Firewalls, Perimeter Protection, and VPNs

GCFW Practical Assignment
SANS Parliament Square, London

Version 1.5e

Chris Roberts

Contents

Assignment 1 – Security Architecture

Objectives

The aim of this design project is to define a security architecture, which will safeguard GIAC Enterprises' business and assets from common Internet threats, whilst enabling them to interact with business partners and customers.

The primary considerations for this design will be security, business continuity, and provision for expansion. A liberal budget has been assumed.

Security Infrastructure

Establishing good policy and infrastructure will be key to implementing and maintaining a secure environment. To address this need, an IT Security department will be established. They will operate on a 24-hour support basis, with the following broadly defined responsibilities:

- Monitoring of perimeter defence systems, and their logs, for signs of intrusion.
- Monitoring of internal system logs, for abnormalities.
- Analysing network intrusion attempts for trends, and weaknesses in the organisation's security architecture.
- Assisting systems administrators in forensic analysis, and evidence gathering, when successful intrusions are detected.
- Alerting systems administrators to new security issues, by monitoring BugTraq, and equipment vendors' security mailing lists.
- Maintaining records of systems' patch-levels and operating system versions.
- Ensuring patches and updates for new vulnerabilities, and security issues are applied.
- Regularly auditing the organisation's physical, and network security.
- Developing, maintaining, and regularly reviewing appropriate security policy.
- Interacting, when required, with law enforcement authorities.
- Educating the organisation's workforce in safe working practices. e.g. password management, and disclosure.

Network Design

The proposed design for the network is shown over the page. GIAC Enterprises will provide the following mechanisms for customers, suppliers, and partners to gain access to services:

Customers

Requirements:	Purchasing and acquiring bulk online fortune cookie sayings.
Access method:	Customers will have access to a website, which they will be able to access via HTTPS. They will be required to register before making purchases, and will be able to choose a unique account ID, and a password to protect this account. Orders can be made online, with payment either by credit card or purchase order. Once payment has been cleared, customers will be able to collect their sayings at the secure website, by providing their credit card number,

account ID and their account password. The sayings can then be downloaded in a delimited ASCII text file.

Suppliers

Requirements:	Supplying bulk online fortune cookie sayings.
Access method:	Suppliers will also conduct their business with GIAC Enterprises using a HTTPS secured website. Registered suppliers will be able to access an upload area, using an account ID and password. ASCII files may be uploaded, in an agreed delimited format. Payment for supplies will be made via traditional banking methods.

Partners

Requirements:	Read-only access to fortune cookie database.
Access method:	To reflect the flexible requirements of business partners, GIAC Enterprises will provide a VPN supporting IPSEC, to allow partners read-only access to the fortune cookie database.

Based on this access model, the network design is as follows:

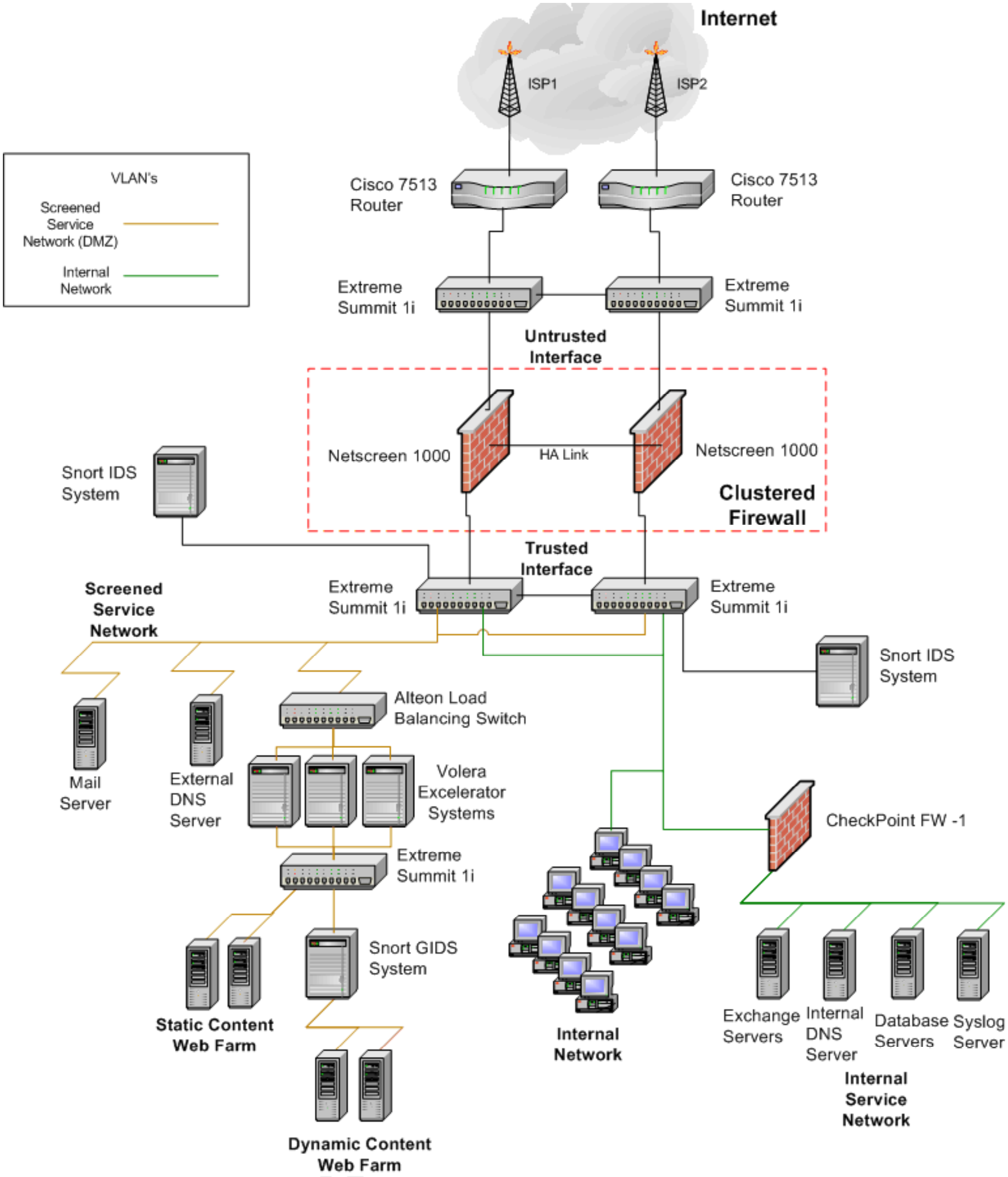


Fig 1: GIAC Enterprises' Network Design Diagram

The Core Network

The network has been designed with security, performance and availability in mind. The devices have been chosen to provide a Gigabit line rate within the core network, to allow for the demands of a rapidly expanding enterprise.

A large degree of redundancy has been provided in the core network, to ensure business continuity in the event of hardware failure. Where possible, spare devices should also be kept, as a backup. These devices should be kept in a physically secure location, and tested regularly.

Border Routers and Internet Connections

GIAC Enterprises will purchase two T3, or equivalent speed connections from separate ISPs. The ISPs should be willing to help their customers, where possible to limit the effects of any Denial-of-Service (DoS) attack mounted against them. Purchasing two Internet connections gives GIAC Enterprises some flexibility when handling DoS attacks, and will also help to preserve their Internet presence, should one connection fail.

The Cisco 7513 routers have built-in hardware redundancy, supporting two power supplies, and two RSP (Route / Switch Processor) modules. In addition, their features include extended ACL (access-control-list) support, traffic shaping capabilities, and the Cisco firewall feature set. The routers support a diverse range of connections, and should provide a good platform for GIAC Enterprises to upgrade their Internet connection, as their business expands.

Although the Cisco 7513 can support firewall features, they will not be used in this design. The ACL's will be used to enforce a global policy, defining the network traffic permitted on the corporate network. The routers will enforce egress filtering, to ensure outgoing network traffic has not been spoofed. They will also support the firewall, by blocking undesirable protocols, such as NETBIOS, SNMP, and blocking external access to broadcast addresses. In addition, the QoS features will be used, to prioritise outgoing traffic For details of the policy applied to the border routers, see the next section.

Core Switches

The GIAC Enterprises network will be fully switched, using connected pairs of Extreme Summit 1i switches in the core. The Summit 1i's support Gigabit interfaces, and can be used in ESRP (Extreme Standby Router Protocol) mode, to provide fast fail-over in the event of a hardware failure. The switches also have built-in protection against common DoS attacks, such as 'Teardrop' and 'LAND' attacks.

