Global Information Assurance Certification Paper

LevelTwo Firewalls, Perimeter Protection, and VPNs
GCFW Practical Assignment

New Orleans, LA

January 28 – February 2, 2001

Submitted By: Kenneth Patrick

Assignment 1 - Security Architecture (25 Points)

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

You must consider and define access for:

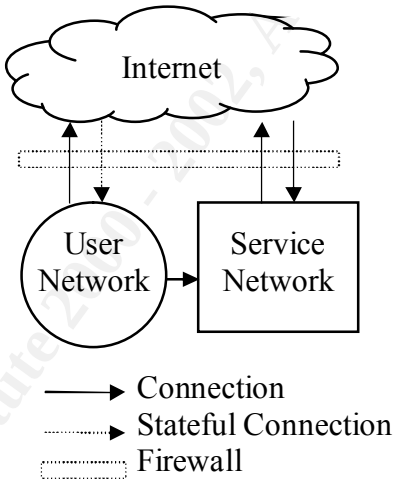
- Customers (the companies that purchase bulk online fortunes);
- Suppliers (the authors of fortune cookie sayings that connect to supply fortunes);
- Partners (the international partners that translate and resell fortunes).

1.0 Assignment 1 - Proposed Solution

1.1 Introduction

The primary goal of this assignment is to define a security architecture for a sizable Internet company, GIAC Enterprises. GIAC Enterprise's livelihood is solely based on Internet sales/transactions of fortune cookie sayings. GIAC must provide a sound and secure means to interact with customers, suppliers and partners via the Internet using services such as Web, FTP, SMTP and VPN access. Different services have different vulnerabilities. The same is true for router/firewall brands, operating systems and applications. Mix these all together and the design of the security architecture can become quite complicated. The required services and access restrictions are normally dictated by the primary functions of the business and how business will be conducted.

It is helpful to determine core access to resources. For example, users of the internal network can usually access the Internet and Service Network. Outside users can usually access resources on the service network to conduct business. The security architecture must be designed around this principle. This is depicted in the diagram below.



1.2 GIAC Questions

Before designing a secure network, it is beneficial to determine what functions are required in order to maintain an Internet company of this type. Several questions must be answered prior to laying out a design. These questions will help identify the details that have the most affect on security design. These details are listed below.

- Type of networking hardware
- Type of required services
- Operating systems
- Server based applications
- Access requirements/restrictions

Required services and access requirements will be addressed in the questions below.

1.2.1 What is the product of GIAC Enterprises?

The product has been identified as fortune cookie sayings. A simple product, no re warehouse is required for this type of product. This type of product can be viewed and sold directly over the Internet. At a minimum, the following services and access requirements are necessary:

- Web servers to display products
  Users must have access to ports 80/443 on Web servers

- Database servers for product storage
  Web server database connectors must have connections to Database servers

1.2.2 Who are GIAC Enterprises clients/customers?

This will help identify the type of services that should be visible from the Internet and the type of user authentication required in order to access those services.

1.2.2.1 Customers

It has been identified that customers are companies that purchase bulk online fortunes. There must be a means to allow these companies to communicate, view products (in this case fortunes) and to make purchases. In order for companies to make purchases, access should be limited to companies that have special accounts. However, any customer should have access to GIAC's main web site or be able to request an account from the web site.

1.2.2.2 Suppliers

Suppliers, authors of fortune cookie saying, must me able to connect to GIAC and upload fortune cookie sayings. Suppliers must be able to authenticate via special login and send fortunes to a special area prior to posting products for sell. This process must be tracked in order to keep up with who uploaded what.

1.2.2.3 Partners

Partners must be able to connect to GIAC via VPN to download products and communicate with GIAC. This will ensure that data is encrypted and kept private. Partners must have a special account and transactions must be tracked.

At a minimum the following services and access requirements are required:

- Web server/s to interact with customers/suppliers/partners
  Users must have access to ports 80/443 on Web servers

- FTP server/s for data transfer for suppliers/partners
  Users must have access to ports 20/21 on FTP servers

- Email Server/s to provide communication with customers/suppliers/partners
  Users must have access to ports 25/110 on Email servers

- Database server/s for transactions and storage of information
- VPN access to provide secure encrypted connections to suppliers/partners

1.2.3 What is GIAC Enterprises size/expected growth?

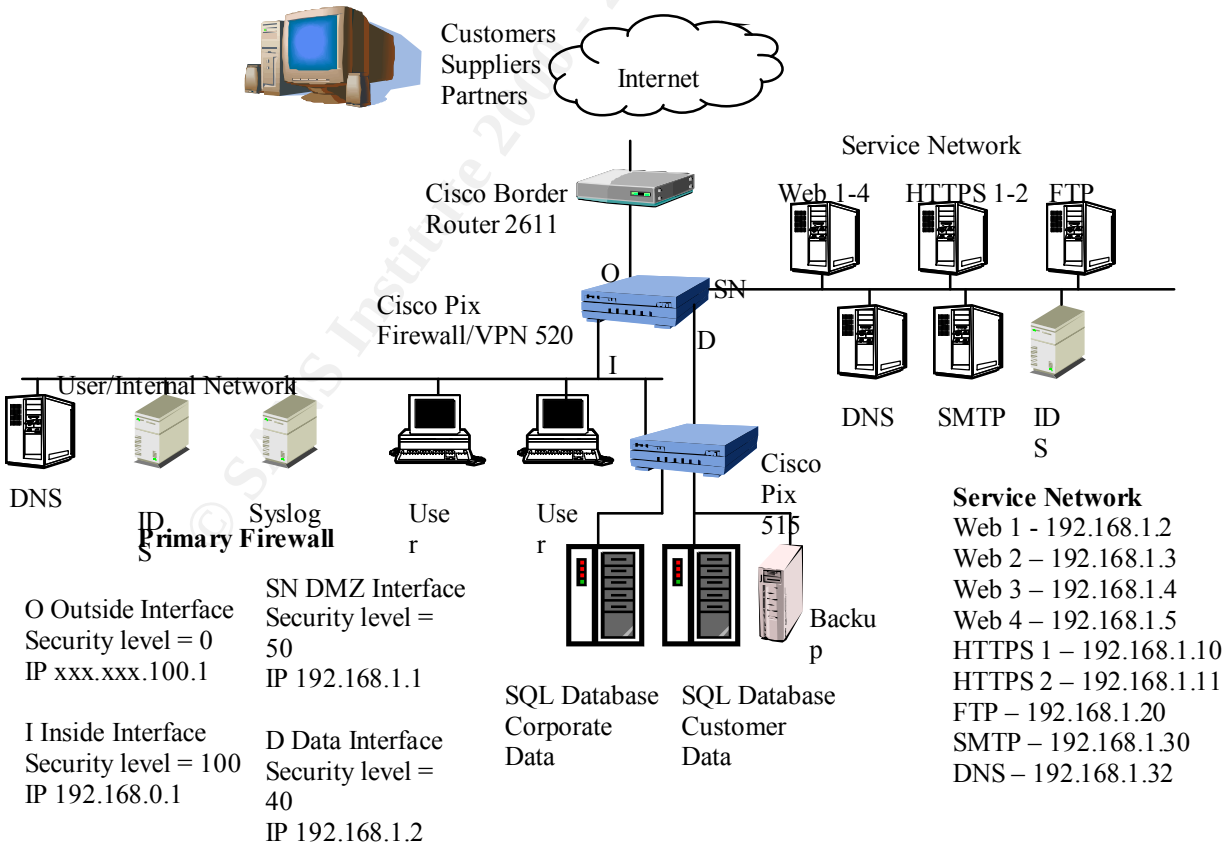
In order to determine the network requirements, the expected growth of the company must be estimated. It has been determined that GIAC expects to earn $200 million per year from online sales. This gives an idea of expected Internet traffic, customer/supplier base, database requirements, equipment requirements and staffing. Answers to this question will help identify the type of routers and firewalls to consider.

1.2.4 What is GIAC's security policy for internal users?

Above and beyond business related services, what other services does GIAC management want to allow for internal network users? The policy should ensure that internal users can only perform functions that they are allowed or authorized to do. For GIAC Enterprises, internal users should be able to access the Internet and services on the service network. Answers to this question will impact the security and architectural design of the network.

1.3 Architecture Diagram

Once all above questions have been clearly answered, the network diagram can be produced.



1.4 Description of Equipment

1.4.1 Border Router – Cisco 2611, IOS version 12.1

Specifications:
Supports up to 64 ISDN B channels
Up to 6 module slots for growth
40 MHz RISC Processor/64 MB Ram

As depicted in the diagram, the Cisco 2611 Router is used for the border router. The border router provides the first line of defense for the GIAC network. Its serial interface is directly connected to the Internet Service Provider (ISP). The router is used as a filter to allow most services and deny unused services or known security risks. The Ethernet interface is directly connect the outside interface of the primary firewall.

1.4.2 Primary Firewall/VPN – Cisco Pix 520, software version 5.3(1)

Specifications:
Supports 250,000 simultaneous connections
370 megabits per second (Mbps) throughput.
350 MHz CPU / 128 MB Ram
Up to 6 Ethernet interfaces for growth
Supports NAT natively
Integrated VPN
Integrated IDS

The primary firewall works in conjunction with the border router to further augment security. The firewall will block all inbound traffic by default. Special access and services must be allowed through the firewall. The firewall is configured with 4 interfaces. The outside interface is directly connected to the border router's Ethernet interface. All inbound Internet traffic must pass through this interface. The inside interface is connected to the internal network and the DMZ interface connects to all public access servers on the service network. The data interface is connected to the internal firewall that secures the data. By breaking up a network in this fashion ensures that if one subnet becomes compromised, other subnets will remain protected. This is accomplished by setting security levels and access lists on each interface of the firewall.

The primary firewall also supports VPN and remote access. These features are integrated into the firewall and can be configured to suit encryption and access needs. Network Address Translation (NAT) is also supported and configured on the firewall. NAT assigns all nodes interior to the firewall IP addresses that are hidden from the outside world. The firewall does all of the IP management and processing.

