

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.

SANS GIAC Firewalls, Perimeter Protection, and Virtual Private Networks

Based on SANS document Version 1.5 for the Network Security 2001 Event



SANS Network Security
New Orleans, LA
January 27-February 1, 2001

Prepared by Tara Silvia
March 17, 2001

© SANS Institute 2000 - 2005, Author retains full rights.

Table of Contents

Assignment 1: Security Architecture……..1-8
1.1 Scope…….…….3
1.2 Corporate
Assumptions……..4
1.3 Security Architecture Assumptions……...……4
1.4 Logical Network Diagram of GIAC Enterprises……..……5
1.5 Perimeter Technologies…….6
1.6 Conditions Based on above Diagram…….6-7
1.7 Equipment Used…….7-8

Assignment 2: Security Policy……9-26
2.1 Scope…….9
2.2 Introduction……...……10
2.3 Defense in Depth Strategy……..…….10
2.4 High Level Security Policy……..……11
2.5 Security Policy broken Down in Depth……..……12-25
2.6 Why are some filter/rules Order-Dependent?…….25-26

Assignment 3: Audit your Security Architecture……..26-42
3.1 Scope……26
3.2 Plan the Assessment……...……26-29
3.3 Implement the Assessment…….29-37
3.4 Analysis/Recommendations……...……38-39
3.5 Perimeter Analysis……..39-42

Assignment 4: Design under Fire…….……....43-48
4.1 Scope……..……..43
4.2 Selected Design……44
4.3 Attack against the Firewall…….……44-46
4.3.1 Yet another Vulnerability…….46
4.3.2 Yet Another…….46
4.4 Denial of Service Attacks using SYN Floods……..……47
4.4.1 What can the Victims do?……47-48
4.5 Attack to Compromise the Internal System through the Perimeter Syst…... 48

References……...…….49

© SANS Institute 2000 - 2005, Author retains full rights.

GCFW GIAC Practical Assignment

Network Security 2001, New Orleans, LA

Introduction

What is SANS GIAC Firewall Certification?

This intent on doing this practical assignment is to demonstrate one's capabilities in the area of firewalls, perimeter protection and VPNs to essentially become a fully certified SANS GIAC Certified Firewall Analyst (GCFW).

Why is Information Security so important?

- An attacker could grab hold of your password file
- An attacker could get a hold of sensitive system files
- A login server at a high port could be started
- An attacker could alter your server logs
- Denial of Service attacks

Assignment 1: Security Architecture

1.1 Scope

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

You must consider access for:

- *Customers (the companies that purchase bulk online fortunes);*
- *Suppliers (the authors of fortune cookies sayings that connect to supply fortunes);*

© SANS Institute 2000 - 2005, Author retains full rights.

- *Partners (the international partners that translate and resell fortunes).*

© SANS Institute 2000 - 2005, Author retains full rights.

1.2 Corporate Assumptions

- There are no set economic constraints.
- The number of GIAC customers, suppliers, and partners is not mentioned.
- We don't know how rapid the company plans on growing.
- The magnitude and role of the applications are not stated.

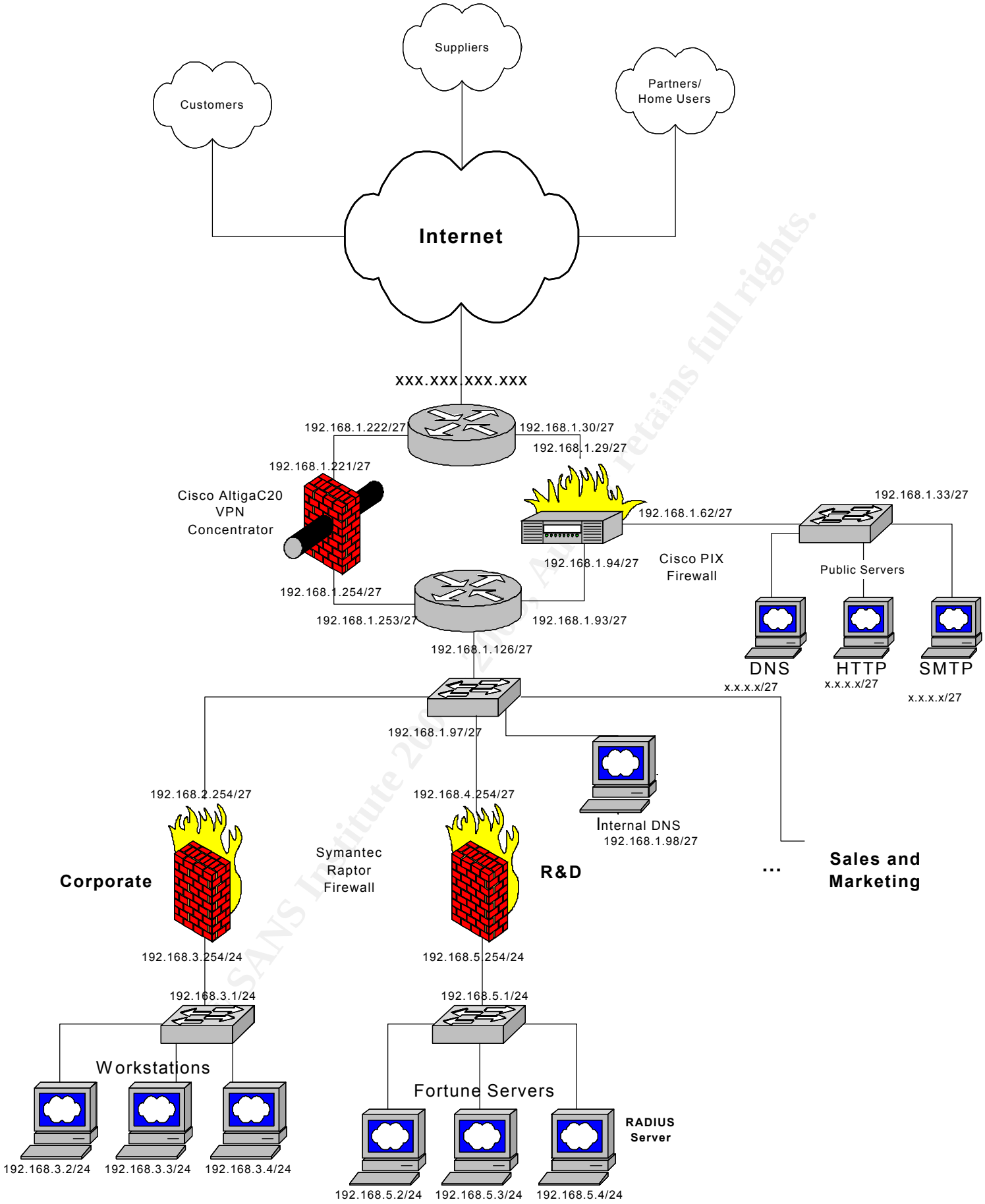
1.3 Security Architecture Assumptions (See Diagram following)

- Each separate division (i.e. corporate, R&D, and sales/mktg.) in the organization will have it's own private Class C address space. This is more modular, allowing each division a maximum number of hosts, and if a new division were added, it would be much easier to setup the addressing without having to reconfigure everything.
- Access to the data on the internal systems by home users and remote offices, and partners are encrypted via VPN.
- Access to the data on the web servers from the Internet by the customers and suppliers are encrypted via SSL (Secure Sockets Layer).[1] SSL is a network protocol layer located directly under the application layer with responsibility for the management of a secure (encrypted) communication channel between the client and server. Basically, the customers can download the fortunes from the web server and the suppliers can upload the fortunes there as well.

1.4 Logical Network Diagram of GIAC Enterprises (Please see image on following page)

[1]Netscape's SSL page: http://home.netscape.com/security/techbriefs/ssl.html?cp=sciln

© SANS Institute 2000 - 2005 Author retains full rights.



© SANS Institute 2000 - 2005 Author retains full rights.

1.5 Perimeter Technologies:

The above network is implemented using a switched network design. A switched network helps protect against sniffing (passive attack), since most traffic is no longer broadcast. The physical network is divided into 2 distinct enclaves: E-Business and Internal Private Area (head office). The E-Business enclave is dedicated to service GIAC's Enterprise Fortune Cookie Sayings business and the Internal Private enclave is dedicated to all the rest of the business. The enclaves are connected to the Internet via a Fractional T1 connection. The Internal Private enclave has a 24 bit subnet mask in which case there are is a total of 254 hosts per network allowing for future growth.

The E-Business sector includes the border router, screened subnet (public web servers) and the primary firewall (first layer of defense from the Internet).
The internal private area is divided into a number of different networks such as Corporate, Development, R&D, Sales/Marketing, etc.

Due to the merger that GIAC Enterprises underwent, it will be critical that all of these divisions have access to the network using the existing architecture, and since there is a good chance that GIAC Enterprises will undergo future mergers, it makes it even that more important.

With regards to remote offices, home users, and partners, we will grant them access to the E-Business and Internal Private perimeters via VPN through an Internet connection. The only individuals that will have restricted access on the network will be the suppliers, customers, and the rest of the world, in which case they will ONLY be granted access to the E-Business sector. It is extremely important that GIAC Enterprises not allow everyone into the Internal Private Area of the organization. We need to keep this separate since our entire company revolves around the Fortune Servers that are located in the R&D portion of the Internal Private Area.

1.6 Conditions based on the above Diagram:

1. Traffic coming into the border router fall under 2 basic categories: VPN and other traffic.
2. VPN traffic will flow through the CISCO Altiga C20 VPN Concentrator.
   - VPN authentication will be done with the host addresses signed by the Altiga.
   - Once connected, the VPN concentrator will enforce split horizon, such that connected hosts can send and receive traffic only over the VPN tunnel thus "[2]enforcing the rule that that a router should never re-advertise a route out of the same interface that it learned it on."
3. Non VPN traffic will pass through the CISCO PIX stateful firewall.
   - The CISCO PIX has high throughput (~170 Mbps)
   - Allows for screened subnets.

[2] Cisco Internetwork Design: Page 147 Split Horizon

© SANS Institute 2000 - 2005, Author retains full rights.

- The Symantec Raptor firewalls will provide application filtering for the VPN traffic ONLY into the Internal Private Area enclave.

4. There are 2 separate firewall types being used. In essence, the CISCO PIX firewall will have different vulnerabilities than the Symantec Raptor firewalls. (Layered approach)
5. Both the PIX and the Raptor will screen outbound activity from GIAC Enterprises.
6. Elements on the Screened subnet will include the following:
   - HTTP servers
   - SMTP servers-Relays all external Internet mail to and from GIAC Enterprises.
   - E-Business DNS servers-No corporate DNS information will be configured on this machine.
7. Elements on the "Internal Private Area" network (Including the R&D and Corporate Areas):
   - An internal Steel-Belted Radius authentication server-This provides authentication to the CISCO Altiga VPN. See the press release: http://www.altiga.com/news/pressroom/19990419_9.cfm
   - Fortune servers-These are the servers that home the fortune sayings for purchase, research and development and so forth. Since the suppliers and customers only have access to the E-business sector, SSL encryption will be used to upload sayings as well as purchase sayings.
   - An internal DNS server will hang off the switch (192.168.1.97/27) in front of the Internal Private Area. This provides all the DNS services to internal hosts.
8. Elements on the internal Sales/Marketing and Corporate network:
   - These include any employees that will be browsing the WWW as well as reading e-mail. They won't have access to the fortune server database or any other "internal" area of the Enterprise unless they have permissions. They will basically stay under their sector and perform their daily work functions. The Corporate sector houses all financial activities and databases as well as supports the public web pages financial section, just as the Sales/Marketing group focuses their attentions on customer testimonial and marketing ploys.
9. Element on the internal R&D network:
   - These include all the employees involved in research in development with respect to the fortune saying business. The fortune servers are located here as well as the most vital company information. The R&D sector also supports the public web page on future developments and comments and suggestions on fortune sayings.

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005, Author retains full rights.

1.7 Equipment Used

Routers

We decided to use two CISCO 3640 routers for our design. [3]The Cisco 3600 Series routers are perfect choice for medium to large size corporations. Because we are unsure of the growth rate of the company, having a router that can be utilized for a large corporation is a smart idea. The router provides solutions for VPNs, hybrid dial access, data, and video voice.



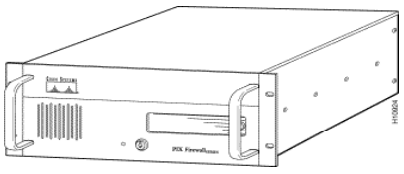
Switches

With regards to our switches, the CISCO Catalyst 2924 series switch was chosen for all of the switches throughout the Enterprise. Because the 2924 series switch is only a little more expensive than the 2912 series, we decided to go with the 24 port option. [4]The 2900 series switch provides outstanding performance, ease of deployment, integrated switching IOS software, security features, and redundancy. These key benefits made the CISCO Catalyst an easy pick.