The trusted and untrusted interfaces on the firewall units will each be connected to a Summit 1i, to provide fail-over should one Cisco 7513 or NetScreen 1000 fail. Implementing a fully switched network throughout the organisation will also make sniffing the network more difficult.

Firewall

The firewall will consist of a pair of NetScreen 1000 systems, operating in HA (High Availability) mode. The NetScreen 1000 systems can operate at Gigabit line speed, providing a high performance firewall solution with transparent fail-over.

The Netscreen 1000's support 'virtual' firewalls, using VLAN tagging. This feature will be used to configure separate rule-sets for the internal network, and the screened service network (DMZ). These firewalls can support up to 100 virtual systems, which can be administered separately. NetScreen-Global Manager software will be used to mange the units. This will allow the configuration of the firewall to be easily backed-up, and allow administrators to change the configuration on both units simultaneously.

As previously defined, business partners will use a VPN to access the internal sayings database. The Netscreen firewall has VPN functionality, supporting IPSEC. This will be used to provide access to partners. The VPN policy is defined in the next section.

The internal network will be screened, using private address space. If required, the Netscreen firewall can also interoperate with a Websense system, to perform content filtering on the web sites visited by employees.

Snort IDS System

The IDS systems will consist of two RedHat Linux 7.1 systems running the free Snort IDS software (http://www.snort.org). The systems will have two NICs, which will be connected to a Summit 1i switch on the trusted interface of the NetScreen firewall. One connection on the switch will be set to port mirroring mode, so that all the network traffic switched by the Summit 1i will be mirrored onto the IDS system's interface. The other connection will be used for management purposes.

The Snort IDS systems will use the arachNIDS rule-set maintained at the WhiteHats.com site (http://www.whitehats.com/ids/). The IDS systems will log data to postgres databases, which the IT Security team will analyse using the ACID analysis engine (http://www.cert.org/kb/acid).

The IDS systems will work in conjunction with the NetScreen firewall, to detect intrusion attempts which the firewall has not blocked.

Obviously the IDS systems will contain sensitive information, and could also be a target for attack, so special measures will be taken to protect them. The systems will be installed with minimal operating systems and software, and will be bastion hardened, using the Bastille hardening scripts (http://www.bastille-linux.org/). The systems will be patched when vulnerabilities occur. To further protect them, the Tripwire file integrity checking software will be installed (http://www.tripwire.org).

The management interface will be screened using NetFilter – a built-in Linux kernel firewall module. Rules will be established, using the iptables tool, which will limit connections on the management interface, to selected systems in the IT Security department. Remote administration will be done using SSH. In addition, all syslog events will be logged to the internal syslog server.

The Screened Service Network (DMZ)

The DMZ will be connected to the Summit 1i switches on the trusted firewall interface. A virtual system will be configured on the NetScreen firewall, using VLAN tagging. This will allow the DMZ to be screened with a separate rule-set from the internal network.

The external DNS server, mail server and Alteon switch will be dual attached to the Summit 1i switches, so that the systems remain available if a core switch or firewall unit fails.

The systems on the DMZ are the most vulnerable to attack, since they will have public IP addresses, and systems on the Internet will have screened access to them. Extra bastion hardening measures should be taken to prevent these systems from being compromised.

External DNS and Mail Server

These services will be provided by RedHat Linux 7.0 based systems. If possible, slave systems should also be run, to provide redundancy and load-balancing. Due to the key nature of these services, they will be bastion hardened using a minimal operating system install, and the PitBull LX intrusion prevention system (http://www.argus-systems.com/). Tripwire would also be installed, to check the file integrity of system binaries. The use of PitBull LX would allow the IT Security team to set up these systems with restricted permission 'root' accounts, and firewall-like network access restrictions, to make system compromise much more difficult.

The systems would log to the internal syslog server, for centralised analysis of system logs.

The external DNS server will hold registrations for only those systems which have public IP addresses, and need to be accessed externally, namely:

- ❑ DNS Servers
- ❑ Mail server
- ❑ GIAC Enterprise's corporate website
- ❑ E-commerce website

The firewall's untrusted interface will also need to be publicly addressable, to allow VPN connections, but its IP address will not be published in the DNS.

To provide extra redundancy, the company's ISP's will also provide DNS hosting services for GIAC Enterprises. The DNS server will handle lookups recursively, so that clients do not need to access the Internet directly for DNS services.

The mail server will be responsible for delivering outgoing mail to the Internet, and accepting incoming mail. Outgoing email will be checked with a policy engine, which will virus-check the email, and add a disclaimer. Mail containing obscenities will be returned non-delivered. The server will only accept incoming mail where the recipient is a valid mail address in GIAC Enterprises, to prevent it being used as a mail relay. Incoming mail will also be virus-checked, and mail containing executable attachments, such as VBScript will be returned. Once it has been virus-checked, incoming mail will be delivered to the internal Exchange Server.

Web Farm Overview

GIAC Enterprises' major business is conducted through the web. The investment in a well-protected web farm should prevent the organisation from suffering website defacements, or outages due to security incidents. Where possible, direct access to the web servers has been restricted, to prevent attack using well-known web server vulnerabilities.

The farm is load-balanced using an Alteon switch, and a series of systems running Volera Excelerator, in a clustered configuration. These technologies are specialised for load-balancing web traffic,

Static Web Farm

The static web farm will provide the corporate website for GIAC Enterprises. This content is expected to change relatively infrequently. The Volera Excelerator systems will cache the site content, and serve it out to the Internet. Connections from the Internet, to the actual web servers will not be permitted. The Excelerator caches will also act as a web proxy for the employees of GIAC Enterprises.

Dynamic Web Farm

These systems could be the most commonly targeted for attack. The e-commerce systems accept purchases, and credit card details, and also provide suppliers with a method to upload fortune cookie sayings. The web servers must have some access to the internal database systems, to record transactions, accept payments, and load new fortune cookie sayings into the database, and so they represent a potential route into the internal network, if they are compromised.

To protect these systems, a GIDS (gateway intrusion detection system) will be used, along with bastion hardening. The GIDS will consist of a RedHat Linux 7.1 system; bastion hardened using the same methods as previously used with the Snort IDS systems. The system will again have two Gigabit NIC cards, but will this time act as a router. The GIDS will use the arachNIDS rule-set as a basis for the Snort configuration, but will only use those rules which detect incoming web-based compromises (typically those with destination port 80).

To protect the e-commerce web servers, the GIDS will make use of the Guardian plug-in for Snort (http://home.golden.net/~elim/), which can dynamically block attacks by creating firewall rules using the iptables tool. The blocks can be put in place for configurable periods of time, to prevent the blocking list from growing too large.

However, all web traffic to the e-commerce sites for purchasers and suppliers will be encrypted, using HTTPS. This makes it impossible for Snort to intercept and compare with attack signatures in real time. To solve this problem, the HTTPS encryption will be done by the Volera Excelerator web cache systems. Digital certificates can be installed on the Excelerator systems, which will then handle the overhead of encrypting web traffic. They will then pass the decrypted requests as HTTP requests to the dynamic web servers. This approach has two advantages – firstly, the overhead of encrypting data is moved to the cache systems, allowing the web servers to concentrate on the tasks of serving web data, and communicating with back end systems. Also, the requests pass from the caches to the web servers as unencrypted HTTP – which can be sniffed by the GIDS, and compared against known attack signatures.

The web servers providing the dynamic content will be Windows 2000 systems, running Microsoft Internet Information Server (IIS) 5.0. They will be installed following the NSA guidelines for securing Windows 2000 systems (http://nsa1.www.conxion.com/win2k/). In addition, the IIS 5.0 installations will be further secured using the SecureIIS software produced by eEye (http://www.eeye.com/html/Products/SecureIIS/), which protects IIS from buffer overflows, and common attacks.

The Internal Network

The employees of GIAC Enterprises, and the systems providing internal services use private IP addresses, and do not have direct access to the Internet. This decision follows analysis of the requirements of staff – it was found that their primary needs were access to the web, and access to email, while at remote locations.

To address these needs, the web caches will provide proxy access to the web for employees, whilst the dynamic web farm will contain servers running the Microsoft Exchange Outlook Web Access component, which will be accessible via the web, using HTTPS.

The Internal Service Network

Access to the internal service systems, and database systems will be restricted using a Solaris system, with Gigabit NICs, running CheckPoint FW-1. This firewall implementation was purposely chosen to use different hardware and software to the core NetScreen firewall. If a software vulnerability is discovered in NetScreen firewall solutions, the internal firewall should still provide some level of protection for the sensitive databases.