1.4.3 Internal Firewall – Cisco 515, software version 5.3(1)

Specifications:
170 megabits per second (Mbps) throughput.
200 MHz CPU
Supports 170,000 simultaneous connections
Up to 6 Ethernet interfaces for growth

Supports NAT natively

The internal firewall is used to provide additional protection to the data. If the rest of the network is compromised, the data will still remain protected. The internal firewall also implements NAT.

1.4.4 Services and Software

The following server based applications are used on the GIAC network.
Web Services – Microsoft IIS
Email – Microsoft Exchange
Database – Microsoft SQL
DNS – Microsoft Implementation

Assignment 2 - Security Policy (25 Points)

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

- Border Router
- Primary Firewall
- VPN

You may also wish to include one or more internal firewalls used to implement defense in depth or to separate business functions.
By 'security policy' we mean the specific ACLs, firewall ruleset, IPSec policy, etc. (as appropriate) for the specific component used in your architecture. For each component, be sure to consider internal business operations, customers, suppliers and partners. Keep in mind you are an E-Business with customers, suppliers, and partners - you MAY NOT simply block everything!
(Special note VPNs: since IPSec VPNs are still a bit flaky when it comes to implementation, that component will be graded more loosely than the border router and primary firewall. However, be sure to define whether split-horizon is implemented, key exchange parameters, the choice of AH or ESP and why. PPP-based VPNs are also fully acceptable as long as they are well defined.)
For each security policy, write a tutorial on how to implement each ACL, rule, or policy measure on your specific component. Please use screen shots, network traffic traces, firewall log information, and/or URLs to find further information as appropriate. Be certain to include the following:

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

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

2.0 Assignment 2 - Proposed Solution

2.1 Introduction - Border Router Configuration

The router should provide protection from the most basic type of attacks. Access Control Lists (ACL) are applied to the router interfaces and used to permit or deny packets based on matching criteria. ACLs work on a first match basis. Once a match is made, the packet is either denied or permitted. ACLs are stored in a configuration file on the router. ACLs can be manually typed in from the router command line while connected to the router in enable mode. There are several ways to connect to a router. Some of the most common are using the telnet command to establish a connection or connecting a laptop/PC directly into the console port of the router using a special cable. Documentation on Cisco router configuration fundamentals can be found at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun_c/index.htm

2.1.1 Standard and Extended Access Lists

There are two types of access lists: Standard and Extended. Standard access lists only filters traffic based on the packets source IP address. Extended access lists are more powerful and can filter by source/destination IP address, protocol and port. The basic syntax for each access type is listed below.

2.1.1.1 Standard Access Lists

Access-list <1-99> <permit/deny><ip address/any> or host< ip address><netmask>

The standard access list must be assigned a number for the range of 1-99 so that all access rules can be placed in the same grouping. The next portion indicates what to do with the packet if it matches the source IP or IP range, permit or deny it. The last portion can indicate a single IP address, range of IP addresses or all hosts as the matching source IP address.

2.1.1.2 Extended Access Lists

Access-list <100-199><deny/permit><protocol type><Source ip address/any><netmask><Destination ip address/any>><netmask>

Access-list <100-199><deny/permit><protocol type>host<ip address><eq/lt><port number>

These are two of the most popular uses of extended access lists. There are many different variations. The examples above are similar to the ones used within this assignment. Extended access lists are similar to standard access lists except packets can also be filtered by protocol type, destination address and port.

2.2 Border Router Configuration

Typically, the border router is the first line of defense against outside attacks of a network. The router's primary functions are to provide routing and to deny or permit access based on a set of predefined rules. The first two sets of rules to apply are ingress

and egress filtering. This will prevent spoofed IP packets from entering or leaving the GIAC internal network.

2.2.1 Ingress filtering

Ingress filtering is used to prevent packets from the Internet that contain source IPs addresses from reserved networks from entering the GIAC network. An Ingress ACL should be applied to the inbound serial interface of the border router as listed below. This will prevent packets containing spoofed source IPs addresses from entering the GIAC network.

2.2.1.1 Ingress ACL

Using the ACL listed below, source IPs addresses from known reserved networks (192.168.0.0, 172.16.0.0, 10.0.0.0), multicast addresses, loop-back addresses and the GIAC internal network are denied access to the network. This ACL is applied to the inbound serial interface of the router. Once an access list is created and applied to an interface, the packet must match at least one of the rules in the access list. There is an implied deny at the end of every ACL. If the packet does not match any rule, it will automatically be denied. Notice that the last rule permits all traffic. This rule is required because the implied deny will not allow any traffic into the GIAC network.

Interface serial0
Access-list 111 deny ip 192.168.0.0 0.0.255.255 any echo log
Access-list 111 deny ip 172.16.0.0 0.15.255.255 any echo log
Access-list 111 deny ip 10.0.0.0 0.255.255.255 any echo log
Access-list 111 deny ip 224.0.0.0 31.255.255.255 any echo log
Access-list 111 deny ip 127.0.0.0 0.255.255.255 any echo log
Access-list 111 permit ip any any
IP access-group 111 in

2.2.2 Egress filtering

Egress filtering ensures that all outbound traffic, traffic leaving the GIAC internal network, have source IPs addresses from the GIAC internal network. An Egress ACL should be applied to the inbound Ethernet interface of the border router as listed below. This will prevent the GIAC network from becoming a target and sending spoofed packets.

2.2.2.1 Egress ACL

Using the ACL listed below, source IPs addresses from GIAC's internal network are permitted to leave the internal network (192.168.1.0 and 10.0.0.0). As stated above, there is an implied deny at the end of every ACL. However, this ACL has listed it's own deny statement in order to log suspicious packets. This ACL will only permit traffic from the GIAC network to leave the network. All other traffic will be denied.

Interface Ethernet0
Ip access-group 12 in
Access-list 12 permit 192.168.1.0 0.0.0.255

Access-list 12 permit 10.0.0.0 0.0.0.255
Access-list 12 deny any any echo log

2.2.3 NETBIOS

NETBIOS, primarily utilized by Microsoft networks, allows users to provide shared file access. NETBIOS shares create a number of vulnerabilities and access should be limited to the internal network. An ACL for inbound traffic should be applied to the outside interface to deny access and log any attempts. The log command logs information to a predefined syslog server when a packet matches the ACL rule.

2.2.3.1 NetBIOS ACL

Access-list 111 deny tcp any any eq 135 echo log
Access-list 111 deny udp any any eq *135 echo log*
Access-list 111 deny udp any any eq 137 echo log
Access-list 111 deny udp any any eq 138 echo log
Access-list 111 deny tcp any any eq 139 echo log
Access-list 111 deny tcp any any eq 445 echo log
Access-list 111 deny udp any any eq 445 echo log

2.2.4 ICMP

ICMP based packets should be blocked at the inbound border router level. This will prevent Denial of Service (DOS) related attacks that force systems to become non-responsive to legitimate client requests.

2.2.4.1 ICMP ACL

Access-list 111 deny icmp any any echo log
This ACL denies all ICMP traffic to all destinations.

2.2.5 Complete ACL for Border Router

When creating an ACL that is applied to an interface, it is important to place each rule in the proper sequence. The ACL is applied to each packet starting with the first rule in the ACL. When a rule condition is met, the packet is either permitted or denied based on the ACL type. If a rule is not in the proper sequence, a packet could inadvertently be permitted when it should be denied or vice versa.

Interface serial0
Access-list 111 deny ip 192.168.0.0 0.0.255.255 any echo log
Access-list 111 deny ip 172.16.0.0 0.15.255.255 any echo log
Access-list 111 deny ip 10.0.0.0 0.255.255.255 any echo log
Access-list 111 deny ip 224.0.0.0 31.255.255.255 any echo log
Access-list 111 deny ip 127.0.0.0 0.255.255.255 any echo log
Access-list 111 deny tcp any any eq 135 echo log
Access-list 111 deny udp any any eq 135 echo log
Access-list 111 deny udp any any eq 137 echo log
Access-list 111 deny udp any any eq 138 echo log
Access-list 111 deny tcp any any eq 139 echo log
Access-list 111 deny tcp any any eq 445 echo log

Access-list 111 deny udp any any eq 445 echo log
Access-list 111 deny icmp any any echo log
Access-list 111 permit ip any any
<implied deny>
IP access-group 111 in

Interface Ethernet0
Access-list 12 permit 192.168.1.0 0.0.0.255
Access-list 12 permit 10.0.0.0 0.0.0.255
Access-list 12 deny any any echo log
Ip access-group 12 in

2.3 Firewall Configuration

2.3.1 Introduction/Pre configuration

One of the first steps in setting up a new firewall is to power on the unit and update the software to the latest version. It is always best to do this before the firewall is configured and placed into action. Usually the software must be downloaded from the manufacture web site. This should always be done. This ensures that any known vulnerabilities and software bugs have been resolved. It is assumed that the first time basic firewall settings such as installing the software, setting up default routing, IP assignment are already completed and will not be discussed in detail unless it pertains to the security architecture.

Firewall configuration is very similar to configuring a router as mentioned above. Command statements are typed in at the firewall command prompt while in enable mode. As with router ACLs, the sequence of a firewall rule set is also important. Documentation on Cisco PIX firewall configuration for software version 5.3(1) can be found at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v53/config/index.htm

2.3.1.1 Interface IDs/Security Levels

It is helpful to assign an ID name to each interface of the firewall. This will aid in configuration and troubleshooting problems during installation and long after the firewall has been in place. Typically the outside interface, the interface attached to the border router is labeled "outside" and the interface attached to the internal network is labeled "inside". If there are additional interfaces on the firewall, they can be labeled according to function. For instance the service networks can be labeled "DMZ","DMZ2", etc. Also when assigning IDs to interfaces, a security level can also be set. Each interface, along with an ID name, should have a security level setting. Assigning security levels allows the firewall to determine if traffic from one interface can access services or initiate connections on another interface. The security level can be set within the range of 0-100, with 100 being the most secure. The outside interface is always set to the least secure level of 0 and the inside interface is always set to 100.

For the GIAC exterior firewall, the ID names and security level configurations listed below will be set. In order for a client on a lower security level to access services on a higher security level, static addresses and access lists must be setup and applied. For

example, for Internet clients to access a web server located on the DMZ interface (the service network), the web server must have a static IP address assigned and specific access must be given to permit access to that IP address. For interfaces with a higher security level (i.e. clients from the internal network) to access services on an interface with a lower security level (i.e. service network), NAT must be configured and a global IP address must be assigned.