Firewalls

Again, we selected the CISCO PIX 520 firewall for our primary firewall as a first layer of defense from the Internet. [5]"Unlike typical CPU-intensive full-time proxy servers that perform extensive processing on each data packet at the application level, Cisco Secure PIX Firewalls use a non-UNIX, secure, real-time, embedded system. The Cisco Secure PIX Firewalls deliver outstanding performance of up to 250,000 simultaneous connections, over 6,500 connections per second, and nearly 170 Mbps throughput." With regards to security, it supports a number of different features such as RADIUS authentication.



[3] Cisco 3600 Series Routers http://www.cisco.com/warp/public/cc/pd/rt/3600/
[4] Cisco 2900 Family Switches http://www.cisco.com/warp/public/cc/pd/si/casi/ca2900/
[5] Cisco Secure PIX Firewall Series http://www.cisco.com/univercd/cc/td/doc/pcat/fw.htm

© SANS Institute 2000 - 2005 Author retains full rights.

Virtual Private Network (VPN)
Because there are a considerable number of partners and home users, the Altiga C20 VPN Concentrator was the VPN of choice. [6]The Altiga C20 is ideal for mid-size corporations that need to support a large number of remote users and several remote offices, while ensuring a flexible path for future growth and redundancy. The Altiga Concentrator is scalable up to 5000 simultaneous encrypted sessions, supports a wide range of authentication and data privacy standards, has excellent performance, and provides a complete management solution.



Assignment 2: Security Policy

2.1 Scope

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

- *Border Route*
- *Primary Firewall*
- *VPN*

You may also wish to include one or more internal firewalls used to implement defense in depth or to separate business functions.
By security policy, we mean the specific ACL's, firewall rulset, IPSec Policy, etc. For each component, be sure to consider internal business operations, customers, suppliers, and partners.
For each security policy, write a tutorial on how to implement each ACL, rule, or policy measure on your specific component. Be certain to include the following:

1 *The service or protocol that may be considered a vulnerability.*
2 *Any relevant information about the behavior of the service or protocol on the network.*
3 *The syntax of the ACL, rule, or filter.*
4 *A description of each of the parts of the filter.*
5 *An explanation of how to apply the filter.*
6 *If the filter is order-dependent, list any rules that should precede or follow this filter and why this order is important.*

[6] Altiga Networks- C20 VPN Concentrator Series http://www.altiga.com/products/C20.cfm

© SANS Institute 2000 - 2005 Author retains full rights.

7 *Explain how to test the ACL/filter/rule.*
8 *Point out tips, tricks, or gotchas.*

2.2 Introduction

When deciding the reasons to have security policies, I did a bit of research and found that PentaSafe Security had the right idea:

[7]**"Reasons to Have Security Policies:**

Save money

- *Reduces costs of security incidents*
- *Accelerate development of new application systems*
- *Justify additional information security budget*
- *Establish definitive reference points for audits*
- *Avoid disputes and related internal politics*

Be prepared

- *Educate, train, and motivate staff*
- *Coordinate activities of internal decentralized groups*
- *Clarify appropriate responses to security incidents*
- *Generate information security effort credibility and visibility*
- *Assure consistent product selection and implementation*

Protect assets

- *Maintain trade secret protection for information assets*
- *Establish a basis for disciplinary actions and termination*
- *Demonstrate quality control processes (ISO 9000 compliance)*
- *Document contract, law, and regulation compliance*
- *Avoid liability for negligence and breach of fiduciary duty"*

2.3 Defense in Depth Strategy

While perfect security is an information-sharing environment is impossible, there is much that can be done within the limits of the present state of practice to minimize system vulnerabilities and counter potential threats. This defense in depth strategy uses a layered system of defense much the same way a bank vault may be built with sequential doors and many alarm systems. It is designed to protect the confidentiality, integrity, authenticity, and availability of the information. In essence, the defense in depth strategy will eliminate a single point of failure.

This section presents the components that will be used to implement Defense in Depth.

Protection Tool	Confidentiality	Integrity	Authenticity	Availability
Firewalls and Packet Filtering	Yes		Yes	Yes
Content Filtering		Yes		
Virtual Private Network	Yes	Yes	Yes	
Encryption	Yes	Yes	Yes	

[7] Taken from PentaSafe Security home page: http://www.baselinesoft.com/

© SANS Institute 2000 - 2005 Author retains full rights.

2.4 High Level Security Policy

These are some basic high level policies that will be carried out in GIAC Enterprises. They were taken from a general rule of policies that virtually every company should be implementing. This basic policy covers what each member of the Enterprise should be aware of and following ranging from the employee, manager, and technician.

- All users who require access to Internet services must do so by using GIAC-approved software and Internet gateways.
- A firewall has been placed between our private networks and the Internet to protect our systems. Employees must not evade the firewall by using modems or network tunneling software to connect to the Internet.
- Some protocols have been blocked or redirected. If you have a business need for a particular protocol, you must raise the issue with your manager and the Internet security officer.
- A firewall shall be placed between the GIAC Enterprise's network and the Internet to prevent untrusted networks from accessing GIAC's network. The firewall will be selected by and maintained by the Network Services Manager.
- All other forms of Internet access (such as dial-out modems) from sites connected to GIAC's WAN are prohibited.
- The firewall administrators and managers shall review the network security policy on a regular basis (every two-three months minimum).
- The firewall shall not accept traffic on its external interfaces that appear to be coming from internal network addresses.
- The firewall shall provide detailed audit logs of all sessions so that these logs can be reviewed for any anomalies.
- Firewalls shall be tested off-line and the proper configuration verified.

© SANS Institute 2000 - 2005 Author retains full rights.

2.5 Security Policy Broken down in Depth

Border Router

- Block RFC 1918 addresses from coming in
- Block Anti-Spoofing (Ingress)
- Block Anti-Spoofing (Egress)
- Allow only traffic from partners/home users to VPN (192.168.1.221)
- Allow SMTP traffic to the firewall (192.168.1.29)
- Allow DNS traffic to the firewall (192.168.1.29)
- Allow HTTP traffic to the firewall (192.168.1.29)

Primary Firewall

- Allow HTTP port 80 TCP traffic to the Web server (192.168.1.35)
- Allow HTTP replies to internal private network
- Allow port 53 UDP DNS (192.168.1.34)
- Allow SMTP port 25 TCP traffic to Mail server (192.168.1.36)
- Allow Web server to access Fortune database servers (192.188.5.2-4)via SSL
- Deny All

Secondary Firewall

- Allow HTTP port 80 TCP destined to anywhere
- Allow SMTP port 25 traffic to Mail server (192.168.1.36)
- Allow DNS port 53 UDP to 192.168.1.98
- Allow Web server via SSL to access database server under R&D
- Allow traffic from VPN (192.168.1.254) to access R&D's Fortune servers (192.188.5.2-4)
- Allow RADIUS traffic (192.168.5.4)to VPN (192.168.1.254)
- Deny All

VPN

- Implement SHA-1 for an authentication algorithm
- The encryption algorithm will be168-bit Triple DES (IPSec)
- Key Management: Internet Key Exchange (IKE)
- Tunneling Protocol: IPSec with IKE Key Management

© SANS Institute 2000 - 2005, Author retains full rights.

General Syntax for Applying an Access-List on a Router

- *access-list <Number><deny/permit><protocol><source address><mask address><destination address><mask address>log*

If a protocol involving a port was used such as TCP or UDP use this syntax:

- *access-list <Number><deny/permit><protocol><source address><mask address><port><destination address><mask address><port>log*

General Syntax for a rule on the Cisco PIX

Outbound Rules

- *outbound List_ID deny/permit ip_address netmask port(range) protocol*

Apply Rules

- *apply(if_name) List_ID outgoing_src/outgoing_dest*

Conduit Rules

- *conduit deny/permit protocol host ip_address <statement of equality port> <source>*

Block Spoofed Addresses (Inbound)

IP Address spoofing is a very common attack that hackers undertake. Hackers basically use it so that no one can trace their actions. A hacker must first use a variety of techniques to find an IP address of a trusted port and then modify the packet headers so that it appears that the packets are coming from that port. This can be very dangerous unless the proper tools are in place so that a hacker cannot compromise any of the tools that support IP address authentication. A filter needs to be in place that blocks this for both inbound and outbound packets.

Block RFC 1918

The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private Internets: (http://www.iana.org)

10.0.0.0	- 10.255.255.255	(10/8 prefix)
172.16.0.0	- 172.31.255.255	(172.16/12 prefix)
192.168.0.0	- 192.168.255.255	(192.168/16 prefix)

Syntax and Application

Once in the router enter these commands at the prompt:

routera>enable

Password: xxxxxxxx

© SANS Institute 2000 - 2005 Author retains full rights.

```
routera# configure terminal

routera (config)# interface fastethernet 0/0

routera (config-if)# ip access-group 110 in
routera (config-if)# exit

routera (config)# access-list 110 deny ip 10.0.0.0 0.255.255.255 192.168.0.0 0.0.255.255 log
routera (config)# access-list 110 deny ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255 log
routera (config)# access-list 110 deny ip 172.16.27.0 0.0.0.255 192.168.0.0 0.0.255.255 log
routera (config)# access-list 110 permit any 192.168.0.0 0.0.255.255 log

routera (config)# Ctrl Z
routera #
```

Description of the Filter

In the above example, we are using a Cisco extended access-list. An extended access list can, in addition to source IP address, also include entries for:

- Destination IP address
- Port number
- Protocol type

This particular access list is for blocking spoofed addresses for inbound traffic and blocking RFC 1918. Once the router starts receiving traffic, it will know whether or not to drop the packets depending on the access list. This ACL is used to filter private addresses to GIAC's network.

- *access-list 110 deny ip 10.0.0.0 0.255.255.255 192.168.0.0 0.0.255.255 log*
  The above access-list says that the router will deny any packet with a source address of 10.X.X.X. Because the wildcard is 0.255.255.255, only the first octet of the packet will be looked at.
- *access-list 110 deny ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255 log*
  This access-list says that the router will deny any packet with a source address of 192.168.X.X. Because the wildcard is 0.0.255.255, the first two octets of the packet will be looked at.
- *access-list 110 deny ip 172.16.27.0 0.0.0.255 192.168.0.0 0.0.255.255 log*
  This access-list says that the router will deny any packet with a source address of 172.16.27.X. Because the wildcard is 0.0.0.255, only the last octet of the packet will be looked at.
- *access-list 110 permit any 192.168.0.0 0.0.255.255 log*
  This access-list says that any packet that is not dropped is allowed through the 192.168.0.0 network.

How to Test the Filter

© SANS Institute 2000 - 2005, Author retains full rights.

To actually the test the filter, you can check that the router is actually blocking these packets through the log. An IDS can also be used to examine what packets did and did not go through the router. There are a million IDSs on the market, find one that you enjoy using or find simple to use. There are also tools out there that allow source address spoofing. By using this type of tool, you can send packets to your network

Sample Log
For purposes of this paper, I decided to show you what a log would look like. They tend to take up a lot of space, but I wanted to give you a general idea of what one looked like and the type of information that was there.

```
01:27:01: %SEC-4-IPACCESSLOGDP: list 110 denied ip 10.1.2.3-> 192.168.0.0 (0/0), 1 packet
01:27:35: %SEC-4-IPACCESSLOGDP: list 110 denied ip 192.168.1.2 -> 192.168.0.0 (0/0), 1
packet
01:27:18: %SEC-4-IPACCESSLOGDP: list 110 denied ip 172.16.27.1 -> 192.168.0.0 (0/0), 1
packet
```

Block Spoofed Addresses (Outbound)

Syntax and Application
Once in the router enter these commands at the prompt:

```
routera> enable
Password: xxxxxxxxx

routera# configure terminal

routera (config)# interface ethernet 1/0

routera(config-if)# ip access-group 111 in
routera (config-if)# exit

routera(config)# access-list 111 permit ip x.x.x.x x.x.x.x  any log

routera(config)# cntrl Z

routera#
```

Description of the Filter

© SANS Institute 2000 - 2005 Author retains full rights.