Microsoft Exchange Servers

The Exchange servers will hold employees' mail, and schedules. The servers will not have direct access to the Internet, but will use the mail server in the DMZ as a mail gateway to send and receive mail. The groupware features of Microsoft Exchange mean that employees will be able to check their diaries, and have access to other corporate data, whilst on the move, since they will be able to use the web servers running Outlook Web Access to get access to their mail. The Web Access sites will use 128-bit encryption, to prevent data being intercepted and decrypted on insecure networks.

Only one Exchange Server will be used to handle all Web Access traffic, to limit the exposure of the systems. This system will additionally be a BDC for the internal NT domain, to allow the Web Access to authenticate employees, without full access to the domain controllers. This Exchange Server will be dedicated to that task, and will not hold employees' mailboxes.

Selected corporate data will be made available in the Exchange Public Folders – this facility can be used by travelling employees to gain access to departmental reports, etc. The Public Folders will have ACL's to prevent unauthorised access, and content will be moderated by senior management, to mitigate the risk of sensitive documents being made available erroneously.

Syslog Server

Servers in the DMZ will log to the syslog server, as will other internal Unix systems, to provide a centralised repository of logs. These will be regularly backed-up, for reference. The syslog server will based on a Linux 7.0 system, bastion hardened with PitBull, and using Tripwire for file integrity checking.

Internal DNS Server

Employees' desktop computers, and the internal service systems will use the internal DNS system for name resolution. The internal DNS system must not be accessible from the Internet. It will be bastion hardened in the same manner as the external DNS server.

Database Servers

Fortune cookie sayings are held on these database systems, along with the corporate data, such as accounting data required by the organisation. Corporate partners will be granted access to these database systems, along with the web servers which handle the web-based transactions of customers and suppliers.

The databases servers will run Oracle 9i database software, on Unix platforms, bastion hardened with PitBull. Application middleware will be developed in-house, which will broker supplier and purchaser requests from the e-commerce web site. The web servers will not have direct access to the databases. This limits the access the web servers have to the databases, and provides an extra layer of authentication.

Summary

This design is an attempt to apply the principle of defence-in-depth to GIAC Enterprises network architecture. A variety of hardware and software solutions have been used, to minimalise the risk of GIAC Enterprises' being successfully compromised using vulnerabilities discovered in the solutions being deployed.

Bastion hardening has also been a key element, since host-based defences, and damage limitation can play an important role in successfully repelling an attack.

Assignment 2 – Security Policy

Objectives

This report will outline appropriate policy and configuration for the network security architecture defined in the last section. GIAC Enterprises will require the most secure policy possible, and so this policy will be tailored to implement a policy of 'default deny'.

In addition, it has been stipulated that no authenticating protocols, which do not use encryption will be blocked outbound on the border router.

Global policy

The IT Security department will be responsible for developing and maintaining the global security policy for GIAC Enterprises. The policy will consider key areas of security, such as:

- Physical security
- Password policy
- Disaster recovery
- Virus incident management
- Security incident management
- Auditing

A full analysis of GIAC Enterprises' security policy is beyond the remit of this report, but the following policies are relevant to the network security architecture:

Password policy
System service passwords (e.g. root, Administrator) must be changed at least once a month. Employees' passwords must be changed every 3 months. The following guidelines will apply, when choosing passwords:

In order to be safe and secure passwords **MUST**

1. Be at least 8 characters in length

2. Contain characters from **3** of the following groups:
   Uppercase letters A,B,C... Z
   Lowercase letters a,b,c... z
   Numerals 0,1,2... 9
   Special characters -_ ! * ^ + = [ ]

3. Avoid **any** of the following:
   - Proper names
   - Place names
   - Brand, product or company names
   - Ordinary words
   - Obscene words or derivatives of them

4. Avoid simple letter/numeric substitutions in any of the above, e.g. substituting zeroes and ones for the letters O and L.

5. Not be based upon previous passwords

Hardware failure
Where possible, spares will be kept, to allow the complete replacement of networking equipment, or server systems providing external services. Maintenance contracts should exist for this equipment, which guarantees on-site repair or replacement of the system, within 24 hours.

Auditing
Networking equipment, and server systems providing external services will be audited on a bi-weekly basis. Where access control lists exist on networking equipment and firewalls, they will be tested to ensure they function as expected.

GIAC Enterprises' Address Space

To clarify the policies defined for the network architecture, it is necessary to first define the private and public IP addresses used by GIAC Enterprises. These are as follows:

Public IP Addresses
GIAC Enterprises have purchased a Class 'C' network, consisting of previously reserved address space (see RFC1466 for details of reserved address space). The IP addresses purchased are the range 219.1.1.0 – 219.1.1.255. The following public IP addresses will be assigned:

Mail Server =	219.1.1.5	(mail.giac-enterprises.com)
External DNS Server =	219.1.1.6	(nameit.giac-enterprises.com)
Corporate Web Site =	219.1.1.10	(www.giac-enterprises.com)
E-Commerce Web Site =	219.1.1.15	(commerce.giac-enterprises.com)
VPN =	219.1.1.240	(not registered)
Web Cache Servers = (Volera Excelerator Systems)	219.1.1.50 – 219.1.1.52	(not registered)

The web site addresses represent the publicly advertised address of the sites. In reality, the Alteon switch and Excelerator systems will perform load-balancing operations.

Private IP Addresses
The Internal Network will use private address space (see RFC 1918). GIAC Enterprises has decided to use the range 192.168.0.0 – 192.168.255.255. The following important addresses should be noted:

Exchange Servers =	192.168.3.2 – 192.168.3.5	(exchange1.giac-internal.com, etc.)
Database Server 1 =	192.168.4.2	(hr-data.giac-internal.com)
Database Server 2 =	192.168.4.3	(fortune-data.giac-internal.com)
Internal DNS Server =	192.168.5.2	(dns.giac-internal.com)
Syslog Server =	192.168.5.3	(syslog.giac-internal.com)
Snort IDS systems =	192.168.8.2 – 192.168.8.3	(snort1.giac-internal.com, etc.)

The DNS information will only be available internally.

Border Router Policy

The border routers will be used to enforce policies to block certain types of traffic not welcome from the Internet, and also to filter out traffic from spoofed addresses. The following services will be publicly available:

- ❑ DNS
- ❑ Mail
- ❑ Web (www.giac-enterprises.com)
- ❑ Secure web (https://commerce.giac-enterprises.com)
- ❑ VPN services to corporate partners

Securing the Routers

Best practices will be observed, when setting up the routers, to ensure that they are secured as much as possible. Following the guidelines of the SANS Firewall course, these options will be used when configuring the router:

service password-encryption
encrypts passwords, when displayed

no ip unreachables
prevents ICMP replies to network scans

no ip-source route
blocks packets which have source routing options set

no snmp
disables SNMP management of the router

logging 192.168.5.3
logs to the internal Syslog server

banner / Unauthorised access prohibited /
creates a warning banner on all remote administration interfaces

Inbound Traffic

An extended access-list will be used for the incoming traffic, to give the maximum flexibility. The access-list will be created on the routers for the interface to the respective ISP. The access-list will be defined as:

```
ip access-list extended inbound
ip access-group inbound in
```

The access-lists for each direction will now be defined, including explanations for each entry.

Inbound Traffic

Ingress Filtering

Description: Following recommendations in RFC1918, the border router will drop network packets where the source or destination is in the private IP address space. In addition, packets with source or destination of the reserved loopback IP address will also be dropped.

CLI:
```
access-list inbound deny ip 10.0.0.0 0.255.255.255 any log
access-list inbound deny ip 192.168.0.0 0.0.255.255 any log
access-list inbound deny ip 172.16.0.0 0.240.255.255 any log
access-list inbound deny ip 205.150.100.0 0.0.0.240 any log
access-list inbound deny ip host 127.0.0.1 any log

access-list inbound deny ip any 10.0.0.0 0.255.255.255 log
access-list inbound deny ip any 192.168.0.0 0.0.255.255 log
access-list inbound deny ip any 172.16.0.0 0.240.255.255 log
access-list inbound deny ip any 205.150.100.0 0.0.0.240 log
access-list inbound deny ip any host 127.0.0.1 log
```

Broadcast Addresses

Description: Incoming packets, with destination address set to the broadcast addresses will be dropped. This should prevent the network being used for Smurf attacks.

CLI:
```
no ip direct-broadcast log
```

GIAC Enterprises have decided that certain insecure services should never be granted access to the network. Therefore, the following access-list entries will be explicitly included, even though later policies will ensure that these services would be implicitly denied. This will enforce the 'deny' policy, even in the event of a later change to the access policy.