Setup name ID and security level
Nameif ethernet0 outside security0
Nameif ethernet1 inside security100
Nameif ethernet2 dmz security50
Nameif ethernet3 data security40

The above settings set the ID name and security level for each interface. For instance, Ethernet0 on the firewall is labeled outside and the security level is set to 0.

2.3.2 Setup NAT and Global settings

A NAT statement is used when clients from a higher level interface wish to access resources or connect to an interface with a lower security level. For instance, clients from the internal network wish to access servers in the service network. This is not setup by default. Access must be given by the firewall rule set. The global statement is used to automatically assign valid IP addresses for each connection made to the specified interface. It translates connections from a higher level interface to a lower level interface so users of the higher interface can access the services of a lower interface.

2.3.2.1 NAT/Global Rule set

Nat(inside) 1 0 0
Global (outside) 1 xxx.xxx.xxx.100-xxx.xxx.xxx.200 netmask 255.255.255.0
Global (dmz) 1 192.168.1.40-192.168.1.240 netmask 255.255.255.0

This ACL allows all clients on the inside interface to access interfaces with lower security levels. For instance, all internal users can now access the Internet and servers on the service network. Note that servers in the service network cannot access the user network. The first global statement assigns routable IP addresses from the listed range for all connections made to the Internet. For example, all nodes from the user network that establish a connection to the Internet, must receive an IP address from this range. The second global statement assigns IP addresses from the listed range for all connections made to the service network from the user network.

2.3.3 Static and Access Lists

By default the firewall will deny all attempted access from outside hosts to the GIAC network. In order for the firewall to permit outside hosts to access servers in the service network, a routable static IP address must be assigned to each server in the service network and special access must be permitted using access lists.

2.3.3.1 Static/Access Lists Rule Set

The rule set below assigns a routable static IP address to all servers on the service network and permits access through the firewall for the appropriate service. From the example below, the web servers are assigned static IP addresses of xxx.xxx.100.102 through xxx.xxx.100.105. This is the IP address the host from the Internet will use to access this server. The associated access list allows any host from the Internet to only access web services. No other service can be accessed from the Internet unless permitted via an ACL. The same rules are shown for each server/service within the service network. These include HTTPS, FTP, SMTP and DNS. The last rule applies all of these access lists to inbound traffic on the outside interface.

Rule set for HTTP/Web
Static (dmz,outside) xxx.xxx.100.102 192.168.1.2 netmask 255.255.255.255
Static (dmz,outside) xxx.xxx.100.103 192.168.1.3 netmask 255.255.255.255
Static (dmz,outside) xxx.xxx.100.104 192.168.1.4 netmask 255.255.255.255
Static (dmz,outside) xxx.xxx.100.105 192.168.1.5 netmask 255.255.255.255

Access-list acl_out permit tcp any host xxx.xxx.100.102 eq www
Access-list acl_out permit tcp any host xxx.xxx.100.103 eq www
Access-list acl_out permit tcp any host xxx.xxx.100.104 eq www
Access-list acl_out permit tcp any host xxx.xxx.100.104 eq www

Rule set for HTTPS/Web
Static (dmz,outside) xxx.xxx.100.110 192.168.1.10 netmask 255.255.255.255
Static (dmz,outside) xxx.xxx.100.111 192.168.1.11 netmask 255.255.255.255

Access-list acl_out permit tcp any host xxx.xxx.100.110 eq 443
Access-list acl_out permit tcp any host xxx.xxx.100.111 eq 443

Rule set for FTP
Static (dmz,outside) xxx.xxx.100.120 192.168.1.20 netmask 255.255.255.255
Static (dmz,outside) xxx.xxx.100.121 192.168.1.21 netmask 255.255.255.255

Access-list acl_out permit tcp any host xxx.100.100.120 eq ftp
Access-list acl_out permit tcp any host xxx.100.100.121 eq ftp

Rule set for SMTP
Static (dmz,outside) xxx.xxx.100.130 192.168.1.30 netmask 255.255.255.255
Access-list acl_out permit tcp any host xxx.xxx.100.120 eq smtp

Rule set for DNS
Static (dmz,outside) xxx.xxx.100.132 192.168.1.32 netmask 255.255.255.255
Access-list acl_out permit tcp any host xxx.100.100.120 eq dns

Access-group acl_in in interface outside
Apply rule set to inbound traffic of the outside interface

2.3.4 ActiveX and Java Applets

ActiveX and Java Apples can be potential vulnerabilities to a network. Malicious code can attack hosts or servers within a network causing them to fail or open additional security risks. Both can be filtered out from the firewall. ActiveX and Java applets are referenced from within web/html documents by using the html <object> tag. When the rule set is applied, the firewall will filter and comment out the html code of the <object> tag, causing the code to be skipped and not executed.

2.3.4.1 ActiveX/Java Applets Rule Set

Apply this rule to port 80 for all hosts

Filter activex 80 0 0 0 0
Filter java 80 0 0 0 0

2.3.5 VPN

A VPN is used to interact with Partners and Suppliers. Data from Partners and Suppliers should be IPSEC encrypted. When Partners and Suppliers establish connections to the GIAC network, data is encrypted using Encapsulating Security Payload (ESP). ESP was selected because of its wide use and straightforward configuration. In addition, ESP offers more security features that AH (Authentication Header). Below is the configuration that will be implemented on the primary firewall. Internet Key Exchange (IKE) is used to exchange security associations between VPN partners. IKE protocol uses ISAKMP and Oakey to exchange the authentication and encryption algorithms and sets the duration that the algorithm will be used.

2.3.5.1 VPN Rule Set

Access-list 101 permit <Partners fw ip> <mask> xxx.x.100.100 255.255.255.0
Access-list 101 permit <Suppliers fw ip> <mask> xxx.x.100.100 255.255.255.0
An access list must be created to indicate which traffic will be encrypted. In this case traffic for partners and suppliers will be encrypted.

Crypto ipsec transform-set Partners_set esp-des esp-sha-hmac
Crypto ipsec transform-set Suppliers_set esp-des esp-sha-hmac
Define a transform set which indicates the type of encryption and authentication to utilize. In this case two transform sets are configured with ESP and DES.

Crypto map GIAC_map 10 ipsec-isakmp
Create a crypto map to assign a map number, in this case 10. This is used to indicate sequencing in case multiple maps are used.

Crypto map GIAC_map 10 match address 101
Assign an access list the cryto map.

Crypto map GIAC_map 10 set peer <Partners fw ip>
Crypto map GIAC_map 10 set peer <Suppliers fw ip>

List the IP addresses of the VPN partners which VPN traffic can be sent to, in this case Partners and Suppliers.

Crypto map GIAC_map 10 set transform-set Partners_set Suppliers_set
List the transform sets that will be accepted for this entry. Map sets for Partners and Suppliers created above will be accepted.

Crypto map GIAC_map interface outside
Sysopt connection permit-ipsec
Apply the map to the outside interface and specify that IPSEC traffic will be permitted.

2.3.6 Logging

Logging is an important part of network security. A syslog server is able to log certain messages that the firewall designates to be possible risks. Logging must be enabled on the firewall and identify a log server by an IP address. There are certain levels of logging. Initially, all possible messages will be sent to the syslog server. The rules for this configuration are set below.

2.3.6.1 Logging Rule Set

Logging on
Logging host <ip of log server>
Logging trap 7

2.3.7 IDS

The firewall does not protect against attacks that originate from the inside. If a vulnerability is discovered that allows an attacker past the firewall, an IDS system is the next level of defense. GIAC has placed two IDS systems, one in the service network and the other in the user network. A properly monitored IDS system will give advanced notice of suspicious activity within the GIAC network.

2.3.8 Disabling Services

It is important to disable services on all systems that are not required. For example, FTP services on web servers should be disabled if it is not used. The same is true for all services. Many applications and operating systems install and enable services by default without any indication of their existence. These services may pose hidden vulnerabilities if their existence is not known.

2.4 ACL/Rule Set Testing and Tips

After all ACLs, rule sets and filters have been created and applied to interfaces, the first step is to view the configuration of each device to ensure that all rules have been entered correctly. The configuration can be viewed by using the following command statements: *show interface*, *show access-list, show access-group* and *show configuration*. Rules can have errors even though they have the correct syntax and are accepted by the system. For instance, an IP address or netmask can be mistyped which could counteract the purpose of the entire ACL. It is best to print the configuration of each device and step through each rule one at a time.

Once the rules are checked for grammatical and syntax errors, the next step is to verify that the rules are in the correct order. Rules that are out of sequence can permit packets that were intended to be denied or deny packets that were intended to be permitted.

The next step is to verify that each ACL or rule set is applied to the correct interface and bound in the right direction. When dealing with multiple ACLs or rule sets, it is easy to become confused and apply ACLs or rule sets to the wrong interface or direction. Once all ACLs and rule sets have been confirmed, the first method of testing an ACL or rule set is to step through each rule with an imaginary packet. Compose imaginary packets that should be accepted on the GIAC network. Test these packets against the ACL or rule set line by line. Also do the same for packets that should be denied access to the GIAC network.

Once the configuration has been verified the next step is to test the connectivity of each device. Use the *show interface* command to verify that the line protocol and interface are up. This gives an indication that interface and cabling are connected and functioning correctly. Use the ping command to test network connectivity. Accessing each service on the service network will verify connectivity and that appropriate services are functioning correctly. For example, see if Web, FTP and other services are functioning by accessing these services from the outside. Check to make sure that systems in other security levels do not have access to systems on other security levels unless it is allowed through the firewall. Also verify that users in the user network are able to perform functions that they are indented to do.