In the above example, we are using a Cisco extended access-list. An extended access list can, in addition to source IP address, also include entries for:

- Destination IP address
- Port number
- Protocol type

This particular access list is for blocking spoofed addresses for inbound traffic. Once the router starts receiving traffic, it will know whether or not to drop the packets depending on the access list. This particular ACL is used to filter all the packets on the Internet destined to the private network of GIAC Enterprises. *Note: The source address is the range of public addresses assigned to GIAC Enterprises.*

Information on Outbound (egress) filters: http://www.sans.org/dosstep/index.htm

- *access-list 111 permit ip x.x.x.x x.x.x.x any log*
  This access-list says that the router will permit all packets with a source address of x.x.x.x x.x.x.x. The wildcard bits used determine what octets of the address are looked at.

How to Test the Filter

To test the filter, all you would have to do is generate packets that don't begin with a source in your network. Again, you can use a tool that allows spoofed addresses or you can manually change the IP address of an internal host to something that doesn't start in your address space.

Allow only traffic from partners/home users to VPN (192.168.1.221)

With regards to allowing only traffic from our remote sites to the VPN implies that we know all of the IP addresses of our remote sites. This case is actually true. By knowing the IP addresses, we can configure the router to follow only the known IP addresses to the VPN. This is a nice security measure. By setting this particular rule, only specific IP addresses are permitted to the VPN.

Syntax and Application

routera> enable
Password: xxxxxxxxx

routera# configure terminal

routera (config)# interface ethernet 1/0

routera(config-if)# ip access-group 110 in
routera (config-if)# exit

routera(config)# access-list 110 permit ip x.x.x.x x.x.x.x 192.168.1.221 128.255.255.255 log

© SANS Institute 2000 - 2005 Author retains full rights.

routera(config)# cntrl Z

routera#

Description of the Filter
This access-list is an extended list and can be applied to for all known source IP Addresses of our remote sites including the home offices and business partners that VPN to the internal private enclave of GIAC Enterprises.
This access-list is saying to allow anything through with x.x.x.x x.x.x.x to the VPN at 192.168.1.221. The x.x.x.x x.x.x.x is the IP addresses of the remote sites that are not located at the GIAC Enterprise's headquarters. *Note: You will need a separate rule for every address that is remotely located.*

How to Test the Filter
To actually test the filter, you can attempt to use a different IP address than the ones listed in the ACLs. If you are actually allowed through than you know that the filter isn't working correctly even if you have the correct username and password. The router will have a list of all the known IP addresses. If yours isn't on there, you aren't getting in. Just a note, you can always check the log.

Allow DNS, HTTP, and SMTP traffic
In this case we are allowing any source IP address from anywhere on the Internet to be routed to our DMZ or screened subnet. The reason for this is this is where all of our public servers are located. If a customer wanted to buy a GIAC fortune sayings, or if a supplier needed to upload a product, they could from our E-Business area. Also, if a user just wanted to browse our site, they ultimately would need access to our E-business sector of the corporation. Because the HTTP server, SMTP server, and DNS hang off the PIX, they are considered a screened subnet. We need to essentially allow these different types of traffic to the public screened subnet (DMZ). This particular area with the above three mentioned servers is considered the E-business sector of GIAC Enterprises. Our customers will purchase fortune sayings from the web server and our suppliers will upload the sayings there as well.

Allowing DNS Traffic
DNS is one of the most vulnerable areas on your network. You need to be extremely careful that attackers don't gain a full understanding of your network from your DNS records. One way to do this would be to have an internal DNS and a DNS that would exist on your DMZ or screened subnet. By having two separate DNS servers, you can protect your internal records and have only the mail, external web server, and other public information available. This ensures that your internal network is safe in that the attacker won't know the internal network map from the DNS records. Currently, there are two major vulnerabilities that you have to be aware of:
1. A remote intruder can gain root-level access to your name server via a buffer overflow.
2. A remote intruder is able to disrupt normal operation of your name server.

© SANS Institute 2000 - 2005, Author retains full rights.

Go to the CERT Advisories for more information at: http://www.cert.org/advisories/ Although there are some resolutions, you need to ensure that you stay on top of things like updating patches and upgraded software and patches.

Syntax and Application (Router)

routera> enable
Password: xxxxxxxxx

routera# configure terminal

routera (config)# interface ethernet 1/0

routera(config-if)# ip access-group 110 in
routera (config-if)# exit

routera(config)# access-list 110 permit udp any host x.x.x.x x.x.x.x eq 53

routera(config)# cntrl Z

routera#

Description of the Filter

- *access-list 110 permit udp any host x.x.x.x x.x.x.x eq 53*
  This says that the router will allow access from any host on the Internet to the external DNS server on port 53 UDP. The x.x.x.x x.x.x.x is a public address.

How to test the Filter

To test the filter just try a connection from anywhere and you should be allowed through.

Syntax and Application (firewall)
primarypix>enable
Password: xxxxxxxx

primarypix# configure terminal

primarypix(config)# outbound 11 permit x.x.x.x x.x.x.x 53 udp
primarypix(config)# apply (inside) 11 outgoing_dest
primarypix(config)^Z

primarypix#write mem
primarypix#

© SANS Institute 2000 - 2005, Author retains full rights.

Description of the Filter

- *outbound 11 permit x.x.x.x x.x.x.x 53 udp*
  This says that the firewall will permit traffic that is outgoing on port 53 UDP. The x.x.x.x x.x.x.x is the public address of the server.
- *apply (inside) 11 outgoing_dest*
  This says that the firewall will apply rule 11 on the inside interface thus saying that the internal DNS can only talk to the public DNS when need be.

How to test the Filter
To test the filter, just ensure that that only UDP traffic is allowed though on port 53. By checking the logs you will be able to see if there were any variations of this.

Allowing SMTP traffic
Just as DNS, mail protocols also are inundated with vulnerabilities. Some of these vulnerabilities include MIME buffer overflow, SPAM, Mail Relay, and old send mail versions. Information can be found more on this on the CERT Advisories as well as Bugtraq.
One of the newer vulnerabilities is with the content filter that allows mail to pass against filter rules. Although it has been setup to stop messages that have attachments with *.exe, it is allowing certain characters to be let through.
For more information see: http://www.dataguard.no/bugtraq/2000_4/0793.html

Syntax and Application (Router)
routera> enable
Password: xxxxxxxxx

routera# configure terminal

routera (config)# interface ethernet 1/0

routera(config-if)# ip access-group 110 in
routera (config-if)# exit

routera(config)# access-list 110 permit tcp any eq 25 host x.x.x.x eq 25
routera(config)# access-list 110 deny tcp any any eq 25 log
routera(config)# access-list permit ip any any

routera(config)# cntrl Z

© SANS Institute 2000 - 2005 Author retains full rights.

routera#

Description of the Filter
In the above example, we are using a Cisco extended access-list. An extended access list can, in addition to source IP address, also include entries for:

- Destination IP address
- Port number
- Protocol type

- *access-list 110 permit tcp any eq 25 host x.x.x.x eq 25*
  This says that the router will allow traffic from any host on the external mail server on port 25. The x.x.x.x is the public address of the SMTP server.
- *access-list 110 deny tcp any any eq 25 log*
  This says that the router will deny any host that is trying to connect to any internal host on port 25
- *access-list permit ip any any*
  This says that the router will allow anything else through that is not allowed through in the above rules.

How to Test the Filter

To test the filter, send packets that are destined to the external mail server. You should see that the packets being sent to the external mail server go through successfully and that any packets trying to connect to any internal host on port 25 are blocked. Check this by looking at the log.

Syntax and Application (Firewall)

pimarypix>enable
Password: xxxxxxxxx

pimarypix# configure terminal

pimarypix(config)# conduit permit tcp host x.x.x.x eq 25 any eq 25
pimarypix# outbound 8 permit x.x.x.x x.x.x.x 25 tcp
pimarypix(config)# apply (screened) 8 outgong_src
pimarypix(config)# cntrl Z

primarypix# write mem
primarypix#

Description of the Filter

- *conduit permit tcp host x.x.x.x eq 25 any eq 25*
  This says that the firewall will allow incoming mail to the mail server via port 25 from any host on port 25. The x.x.x.x is the public address of the mail server.

© SANS Institute 2000 - 2005, Author retains full rights.

- *outbound 8 permit x.x.x.x x.x.x.x tcp*
  This says that the firewall will allow there to be outgoing traffic on port 25. The x.x.x.x x.x.x.x is the public address and netmask of the mail server.
- *apply (screened) 8 outgong_src.*
  This says that the firewall will allow the external mail server to send mail to any other server.

How to Test the Filter

To test the filter, you can send mail inbound to the mail server which should allow packets though which can be viewed in the log-or- you can send mail from any other machine besides the mail server on the screened subnet. The packets will be blocked and the information can be viewed in the log as well.

Allowing HTTP Traffic

HTTP traffic has some vulnerabilities as well. One for example is that unless the HTTP server is explicitly disabled, it can be used to make changes to the router configuration, and/or to gain information about that configuration. Other types of vulnerabilities may also include buffer overflow. Both of these issues can compromise the network and we all need to be aware of them.

Syntax and Application (router)

routera<enable
Password: xxxxxxx

routera# configure terminal

routera (config)# interface ethernet 1/0

routera(config-if)# ip access-group 110 in
routera (config-if)# exit

routera(config)# access-list 110 permit tcp any host x.x.x.x eq 80
routera(config)# access-list permit ip any any

routera(config)# cntrl Z

routera#

Description of Filter

- *access-list 110 permit tcp any host x.x.x.x eq 80*

© SANS Institute 2000 - 2005 Author retains full rights.

This says that the router will permit tcp packets from anywhere to the public web server on port 80. The x.x.x.x is the public address of the web server.

- *access-list permit ip any any*
  This says that the router will permit any packet that is not blocked from the above list.

How to test the Filter

To test the filter try connecting with a tcp connection to ensure that the packets are sent to the public web server. This is important such that customers or Internet users that want to browse the site have access.

Syntax/Application (Firewall)

pimarypix>enable
Password: xxxxxxxxx

pimarypix# configure terminal

pimarypix(config)# conduit permit tcp host x.x.x.x eq 80 any
pimarypix# outbound 8 permit x.x.x.x x.x.x.x 80
pimarypix(config)# conduit permit tcp 192.168.5.2 255.255.255.224 eq 443 x.x.x.x x.x.x.x eq 443
pimarypix(config)# conduit permit tcp 192.168.5.3 255.255.255.224 eq 443 x.x.x.x x.x.x.x eq 443
pimarypix(config)# conduit permit tcp 192.168.5.4 255.255.255.224 eq 443 x.x.x.x x.x.x.x eq 443
pimarypix(config)# apply (inside) 8 outgong_dst
pimarypix(config)# cntrl Z

primarypix# write mem
primarypix#

Description of Filter

- *conduit permit tcp host x.x.x.x eq 80 any*
  This says that the firewall will permit WWW traffic from the Internet to the public mail server on port 80 tcp. The x.x.x.x is the public address of the mail server.
- *outbound 8 permit x.x.x.x x.x.x.x 80*
  This says that the firewall will permit on outbound number 8, web traffic on port 80.
- conduit permit tcp 192.168.5.(2-4) 255.255.255.224 eq 443 x.x.x.x x.x.x.x eq 443
  This says that the firewall will allow web replies to the internal private enclave on port 443. Basically if something is sent to you from the Internet, you will be able to respond back. Again, the x.x.x.x x.x.x.x is the public address. As you can see this are for all the fortune database servers.
- *apply (inside) 8 outgong_dst*

© SANS Institute 2000 - 2005 Author retains full rights.

This says that the web server can communicate with the Internet.

How to test the Filter

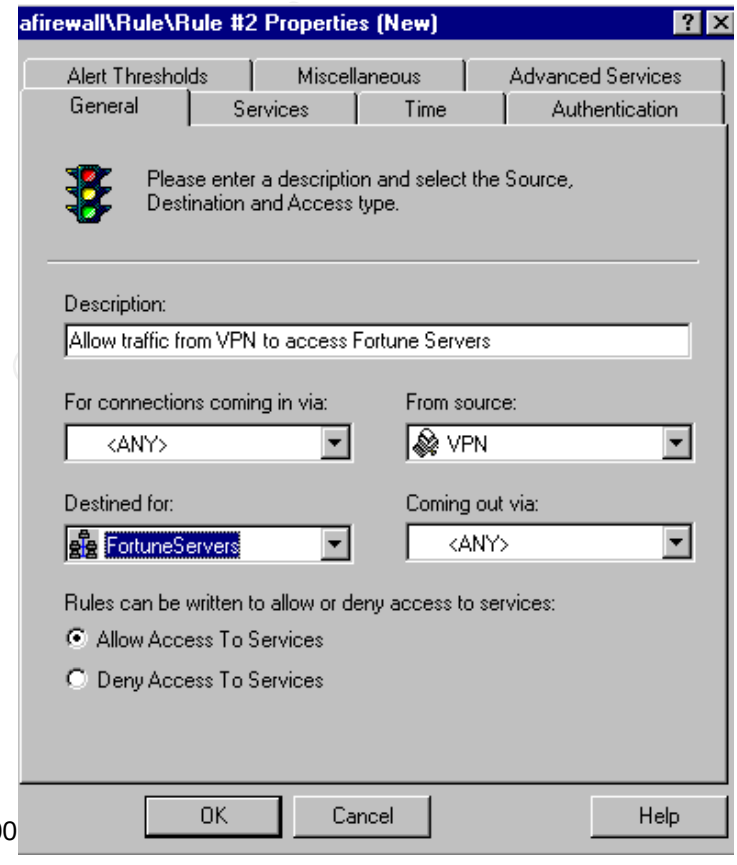
To test the filters have the public web server attempt to send traffic to the Internet on a port that is not 80. This should be blocked. To ensure that traffic is received from the WWW, try sending traffic to the Internet to the mail server on port 80 and make sure that the connection is working.