Block insecure Unix services

Description: Unix systems provide a number of services, which GIAC Enterprises have decided they would not wish to allow publicly, under any circumstances.

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

prevent access to the echo, chargen, discard services running on Unix systems. These services are used largely for development purposes, and so there is no reason to provide these services publicly.

```
no service  finger
```

prevent access to the finger service running on Unix servers, which can give information on valid accounts on the server.

```
access-list inbound deny tcp any any range 512 514 log
```

block requests to insecure r-services – rsh, rexec, rlogin

```
access-list inbound deny tcp any any eq 23 log
```

block telnet, which passes authentication information in clear-text

```
access-list inbound deny ip any any eq 111 log
```

block access to Unix portmapper service , which provides information on RPC services running on a system.

Block NetBIOS traffic

Description: Due to the large number of NetBIOS scans which occur on the Internet, it has been decided to block these requests explicitly at the border routers.

CLI:

```
access-list inbound deny ip any any range 135 139
access-list inbound deny ip any any eq 445
```

Block FTP traffic

Description: Block FTP traffic, which handles authentication and file transfer in clear-text.

CLI:

```
access-list inbound deny tcp any any eq 21 log
```

The following access-list entries explicitly permit certain public services to be accessed from the Internet:

Access to Public DNS Server

Description: External systems will be permitted to gain access to the organization's DNS server. The server will respond to UDP only, to prevent zone transfers.

CLI:

```
access-list inbound permit udp any host 219.1.1.6 eq 53
```

Access to Mail Server

Description: GIAC Enterprises will require that external systems can access their mail server, to deliver email.

CLI:

```
access-list inbound permit tcp any host 219.1.1.5 eq smtp
```

Access to Web Services

Description: The corporate web site, and secure e-commerce site must be accessible externally. A reflexive ACL could be used, since the web sites will not initiate connections, but it has been decided, for performance reasons, not to do this. Instead, the firewall will be used to permit responses to established connections only.

CLI:

```
access-list inbound permit tcp any host 219.1.1.10 eq http
access-list inbound permit tcp any host 219.1.1.15 eq 443
```

Corporate Partner Access to VPN

Description: As defined in the previous section, corporate partners will be able to access the fortune cookie databases, using VPN services provided by the NetScreen firewall. For each corporate partner a rule will exist to permit them access the VPN. For illustrative purposes, the access-list entry for their partner, Hollywood-One-Liners Corp. has been included below. Both the ISAKMP and ESP protocols must be permitted.

CLI:

```
access-list inbound permit udp host 220.10.10.76 host 219.1.1.240 eq 500 log
access-list inbound permit 50 host 220.10.10.76 host 219.1.1.240 log
```

Outbound Traffic

The access-list for outbound traffic will be simpler than that for inbound traffic. It will be used to prevent unauthorised traffic leaving the organisation. Again, an extended ACL will be used:

```
ip access-list extended outbound
ip access-group outbound out
```

For the most part these rules are mirrors of the rules applied to the inbound interface.

Egress Filtering

Description: An access-list will be applied to prevent packets from the internal network being routed onto the Internet. The access-list will also block other private (RFC1918) addresses from being routed. The access-list entries are a copy of the ones used to enforce ingress filtering.

CLI:

```
access-list outbound deny ip 10.0.0.0 0.255.255.255 any log
access-list outbound deny ip 192.168.0.0 0.0.255.255 any log
access-list outbound deny ip 172.16.0.0 0.240.255.255 any log
access-list outbound deny ip 205.150.100.0 0.0.0.240 any log
access-list outbound deny ip host 127.0.0.1 any log

access-list outbound deny ip any 10.0.0.0 0.255.255.255 log
access-list outbound deny ip any 192.168.0.0 0.0.255.255 log
access-list outbound deny ip any 172.16.0.0 0.240.255.255 log
access-list outbound deny ip any 205.150.100.0 0.0.0.240 log
access-list outbound deny ip any host 127.0.0.1 log
```

Access to Public DNS Server

Description: The public DNS server will perform recursive lookups for clients on the internal network, so must be permitted to initiate outbound DNS requests.

CLI:

```
access-list outbound permit udp host 219.1.1.6 any eq 53
```

Access to Mail Server

Description: The mail server will deliver outgoing email; so it will need to initiate SMTP connections to mail hosts on the Internet.

CLI:

```
access-list outbound permit tcp host 219.1.1.5 any eq smtp
```

Access to Web Services

Description: GIAC Enterprises' web sites will only be permitted to respond to HTTP and HTTPS requests.

CLI:

```
access-list outbound permit tcp host 219.1.1.10 eq http any
access-list outbound permit tcp host 219.1.1.15 eq 443 any
```

Corporate Partner Access to VPN

Description: The VPN will permitted to return traffic to requests. The access-list entry for Hollywood-One-Liners Corp. has been used again, for consistency. Again, both the ISAKMP and ESP protocols must be permitted.

CLI:

```
access-list outbound permit udp host 220.10.10.76 host 219.1.1.240 eq 500 log
```

```
access-list outbound permit 50 host 220.10.10.76 host 219.1.1.240 log
```

Additional Considerations

The policy for the border routers outlined above uses a ‘default deny’ policy, and we have clearly defined the access-lists which permit systems to have access the Internet. Certain services have been explicitly denied, to enforce GIAC Enterprises’ policy, that insecure protocols will never be used on the network. If the case arises that additional network access is granted to a server in future, the explicitly denied services must still remain blocked.

Firewall Policy

The clustered NetScreen firewalls will be used to control access to the public servers on the DMZ, and the employees' systems on the internal network. Again a 'default deny' policy will be enforced, with access being explicitly defined, to prevent a system being exposed through oversight. The NetScreen system uses IEEE 802.1Q compliant VLANs to separate virtual firewalls. The VLANs defined in the network design diagram in previous section will be used to separate the DMZ, and internal networks. The VLAN numbering system will be:

DMZ (Screened Service Network)	=	10
Internal Network =		50

Policies will be defined separately for each virtual firewall on the NetScreen system. Identical ACL's will be applied to both firewalls in the cluster. The virtual system for the DMZ will be created as follows:

```
set vlan dmzvlan tag 10
```

creates a VLAN definition in the firewall

```
set interface trust/10 ip 219.1.1.0 255.255.255.0 vlan dmzvlan
```

defines the interface for the VLAN

```
set vsys dmz
enter vsys dmz
```

define and enter a virtual system

```
set interface trust/10
```

binds the defined interface with the virtual system

Similarly, for the internal network VLAN:

```
set vlan internalvlan tag 50
set interface trust/50 ip 192.168.1.0 255.255.0.0 vlan internalvlan
set vsys internal
enter vsys internal
set interface trust/50
```

The access policies for the DMZ and the Internal network will be defined separately, as each policy is applied to its respective virtual system.

Many of the pre-defined services configured into NetScreen firewalls are reflexive, so that only one service need be defined to permit client requests and server replies to standard network services, such as DNS, and SMTP.

DMZ (Screened Service Network)

The virtual firewall used to control access to the DMZ will be applied to VLAN 10. All access to and from the DMZ will be explicitly defined. The NetScreen firewalls use pre-defined IP addresses, in an 'Address Book', to which policies can be applied. For the purposes of implementing the firewall policy, the following addresses will be configured for the DMZ virtual system:

```
set address trust “DMZ Servers” 219.1.1.0 255.255.255.0
set address trust “Mail Server” 219.1.1.5 255.255.255.255
set address trust “Public DNS Server” 219.1.1.6 255.255.255.255
set address trust “Web” 219.1.1.10 255.255.255.255
set address trust “EWeb” 219.1.1.15 255.255.255.255
set address trust “Web Caches” 219.1.1.50 255.255.255.52

set address untrust “Internal Network” 192.168.0.0 255.255.0.0
set address untrust “Exchange Servers” 192.168.3.0 255.255.255.0
set address untrust “Database Servers” 192.168.4.0 255.255.255.0
set address untrust “Internal DNS Server” 192.168.5.2 255.255.255.255
set address untrust “Syslog Server” 192.168.5.3 255.255.255.255
set address untrust “IDS Systems” 192.168.8.0 255.255.255.0
```

Mail Server

Description: The mail server will receive incoming mail, and deliver it to the Exchange servers. It will also deliver mail to the Internet, received from the Exchange Servers.