Assignment 3 - Audit Your Security Architecture (25 Points)

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

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

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

3.0 Assignment 3 – Proposed Solution

3.1 Introduction

When planning an audit, several things must be taken into consideration prior to the actual implementation. Security policies and network diagrams must be reviewed. Router configurations and firewall rule bases must be checked for mis-configurations and efficiency. Log files from syslog servers and IDS systems must be reviewed to ensure that they are properly configured. Also, operating systems and server based applications must be identified. This will assist in identifying the type of audit tools to utilize in the assessment. The assessment should be conducted in two phases. The assessment should take place during normal business hours to assess the network at its peak usage and under its normal operating conditions. This gives an idea of the type of network traffic that takes place. The assessment should also take place during off hours so that certain tests and scans do not interface with normal business functions.

3.1.1 Security Policy

The first step in planning out an assessment is to obtain and review the written security policies of GIAC. It will state the functions and access rules within the network and help identify who can access what internally and externally. It will also identify operating systems and server applications that reside on the GIAC network. It is very important to understand the inter workings of the network to ensure that business functions can work as GIAC management intended. The security policy has the most important impact on the assessment. If the policy is weak and not properly understood, it will affect the entire assessment. It is important to ensure that the policies are thoroughly reviewed. Any security inconsistencies should be confronted and resolved at this level prior to assessment implementation.

3.1.2 Network Diagram

It is important to obtain or generate a current, complete and detailed diagram of the network. This is normally part of the security policy. This will assist in the initial planning of the assessment. It is important to identify all perimeter devices, internal devices, connections to outside networks, subnets and public access servers within the GIAC network. This will help identify systems or devices that are located in areas that pose greater security risks and could affect the security of the primary firewall.

3.1.3 Review Router Configurations/Firewall Rule Bases

The next step is to obtain configurations of routers and rule bases of firewalls from the GIAC network. These must be reviewed for inconsistencies, mis-configurations and security vulnerabilities. It is important to examine the perimeter devices first to ensure that known security issues are taken care of and denied access to the GIAC network. Next review the configurations of internal routers and rule bases of internal firewalls. This will indicate access restrictions internally, which could have an affect of the primary firewall. For instance, the service network should never have direct access to the user network, however the user network may be able to access services on the service network. Also ensure that default settings and configurations that are part on the initial setup, do not pose security vulnerabilities. Some versions of router IOS/firewall software

place statements in the ACL/rule base by default that may counteract the GIAC security policy.

3.1.4 Reviewing Log Files

It is helpful to gather and examine logs from syslog servers and IDS monitors. It is important to see if any known problems or potential security risks currently exist. This also ensures that syslog servers and IDS monitors are performing properly.

3.1.5 Operations Systems (OS) and Service Applications

It is important to identify required services and operating systems that are on the GIAC network. This will help identify the type of audit tools to use when probing the internal network. Different services have different vulnerabilities. The same is true for different versions and types of operations systems. The GIAC network will consist primarily of Microsoft products. IIS is used for Web and FTP servers. Exchange is used for email and DNS is Microsoft implemented. It is crucial that the latest service packs and security updates are applied to each OS and service application. These updates protect systems from known security issues.

3.1.6 Router/Firewall Devices

All perimeter/internal routers and firewalls should be identified and reviewed by type, model and specifications. It must be ensured that the network equipment can support the existing network requirements and any potential growth. Also, the IOS and firewall software on each device should be updated to the most current version. This will ensure that known security problems are not an issue. The border router of the GIAC network is a Cisco 2611 with the latest IOS. The primary firewall is a Cisco PIX 520 with the latest software. The specifications of each device exceed the traffic and growth requirements of the network.

3.1.7 Audit Tools/Special Equipment

Once the network devices, operating systems and service applications have been identified, the tools used to assist in the audit can be defined. Since GIAC is primarily a Microsoft orientated network, a plan can be developed to determine the type of tools to use. Also network probes; packet sniffers and network monitors can help determine protocols and traffic patterns.

3.1.8 Probing/Scanning

Once the audit tools are identified, it can be determined how to go about the probing and scanning of the GIAC network. This will help identify the layout of internal subnets, access restrictions and the services of the network.

3.1.9 Level of Effort (LOE)

Once the planning stages have been outlined, the LOE can be estimated. As stated above, the assessment should include the primary firewall of the GIAC network. In doing this, the security policy and network diagram should be thoroughly reviewed to see what role the primary firewall has on the network. Keep in mind that not only does the primary firewall have to be assessed, but also any surrounding devices. Connecting devices

should be reviewed for security implications that may have affects on the primary firewall security. For instance, the border router configuration must be reviewed and compared to the primary firewall rule base to ensure that security is covered and unnecessary redundancies do not exist between the two devices. The same is true for other connecting networks and devices. At a minimum, the border router will have to be considered in the assessment in additional to the primary firewall. Audit software tools must be ran from each connecting subnet through the primary firewall to determine if the firewall rule base is working accordingly. Below is an estimate of the LOE from the assessment of the primary firewall.

LOE Estimate

Function	LOE (persons)	Position	Duration (days/person)
Review of Security Policies/Network diagram	1	Sr. Network Analyst	.5
Review of Border Router Configuration/Primary Firewall rule base	1	Sr. Firewall Analyst	.5
Use of auditing tools for connecting subnets/Gathering Information	3	Network Analyst	1
Summary of Assessment	1 1	Sr. Network Analyst Sr. Firewall Analyst	1.5 1

3.1.10 Cost

The cost of the assessment is directly related to the LOE plus any specialized equipment used in the assessment. If no special equipment has to be purchased in order to carry out the assessment, then the cost is basically the sum of the loaded rate of each person multiplied by the number of hours. A break down of the estimated cost is listed below.

Cost Estimate

Position	Man Hours	Rate (per hr)	Total $
Sr. Network Analyst	16	95	$1520
Sr. Firewall Analyst	12	110	$1320
Network Analyst	24	80	$1920
Total	52		$4760

3.1.11 Risks and Considerations

The primary risk associated with the security assessment of a network is to ensure that the security policy is well defined. If the policy does not impose a properly configured

network design or contains inaccuracies, inconsistencies or is incomplete, this will impact or delay the results of the assessment.

If the network consists of legacy software or operating systems that simply cannot be updated, this can lead to potential security risks that cannot be corrected. The same is true for network devices, router IOS and firewall software. Other considerations are to ensure that primary systems and devices are properly functioning when probing or scanning the network. If certain key systems or devices are down, temporarily out of service or not functioning properly, this can lead to an incomplete assessment.

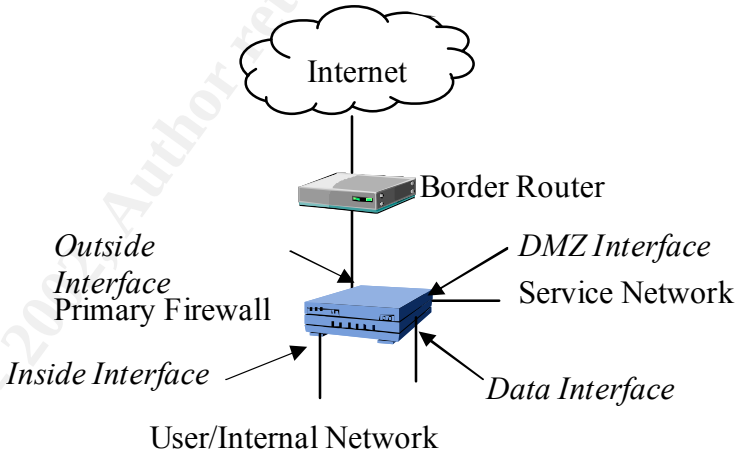
3.2 Assessment Implementation

3.2.1 Introduction

Review the security policy and network diagram to determine the role of the primary firewall and its impact on the GIAC network. The network diagram indicates that a border router provides routing to the Internet and is the first level of defense for the GIAC network. The border router's Ethernet interface connects directly to the primary firewall. The firewall has four interfaces labeled, Outside, Inside, DMZ and Data. Each interface has a different security level setting. Access through each interface must be tested from each network segment to ensure access restrictions are in place. Running a port scan from each subnet on the other subnets can test this.

Firewall Policy			
Interface	**Host**	**Access**	**Security**
Outside	Outside Users	DMZ	0
Inside	Internal Users	DMZ, Data Outside	100
DMZ	Service Network	Data	50
Data	NA	NA	40

1) Outside users can only access the DMZ services
2) Inside users can access DMZ services and the Internet
3) DMZ can only access the Data interface
4) Data interface cannot initiate a connection to anyone



The border router's configurations should be examined for mis-configurations and vulnerabilities. The border routers IOS version and firewall software version can be viewed using the *show version* command from the command prompt to ensure that the most recent software is running on the device. The border router ACL and primary firewall rule set are listed below.

Border Router ACL	Primary Firewall Rule Base
Ingress filtering *Interface serial0* *Access-list 111 deny ip 192.168.0.0 0.0.255.255 any echo log* *Access-list 111 deny ip 172.16.0.0 0.15.255.255 any echo log* *Access-list 111 deny ip 10.0.0.0 0.255.255.255 any echo log* *Access-list 111 deny ip 224.0.0.0 31.255.255.255 any echo log* *Access-list 111 deny ip 127.0.0.0 0.255.255.255 any echo log* NETBIOS filtering *Access-list 111 deny tcp any any eq 135 echo log* *Access-list 111 deny udp any any eq 135 echo log* *Access-list 111 deny udp any any eq 137 echo log* *Access-list 111 deny udp any any eq 138 echo log* *Access-list 111 deny tcp any any eq 139 echo log* *Access-list 111 deny tcp any any eq 445 echo log* *Access-list 111 deny udp any any eq 445 echo log* ICMP filtering *Access-list 111 deny icmp any any echo log* Allow everything else *Access-list 111 permit ip any any* *<implied deny>* *IP access-group 111 in* Egress filtering *Interface Ethernet0* *Access-list 12 permit 192.168.1.0 0.0.0.255* *Access-list 12 permit 10.0.0.0 0.0.0.255* *Access-list 12 deny any any echo log* *Ip access-group 12 in*	Rule set for HTTP/Web *Static (dmz,outside) xxx.xxx.102 192.168.1.2 netmask 255.255.255.255* *Static (dmz,outside) xxx, xxx.100.103 192.168.1.3 netmask 255.255.255.255* *Static (dmz,outside) xxx. xxx.100.104 192.168.1.4 netmask 255.255.255.255* *Static (dmz,outside) xxx. xxx.100.105 192.168.1.5 netmask 255.255.255.255* *Access-list acl_out permit tcp any host xxx.100.100.102 eq www* *Access-list acl_out permit tcp any host xxx.100.100.103 eq www* *Access-list acl_out permit tcp any host xxx.100.100.104 eq www* *Access-list acl_out permit tcp any host xxx.100.100.104 eq www* Rule set for HTTPS/Web *Static (dmz,outside) xxx.xxx.100.110 192.168.1.10 netmask 255.255.255.255* *Static (dmz,outside) xxx.xxx.100.111 192.168.1.11 netmask 255.255.255.255* *Access-list acl_out permit tcp any host xxx.100.100.110 eq 443* *Access-list acl_out permit tcp any host xxx.100.100.111 eq 443* Rule set for FTP *Static (dmz,outside) xxx.xxx.100.120 192.168.1.20 netmask 255.255.255.255* *Static (dmz,outside) xxx.xxx.100.121 192.168.1.21 netmask 255.255.255.255* *Access-list acl_out permit tcp any host xxx.100.100.120 eq ftp* *Access-list acl_out permit tcp any host xxx.100.100.121 eq ftp* Rule set for SMTP *Static (dmz,outside) xxx.xxx.100.130 192.168.1.30 netmask 255.255.255.255* *Access-list acl_out permit tcp any host xxx.100.100.120 eq smtp* Rule set for DNS *Static (dmz,outside) xxx.xxx.100.132 192.168.1.32 netmask 255.255.255.255* *Access-list acl_out permit tcp any host xxx.100.100.120 eq dns* *Access-group acl_in in interface outside* Apply rule set to inbound traffic of the outside interface Rule set ActiveX/Java Applets *Filter activex 80 0 0 0 0* *Filter java 80 0 0 0 0*