Using the Raptor Firewall (Secondary Firewall)

The Raptor firewall uses a GUI for the management and configuration of the firewall. I don't want to bore you with multiple screen shots of the GUI, so here are a few below that shows you how the filter is implemented easily by just entering the source address, destination address etc. in the clearly marked dialog boxes. Please refer to the security policy to see what was allowed. All of the vulnerabilities of HTTP, SMTP, and DNS are listed above when speaking about the primary firewall and router. Since all of the rules are allows, all you would need to do is to test them by sending connections to the different ports to see if they are being allowed through. If they aren't, obviously one of the rules was setup incorrectly.

Below is an example of what the Raptor's interface looks like. This is an example that we performed at GIAC for the one of the security policies:

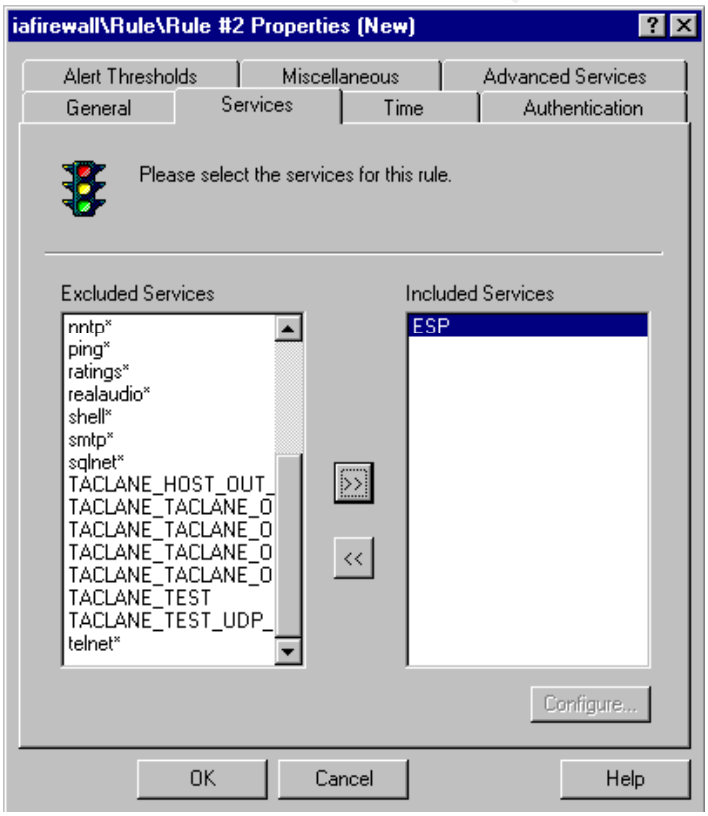
- In this first step, we had to perform some general functions such as entering the source address and destination address



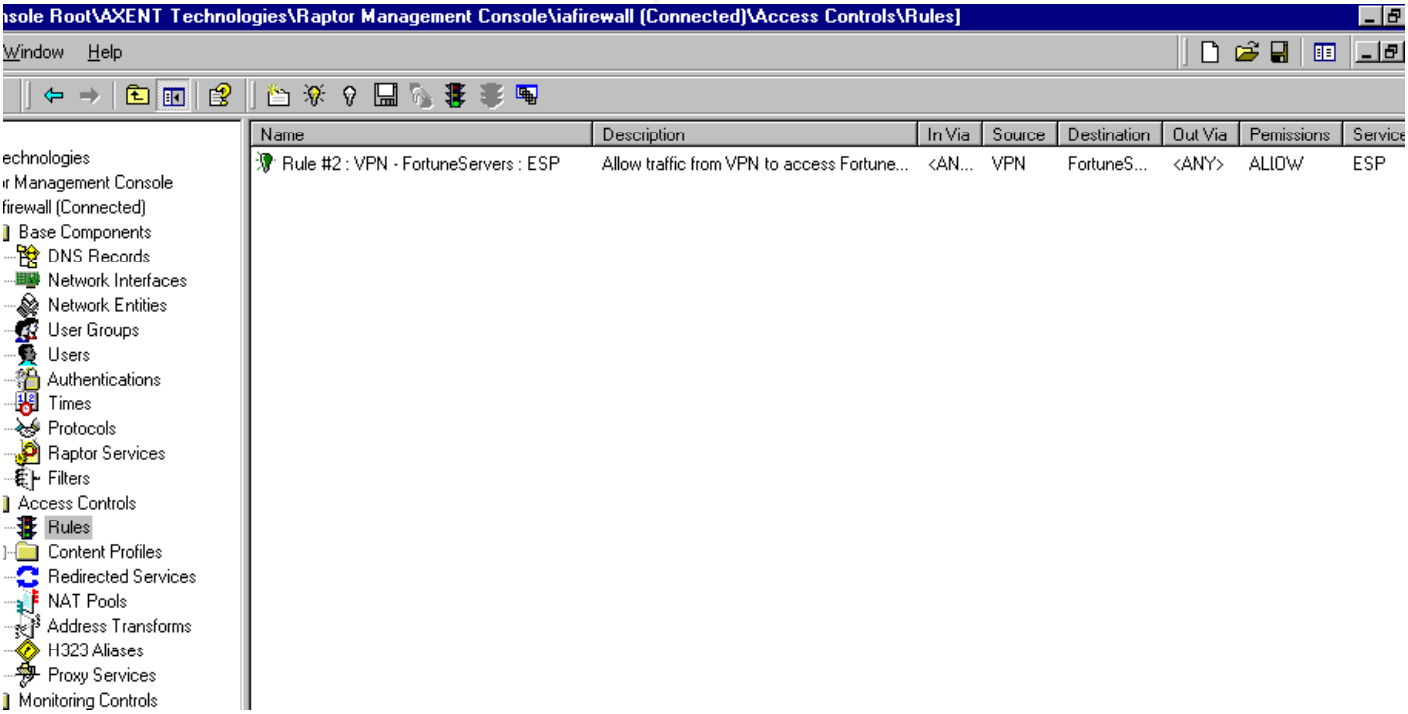
© SANS Institute 2000 - 200 Author retains full rights.

2005, Author retains full rights.

- In the second step, we had to include any services for this rule.



- As you can see, the rule is listed and it can now be saved and implemented.



Using the Altiga C20 VPN Concentrator

© SANS Institute 2000 - 2005 Author retains full rights.

A Virtual Private Network (VPN) is erected by using the Internet to connect two nodes. It uses encryption and authentication mechanisms to ensure that only authorized users can access the network.
One of the most widely used and known protocols is IPSec.
The Altiga supports: **IPSec with IKE Key Management**, PPTP with MPPE encryption, L2TP, and L2TP over IPSec). Altiga uses **Scalable Encryption Processing (SEP**) modules for encryption and for GIAC Enterprises we are using **168-bit Triple DES (IPSec).** For an authentication algorithm, **SHA-1** will be implemented. The main reason we choose the Altiga was mainly because of its scalability and use for the future. For more information on the Cisco Altiga, please go to http:\\www.altiga.com

2.6 Why are some filters/rules Order-Dependent?

The reason that some of these rules/filters are order-dependent is because if you block something in an earlier rule but then allow something else in a later rule, the system may never have a chance to get to the lower set of rules. Remember that the order of the access list statements is important, because the access-list is not processed further after a match has been found.
Follow these simple steps for access-lists:

- Go from the Top-Down-Arrange your access-list so that more specific references in a network or subnet appear before more general ones. Place more frequently occurring conditions before less frequent conditions.
- Ensure that any successive additions are ALWAYS added at the end of the access-list.

In using the Cisco PIX firewall, the rule order is also sequential. It implements the rules from the top down, so ensure that the rules are listed with the more specific ones first. Remember that you don't want a rule skipped because of the order.

Assignment 3: Audit your Security Architecture

3.1 Scope

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

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

© SANS Institute 2000 - 2005 Author retains full rights.

here.

3.2 Plan the Assessment

For preparation of the audit, GIAC Enterprises must realize that this is only an audit and that we are not trying to bring down the entire Enterprise. Since this is being performed on our own network, we already have the vital information about our network (IP Addresses, internal setup, local of vital data servers, etc.). This information can save us a great deal of time, something that a hacker would have to find out on his own. An important note is that because we do know our network so well, we don't want to jump over or skip any important security measures.
The audit will forego a number of steps that will be used to provide an assessment against the network itself and the other critical systems that are an integral function to our daily business.

Development Steps:

1. Acquire permission to provide the audit from the appropriate person(s).
2. Begin a plan for the audit to undergo.
3. Focus on business results
4. Materiality
5. Documentation
6. Focus on principles
7. Obtain the essential tools to perform the audit (whether it is using existing technology or creating your own building blocks)
8. Configure the tools so that they are ready to go and assess the defenses.
9. Provide a time line, possible cost estimations, manpower, and overall intent to the appropriate person(s) providing approval for the audit.
10. Use the computer by automating the audit
11. Stress audit efficiency
12. Analyze the results from the audit
13. Provide the information from the audit to the appropriate person(s).

Risks/Considerations:

When performing an audit, there were a few things that we had to keep in mind to ensure that we did not disrupt everyday business as well as system crashes and application failures:

- When scanning the network make sure that the latest versions of the software are in use. Older versions potentially cause system crashes and CPU usage to MAX-Out.
- There is a possibility that if a scanner were added, existing services would be disrupted and thus cause operational downtime.
- While the assessment is taken place, one needs to ensure that a hacker isn't trying to

© SANS Institute 2000 - 2005, Author retains full rights.

piggyback the attack during the scan.
- We must be able to stop the audit at any given time if an attack is detected while performing the assessment.
- We must be able to fix any problems that may occur during the scan in a timely fashion not to interrupt business.
- We must not put the employees at risk for not being able to get their jobs done.

Gathering Appropriate Assessment Tools

The scanning platform used is a PC laptop that allows dual boot for both Windows/LINUX. The reason we chose for a laptop and not a desktop was to allow for easy mobility when testing different sides of the router or moving to different locations throughout the Enterprise during the audit. Because we chose to allow for a dual boot system, all of the scanning tools can be performed from the scanning platform, making the process more time efficient.

The scanning tools include: Nessus Security Scanner, Shields UP!, Nmap, Sam Spade, and the general network tools found on the operating systems.

The tools that were chosen were based on the fact that they would provide the appropriate assessment on the network.
Nessus Security Scanner, for example, was chosen because of the following:
- It's FREE
- There is an automatic signature update feature
- CVE cross-references
- Open Source
- Command-line automation
- Capable of custom security checks (NASL)
- Well liked by the community
- Easy to use web interface

Sam Spade
Sam Spade for Windows was used to for getting DNS information. The Sam Spade application tool displays it's output in it's own window. Because everything is multi-threaded, you don't need to wait for one query to complete before starting the next one. Reverse DNS lookups are allowed because of the extensive threading so you will never have to do a traceroute –n again. The output from each query is hot-linked, so you can right click on an email address, IP address, hostname or internic tag to run another query on it.
Much help is available online through the use of WINHelp or hard documentation.

Nmap
Nmap was chosen for port scanning. Nmap covers everything from TCP ACK and window scanning to Reverse-Ident scanning. The neat thing about Nmap is that

© SANS Institute 2000 - 2005 Author retains full rights.

incorporates a number of different protocols used for scanning.

Shields UP!
Shields UP! was chosen for scanning ports and Windows specific NetBIOS for our home users and business partners. Because both our home users and business partners have direct access to our internal corporate enclave at GIAC Enterprises, it is essential that we ensure that no Spoofing is occurring. Attackers, if they cannot get into the main frame, sometimes will attack business partners or home users as other methods of causing harm to the network. Whatever means they can, they will.