CLI:
```
set policy incoming “outside any” “Mail Server” SMTP permit
set policy outgoing “Mail Server” “outside any” SMTP permit
```

Public DNS Server

Description: The public DNS server will handle DNS lookups for clients, as well as providing DNS information for GIAC Enterprises to external systems. On NetScreen systems, the pre-defined DNS service applies only to the UDP protocol.

CLI:
```
set policy incoming “outside any” “Public DNS Server” DNS permit
set policy outgoing “Public DNS Server” “outside any” DNS permit
```

Web Servers

Description: GIAC Enterprises’ corporate web site will be accessible publicly, as will their e-commerce site, via HTTPS

CLI:
```
set policy incoming “outside any” “Web” HTTP permit
set policy outgoing “Web” “outside any” HTTP permit
set policy incoming “outside any” “EWeb” HTTPS permit
set policy outgoing “EWeb” “outside any” HTTPS permit
```

Web to Database Communication

Description: The e-commerce web site will communicate with the backend databases using encrypted ADSI.

CLI:
```
set service MSSQL-TCP protocol tcp src-port 0-65535 dst-port 1433 reflect
set policy incoming “Database Servers” “EWeb” MSSQL-TCP permit
set policy outgoing “EWeb” “Database Servers” MSSQL-TCP permit
```

Web-proxy Services

Description: The web-cache systems will handle web requests for clients in the internal network.

CLI:
```
set service HTTP-PROXY protocol tcp src-port 0-65535 dst-port 8080 reflect
set policy incoming “Internal Network” “Web Caches” HTTP-PROXY permit
set policy outgoing “Web Caches” “Internal Network” HTTP-PROXY permit
set policy outgoing “Web Caches” “outside any” HTTP permit
set policy incoming “outside any” “Web Caches” HTTP permit
set policy outgoing “Web Caches” “outside any” HTTPS permit
set policy incoming “outside any” “Web Caches” HTTPS permit
```

Syslog Server

Description: All servers in the DMZ will be permitted to log to the internal Syslog server.

CLI:

```
set policy outgoing “DMZ Servers” “Syslog Server” SYSLOG permit
set policy incoming “Syslog Server” “DMZ Servers” SYSLOG permit
```

SSH Access

Description: Systems in the DMZ will be managed via SSH

CLI:

```
set policy incoming “Internal Network” “DMZ Servers” ssh permit
set policy outgoing “DMZ Servers” “Internal Network” ssh permit
```

Internal Network

The employees of GIAC Enterprises, and the data systems will reside on the internal network. They will be restricted in their operations, to provide the maximum resistance to Internet threats. In fact, the internal network will not be permitted to communicate directly with the Internet at all. The public servers on the DMZ will provide proxying services for mail, DNS, and web. This allows simpler monitoring too. The virtual firewall system controlling access to the internal network is separate from the one controlling access to the DMZ, and in fact the two are managed on different IP addresses, with different administrator passwords. As before, all addresses must first be defined in the address book, before policies can be applied:

```
set address trust “Internal Network” 192.168.0.0 255.255.0.0
set address trust “Exchange Servers” 192.168.3.0 255.255.255.0
set address trust “OWA Exchange Server” 192.168.3.10 255.255.255.255
set address trust “Database Servers” 192.168.4.0 255.255.255.0
set address trust “Internal DNS Server” 192.168.5.2 255.255.255.255
set address trust “Syslog Server” 192.168.5.3 255.255.255.255

set address untrust “DMZ Servers” 219.1.1.0 255.255.255.0
set address untrust “Mail Server” 219.1.1.5 255.255.255.255
set address untrust “Public DNS Server” 219.1.1.6 255.255.255.255
set address untrust “Web” 219.1.1.10 255.255.255.255
set address untrust “EWeb” 219.1.1.15 255.255.255.255
set address untrust “Web Caches” 219.1.1.50 255.255.255.52
set address untrust “IDS Systems” 192.168.8.0 255.255.255.0
set address untrust “Corporate Partners” 220.10.10.76 255.255.255.255
```

These policies will be applied:

Exchange Access

Description: The Exchange Mail Servers will send and receive mail via the mail server on the DMZ network.

CLI:

```
set policy incoming “Mail Server” “Exchange Servers” SMTP permit
set policy outgoing “Exchange Servers” “Mail Server” SMTP permit
```

Outlook Web Access

Description: Travelling Employees can check their mail on the E-Commerce server, using the Outlook Web Access product. The E-Commerce server will need to communicate with the Exchange servers, to retrieve data, using Microsoft TechNet articles Q155831 and Q148732 to set the port to TCP port 135, which the Exchange server, and the MAPI client on the E-Commerce Server will use for communication. NetBIOS will also need to be permitted, for authentication. Only one of the Exchange servers will permit connections in this manner, to limit the exposure.

CLI:
```
set service EXCHANGE protocol tcp src-port 0-65535 dst-port 135 reflect
set policy incoming “EWeb” “OWA Exchange Server” EXCHANGE permit log
set policy outgoing “OWA Exchange Server” “EWeb” EXCHANGE permit log
set policy incoming “EWeb” “OWA Exchange Server” NETBIOS permit log
set policy outgoing “OWA Exchange Server” “EWeb” NETBIOS permit log
```

Web to Database Communication

Description: The e-commerce web site will communicate with the databases on the internal network.

CLI:
```
set service MSSQL-TCP protocol tcp src-port 0-65535 dst-port 1433 reflect
set policy incoming “EWeb” “Database Servers” MSSQL-TCP permit
set policy outgoing “Database Servers” “EWeb” MSSQL-TCP permit
```

Web-proxy Services

Description: The web-cache systems will handle web requests for clients in the internal network.

CLI:
```
set service HTTP-PROXY protocol tcp src-port 0-65535 dst-port 8080 reflect
set policy outgoing “Internal Network” “Web Caches” HTTP-PROXY permit
set policy incoming “Web Caches” “Internal Network” HTTP-PROXY permit
```

Syslog Server

Description: All servers in the DMZ, and the Snort IDS systems will be permitted to log to the internal Syslog server.

CLI:
```
set policy incoming “DMZ Servers” “Syslog Server” SYSLOG permit
set policy outgoing “Syslog Server” “DMZ Servers” SYSLOG permit
set policy incoming “IDS Systems” “Syslog Server” SYSLOG permit
set policy outgoing “Syslog Server” “IDS Systems” SYSLOG permit
```

SSH Access

Description: Internet network systems will be allowed to administer DMZ systems with SSH.

CLI:
```
set policy outgoing “Internal Network” “DMZ Servers” ssh permit
set policy incoming “DMZ Servers” “Internal Network” ssh permit
```

VPN Access to Database Servers

Description: This policy will allow Corporate Partners (in this case, Hollywood-One-Liners Corp.) to access the database servers. The policy is defined in one direction, but implicitly incoming connections are also permitted. The VPN is defined in the next section.

CLI:
```
set policy outgoing “Database Servers” “Corporate Partners” any encrypt
```

VPN Policy

As specified before, GIAC Enterprises' corporate partners will use a VPN to connect to the database servers holding the fortune cookie sayings, and transaction data. This provides the maximum flexibility for integration of business ventures.

It has been decided that the VPN features offered by the NetScreen firewalls will be used to implement a VPN between these partners and the database servers. The access policy defined for the internal network has been purposely defined to be as strict as possible – with systems on the internal network having no direct access to the Internet. This simplifies the configuration of the border routers and firewall, because no NAT needs to be done – application proxy servers handle client requests, and limit the access to the Internet, which clients on the internal network can have.

The drawback of this approach is that the external interface to the firewall must be publicly addressable, as the firewall will act to tunnel VPN communications between the database servers and the corporate partners. It has been decided that the simplicity of this solution, and extra protection this affords the database servers is worth the risk. The border router policy should also block access attempts to the VPN tunnel gateway (firewall external interface), from unauthorised hosts on the Internet.

Manual keys will be used in the VPN, as this will allow GIAC Enterprises the greatest control over the issuing of keys, and their revocation. The NetScreen firewalls only support limited options when using IKE (phase 1 proposal "pre-g2-des-md5"), which is also a factor. Using manual keys usually places a large administrative overhead on the management of a VPN, but in this case only key corporate partners will be granted access via VPN, and so this should not prove to be a problem.

The VPN tunnel will use ESP, to allow the data contents of packets to be encrypted. It was decided that protection of the data passing over the Internet was of more importance than the advanced authentication offered by the AH protocol.

