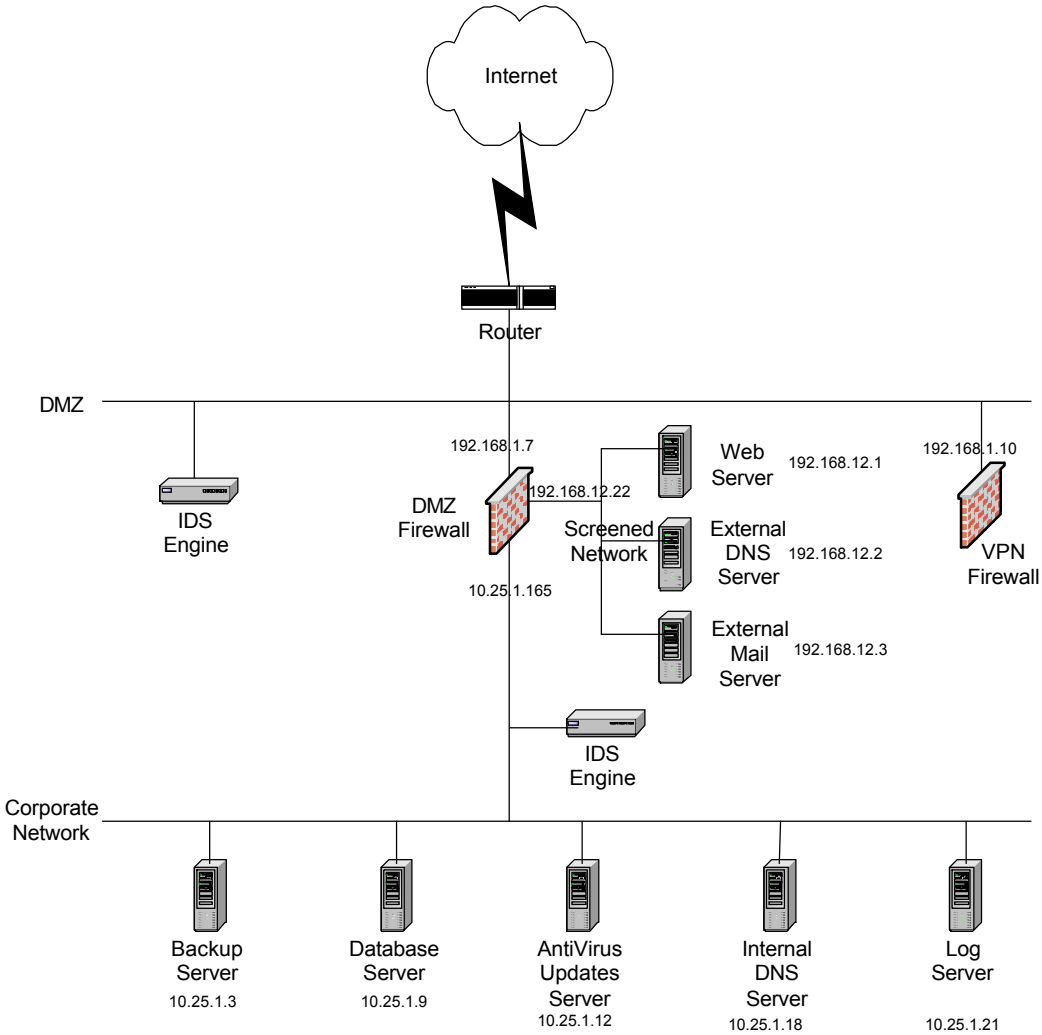
4. ASSIGNMENT 4 – Design Under Fire

The purpose of this assignment is to make an administrator aware that there are always potential threats to their security architectures. Even the most advanced infrastructures can and will be susceptible to attack at some time, much like successful attacks that have taken place against the pentagon.