All of the tools gathered information about the network environment, evaluated any loose ends through the defensive system, and evaluated the host vulnerability from attacks. Other tools for the analysis of web based applications and separate functional teams of the auditing entourage will explore other vulnerable areas.

Collecting Necessary Data

To ensure that the Security Policy, in the previous section, has been implemented, we ensure that we have it in hands and eyes focus.

All site survey information is provided including system configurations, physical and logical network diagrams, and IP Addresses.

Scheduling

To effectively schedule when and at what time the audit will occur, employee schedules, operating schedules, and server loading schedules were at hand. When deciding when the assessment was actually going to take place, a number of considerations and thoughts were accessed. We knew that we didn't want any disturbance in the daily routine, we didn't want anyone to slack on his or her normal duties and responsibilities, and we wanted to do this when the employees were readily available. Other considerations were that if a hacker were to attack, it most likely wouldn't be in the middle of a business day, but more likely a holiday or weekend. Also, if we did interrupt the system, we wanted to ensure that the problem could be fixed. For example, when scanning the network it may freeze a machine that would just require a reboot. We are just noting that problems could arise, we probably wouldn't need a "babysitter" (for lack of a better word), but just someone to keep their eyes out.
Just From this information we knew it needed to happen on a business day. The next pertinent information was what time and day the server loading takes into effect. At GIAC Enterprises, Thursday afternoons are not heavily loaded, so the scans involving significant network or host based loading would be done at this time.

Costs

Cost estimates would be based not only on training and personnel, but also on scanning

© SANS Institute 2000 - 2005, Author retains full rights.

platform and scanning tools.

- $ 2,500 (2 days) obtain scanning platform and necessary tools
- $4,500 (3 days) Conducting Audit
- $2,500 (2 days) Review of Security Policy/Architecture
- $1,800 (1 days) Create Analysis Findings

Total cost about $11,300.
Note: Remember this is only an estimate and may change depending on availability, timing, etc.

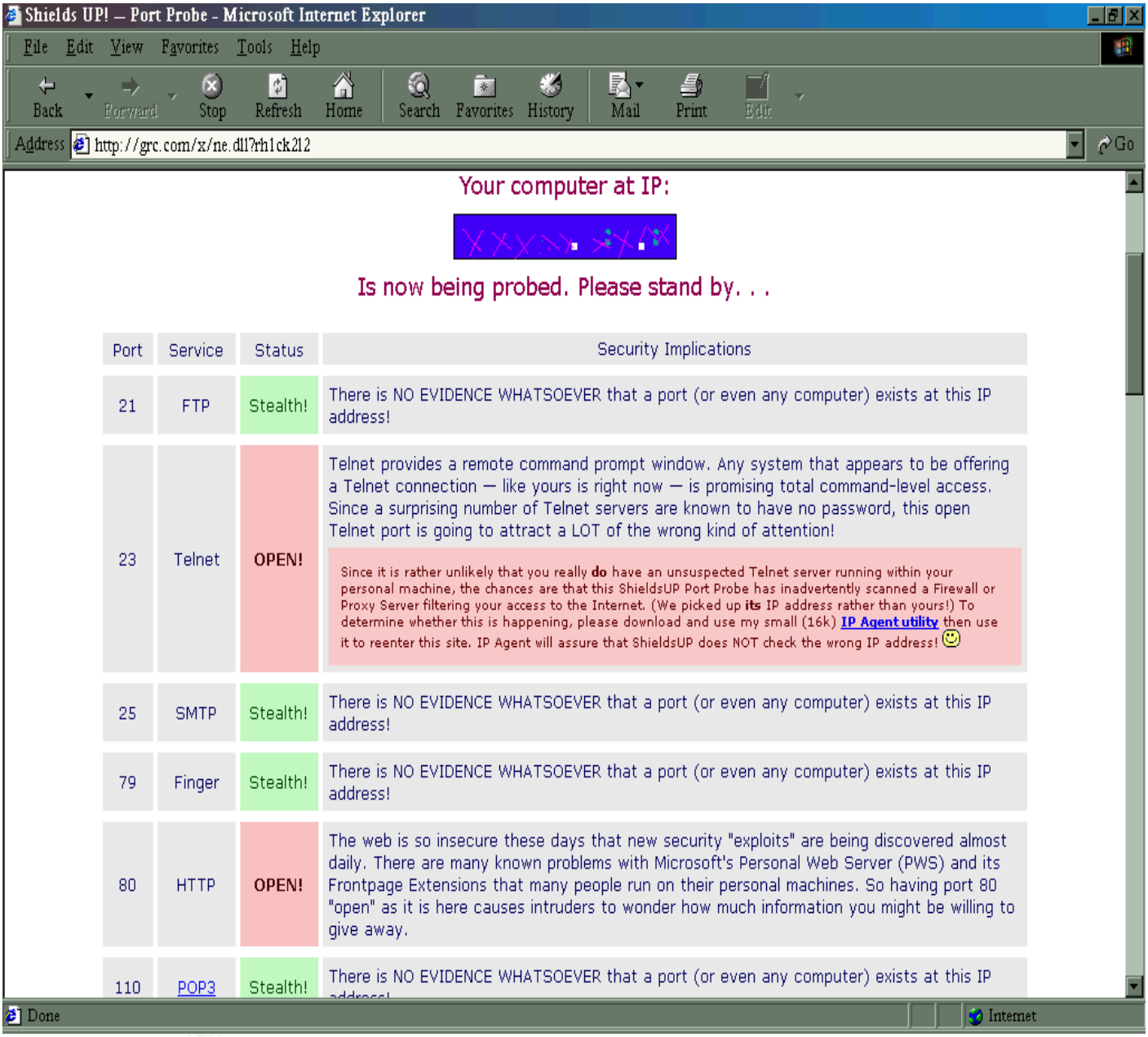
3.3 Implement the Assessment

Outer Entrance-Home Users and Business Partners
In order to implement the assessment, we need to sit back for a second and go into the deep, mysterious mind of an attacker. Some thoughts they may have: What is open and unblocked? Can we see their network layout? Is there a way for me to peer in to see their vital information, IP addressing scheme, system configurations? If I can't get into the network this way, how else can it be done? Can I go through a business partner and get in that way? Can I piggyback the company when they are doing security scans? These are just a few thoughts that may be going through the attacker's mind. We need address each and every one of these thoughts to check our entire network arena.

Since our Business Partners and Home Users are the only non-GIAC present persons allowed into the corporate enclave, we would need to setup a scan for them to do either at their homes or offices. The type of scan chosen is called ***Shields UP!*** With Shields UP!, you can check the security of your computer's connection to the Internet.
By testing your access once with the VPN in place and once with the normal configuration, you will be able to see what kind of defense against the Internet you have at the home office. Also, it would be a good idea to have the remote sites gain Internet access via a dial-in connection as well as the use of an extranet client from the ISP. Just a note that we must also stress to the business partners that this is a necessary action and something that needs to be done in order to maintain a secure setting.

© SANS Institute 2000 - 2005 Author retains full rights.

The Shields UP! Web site loads an extremely small Windows application and allows you to test your shields-NetBIOS scan and then scan your ports (telnet, http, etc.). This is one of the results from a home user.



© SANS Institute 2000 - 2005

Author retains full rights.

Another choice is **Bullet "rumor"**. Although we didn't have a chance to look at this in depth, it may be another excellent choice.
ON Line Internet Security Systems, Inc https://onlinescanner.iss.net/about.html
The ISS Online Scanner helps you protect your computer at home. Online Scanner looks at your computer configuration and recommends changes that can help you prevent unwanted intruders from reading or changing your sensitive personal files or using your computer as their own. Online Scanner also surveys your hard drive to ferret out any potentially dangerous programs that may have been placed on your machine without your knowledge by intruders. It also helps you manage your security by checking that you have appropriate virus scan software, that you use it regularly, and that you keep your virus scan files current to help protect you from evolving attack techniques.

Firewall Maintenance
For Firewall, we want to ensure that we maintain a working and secure firewall to protect corporate data from the Internet. There are a few things that we are going to check to ensure a secure firewall. We are going to use Sam Spade to perform a whois, a zone transfer, a trace, and a port scan.

Whois
A whois has been done on our external web site to ensure that the correct information exists such as Company name, addresses, administrative contact, etc.
Below is an example of what a typical whois looks like.

03/09/01 10:16:34 whois ask.org
.org is a domain of Non-Profit Organizations
Searches for .org can be run at http://www.crsnic.net/

whois -h whois.crsnic.net ask.org ...
Redirecting to NETWORK SOLUTIONS, INC.

whois -h whois.networksolutions.com ask.org ...

Registrant:
GIAC Enterprises Corp. (ASK10-DOM)
5858 Morton St. Ste. 350
Lally, CA 94608
US

Domain Name: ASK.ORG

Administrative Contact, Technical Contact:
DNS Administrator (DA17775-OR) dns@GIACEnterprises.org
GIAC Enterprises Corp.
5858 Morton Street, Suite 350
Lally, CA 94608
US
510-555-1212
Billing Contact:
Account Payable (AP3535-ORG) AP @ GIACEnterprises.com

© SANS Institute 2000 - 2005, Author retains full rights.

GIAC Enterprises Corp.
5858 Morton Street, Suite 350
Lally, CA 94608
US
510-555-1212
Fax- - (510) 649-6666

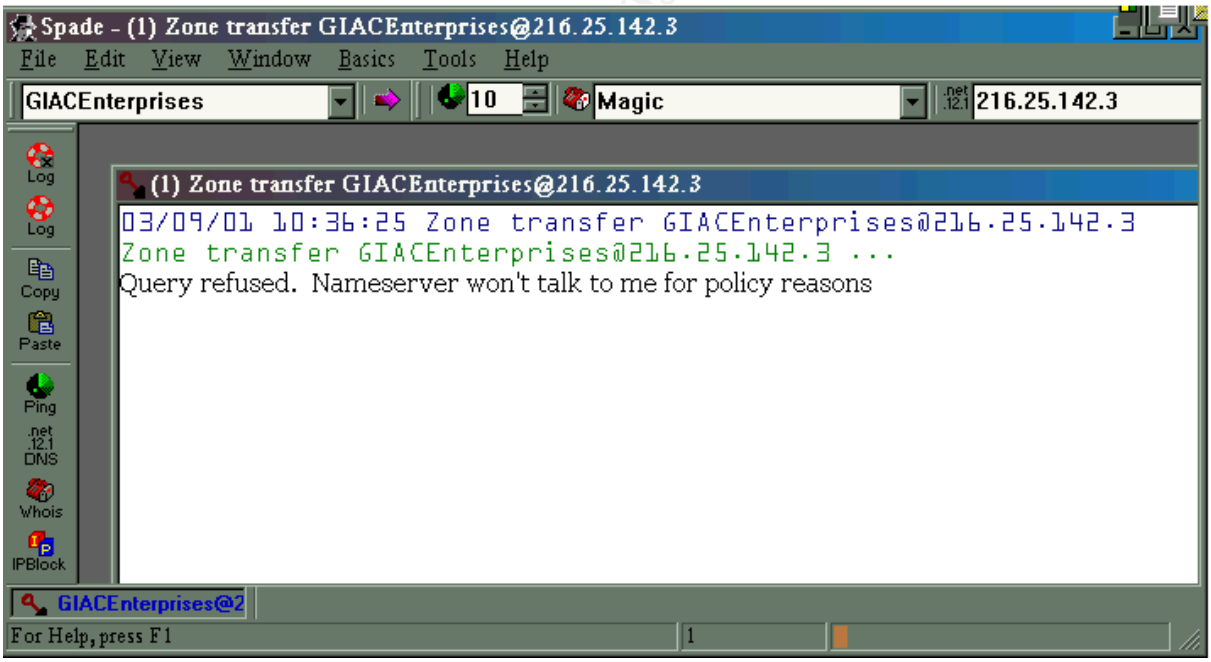
Record last updated on 26-Feb-2001.
Record expires on 26-Feb-2003.
Record created on 26-Feb-1998.
Database last updated on 9-Mar-2001 08:10:52 EST.

Domain servers in listed order:

NAME1.GIACENTERPRISES.COM 216.132.55.124
NAME2.GIACENTERPRISES.COM 218.185.141.11

Zone Transfer

Next we decided to perform a zone transfer. It is very important that the GIAC Enterprises Corp. does NOT allow zone transfers from DNS servers. The zone transfer may be allowed for an authorized DNS server but that is all. Remember: All zone transfers should be limited by the firewall. Below is an example of what that a zone transfer should look like.