The following setup guide has been adapted from the NetScreen 1000 User's Guide. The following parameters will be used to set up the VPN tunnel on the NetScreen firewalls:

- VPN tunnel name: Corp_Part
- VPN method: Manual
- Local security index number: 4444
- Remote security index number: 5555
- Header type: Encapsulating Security Payload (ESP)
- Encryption method: 3DES-CBC encryption algorithm
- Hex Key: c2c4c70101010101 f8899b6e6d7c8f9e 4f5b68b094a4b6c7
- Authentication Method: 128-bit Message Digest version 5 (MD5) hash
- Hex Key: c8cbcd0101010101 a4b6439e8c9faeb1

Using these options, the VPN is set up with the following command on the NetScreen firewalls:

```
set vpn "Corp_Part" manual 4444 5555 gateway 219.1.1.240 esp 3des
c2c4c70101010101 f8899b6e6d7c8f9e 4f5b68b094a4b6c7 auth md5
```

Internal Service Network Firewall

For the most part, the policies on the internal Checkpoint FW-1 firewall will mirror those installed on the NetScreen system, on the internal network virtual system. The most notable exception will be a rule permitting the NT domain servers on the internal network to communicate with the Exchange Server, installed as a BDC, for authentication purposes. All authentication can be done via this system, rather than exposing all the NT domain controllers in the domain.

Assignment 3 – Audit your Security Architecture

Overview

GIAC Enterprises have deployed the network architecture and polices defined in the previous sections. The IT Security department is charged with the task of verifying that the components of the perimeter network are secure, and that the security measures have been correctly configured. A network audit is suggested, broken into two parts: an external audit of the perimeter, and an internal audit, from inside the corporate network.

Planning

As outlined, the network perimeter will be audited from the outside, and from inside the perimeter. Both audits will be performed twice, one during office hours, and the other during the night, to test for time dependant vulnerabilities. Once the audit infrastructure has been established, regular audits will take place monthly – without prior warning, so that systems administrators cannot anticipate them.

The external audit will be undertaken, with an assumption of no prior knowledge of GIAC Enterprises' network. Enumeration techniques will be employed to gain information about the network. Using the information gained, the network perimeter will be probed for weaknesses. The external audit will be conducted using the following basic framework:

- ❑ Enumeration
  - o Information available on web
    web search-engines, financial websites, GIAC Enterprises corporate website
  - o Registered domain information
    IANA domain registration information, information from GIAC Enterprises' DNS server
  - o Network Scan
    network scan, using nmap, and Nessus tools
- ❑ Vulnerability testing
  - o Publicly accessible services
    version checking of mail and DNS services, for published vulnerabilities
  - o Web Services
    vulnerability scan using Retina tool
  - o IDS detection of attempted compromises
    Snot used to test Snort successfully matches attack signatures

The audit undertaken inside the network will test host-based security, consisting of a vulnerability scan, using Nessus and password cracking exercises using L0phtcrack, and John the Ripper.

The IT Security department offer the following cost estimates, based upon a rate of $30 per man hour:

External audit cost estimate

Task	Estimated Time Cost	Estimated Cost
Enumerating information available on web	2 person hours	$60
Enumerating publicly registered domain information	1 person hour	$30
Network scan	1 person hour	$30
Probing publicly accessible services	2 person hours	$60
Probing web services	5 person hours	$150
Verifying IDS detection	5 person hours	$150
Producing report	8 person hours	$240
Total	24 person hours	$720

Internal audit cost estimate

Task	Estimated Time Taken	Estimated Cost
Vulnerability scan	3 person hours	$90
Password cracking	2 person hours	$60
Producing report	6 person hours	$180
Total	11 person hours	$330

External Audit

Following the guidelines above, the audit was conducted twice, at different times of the day, and the results collated. The cooperation of an external ISP was sought, to provide a connection for the external audit. In this way, the auditors will be subject to the same access restrictions as members of the public.

Enumeration

Information available on web

The search engines proved useful for finding the names of the CEO and senior staff of GIAC Enterprises, since their names were associated with sections on the corporate web site, and public financial information available on the company. In addition, the search found newsgroup postings to technical forums, sent by GIAC Enterprises' employees.

This information represents valuable data to potential hackers, who could use the executives' names provided for social engineering purposes. The newsgroup postings give away valuable information about the types of technology used in the organisation, and the skill level of the staff.

Registered domain information

The IANA domain registration information revealed the public IP addresses used by the organisation, as well as the network manager for the GIAC Enterprises domain. The Public IP address information would be useful for scanning, whilst the network manager contact is another possibility for social engineering.

Network Scan

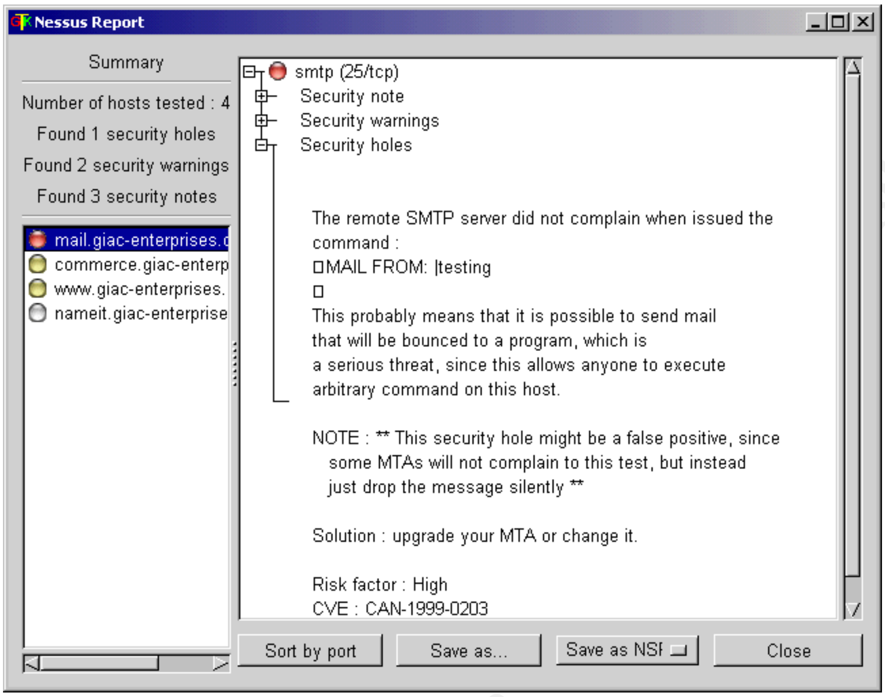
The public IP addresses registered to GIAC Enterprises (219.1.1.0/24) were scanned using nmap. The output results are shown below:

```
Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
# Nmap (V. nmap) scan initiated 2.53 as: nmap -oM - 219.1.1.0/24
Host: 219.1.1.5 ()    Ports: 25/open/tcp//smtp///     Ignored State: closed (0)
Host: 219.1.1.6 ()    Ports: 53/open/tcp//domain///   Ignored State: closed (0)
Host: 219.1.1.10 ()   Ports: 80/open/tcp//http///     Ignored State: closed (0)
Host: 219.1.1.15 ()   Ports: 443/open/tcp//https///   Ignored State: closed (0)
# Nmap run completed at Thu Aug  9 16:05:20 2001 -- 256 IP address (4 host up) scanned
in 100 seconds
```

The ports found to be open all match the expected publicly accessible ports, which would indicate that the border router and firewall have been correctly configured, to drop ICMP reply (ping) requests, and to block access attempts to unauthorised services.

The session-based blocking on the web caches would also appear to be functioning correctly, since no reply was received from these systems, with the border router being configured to only allow established sessions.

Following the nmap scan, Nessus was used to scan the network for vulnerabilities. The output report is shown below, with the full output included in Appendix A.



Number of hosts tested : 4
Found 1 security holes
Found 2 security warnings
Found 3 security notes

mail.giac-enterprises.c
commerce.giac-enterp
www.giac-enterprises.
nameit.giac-enterprise

smtp (25/tcp)
Security note
Security warnings
Security holes

```
The remote SMTP server did not complain when issued the
command :
□MAIL FROM: |testing
□
This probably means that it is possible to send mail
that will be bounced to a program, which is
a serious threat, since this allows anyone to execute
arbitrary command on this host.

NOTE : ** This security hole might be a false positive, since
   some MTAs will not complain to this test, but instead
   just drop the message silently **

Solution : upgrade your MTA or change it.

Risk factor : High
CVE : CAN-1999-0203
```

Fig 2: Nessus report of external scan

As can be seen from the Nessus scan results, a number of issues were highlighted. The mail server was further investigated, and found not to be acting as an open mail relay, but silently dropping messages. Nessus can be prone to false-positives, but is available free and scans for a wide range of vulnerabilities.