I have chosen to attack the architecture of Janice Southerland (that can be viewed with the following link http://www.sans.org/y2k/practical/janice_southerland_GCFW.doc) for the following reasons:

- Janice is running Firewall-1 version 4.1, but has not mentioned what service pack she has installed.
- There are a number of other possibilities that I have on the Firewall. If some of the default settings have not been changed such as DNS and ICMP usage then I can use this to attack even if the firewall had a deny any any all rule in place.
- She has an IDS system installed outside the firewall which may pick up some of the attacks that I might try against her architecture, but IDS systems outside the firewall take much administration and original configuration to remove all false positives, so keeping the external IDS busy shouldn't be a problem.

- There is no IDS system on the screened network. This gives me a great window of opportunity to attack servers on this network without her knowing. The only traces she might find are with the help of file integrity checkers.



GIAC Enterprises
Nework Diagram

The above diagram has been taken from Janice's paper.

4.1 The Attack

I am going to attempt to crash the firewall by sending illegally fragmented packets directly to the machine. By doing this I can potentially cause the firewall to use all available processing power to log the fragmentation events thus rendering the firewall unable to provide service.

Lance Spitzner discovered the weakness with a tool called jolt2.c. Below is a description of the weakness by Checkpoint Software.

"For security reasons (e.g., overlay attacks) FireWall-1 reassembles all IP fragments of a

datagram prior to inspection against the security policy. After reassembly, the packet is processed by the FireWall-1 Stateful Inspection engine, and if allowed by the security policy to proceed, the packet is refragmented and forwarded. To identify and audit attacks such as Ping of Death, Check Point added a mechanism to FireWall-1 - outside of its standard logging capability - to log certain events that occur during the FireWall-1 virtual reassembly process. This fragmentation logging takes place on the gateway itself and not on the management station (relevant for distributed management deployments).

The authors used jolt2 to send a stream of extremely large IP fragments to a FireWall-1 gateway, which in some cases can cause the write mechanism to grab all host CPU resources. There is no fragmentation tracking resource that is exhausted; it is the case that the fragmentation logging process is the cause of this issue.
http://www.checkpoint.com/techsupport/alerts/ipfrag_dos.html

4.2 Denial of Service Attack

Considering that I have fifty compromised systems to work with I will look at using a Trojan called Tribe FloodNet 2K (TFN2K). TFN2K is used to launch controlled distributed denial of service attacks from multiple hosts on the Internet to a victim host or network. TFN2K is not platform specific, in fact any host that is connected to the Internet is vulnerable to this attack.

TFN2K is a 2-part system, consisting of a client (master) and slaves (agents). The master communicates via encrypted TCP, UDP or ICMP with the agents (which listen be means of a daemon) to launch a simultaneous TCP/SYN, UDP and ICMP or a mixture of all three floods against the selected targets. Figure 4.0 shows diagrammatically how TFN2K works.