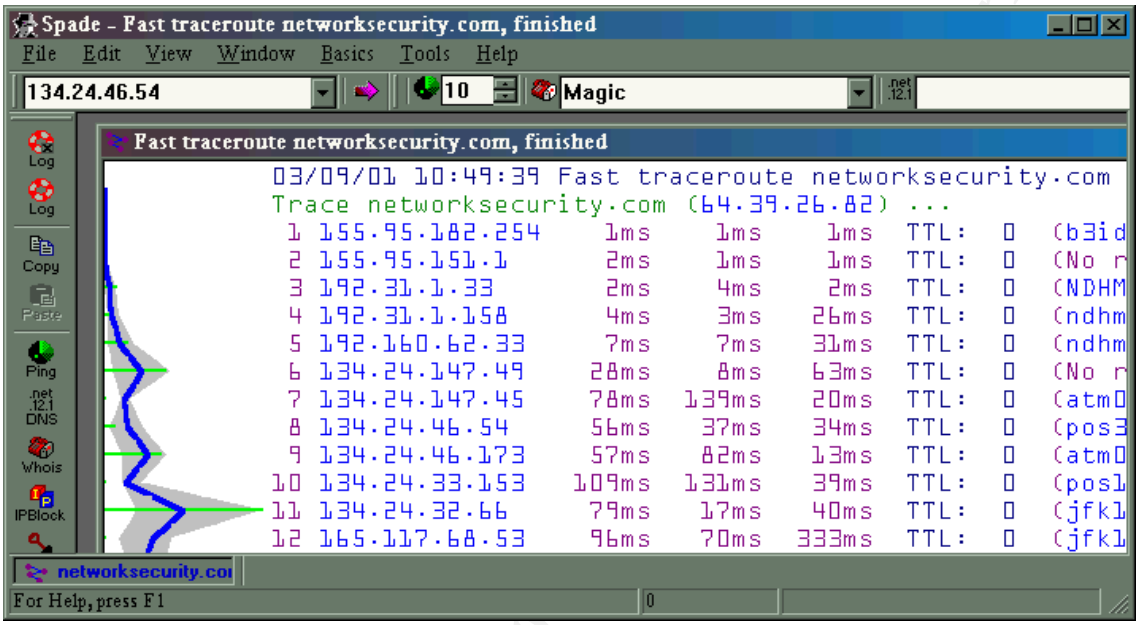


Fast Traceroute (Trace)

A fast traceroute finds the route packets taken between you and the selected address. Although traceroute is not infallible, some networks block ICMP packets at their boundaries making it impossible to run traceroute into their systems. Traceroute will send three packets for each hop of the route. Each packet that doesn't return is shown as an

© SANS Institute 2000 - 2005 Author retains full rights.

asterisk. If none of the three packets return from a stage they will be shown as * * * failed. If a single stage fails, but later stages return data, it means the one stage doesn't respond to traceroute packets. If traceroute returns data up to a stage, but all stages after that fails it usually means that the stage after the final one is a firewall blocking ICMP packets. This can be viewed as suspicious behavior. Below is a trace that would look similar to that of GIAC Enterprises Corp.



Our final step in checking the firewall is to do a port scan on the firewall and border router, for that matter, to see what ports are detected. There are no services on the router or firewall. The following is a list of firewall and router filters.

- Web Server (Public) port 80 TCP
- Fortune Server (Private) port 443 TCP
- SMTP Server (Mail) port 25 TCP
- Primary DNS Server port 53 UDP

If any of these digress from our Security Policy they will have to be handled accordingly. To maintain the firewall, it is important to test for any vulnerability that has not thus far been determined. We have decided to use **Nessus Security Scanner**. Nessus Security Scanner is software that will audit a given network and determine whether attackers may break into it. Since Nessus is modular and easy to use, it is a great choice!
There are three steps to ensure that the scanning can be performed.

Below is a Sample Scan:

1. Install Nessus

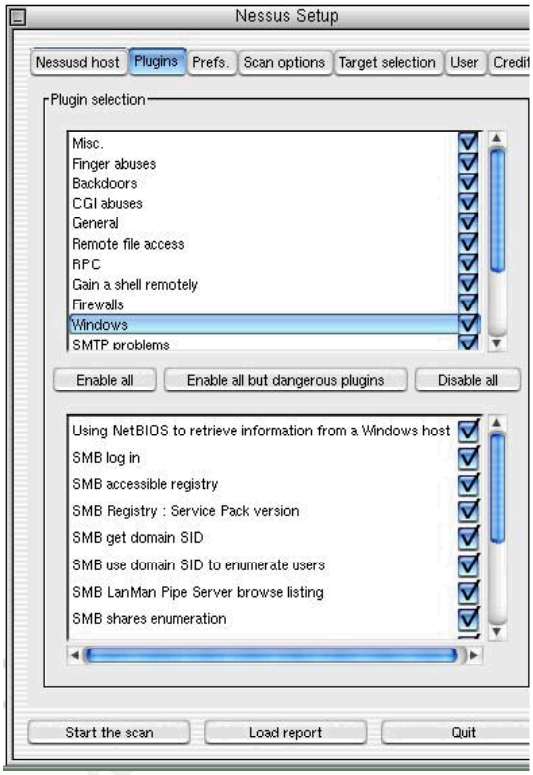
Download and install nessusd and nessus. Create a user account, configure your nessus deamon, and then fire-up nessus.

© SANS Institute 2000 - 2005 Author retains full rights.

2. Configuring the Client

After configuring the root, the next step is in configuring the client. Essentially, we need to connect it to a simple user.

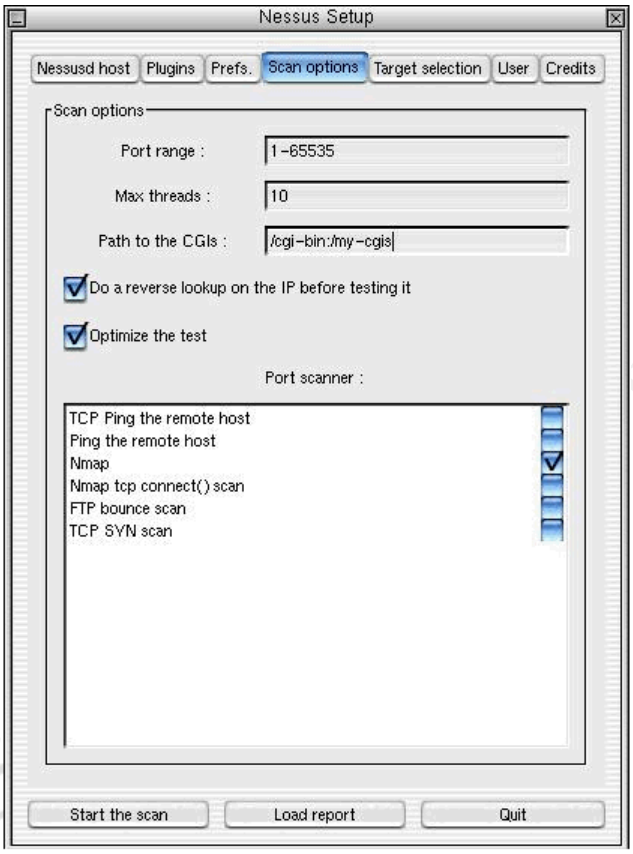
After firing up Nessus and connecting to the user by entering the Nessusd host, Port, and Encryption, we can then login.



As you can see here, we have decided all the security checks to be performed except the DoS attacks if you were to keep scrolling down. The reason that we have chosen not to perform the Denial of Service attacks is because some of the host computers may crash or fail. Obviously we do NOT want a host computer to fail during an audit. This could potentially cause problems for some employee or the enterprise as a whole.

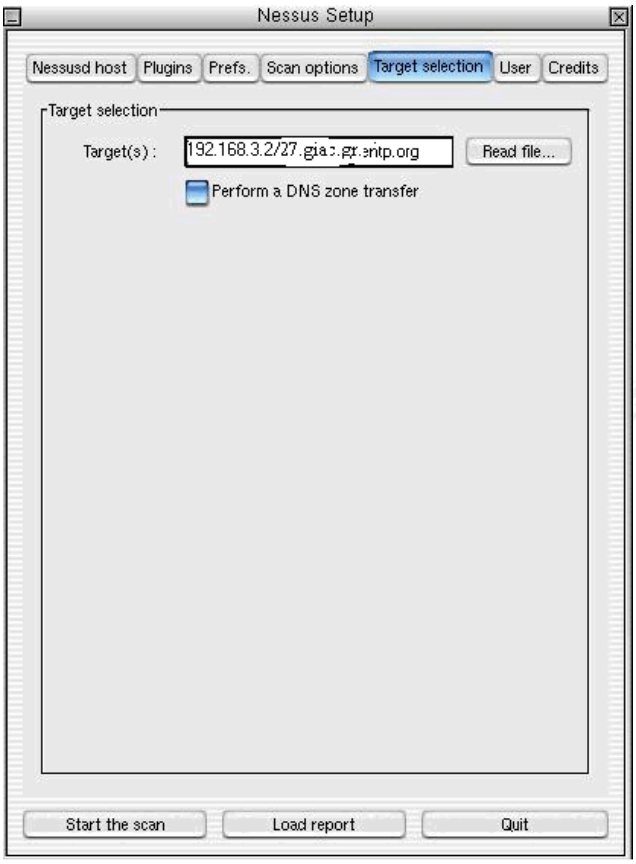
In the Scan Options section, we can decide to use whatever is appropriate. In this case, Nmap was chosen due to the fact that it is one of the quickest. Just a note that multiple options for testing is an option. Just check off how many san option you prefer.

© SANS Institute 2000 - 2005 Author retains full rights.



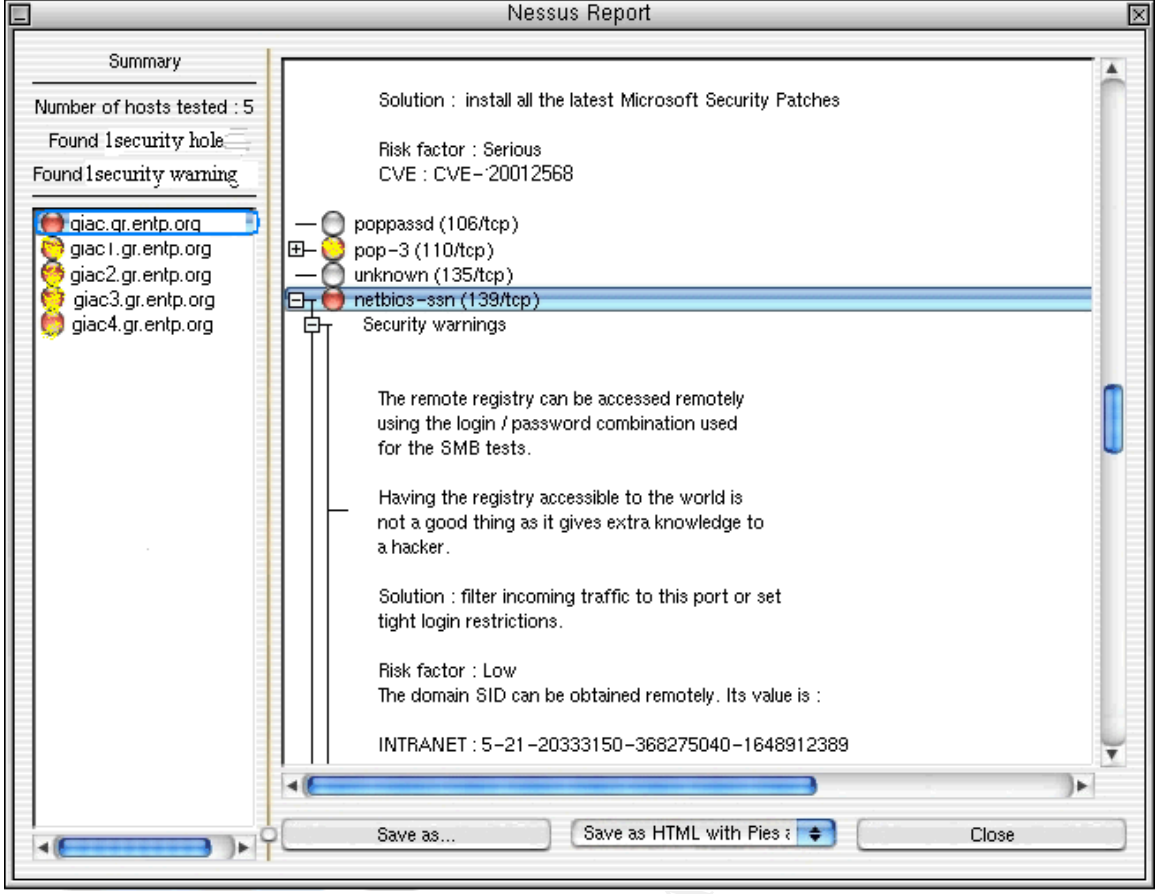
After we decide the port scanner, we then need to define the targets as shown below. Since our host addresses are using Private IP addresses we can enter that in as the target.