The Nessus scan did correctly reveal the operating system of the web servers, however.

Vulnerability Testing

The enumeration techniques failed to reveal any obvious security problems, which could be used to compromise the site, but the additional information gained about the web servers means that they can be probed for Microsoft IIS-specific vulnerabilities.

Publicly accessible services

The public-facing services should be patched against vulnerabilities, since they represent an obvious route into the internal network, if the services can be compromised. Firstly, the mail server is queried, using a telnet connection to port 25:

```
# telnet mail.giac-enterprises.com 25
Trying 219.1.1.5...
Connected to mail.giac-enterprises.com (219.1.1.5).
Escape character is '^]'.
```

```
220 mail.giac-enterprises.com ESMTP Exim 3.31 #1 Fri, 10 Aug 2001 15:25:21 +0100
```

There is a vulnerability for this version of Exim, but the **headers_check_syntax** option is not enabled on GIAC Enterprises' mail server, so it is not vulnerable. The current release version of Exim is 3.32.

Next, the dig tool is used to query the DNS server:

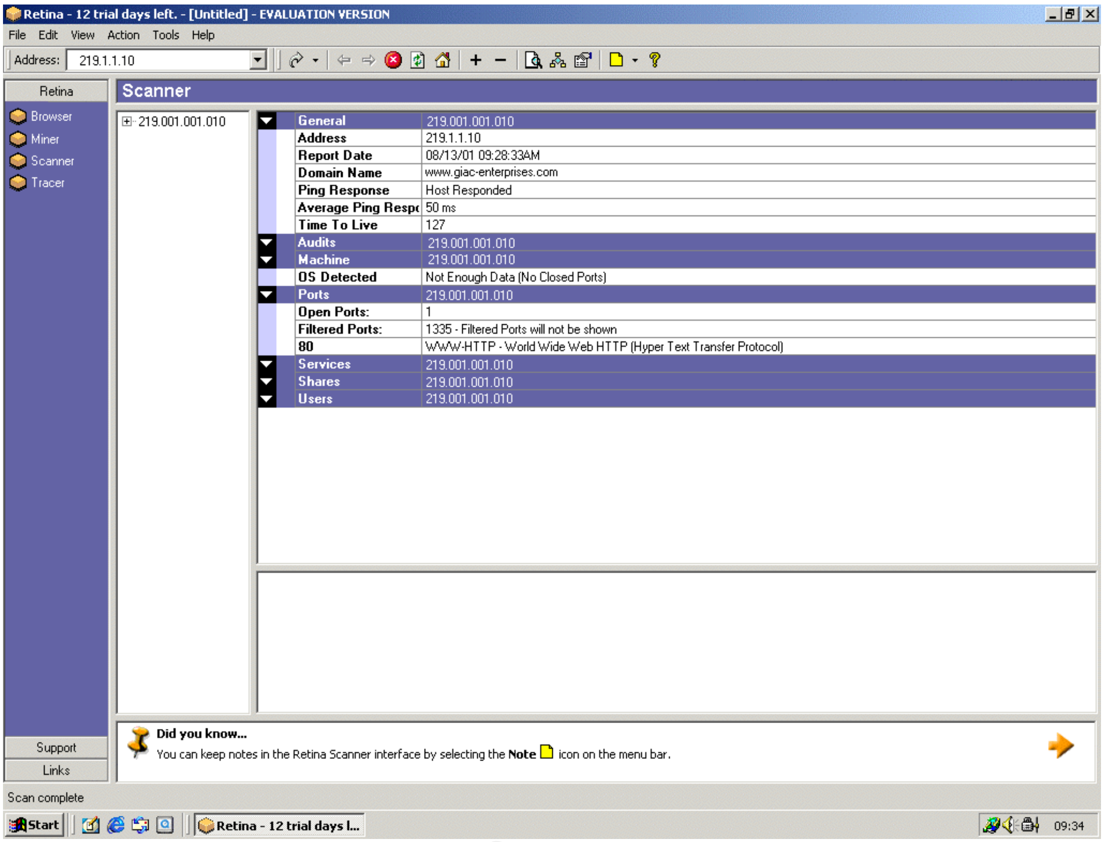
```
dig @219.1.1.6 version.bind txt chaos

; <<>> DiG 9.1.0 <<>> @219.1.1.6 version.bind txt chaos
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27851
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;version.bind.                  CH      TXT

;; ANSWER SECTION:
VERSION.BIND.           0       CH      TXT     "8.2.3-REL"

;; Query time: 64 msec
;; SERVER: 219.1.1.6 #53(219.1.1.6)
;; WHEN: Fri Aug 10 14:47:21 2001
;; MSG SIZE  rcvd: 64
```

This version of BIND does not have any vulnerabilities, although it is concerning that the chaos record was available, since it gives the current version of the server.

Since the operating system of the web services has already been identified, there is no need to enumerate these services, as they must be running IIS 5.0. The next phase of the audit will test them for vulnerabilities.

Web Services

The Retina scanner, available from eEye (www.eeye.com) was used to scan the corporate web site. The results are shown below:



General	219.001.001.010
Address	219.1.1.10
Report Date	08/13/01 09:28:33AM
Domain Name	www.giac-enterprises.com
Ping Response	Host Responded
Average Ping Respc	50 ms
Time To Live	127
Audits	219.001.001.010
Machine	219.001.001.010
OS Detected	Not Enough Data (No Closed Ports)
Ports	219.001.001.010
Open Ports:	1
Filtered Ports:	1335 - Filtered Ports will not be shown
80	WWW-HTTP - World Wide Web HTTP (Hyper Text Transfer Protocol)
Services	219.001.001.010
Shares	219.001.001.010
Users	219.001.001.010

Did you know...
You can keep notes in the Retina Scanner interface by selecting the Note icon on the menu bar.

Scan complete

Fig 3: Retina report of corporate web site scan

The scan does not highlight any problems, and the lack of information available in the scan indicates that the access restrictions are successfully working to limit the information available. The scan for the e-commerce site reveals the same results.

IDS detection of attempted compromises

To ensure that the IDS is functioning correctly, we shall choose the ten most common current exploits, with data extracted from the ARIS Predictor resource. From the report generated, the 10 most common attacks were listed as:

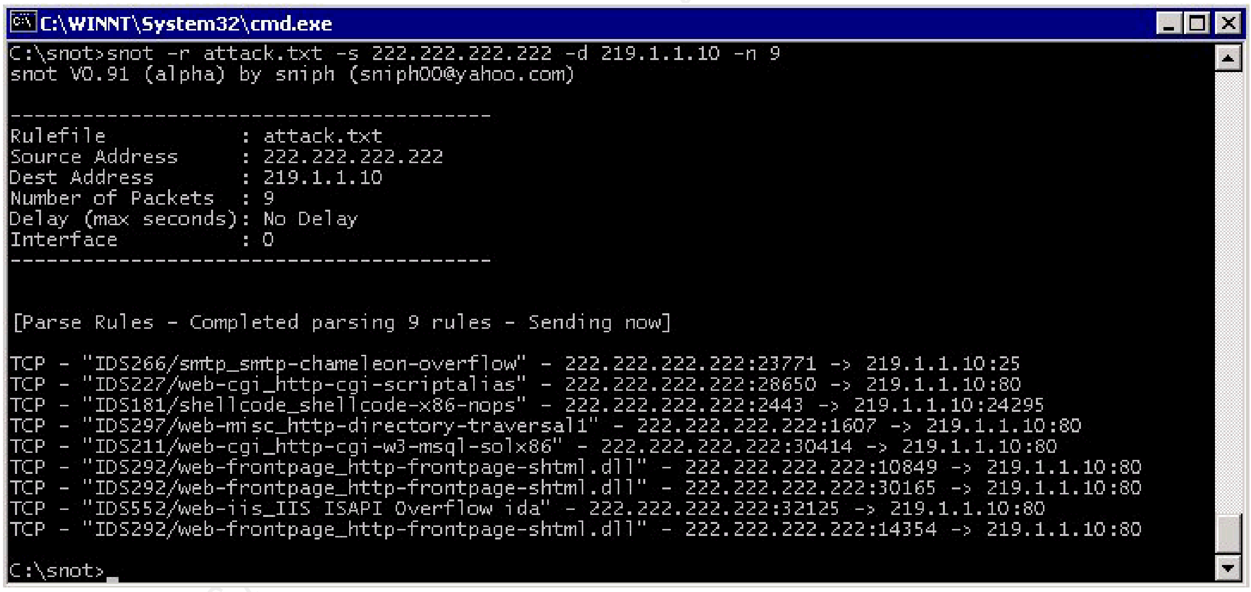
1. Microsoft Indexing Server/Indexing Services ISAPI Buffer Overflow Attack
2. Generic HTTP 'cmd.exe' Request Attack
3. Generic "../" Directory Traversal Attack
4. Microsoft FrontPage Server Extensions Probe
5. NCSA ScriptAlias CGI Source Disclosure Attack
6. Netmanage Chameleon SMTPD Buffer Overflow Attack
7. Microsoft FrontPage Server Extensions DoS Attack
8. Generic HTTP UNIX Shell
9. Microsoft FrontPage Server Extensions Path Disclosure Attack
10. Generic X86 Buffer Overflow (TCP NOPS) Attack