3.2.2 Audit Tools

Auditing tools allow the gathering of information from networks and hosts. They provide a means to test connectively, conduct port scans, provide queries and obtain other information about networks. Tools can be useful to gather information about the GIAC network and test to ensure that security policies are in place. Below are a few tools that can be use for auditing purposes.

Windows Tools: ping, tracert, nbtstat, nslookup
SuperScan - http://keir.net/software.html
WS Ping Pro Pack - http://www.ispwitch.com/Products/WS_Ping
Sam Spade – http://www.blighty.com/products/spade
Project R3x - http://hackersclub.com

3.2.3 Border Router

3.2.3.1 Ingress/Egress Filtering

Ensure that the border router is denying all packets that are not allowed on the GIAC network. The border router does not allow packets with source IP addresses from reserved networks into the GIAC network. This is known as Ingress filtering. Egress

filtering only allows packets with source IP addresses from the GIAC network to leave the network. Both of these filtering methods prevent address spoofing. To test Egress filtering, place a laptop on the user network with an IP address that is not in the 192.168.1.0 or 10.0.0.0 subnets range. See if the laptop can ping the outside interface of the border router. The GIAC network also does not allow packets to NETBIOS or ICMP ports. This will cut down on the most common type of attacks.

3.2.3.2 ICMP Filtering

To test ICMP filtering, try to ping the outside interface of the border router. The test results are listed below. The border router did not respond to the ping request. The request was timed out.

C:\>ping xxx.xxx.xxx.1

Pinging xxx.xxx.xxx.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for xxx.xxx.xxx.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

3.2.3.3 NETBIOS Filtering

To test NETBIOS filtering, from an outside host, try to map a drive to one of the web server's administrative share. If NETBIOS is allowed passed the firewall, it will ask for a login and attempt to connect to the share. The results for the NETBIOS tests are listed below. The drive mapping was unsuccessful. The nbtstat command can also be used to test for NETBIOS communications. If the host responds to the nbtstat request, NETBIOS is allowed to pass through the firewall. The nbtstat example below is unable to locate a host. Without NETBIOS blocking enabled, an attacker can obtain valuable information about the GIAC network.

Share Map
*C:\ >net use * \\ xxx.xxx.100.102\c$*
System error 67 has occurred.

The network name cannot be found.

Nbtstat
C:\>Nbtstat –a xxx.xxx.100.102

Local Area Connection:
Node IpAddress: [xxx.xxx.xxx.xxx] Scope Id: []

Host not found.

3.2.4 Primary Firewall

The GIAC primary firewall consists of four interfaces. The outside interface is directly connected to the Ethernet interface of the border router. All inbound traffic must pass through the outside interface prior to entering the internal network. The outside interface is where most of the access rules are placed. The inside interface hosts the internal user network. This is where the user network is located. The DMZ interface connects to the service network. The service network consists of Web, HTTPS, FTP, SMTP and DNS servers. Internet and inside users are allowed to access services in the service network. Each interface is assigned a security level value that is used to allow or prevent access to subnets within the GIAC network.

3.2.4.1 Outside Interface

The firewall primarily denies all packets into the GIAC network expect those packets that are given special access via the firewall rule base listed above. Special access is given to Internet users to access servers in the service network. This is done by allowing access by server IP address and service port. For example, to allow Internet users to access one of the GIAC web servers (Web 1), the following rule set must be in place on the primary firewall:

Static (dmz,outside) xxx.xxx.100.102 192.168.1.2 netmask 255.255.255.255
Access-list acl_out permit tcp any host xxx.xxx.100.102 eq www
Access-group acl_in in interface outside

This rule set first assigns the external routable IP address xxx.xxx.100.102 to the web server (Web 1) and then permits access to www services (port 80) for all outside hosts. These rules are applied to all traffic coming inbound from the Internet. As listed in the table above, similar rules are applied on the primary firewall to allow Internet users to make connections to the other servers on the service network. These include additional web servers, HTTPS servers, an FTP server, a DNS server and a SMTP server.

To test each rule set, outside access to the servers in the service network must be verified. This can be done using the following tools: web browsers (for www service), ping, tracert and port scanners. Prior to testing, the ICMP protocol must be temporarily enabled on the border router and firewall to allow ICMP requests. Ping will verify that the server is functioning and at the assigned IP address. Tracert will also verify this and list the route that packets take from the host running tracert and the server on the service network. Both of these commands are part of the Windows OS. A port scanner will verify active ports on servers in the service network. These tools are applied to Web 1 and the results are listed below. Each server should be tested to ensure that it is accessible from the Internet and that only the corresponding services are listening. By default, Web servers listen on port 80, HTTPS servers listen on 443, FTP servers listen on ports 20-21, DNS servers listen on port 53 and SMTP servers listen on port 110.

3.2.4.1.1 Ping Test (Web 1)
The results of the ping command on the GIAC web server, web 1 with IP address xxx.xxx.100.102 are listed below. Notice the results of the ping command, the web server sends a reply back.

C:\>ping xxx.xxx.100.102

Pinging xxx.xxx.100.102 with 32 bytes of data:

Reply from xxx.xxx.100.102: bytes=32 time=201ms TTL=116
Reply from xxx.xxx.100.102: bytes=32 time=190ms TTL=117
Reply from xxx.xxx.100.102: bytes=32 time=181ms TTL=117
Reply from xxx.xxx.100.102: bytes=32 time=180ms TTL=117

Ping statistics for xxx.xxx.100.102:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 180ms, Maximum = 201ms, Average = 188ms

3.2.4.1.2 Port Scan Test (Web 1, Using SuperScan)
The results from the port scan show that the web server is only listening on port 80 (www services) when the port scan is run from an outside host. When the port scan is ran from the service network, the firewall does not play a role, thus all listening ports will respond to the port scan. A web browser can also verify that web services are operational and functioning on Web 1.

Port Scan From Internet
+ xxx.xxx.100.102
|___ 80 http
|___ HTTP/1.1 401

Port Scan from within the service network
** + xxx.xxx.100.102*
|___ 80 http
|___ HTTP/1.1 401
|___ 135 epmap
|___ 139 netbios-ssn
|___ .....
|___ 427 svrloc

3.2.4.1.3 DNS Zone Transfer Test
Nslookup ensures that the DNS server does not answer zones transfers for non-qualifying hosts or servers.

C:\>nslookup
Default Server: ns1.GIAC.com
Address: xxx.xxx.xxx.132

> ls
Server: ns1.GIAC.com
Address: xxx.xxx.xxx.132
[ns1. ns1.GIAC.com]
**** Can't list domain ns1.GIAC.com: Query refused*

As in the case of Web 1, each server on the service network should be tested in this fashion. The Project R3x tool, mentioned above, has the capability to ping multiple hosts from a listed range. This can be used to ping the entire service network range without having to use the ping command for each individual IP address.

3.2.4.2 Inside Interface
Users within the inside interface must be able to connect to the Internet and servers within the service network. The primary firewall allows this to happen by the rule set below.

Nat(inside) 1 0 0
Global (outside) 1 xxx.xxx.200.100-xxx.xxx.200.200 netmask 255.255.255.0
Global (dmz) 1 192.168.1.40-192.168.1.240 netmask 255.255.255.0

This rule allows all users on the inside interface to access interfaces with lower security levels. For instance, all internal users can now access the Internet and servers on the service network. Note that servers in the service network cannot access the internal network. The first global statement assigns IP addresses from the listed range for all connections made to the Internet. The second global statement assigns IP addresses from the listed range for all connections made to the service network from the inside network. This can be tested using the ping command or a web browser. From the user network, ping all of the servers on the DMZ interface. Each server will reply to the ping. The same will be true for connections to the Internet. The ping and browser tests are listed below. Testing each server on the service network will show that each service is functioning correctly on the appropriate port. It is important to note that even though tests are shown for one server, each server in the service network should be tested. For instance, a web browser can test web servers, FTP clients can test FTP access and the same applies to every other server. A port scanner is typically used in a situation similar to this. A port scanner ran from the user network will verify the active ports on each server that users can access. This is listed below.