© SANS Institute 2000 - 2005 Author retains full rights.



If we wanted to restrict any rules, we would select the rule tab. In this particular case, we do not. Now we are ready to run the test.
The test results are shown below for GIAC enterprises. Here, we tested 5 different hosts and found only 1 security warning that we should be aware of as well as 1 security hole. This obviously is not the best thing and needs to be fixed to eliminate the security holes.

© SANS Institute 2000 - 2005 Author retains full rights.



The above report shows you the total security risks that we have on our 5 hosts as well as recommendations on how to fix the issue. The download is free so you may want to try it out. Generally, we use SARA, but because of the overwhelming interest in the community we have decided to use it here.

Not that we have checked the "outside", such as home users/partners and host computers, we now need to focus our efforts towards the inside. Many times we neglect certain areas like access to server/network rooms, passwords, etc.

Internal Arena

- Ensure that the access list to enter the network area/server area is restricted and up to date. If anyone has left the company, make sure that their access is cancelled, and ensures that the surveillance cameras are recording properly.
- Scan the internal address for any host vulnerabilities using tools like Nessus Security Scanner or SARA.
- Use Sam Spade to gather DNS information or any of the other functions that it performs.
- Perform a Ping on the internal corporate enclave to ensure that everything is recognized and that everything is connected, as it should be.

© SANS Institute 2000 - 2005

Author retains full rights.

3.4 Analysis/Recommendations

For the analysis of the audit, we need to compare our findings with the Security Policy to see where it complies or where it does not comply; in which case we need to correct the issue. For when our analysis doesn't comply with the Security Policy, an action needs to take place offering future recommendations.

General Recommendations:

- Ensure that anti-virus software (Norton) is update and accurate.
- Ensure that everyone needing passwords is using unique passwords of at least 8 characters long with a mix of numbers, letters, and characters. DO NOT use the default ones such as <passwd>
- Ensure that all security patches are up to date. It would also be a great idea to make sure that you are on all the security mailing lists. http://xforce.iss.net/maillists/index.php
- Ensure that encrypt data is sent across the network
  To audit the VPN: tcpdump –n host testhost and host firewall>output.log
  To audit SSL: tcpdump –n host testhost and host secure_web_server>output.log
- Design a test verifying that a remote network manager can securely manage the internal network.
- Design a test verifying that proper operation is underway after network element experiences a power failure.
- Perform a "Stress Test" on the firewall to determine its maximum traffic load.

Home Users/Partners

Analysis

With regards to our home users and partners, a good percentage of the home users replied with their results. From the results, it shows that Port 80 HTTP is open. By having this port open, it causes attackers to wonder how much information you are will to give away. Not a great idea! Also, Telnet port 23 is found to be open. This message implies that these particular machines have unsuspected telnet servers running within them. Most likely this is not the case and is caused by a firewall or proxy server that is filtering the access to the Internet. From the business partners, we didn't get the type of results that we were expecting. If their network isn't tight and secure, that makes out arena untaught and less secure. Most of our business partners are Pre-IPO companies like our own, but they have been around for only a few months. Their Security Policies still haven't been decided and security seems to be an issue.

Recommendations

Next time use an IP agent tool to ensure that the wrong IP address was not being checked. When you re-perform the test, you should notice that the telnet port 23 does not even exist at this IP address…. Stealth! We could also block inbound telnet on all machines receiving this warning. In general, we need to have the home users monitor these results on a weekly or monthly basis reporting their findings.

With regards to our business partners, we need to motivate them on the importance of a Security Policy and security in general. The need to ensure that their systems are not

© SANS Institute 2000 - 2005 Author retains full rights.

exploiting GIAC Enterprises in any bit. We will work with them now and in the future to protect our needs.

Maintaining the Firewall

Analysis/Recommendations

With regards to the firewall testing, there was 1 security hole:

- netbios-ssn (139/tcp) (Security hole found)

Vulnerability found on port netbios-ssn (139/tcp)

It was possible to log into the remote host using the following login/password combinations:
'guest'/''.
.It was possible to log into the remote host using a NULL session.
The concept of a NULL session is to provide a null username and a null password, which grants the user the 'guest' access.
The remote host defaults to guest when a user logs in using an invalid login. For instance, we could log in using the account 'nessus/nessus'

. All the smb tests will be done as 'guest'/''

Vulnerability found on port netbios-ssn (139/tcp)

The following shares can be accessed as guest:

- NETLOGON
- A
- C
- IAS1$
- src$

Solution: To restrict their access under Windows NT, open the explorer, do a right click on each, go to the 'sharing' tab, and click on 'permissions'
Risk factor : High
CVE : CAN-1999-0519

- Security Warning-Information found on port 25 TCP

Information found on port SMTP (25/tcp)

The remote STMP server seems to allow remote users to send mail anonymously by providing a too long argument to the HELO command (more than 1024 chars).

This problem may allow bad guys to send hate mail, or threatening mail using your server and keep their anonymity.

Risk factor: Low.

Solution: If you are using sendmail, upgrade to version 8.9.x. If you do not run sendmail, contact your vendor.
CVE : CAN-1999-0098

© SANS Institute 2000 - 2005, Author retains full rights.

The beautiful thing about Nessus is that it not only tells you your vulnerabilities, but it also provides an in-depth solution to the problem.

3.5 Perimeter Analysis

Based on the above audit, there are a few things that we would like to add to the existing network architecture.

- **Smart Cards** (http://www.scia.org) **Biometrics, and PKI**

By using a Smart Card, similar to credit card, the person with access must have the card at hand to have access to a particular machine. With Biometrics, things like Iris Scanners, Fingerprint Scanners, and even Body Scent Scanners, are making communications that much more secure. The ideas of Smart Cards and Biometrics go beyond the basics of having a username and password; something a hacker can easily crack. By having these technologies, it makes it that much more difficult for a hacker to exploit.
PKI (Public Key Infrastructure) is another good idea to use. PKI provides electronic authentication providing for a more secure environment.

- **Installation of Intrusion Detection Systems**

The reason we choose IDSs is because firewalls can't really detect if there is a hacker. The problem with firewalls is that they are only at the boundary to your network. Almost all financial losses due to hacking come from inside the network. A firewall a the perimeter of the network sees nothing going on inside; it only sees that traffic which passes between the internal network and the Internet.
Some reasons for adding IDS to you firewall are:

- Double-checks for firewalls that have been configured incorrectly.
- Catches attacks that firewall legitimately allow through (such as attacks against web servers).
- Catches insider hacking. (This is why we cannot trust ANYONE in the corporation)

To check out some available IDSs on the market, go to http://www.networkintrusion.co.uk

- **Warning Banner**

Add a warning banner stating that it would be unlawful to enter or attempt to enter without proper authorization. This would warn attackers that our network is secure and that it should not be tampered with.

- Ensure that Echo, Discard, Chargen, and Daytime services are disabled.
  no service tcp-small servers
  no service udp-small servers

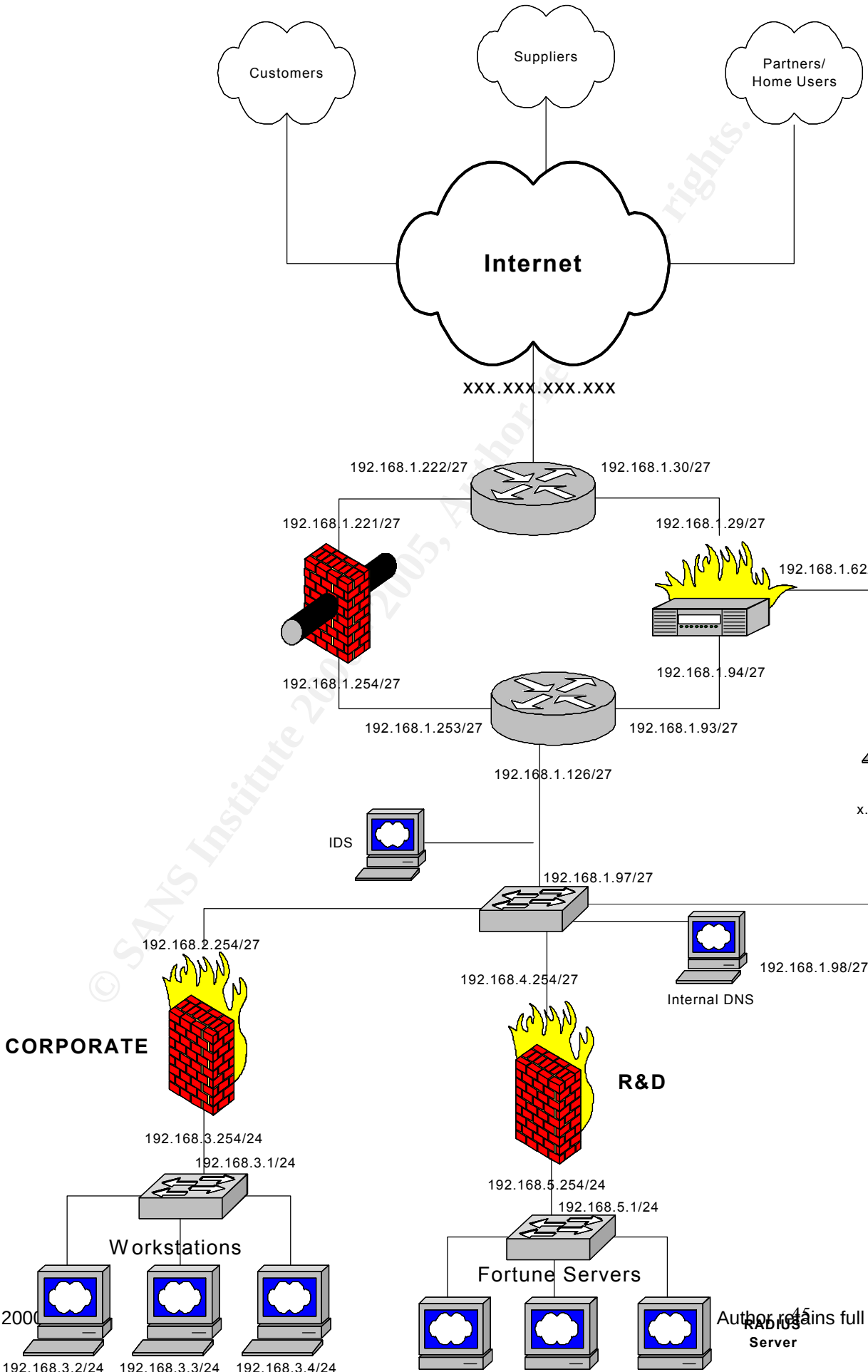
- Ensure that finger service is unavailable and also with regards to servers, ensure:
  no ip http
  no ip bootp

© SANS Institute 2000 - 2005 Author retains full rights.

As far as the rest of the network goes, we honestly believe that we designed a well secure network. We have defense in depth, the layering approach with multiple firewalls, and have used VPN tunneling and encryption for our servers.
Below is an example of recommendations for our current network architecture. We have decided to add 2 IDSs to log everything that goes through those different areas. The first IDS is placed off of 192.168.1.33 (Cisco switch). This allows us to log everything coming into the public area or E-business sector. The second IDS, and probably the most important, is between the secondary router and switch into the Internal Private enclave. Since out Fortune Servers are located here, it is extremely important to see the type of traffic coming in this arena.

(See re-design below)

© SANS Institute 2000 - 2005, Author retains full rights.



© SANS Institute 2000 - 2005, Author retains full rights.