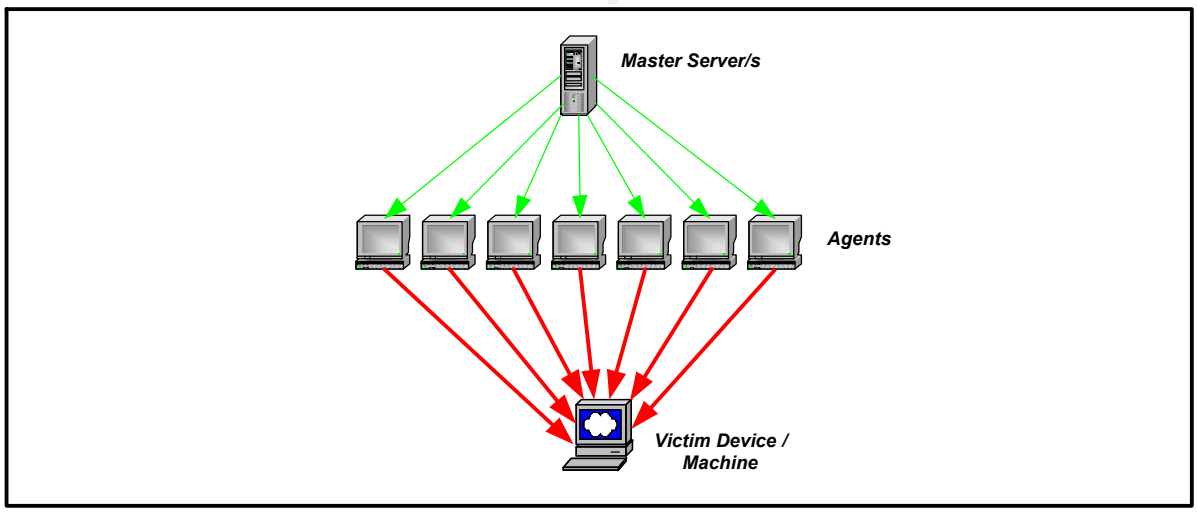


Figure 4.0

TFN2K is similar in many ways to TFN but has some interesting characteristics that make it much more difficult to detect than its predecessor. The agent daemons run in silent mode i.e. they don't respond to the master. Instead the master sends the command approximately 20 times and assumes that the agent will receive at least one of them. TFN2K also has the ability to spoof packets making tracing source IP addresses difficult.

The first time round we are going to attack GIAC's connection to the Internet by focusing the flood on the border router using UDP. With 50 cable/DSL systems we should easily be able to choke a 2 Meg connection (unfortunately it is not noted what the Internet connection of the selected design is). Following that I could attack the IDS system or Firewall, there is basically not limit to which servers I could attack.

4.2.1 Defense Against TFN2K

Unfortunately there is no known way to protect ones site from such an attack. The best that an administrator can do is use preventative methods such as described below:

- Prevent your systems from being used as masters or agents by applying the latest security patches on servers and workstations.
- Establish a good relationship with your ISP. In the event of other flood attacks they are the only ones who are going to be able to help you.
- If you suspect that one or some of your systems have been infected make use of tools and methods described by advisories to check your systems. If indeed your systems have been compromised contact the necessary authorities.
- Apply ingress and egress filtering on routers. By applying egress filters you prevent your network from potentially being used as an attack base.
- Where possible apply rate-limiting rules on the Firewall. This helps deal with multiple packets sent to the firewall.

4.3 Internal System Attack

Unfortunately not much can be determined from Janice's project as to the type operating system, the software used to offer the services and patch level for the servers located on the screened network. However we do know that there are no IDS servers present on this segment, which is an added bonus. Also note that the external IDS system is commercial, and most patches for new exploits take some time to be developed for commercial systems.

To try and determine some more information of GIAC's site I'm going to make use of the ***"nslookup"*** command. First off I would like to know the IP addresses DNS servers. I type the following in the table shown below:

CMD Sequence	Command	Description
1	Nslookup	Go into name lookup mode
2	set q=ns	Set the query to name servers
3	giac.com	Check the giac.com domain

Following that I find out the IP addresses of the mail servers using the commands shown in the table below:

CMD Sequence	Command	Description
1	Nslookup	Go into name lookup mode

2	set q=mx	Set the query to mail exchangers
3	giac.com	Check the giac.com domain

After that I would find the IP address of the web server. Using the standard nslookup prompt I would type in ***"www.giac.com"*** assuming that to be the name of their web server. At the same time I could try and list the available servers in that domain by connecting to their DNS server and typing ***"ls giac.com"*** The commands used are shown below:

CMD Sequence	Command	Description
1	Nslookup	Go into name lookup mode
2	www.giac.com	Check for the IP address of their web server
3	server <giac's ns IP>	Change to Giac's name server
4	ls giac.com	Try and list all DNS records for their domain

There are web-based tools that will accomplish the same tasks as completed above and more. One particular site that I use pretty often is http://www.samspade.org

Now that I know all the IP addresses and the like, I can use nmap to determine the type of operating system by using the following options:

Nmap –v –n –sS –O <IP address of target>

I will also check the available ports that are open on the servers and use other tools to determine the version of the servers that are running such as telnet.