3.2.4.2.1 Ping Test (FTP)
The FTP server on the service network is accessible from the user network.
C:\>ping 192.168.1.20

Pinging 192.168.1.20 with 32 bytes of data:

Reply from 192.168.1.20: bytes=32 time=77ms TTL=116
Reply from 192.168.1.20: bytes=32 time=74ms TTL=117
Reply from 192.168.1.20: bytes=32 time=69ms TTL=117

Reply from 192.168.1.20: bytes=32 time=68ms TTL=117

Ping statistics for 192.168.1.20:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 180ms, Maximum = 77ms, Average = 72ms

3.2.4.2.2 Web browser Test (www.Cisco.com)
Users of the GIAC user network can access the Internet.

3.2.4.2.3 Port Scan (Using SuperScan – Web 1, Web 2)
The results using SuperScan show that Web 1 and Web 2 are active on port 80. The remaining servers, not listed, would show similar results except they would be active on their corresponding ports. For instance HTTPS (443), FTP (20&21), DNS(53), SMTP(110).

```
* + 192.168.1.2
        |___  80  http
              |___ HTTP/1.1 401
        |___  135  epmap
        |___  139  netbios-ssn
              |___ .....
        |___  427  svrloc
+ 192.168.1.3
```

|___ *80 http*
|___ *HTTP/1.1 401*
|___ *135 epmap*
|___ *139 netbios-ssn*
|___ *.....*
|___ *427 svrloc*

3.2.4.3 DMZ Interface

As indicated from the primary firewall rule set listed above, the DMZ interface allows access to services on the service network to hosts from the Internet. This makes the service network vulnerable to attacks. If a server in the service network becomes compromised, the attacker will only be isolated to the service network. Services in the service network are not able to initiate connections to systems in the user network. The GIAC firewall does not permit this. It is very important that this is verified in the assessment.

From the service network, try to ping the user network. A host on the service network, cannot establish connects with hosts on the user network. The firewall rule set does not permit this to happen. The results of using the ping command from the service network to a node on the user network are listed below. Test all of the of IP addresses on the user network to verify that no connections can be made from the service network. This can be confirmed by testing the entire IP range.

3.2.4.3.1 ICMP Test

A ping from the service network to a node on the user network is unsuccessful.
All IP addresses must be tested to verify that the same results are obtained.

C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

3.2.5 Firewall Access

Verify that the firewall has an encrypted password set. When setting up a Cisco PIX firewall, the default password is set to "cisco". This can be changed and encrypted by typing the command listed below at the firewall command prompt. Also, verify that telnet and TFTP services from the firewall are not enabled for users from the Internet.

This will eliminate the chance of outside attackers attempting to gain access to the primary firewall.

Passwd <new password> encrypted

3.2.6 Summary of Assessment

Once the assessment is complete, a summary containing the findings should be developed. The summary should show a complete analysis detailing the potential vulnerabilities and security risks and any recommendations that will improve the security and performance of the network.

3.3 Perimeter Analysis

In order to conduct a perimeter analysis, it must be verified that the network equipment meets the requirements to support network traffic. Also, the network must be analyzed to determine if improvements can be made that make the network more secure and efficient. Several security factors need to be considered including fault tolerance designs, location of TFTP servers and IDS systems, password security, backing up configurations and router/firewall maintenance.

3.3.1 Perimeter Equipment Specifications

As indicated, the border router routes traffic from the Internet to the GIAC network and vice versa. It is important that the border router is sufficient to support the required bandwidth, connections, etc. The specifications for the Cisco 2611 are listed below.

Specifications:
Supports up to 64 ISDN B channels
40 MHz RISC Processor/64 MB Ram
Supports up to 6 interfaces

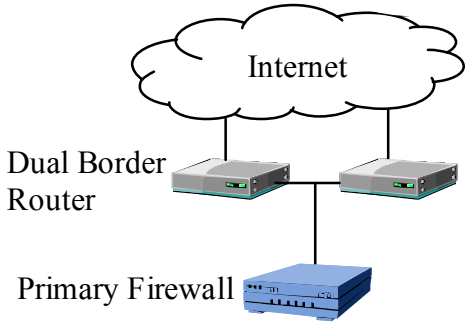
The firewall is directly connected to the border router and connects to all subnets in the GIAC network. It is crucial that the firewall be able to support are inbound/outbound traffic while applying the rule base to each packet. The GIAC firewall is a Cisco PIX 520. The specifications are listed below.

Specifications:
Supports 250,000 simultaneous connections
370 megabits per second (Mbps) throughput.
350 MHz CPU / 128 MB Ram
Up to 6 Ethernet interfaces for growth
Supports NAT natively
Integrated VPN
Integrated IDS

3.3.2 Recommendations

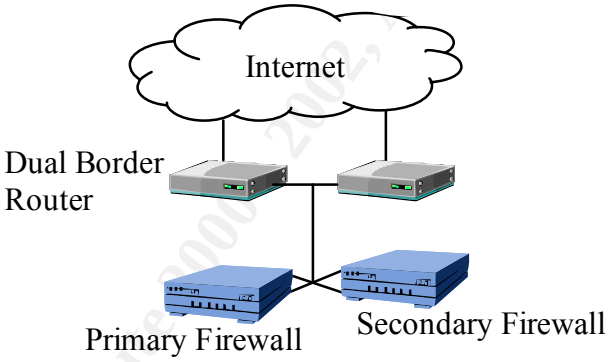
3.3.2.1 Fault Tolerance – Border Router

The current network does not offer any means of fault tolerance in the event that the border router or the line to the Internet should fail. A border router failure would prevent outside users from accessing the GIAC network and result in possible loss of business. One likely solution would be to add a secondary router and connect it to the primary border router in a fail over fashion. If the primary router should fail, the secondary router would kick in. Another solution would be to add an additional border router in parallel to the primary router and connect it to a separate Internet connection or ISP. This would prevent any single failure from shutting down the GIAC network. An example of this type of fault tolerance is illustrated below.



3.3.2.2 Fault Tolerance – Firewall

As indicated with the border router above, the GIAC network does not have any fault tolerance in the event of a firewall failure. If the firewall should fail, this would shut down all access to the GIAC network. To eliminate this type of failure, a secondary firewall could be added in a fail over fashion. If the primary firewall should fail, the secondary firewall would take over the role of the primary firewall. An example of this type of fault tolerance is illustrated below.



3.3.2.3 Router IOS/Firewall Software

Check the router IOS and firewall software versions to ensure that they are the latest versions. The latest version will prevent known vulnerabilities and software bugs from becoming potential security issues. Updating can also provide updated features. An example of this is with the release of software version 5.2; the PIX firewall has integrated IDS capabilities. The latest router IOS and firewall software versions can be downloaded from the Cisco web site.

3.3.2.4 Password Security

The router/firewall enable and telnet passwords can be viewed from the configuration by default. The enable and telnet passwords should be set and encrypted so that they do not become compromised. When the passwords are encrypted, they cannot be viewed from the configuration file.

3.3.2.5 Backups

It is important to make and keep backup copies of router and firewall configurations in the event that the router or firewall is reset or replaced. The router or firewall may fail without notice and give no opportunity for the configuration to be backed up. Backing up the configuration can be done via a TFTP server or simply by copying the configuration while at the command prompt. Ensure that the configurations are stored in a safe place out of reach of anyone who does not administer the router or firewall.

3.3.2.6 Maintenance

Ensure that current maintenance agreements are in place for all network devices. This allows expert advice in the event that assistance is required. Further, this allows access to current troubleshooting information and IOS/software updates.

3.3.2.7 Disabling Unused Services

All services on all systems that are not required must be disabled. Many applications and operating systems install and enable services by default without any indication of their existence. These services may pose hidden vulnerabilities if their existence is not known.

Assignment 4 - Design Under Fire (25 Points)

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:

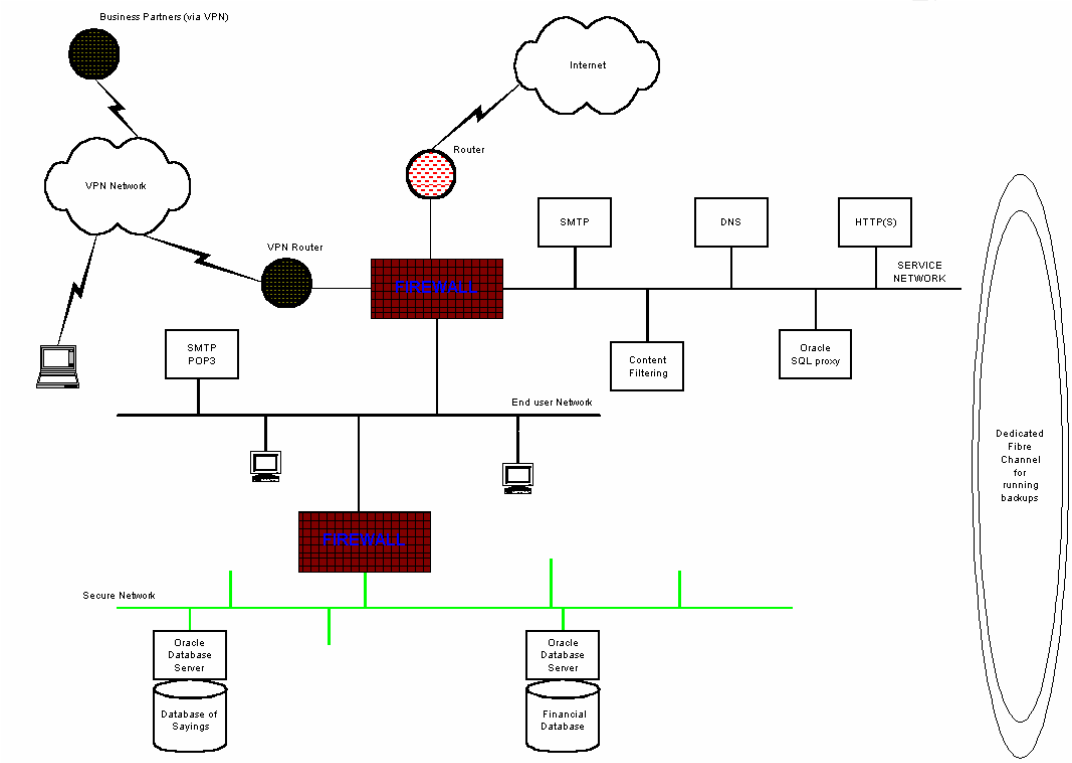
1. An attack against the firewall itself. Research vulnerabilities that have been found for the type of firewall chosen for the design. Choose an attack and explain the results of running that attack against the firewall.
2. A denial of service attack. Subject the design to a theoretical attack from 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.