Assignment 4: Design Under Fire

4.1 Scope

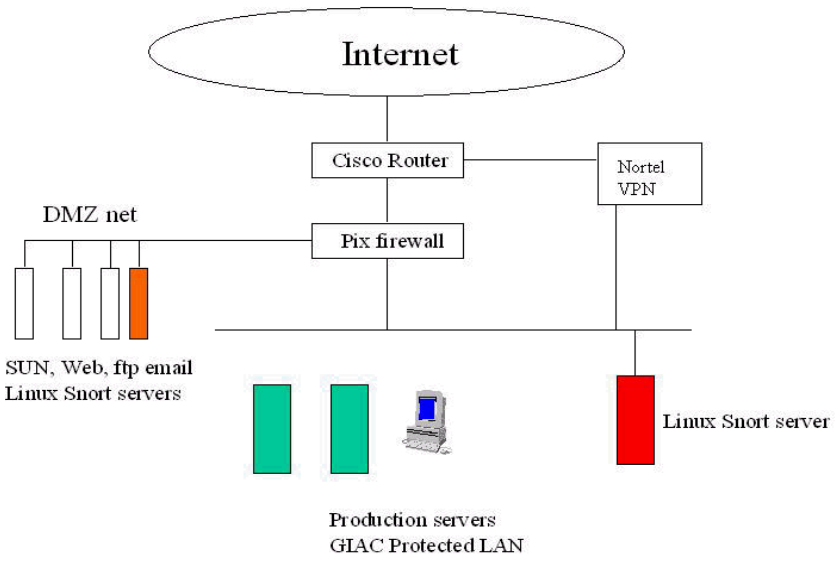
The purpose of this exercise is to help you think about threats to your network and therefore develop a more robust design. Keep in mind that the next certification group will be attacking your architecture!
Select a network design from any previously posted GCFW practical (http://www.sans.org/giactc/gcfw.htm) and paste the graphic into your submission. Be certain to list the URL of the practical you are using. Design the following three attacks against the architecture:

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

Note: *this is the second time this assignment has been used. The first time, a number of students came up with magical "hand-waving" attacks. You must supply documentation (preferably a URL) for any vulnerability you use in your attack, and the exploit code that you use to accomplish the attack. The purpose of this exercise is for the student to clearly demonstrate they understand that firewall and perimeter systems are not magic "silver bullets" immune to all attacks.*

© SANS Institute 2000 - 2005 Author retains full rights.

4.2 Selected Design



The URL is as follows: http://www.sans.org/y2k/practical/chap_wong_GCFW.doc

4.3 Attack against the Firewall

Cisco PIX Firewall SMTP Content Filtering Evasion Vulnerability (Bugtraq 1698)
http://www.securityfocus.com

(This was taken directly from Bugtraq)
"The Cisco PIX firewall reads the contents of packets for application level filtering. With SMTP however; it can be configured such that only certain SMTP commands can be allowed through. (i.e., dropping extra functionality, such as HELP or commands that could be a security concern, like EXPN or VRFY).
By tricking the firewall into thinking the body of the message is being sent when it isn't, the SMTP and the flaws in condition handling of the PIX, could evade the SMTP restrictions.
During communication with a SMTP server, if the "data" command is sent before the more important information is sent, such as "rcpt to", the SMTP server will return error 503, saying that rcpt was required. The firewall on the other hand thinks everything is

© SANS Institute 2000 - 2005 Author retains full rights.

alright and will let everything through until receiving "<CR><LF><CR><LF>. <CR><LF>"." It is then possible for the attacker to do whatever he wishes on the email server; which is obviously a HUGE problem.

Exploiting the bug

Sample Solution with our own twist:

Hello there
mail from: silvia@gd.it
data (From here pix disable fixup)
expn guest (Now I could enumerate user
verify oracle and have access to all commands
help
whatever command I want
quit

Solution

(This was taken directly from Bugtraq)
Cisco is offering free software upgrades. Customers with service contracts may upgrade to any software version. Customers without contracts may upgrade only within a single row of the table below, except that any available fixed software will be provided to any customer who can use it and for whom the standard fixed software is not yet available. As always, customers may install only the feature sets they have purchased.

Fixed Regular Release available
Version Affected now; fix will carry forward into
all later releases
All versions of Cisco Secure PIX up
to version 4.4(5) (including 2.7, |4.4(6)
3.0, 3.1, 4.0, 4.1)
Version 5.0.x up to and including
version 5.0(3) | 5.1(3)
All 5.1.x up to and including
version 5.1(2)* 5.1(3)
Version 5.2(1) 5.2(2)

*For customers who may have engineering releases addressing specific unrelated defects, designated as 5.1(2), version 5.1(3) only includes the SMTP security fixes and does not include any other bugfixes. Customers requiring engineering releases to address specific unrelated defects will need to use 5.1(2) 207 or higher, which also includes the SMTP security fixes.

© SANS Institute 2000 - 2005 Author retains full rights.

4.3.1 Yet another Vulnerability

Cisco PIX PASV Mode FTP Internal Address Disclosure Vulnerability (Bugtraq 1877)

Issue:
During configuration, the Cisco PIX firewall makes it viable to hide the IP address of internal FTP servers from clients connecting to it.
It is not exactly known what can actually cause this condition, but by sending a number of requests to enter passive FTP mode (PASV) during an FTP session, the IP address is eventually unveiled.

What Versions:
Versions 5.2(4) and 5.2(2) of the PIX firmware as well as other non-verified versions.

Exploit
Fabio Pietrosanti <naif@inet.it> performed this attack. It must be run numerous times on the victim's server before the internal IP address will be unveiled.


pixpasv.sh

Solution
Currently, there are no fixes for this bug. Check with Security Focus online for future details.

4.3.2 And Yet Another

Cisco Secure PIX Firewall Forged TCP RST Vulnerability Bugtraq (1454)
"A connection through a Cisco Secure PIX Firewall can be reset by a third party if the source and destination IP addresses and ports of the connection can be determined or inferred. This can be accomplished by sending a forged TCP Reset (RST) packet to the firewall, containing the same source and destination addresses and ports (in the TCP packet header) as the connection to be disrupted. The attacker would have to possess detailed knowledge of the connection table in the firewall (which is used to track outgoing connections and disallow any connections from the external network that were not initiated by an internal machine) or be able to otherwise determine the required IP address and port information to exploit this."

Exploit
The following exploit was written to compile under FreeBSD by Citec Network Securities.


pix_reset_state.c

© SANS Institute 2000 - 2005, Author retains full rights.

Solution
Cisco plans to release updated PIX software to deal with these issues. See the Cisco advisory on this issue for details.

4.4 Denial of Service Attack using SYN Floods

[8]A ``SYN flood'' is a Denial of Service attack that compromises the TCP ``three way handshake'' protocol. A SYN is packet sent to begin a connection with a listening TCP port. The port responds with a SYN/ACK to the initiating port and the places the SYN packet in a partial connection queue. When a corresponding ACK packet is received on the port that is listening, the authorized SYN packet is then removed from the partial connections area and an entry is placed in the established connection area awaiting a socket connection.

Basically any system connected to the Internet and providing TCP based services, such as an HTTP server, FTP server, or a SMTP server, will potentially undergo this attack. Not only are attacks launched at different hosts, but they can also be commenced against any router or other server system if these hosts activate other TCP services. This attack varies depending on what type of system you have. When there is a great number of SYN packets that all of a sudden start appearing on your network, there is probably a SYN Flood attack taking place if there are no equivalent reply packets.

An example that the SANS Institute deployed:
In this particular case, we are going to send a number of SYN packets to this network. To mask our identity, we are going to use IP Spoofing. What will happen here is that the person being attacked will receive the packet and send the packet back with SYN & ACK. Unfortunately, they will wait for some sort of reply but will NOT receive one due to the fact that the spoofed IP address of the attacker's machine is off-line.

Overall, this will keep occurring over and over again until the buffer reaches a maximum. The DoS attack will occur and ultimately cause system overload.

4.4.1 What can the victim do?

To protect against this particular attack, it is a good idea to have the proper filters on your router as well as having the appropriate firewall configuration.

Tools such as Netstat can also be used to check for any unusual traffic coming through. With netstat the user can look for these large numbers of half opened connections to try and detect the attack.

[8] Network World Fusion: http://www.nwfusion.com/columnists/2000/1120gearhead.html

© SANS Institute 2000 - 2005 Author retains full rights.

[9]The Neohapsis Archive also has been discussing, in a mail group, how to defeat a SYN flood attack. Some of the ideas include: FreeBSD versions 4.x or later as well as some kernel source files that will also prevent the attack.

4.5 Attack to Compromise Internal System through Perimeter System

Target: Linux Snort Server

To compromise the Linux Snort Server, we would have essentially 2 ways to compromise the system. We would either have to bypass the router and firewall or find a way to bypass the router and the VPN.

Bypassing the Router

There is a vulnerability in Cisco access lists allows some packets to be erroneously routed which one would expect to be filtered by the access list and vice-versa. This vulnerability can allow unauthorized traffic to pass through the gateway and can block authorized traffic.

If a Cisco router is configured to use extended IP access lists for traffic filtering on an MCI, SCI, cBus or cBusII interface, and the IP route cache is enabled, and the "established" keyword is used in the access list, then the access list can be improperly evaluated. This can permit packets which should be filtered and filter packets which should be permitted.

Bypassing the Firewall

To bypass the firewall, we need to find a vulnerability that exists on the PIX. We could use the Cisco PIX Firewall SMTP Content Filtering Evasion Vulnerability. This would allow us to access the mail servers. Although one may not think this is a big deal, we could start reading people's e-mails and find some confidential information such as passwords and other pertinent information. Once we could obtain the username and passwords, we would be home free. Another interesting ploy would be to have a fake identity and pretend you are an IT person who is requesting your password for an audit or for a password reset situation.

If the hacker has decided that bypassing the firewall is virtually impossible, he has 2 ways to crack through via the VPN.

Bypassing the VPN

- The first way would be discover the password of a home user, business supplier, or partner. We could try the basic, non-unique passwords or try finding that information or depending on their security system, crack into their machines. Obviously having the passwords would be the easiest method and would not require much thought.
- The second way, which seems the coolest and believe it or not the most likely way, would be to have a hat and clipboard. Basically what I am saying is that walk into the main branch of the Enterprise with a hat and clipboard, act nice and sweet, and get to

[9] Neohapsis Archives: http://archives.neohapsis.com/archives/freebsd/2000-11/0598.html

© SANS Institute 2000 - 2005 Author retains full rights.

a machine where you can install a Sniffer on the internal segment. This way, you can leave, and basically access all the juicy information from hacker's headquarters. This idea forces you to think about not only network security, but also physical security- something that can be overlooked.

References:

1 Skoudis, Edward. Computer and Network Hacker Exploits: Step-by-Step, Part 1 and 2. Washington: SANS Institute, July 5-10, 2000.

2 Spitzner, Lance. Firewall 101: Perimeter Protection with Firewalls. New Orleans: SANS Institute, January 28-February 2, 2001.

3 Spitzner, Lance. Advanced Perimeter Protection and Defense-In-Depth. New Orleans: SANS Institute, January 28-February 2, 2001.

4 Brenton, Chris. VPNs and Remote Access. New Orleans: SANS Institute, January 28-February 2, 2001.

5 Brenton, Chris. Network Design and Performance. New Orleans: SANS Institute, January 28-February 2, 2001.

6 Birkner, Matthew. CISCO Internetwork Design. Indianapolis: Cisco Press, 2000. Page 147.

7 SANS Institute http://www.sans.org
Chap Wong's FW: http://www.sans.org/y2k/practical/chap_wong_GCFW.doc

8 Nessus http://www.nessus.org

9 Sam Spade http://samspade.org/ssw

10 Altiga http://www.altiga.com

11 Cisco http://www.cisco.com

12 Cisco 3600 Series Routers http://www.cisco.com/warp/public/cc/pd/rt/3600/
Cisco 2900 Family Switches http://www.cisco.com/warp/public/cc/pd/si/casi/ca2900/
Cisco Secure PIX Firewall Series http://www.cisco.com/univercd/cc/td/doc/pcat/fw.htm

13 Shields UP! https://grc.com/x/ne.dll?bh0bkyd2

14 PentaSafe Security http://www.pentasafe.com/

15 Security Focus/bugtraq http://www.securityfocus.com/

16 Talisker's Network Security Tools http://www.networkintrusion.co.uk

17 Netscape's SSL page http://home.netscape.com/security/techbriefs/ssl.html?cp=sciln

18 CERT/CC Advisories CA-2001-02: Multiple Vulnerabilities in Bind
http://www.cert.org/advisories/

19 Internet Security Systems: Mailing Lists http://xforce.iss.net/maillists/index.php

20 Gibbs, Mark. "After the SYN Flood" Network World Fusion. 11/20/2000
http://www.nwfusion.com/columnists/2000/1120gearhead.html

21 Anderson, Dave "Defeating SYN Flood Attacks" Neohapsis Archives. 12/01/2000

© SANS Institute 2000 - 2005 Author retains full rights.

http://archives.neohapsis.com/archives/freebsd/2000-11/0598.html

© SANS Institute 2000 - 2005, Author retains full rights.