4.3.1 Results

From the above tests I have determined the following about the servers located in the screened network.

Server	OS	Services	Version
DNS Server	Linux 6.2	Bind	8.2.2
Mail Server	Linux 6.2	Sendmail	8.10
Web Server	NT 4.0	IIS	4.0

I am going to attack the IIS 4.0 web server using a recent vulnerability that exploits a buffer overflow in the ISAPI extensions installed with most IIS 4.0 web servers. With this buffer overflow I might be able to run arbitrary code on the system potentially giving me full access to the system. Below is the CERT advisory for this exploit.
http://www.cert.org/advisories/CA-2001-13.html

Once the web server has been compromised I will try a copy the transaction connections in order to connect to the database server and compromise the database that holds a wealth of information. If this is unsuccessful I will attempt a buffer overflow attack using ***sqladv-poc.c*** which if successful will give me full control of the system (assuming that the database is SQL of course). This should be possible considering that ports have to be opened on the firewall in order for the web server to communicate with it.

Below describes the problem found in SQL server from @stake:

"Microsoft's database server, known as SQL Server, contains several buffer overruns vulnerabilities that can be remotely exploited to execute arbitrary computer code on the affected system, thus allowing an attacker to gain complete control of the server. In situations where the SQL Server is protected by a firewall, it may still be possible to launch this attack through a connecting web server - though this depends on how secure the web server's application is." http://www.atstake.com/research/advisories/2000/a120100-1.txt

5. Resources

FBI Stats - http://www.sans.org/infosecFAQ/start/weak_infra.htm
Hardening Servers - http://www.enteract.com/~lspitz/papers.html
http://www.cert.org/security-improvement/#Harden
http://www.sqlsecurity.com/
http://www.microsoft.com/Exchange/techinfo/administration/55/
Cisco Router 3600 - http://www.cisco.com/univercd/cc/td/doc/pcat/3600.htm
PIX Firewall - http://www.cisco.com/univercd/cc/td/doc/pcat/fw.htm
Sun Firewall - http://www.sun.com/software/securenet/
Iptables Firewall - http://netfilter.samba.org
Switch Information - http://www.zdnet.com/zdhelp/stories/main/0,5594,2678853-4,00.html
Snort - http://www.snort.org
Mail Server - http://www.qmail.org/top.html
http://www.mimesweeper.com/products/exchange/default.asp
Syslog and Swatch - http://www.enteract.com/~lspitz/swatch.html
DNS Server - http://djbdns.com/
Auth Server - http://www.rsa.com/products/securid/rsaaceserver.html
Monitoring Station - http://www.bb4.com/features.html
Antivirus - http://www.sophos.com/products/antivirus/savnt.html
Backup - http://www.openview.hp.com/products/omniback/index.asp
Cisco setup and ACL's - http://www.cisco.com/warp/public/707/21.html
http://secinf.net/info/fw/cisco/cisco.html
http://www.sans.org/infosecFAQ/firewall/blocking_cisco.htm
SL4NT - http://www.netal.com/SL4NT.htm
Security Focus - http://www.securityfocus.com
Packetstorm - http://packetstorm.securify.com
PhoneBoy - http://www.phoneboy.com/
TFN2K - http://security.royans.net/info/posts/bugtraq_ddos2.shtml
CERT – http://www.cert.org
SANS – http://www.sans.org
SQL – http://www.microsoft.com/sql/default.asp
Microsoft – http://www.microsoft.com

Brenton, Chris. VPN's and Remote Access. USA: Workbook Sans Institute 2001.

Brenton, Chris. Advanced Perimeter Protection and Defense. USA: Workbook Sans Institute 2001.

Zwicky Elizabeth, Cooper Simon, Chapman Brent. Building Internet Firewalls. USA: O'Reiley June 2000.