4.0 Assignment 4 - Proposed Solution

4.1 Design Under Fire

The overall goal of this assignment is to select a network design from a previous GCFW practical and subject the design to be placed under attack. The design chosen for this assignment is listed below. The URL is http://www.sans.org/giactc/gcfw.htm , by Kofi Arthiabah, GCFW. This design implements Check Point's Firewall-1 V. 4.0 as a means of firewall protection.



Proposed GIAC Enterprises Network Security Architecture

4.1.1 Attack of Firewall

The first step in planning an attack on a network is to gather information and identify the primary firewall. This can be done a number of ways. One of the simplest ways is via a port scan. Using SuperScan, the following results are obtained. Note these are actual results obtained from a real scan.

```
* + xxx.xxx.xxx.xxx
        |___ 21  ftp
             |___ 220 Check Point FireWall-1 Secure FTP server running on checkpfw..
        |___  23  telnet
             |___ Check Point FireWall-1 authenticated Telnet server running on checkpfw.....
        |___  80  http
             |___ HTTP/1.0 400 Bad Request..Pragma: no-cache..Cache-Control: no-cache..Content-
             Type: text/html..Content-Length: 117....<TITLE>Err
        |___  513  login
             |___ .Check Point FireWall-1 authenticated rlogin server running on checkpfw...
        |___ 1500  vlsi-lm
```

The above scan indicates that the primary firewall is running Check Point Firewall-1 software and is allowing FTP, telnet, HTTP and other services to pass through it. This is very very helpful. Now we have a starting point.

4.1.2 Check Point Vulnerabilities

Once the type of firewall has been determined, the next step is to gather a list of known vulnerabilities for Check Point Firewall-1. This can be obtained from hacker web sites, Usenet groups, security web sites and Check Point's web site. Some resources to obtain firewall vulnerabilities are listed below.

Web

http://www.securityportal.com/
http://www.netsys.com/firewalls/
http://www.cert.org/
http://www.ciac.org/ciac/
http://www.securityfocus.com
http://www.packetstorm.securify.com
http://www.insecure.org/
http://www.wiretrip.net/
http://www.checkpoint.com/techsupport/alerts

Usenet

comp.security.firewalls
fa.firewall
cp.products.firewall-1

4.1.2.1 Check Points Vulnerability List

Using the resources from above, a number of recent known vulnerabilities and security issues can be found.

Fast Mode Vulnerability
http://www.checkpoint.com/techsupport/alerts/fastmode.html

ACK DoS Attack Update
http://www.checkpoint.com/techsupport/alerts/ackdos_update.html

Passive FTP Vulnerability
http://www.checkpoint.com/techsupport/alerts/pasvftp.html

4.1.3 Other Check Point Security Issues

Below is a list of security issues directly from Check Point's web site. This is listed to illustrate the type of vulnerabilities that currently exist with Check Point Firewall-1 and also to show how easy it is to obtain.
(Listed from the Check Point's web site located at
http://www.checkpoint.com/techsupport/alerts/list_vun.html)

SMTP Security Server Denial of Service
IP Fragmentation Denial of Service
One-way Connection Enforcement Bypass
Improper stderr Handling for RSH/REXEC
FTP Connection Enforcement Bypass
Retransmission of Encapsulated Packets
Inter-module Communications Bypass
OPSEC Authentication Vulnerability
One-time (s/key) Password Authentication
Getkey Buffer Overflow

Description of Security Issues

SMTP Security Server Denial of Service

A rapid stream of invalid SMTP commands to the SMTP Security Server would raise CPU load on the firewall, disabling mail delivery (although other traffic continued to pass).

Who is affected: Installations employing the SMTP security server for inbound email.

Changed in Service Packs: The SMTP Security Server in the new Service Packs drops SMTP connections after a configurable number of invalid commands.

IP Fragmentation Denial of Service

The mechanism used to log invalid IP fragments consumed a large amount of CPU resources during an IP fragmentation attack.

Who is affected: All versions.

Immediate Workaround: Refer to IP Fragement-droven Denial of Service Vulnerability for information on disabling the invalid fragment logging.

Changed in Service Packs: The logging mechanism has been refined so that it consumes minimal CPU cycles.

One-way Connection Enforcement Bypass

It was possible to bypass FireWall-1's normal directionality check by using specially fragmented TCP connection requests -or by closing and reopening one-way TCP connections- in conjunction with certain complex multi-connection protocols.

Who is affected: Sites allowing protocols employing unidirectional data flow connections (such as FTP and RSH STDERR). NOTE: The directionality check is an additional layer of security which VPN-1/FireWall-1 adds to these protocols. An attack which bypasses this check is not in itself a security risk, however this check would otherwise substantially minimize the effects of items such as (4) below.

Changed in Service Packs: Directionality checks are much more strict in the new Service Packs, and will prevent surreptitious back-channel communication.

Improper stderr Handling for RSH/REXEC

Specially formatted RSH/REXEC connection requests could cause an unauthorized connection to be opened from an external RSH/REXEC server to an internal (protected) RSH/REXEC client. This applied only if the FireWall-1 administrator specifically enabled the RSH/REXEC setting in

the Properties window.

Who is affected: Only those sites which have specifically enabled the VPN-1/FireWall-1 RSH/REXEC property.

Immediate Workaround: Disable RSH/REXEC if not needed.

Changed in Service Packs: The new Service Packs feature tighter control of STDERR connections plus the directionality checks noted in item (3), to prevent misuse of the error channel. NOTE: RSH/REXEC, like other protocol properties, should not be enabled if not needed.

FTP Connection Enforcement Bypass

Specially formatted FTP connections could be redirected from the FTP server to a system other than the FTP client.

Who is affected: Installations allowing inbound write access to those FTP servers which are vulnerable to "FTP Bounce" attacks.

Immediate Workaround: Configure VPN-1/FireWall-1 to allow FTP Read only, if feasible. Verify that your FTP server software is not susceptible to an FTP Bounce attack (the majority are not vulnerable; consult your FTP server vendor for verification).

Changed in Service Packs: VPN-1/FireWall-1's validity checking of FTP commands is much more strict in the new Service Packs, protecting the few FTP servers which are vulnerable to this type of attack.

Retransmission of Encapsulated Packets

The payload of specially encapsulated FWZ packets, which passed normal rule-base checks, would be retransmitted even if the packet did not originate from an FWZ client.

Who is affected: All versions. NOTE: This is not a vulnerability in itself, although it may be used to facilitate an attack.

Immediate Workaround: Correct configuration of IP Spoofing protection will reduce exposure to attack. If SecuRemote with FWZ Encapsulation is not being used, IP Protocol 94 may be blocked at an external router.

Changed in Service Packs: FWZ encapsulation is disabled unless explicitly enabled by the firewall administrator. Additionally, only packets from authenticated FWZ VPN users will be decapsulated.

Inter-module Communications Bypass

Inter-module authentication mechanism (fwa1) was vulnerable to certain attacks, although the encryption used for data exchange was not. This allowed theoretical denial of service attacks.

Who is affected: Installations with rules allowing control connections from locations other than known management stations. NOTE: There is no known risk to customers because of this issue.

Immediate Workaround: For version 4.0 sites not using SecuRemote and version 4.1 sites, allow VPN-1/FireWall-1 control connections only from known management stations in the rule base.

Changed in Service Packs: The authentication mechanism in FWA1 has been strengthened in the new Service Packs. SSL is available in version 4.1 SP2 as an option for inter-module communication, although FWA1 remains the recommended inter-module authentication and

encryption protocol for all VPN-1/FireWall-1 versions.

OPSEC Authentication Vulnerability

The authentication mechanism used by OPSEC communications (fwn1) can be spoofed.

Who is affected: Sites which have not constrained OPSEC communication to specific source/destinations pairs via the rule base. NOTE: Check Point does not recommend or support the use of FWN1 for inter-module authentication.

Immediate Workaround: Ensure that OPSEC communications are allowed only between specific source/destination pairs in the rule base and that IP Spoofing protection is properly configured.

Changed in Service Packs: The authentication mechanism in FWN1 has been strengthened in the new Service Packs.

One-time (s/key) Password Authentication

Inter-module authentication for non-VPN software version 3.0 and 4.0 systems was susceptible to a brute-force attack.

Who is affected: Only installations using S/Key for inter-module authentication.

Immediate Workaround: For VPN-1/FireWall-1 version 4.0 users with an encryption license and all version 4.1 users, use FWA1 rather than S/Key for inter-module authentication and encryption. For version 4.0 users without an encryption license, modify the rule base to ensure that FW-1 control connections are allowed only from the management station. Also verify that IP Spoofing protection is properly configured.

Changed in Service Packs: While the S/Key seed generation mechanism has been strengthened in the new Service Packs, Check Point recommends that all version 4.0 and 4.1 sites use FWA1 for inter-module authentication and encryption. NOTE: With the new Service Packs, FWA1 is now available for all version 4.0 users, regardless of encryption capability.

Getkey Buffer Overflow

Inadequate protocol checking in inter-module communication could be exploited, causing the firewall daemon to terminate. However, policy enforcement continued.

Changed in Service Packs: Protocol checking in the new Service Packs has been strengthened in all areas of the software, preventing malformed instructions from impairing the firewall.
(End - Listed from the Check Point's web site)

4.1.4 The Attack

Normally an attacker will try a number a known vulnerabilities to attempt to shut down or gain access through the firewall. The trick is to select a vulnerability in hopes that the firewall administrator failed to update the software or apply the patch associated with the vulnerability. The vulnerability to be used for the attack on the Check Point firewall is the "IP Fragmentation Denial of Service**"** listed above. In this type of attack, an attacker sends a stream of extremely large IP fragments to the firewall. It forces the firewall to log invalid IP fragments and consumes a large amount of CPU resources, causing the firewall to deny service to legitimate requests or to shut down. This vulnerability affects all versions of Check Point. This type of attack can be generated using a number of hacker tools. One such program, Jolt2 can generate large IP fragments and send them to targeted hosts, causing DOS to occur. More information concerning this program can be

found at http://www.razor.bindview.com/publish/advisories/adv_Jolt2.html . The source code for this program can be located at http://www.packetstorm.securify.com/0005-exploits/jolt2.c .

4.1.4.1 Denial of Service Attack / TCP SYN Flood

A TCP SYN flood attack involving 50 compromised cables modem/DLS systems directed to the network listed above would shut down traffic to the network. This type of attack would not allow the network to be compromised. It would simply cause a DOS to occur to the targeted network. The TCP SYN flood attack sends multiple TCP SYN packets to a targeted host. The host responds with a TCP SYN/ACK and queues all outstanding TCP SYN/ACK responses on a backlog queue. The host waits for another TCP SYN before initiating a connection and de-queuing the TCP SYN/ACK response from the queue. The final TCP SYN never comes and the host's queue becomes full. Once the queue becomes full, the host will ignore all incoming legitimate TCP SYN requests.

If 50 systems start an attack on the network each sending TCP SYN packets with spoofed source IP addresses, the host will responded with a TCP SYN/ACK packets to the spoofed IP addresses. The router/firewall will queue the outstanding TCP SYN/ACK responses until a TCP SYN packet is received from the sending systems. The TCP SYN packets will never come because the sending systems source IP addresses are spoofed. The router/firewall queue will fill up making it impossible for legitimate TCP SYN requests to get to the network.

4.1.5 Countermeasures

Most firewalls have built-in features that protect against TCP SYN flood attacks. The ACL or rule base should ensure that outbound packets contain source IP addresses that are part of the internal network and inbound packets do not contain source IP addresses from reserved networks. These rules deny packets with spoofed IP address from leaving or entering the internal network. As discussed in Assignment 2 above, this is known as Egress and Ingress filtering and is typically applied to the border router.

4.2 Attack – Internal System

The network design shown above has two possible entries points from the Internet. Both the border router and VPN router guard the exterior perimeter of the network. The border router and the VPN router are each directly connected to the primary firewall. The VPN is more secure and has more controlled access than the border router. The border router and primary firewall will allow access to services to the service network. Servers on the service network are more vulnerable because the border router and firewall must allow access to them. Also these servers are exposed to the Internet and heavy outside traffic, thus making it difficult to monitor snooping and probing activities. Because of these reasons, the first place to attack is the service network.

Cisco's web site lists the top five most vulnerable services, 2/03/01,
URL: http://cisco.com/warp/public/778/security/vuln_stats_02-03-00.html . This list is shown below.

Ranking	Service	Percentage Found
1	RPC	23.5
2	HTTP	21.8
3	SMTP	18.9
4	SNMP	12.8
5	FTP	5.6

4.2.1 DNS Zone Transfer

HTTP, SMTP and DNS are all running on the service network of the referenced network. The first step is to attempt a zone transfer from the DNS server. If this were successful, it would list the domain names and IP addresses of internal systems. Additional internal targets can be identified from this information. A zone transfer can be preformed using the nslookup command. An example is below.

Nslookup
>ls –d <dns server>

Use nslookup to list the members of a domain.

4.2.2 Snooping/Probing

Next, attempt to hack into the web server. Determining the Web server platform will identify the hacking tools and vulnerabilities to take advantage of. First try to access the web page via a browser. Browse around on the web page and take notice of the address box of the browser. The file extensions of the web files will give some indication of server platform. For example, Microsoft IIS will have extensions such as htm, html, asp, cfm and default files names such as default.html and default.asp. Unix based platforms will have extensions such as htm, html, shtml, c and pl and default files such as index.html and index.shtml.

Port Scan

A port scan using SuperScan may reveal the server platform as in this case of an actual scan. Port 80 on this system lists Microsoft IIS version 4.0 as the server software. This is very helpful.

```
* + xxx.xxx.xxx.xxx
        |___  80  http
              |___ HTTP/1.1 403 Access Forbidden..Server: Microsoft-IIS/4.0..Date:
              Fri, 09 Mar 2001 14:15:10 GMT..Content-Length: 595..Content-Typ
        |___  443  https
```

Banner Hacking

Try to telnet into the server. If telnet is running on the server, valuable information can be obtained without a valid login. As in the case below of an actual telnet session, the

server platform is displayed prior to logging into the server. Similar information may also be obtained from attempting to FTP into the server.

Telnet xxx.xxx.xxx.xxx

Red Hat Linux release 6.2 (Zoot)
Kernel 2.2.14-5.0 on an i686
login: <don't have one, thanks for the info>

4.3 Hacking In

Once the targeted web server platform is known, existing vulnerabilities and tools can be acquired in order to compromise the web server. There are hundreds of resources to find these vulnerabilities and tools. A few are listed below.

Vulnerabilities Sources

http://www.ciac.org/ciac/
http://www.cert.org/
http://www.insecure.org/
http://www.securityfocus.com/
alt.hacking.in.progress
alt.hacking
alt.binaries.hacking.utilities
alt.www.webmaster

WEB Server Vulnerabilities for Microsoft IIS and Redhat Apache

Below is a list of some of the know vulnerabilities for Microsoft IIS and Redhat Apache web servers obtained from http://www.SecurityFocus.com . This list is not complete and is intended to give an idea of the type of vulnerabilities that exist in which an attacker can gain control of a system.

Microsoft IIS 4.0 ISAPI Buffer Overflow Vulnerability

The ASP ISAPI file parser does not properly execute certain malformed ASP files that contain scripts with the LANGUAGE parameter containing a buffer of over 2200 characters and have the RUNAT value set as 'server'. Depending on the data entered into the buffer, a denial of service attack could be launched or arbitrary code could be executed under the SYSTEM privilege level in the event that a malicious ASP file were locally executed on IIS.

Microsoft IIS Executable File Parsing Vulnerability

When Microsoft IIS receives a valid request for an executable file, the filename is then passed onto the underlying operating system which executes the file. In the event that IIS receives a specially formed request for an executable file followed by operating system commands, IIS will proceed to process the entire string rather than rejecting it. Thus, a malicious user may perform system commands through cmd.exe under the context of the IUSR_machinename account which could possibly lead to privilege escalation, deletion, addition, and modification of files, or full compromise of the server.

NT IIS MDAC RDS Vulnerability
MDAC (Microsoft Data Access Components) is a package used to integrate web and database services. It includes a component named RDS (Remote Data Services). RDS allows remote access via the internet to database objects through IIS. Both are included in a default installation of the Windows NT 4.0 Option Pack, but can be excluded via a custom installation.

RDS includes a component called the DataFactory object, which has a vulnerability that could allow any web user to:
--Obtain unauthorized access to unpublished files on the IIS server
--Use MDAC to tunnel ODBC requests through to a remote internal or external location, thereby obtaining access to non-public servers or effectively masking the source of an attack on another network.

The main risk in this vulnerability is the following:
--If the Microsoft JET OLE DB Provider or Microsoft DataShape Provider are installed, a user could use the shell() VBA command on the server with System privileges. (See the Microsoft JET Database Engine VBA Vulnerability for more information). These two vulnerabilities combined can allow an attacker on the Internet to run arbitrary commands with System level privileges on the target host.

Apache /tmp File Race Vulnerability
A problem has been discovered in the Apache httpd distributed with the Immunix Linux distribution, a distribution based off the RedHat Linux distribution. Apache programs htdigest and htpasswd are used to offer advanced features to users of the web server. However, these two helper programs insecurely create files in the /tmp directory, which could allow for /tmp file guessing. This makes it possible for a user with malicious motives to symblink attack files writable by the UID of the Apache process.

Apache Web Server with Php 3 File Disclosure Vulnerability
Apache Web Server is subject to disclose files to unauthorized users when used in conjunction with the PHP3 script language. By requesting a specially crafted URL by way of php, it is possible for a remote user to gain read access to a known file that resides on the target host. Successful exploitation of this vulnerability could lead to the disclosure of sensitive information and possibly assist in further attacks against the victim.

4.3.1 Use of RDS Vulnerability
Taking advantage of the RDS vulnerability listed above, we are able to execute shell commands on a vulnerable Microsoft IIS system as a privileged user. This allows us to create accounts at our discretion. We can further copy the SAM database to our remote system and crack the passwords at our leisure. This will give us access to accounts and passwords that may be used on additional systems within the network. Once the web server has been compromised, this may lead to additional information that offers clues on other internal systems to attack.

References

"Potential Security Issues in VPN-1/FireWall-1"
URL: http://www.checkpoint.com/techsupport/alerts/list_vun.html . (2001)

"Denial-of-Service Attacks - SYN Attacks"
http://www.zdnet.com/devhead/stories/articles/0,4413,2172763,00.html . (1999)

Spitzner, Lance, Firewalls 101: Perimeter Protection with Firewalls, The SANS Institute, 2001

Spitzner, Lance, Advanced Perimeter Protection and Defense In-Depth, The SANS Institute, 2001

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

Configuration Guide for the PIX Firewall Version 4.4, Cisco Systems, June 1999

Configuration Guide for the PIX Firewall Version 5.3, Cisco Systems, 2001

IPSec User Guide for the Cisco PIX Firewall Version 5.3, Cisco Systems, 2001. 5.1 – 5.6

"Cisco Secure PIX Firewall"
http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/ . (2001)

"Cisco 2600 Series — Modular Access Routers"
http://www.cisco.com/univercd/cc/td/doc/pcat/2600.htm . (2001)

"Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.1"
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun_c/index.htm . (2001)

"Vulnerabilities"
http://www.securityfocus.com . (2001)

"Configuration Guide for the Cisco Secure PIX Firewall Version 5.3"
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v53/config/index.htm . (2001)

"Jolt2 - Remote Denial of Service attack against Windows 2000 and NT4"
http://www.razor.bindview.com/publish/advisories/adv_Jolt2.html .

Cisco Systems, "PIX of the Liter", Packet Magazine First Quarter 2001, 75-77

Cisco Systems, "End To End Confidence", Packet Magazine First Quarter 2001, 81-83

Cisco Systems, "Cisco Experts Pinpoint Network Vulnerabilities", Packet Magazine First Quarter 2001, 5-7

"Vulnerability Statistics Report"
http://cisco.com/warp/public/778/security/vuln_stats_02-03-00.html