Cross-referencing these attacks with the arachNIDS database of rules, the following Snort IDS rules will be tested:

1. IDS552/web-iis_IIS ISAPI Overflow ida
2. (not present in arachNIDS rules)
3. IDS297/web-misc_http-directory-traversal1
4. IDS292/web-frontpage_http-frontpage-shtml.dll
5. IDS227/web-cgi_http-cgi-scriptalias
6. IDS266/smtp_smtp-chameleon-overflow
7. IDS292/web-frontpage_http-frontpage-shtml.dll
8. IDS211/web-cgi_http-cgi-w3-msql-solx86 (closest match)
9. IDS292/web-frontpage_http-frontpage-shtml.dll
10. IDS181/shellcode_shellcode-x86-nops

Using the Snort rules as a guide, Snot was then used to generate traffic which would trigger Snort to produce alerts, if the IDS system was working correctly. Traffic was directed at the corporate web site. Snot was given the rules above, to generate traffic which should trigger the Snort IDS.

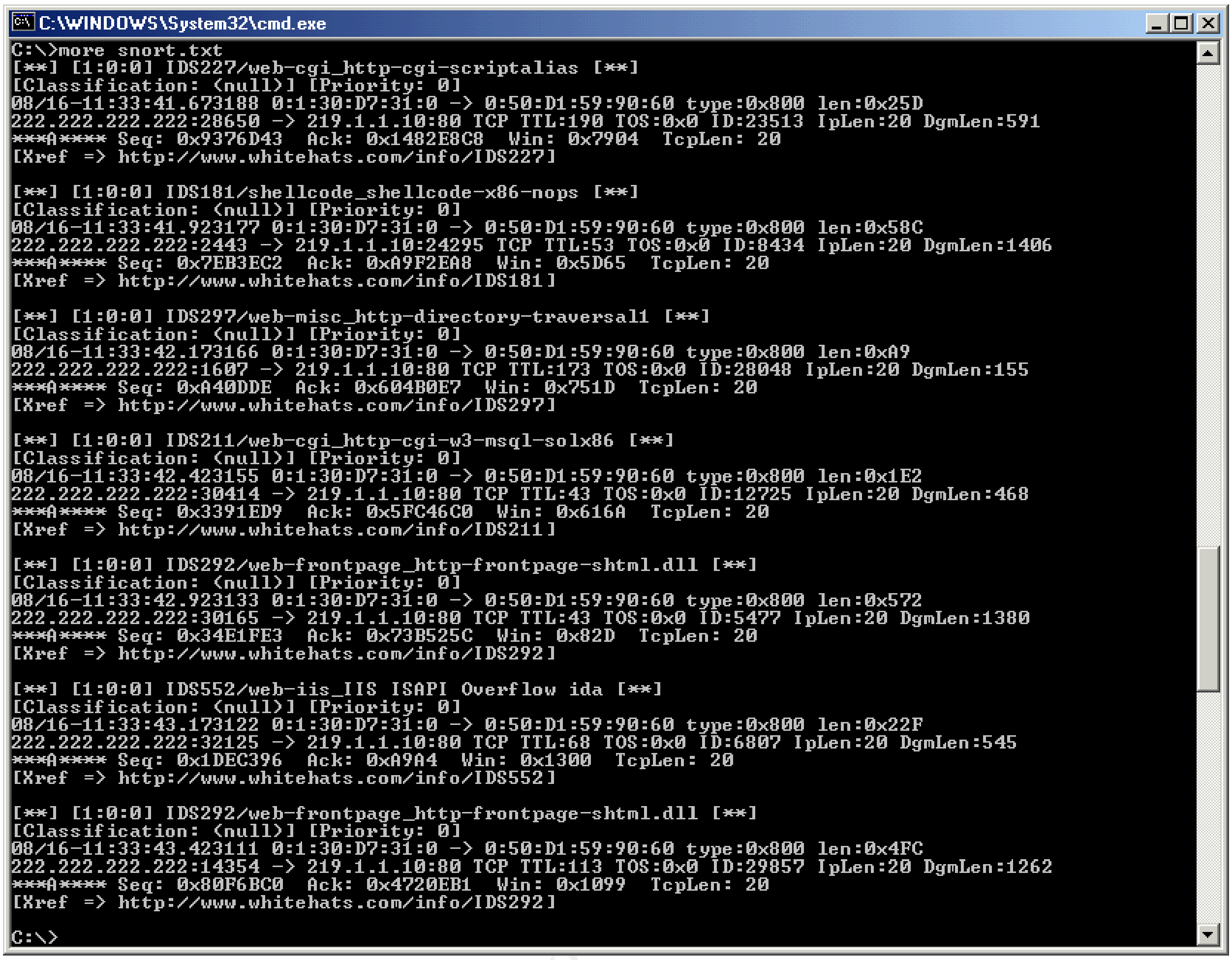
The ISP used to do the external audit has assigned the IT Security department an IP address of 222.222.222.222. Snot generated the following output:



```
C:\snot>snot -r attack.txt -s 222.222.222.222 -d 219.1.1.10 -n 9
snot V0.91 (alpha) by sniph (sniph00@yahoo.com)

----------------------------------------
Rulefile            : attack.txt
Source Address      : 222.222.222.222
Dest Address        : 219.1.1.10
Number of Packets   : 9
Delay (max seconds): No Delay
Interface           : 0
----------------------------------------


[Parse Rules - Completed parsing 9 rules - Sending now]

TCP - "IDS266/smtp_smtp-chameleon-overflow" - 222.222.222.222:23771 -> 219.1.1.10:25
TCP - "IDS227/web-cgi_http-cgi-scriptalias" - 222.222.222.222:28650 -> 219.1.1.10:80
TCP - "IDS181/shellcode_shellcode-x86-nops" - 222.222.222.222:2443 -> 219.1.1.10:24295
TCP - "IDS297/web-misc_http-directory-traversal1" - 222.222.222.222:1607 -> 219.1.1.10:80
TCP - "IDS211/web-cgi_http-cgi-w3-msql-solx86" - 222.222.222.222:30414 -> 219.1.1.10:80
TCP - "IDS292/web-frontpage_http-frontpage-shtml.dll" - 222.222.222.222:10849 -> 219.1.1.10:80
TCP - "IDS292/web-frontpage_http-frontpage-shtml.dll" - 222.222.222.222:30165 -> 219.1.1.10:80
TCP - "IDS552/web-iis_IIS ISAPI Overflow ida" - 222.222.222.222:32125 -> 219.1.1.10:80
TCP - "IDS292/web-frontpage_http-frontpage-shtml.dll" - 222.222.222.222:14354 -> 219.1.1.10:80

C:\snot>_
```

Fig 4: Output from Snot IDS probing tool

In response to this probe, the Snort IDS systems correctly identified most of the spoofed packets generated. The output is shown over:



```
C:\>more snort.txt
[**] [1:0:0] IDS227/web-cgi_http-cgi-scriptalias [**]
[Classification: (null)] [Priority: 0]
08/16-11:33:41.673188 0:1:30:D7:31:0 -> 0:50:D1:59:90:60 type:0x800 len:0x25D
222.222.222.222:28650 -> 219.1.1.10:80 TCP TTL:190 TOS:0x0 ID:23513 IpLen:20 DgmLen:591
***A**** Seq: 0x9376D43  Ack: 0x1482E8C8  Win: 0x7904  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS227]

[**] [1:0:0] IDS181/shellcode_shellcode-x86-nops [**]
[Classification: (null)] [Priority: 0]
08/16-11:33:41.923177 0:1:30:D7:31:0 -> 0:50:D1:59:90:60 type:0x800 len:0x58C
222.222.222.222:2443 -> 219.1.1.10:24295 TCP TTL:53 TOS:0x0 ID:8434 IpLen:20 DgmLen:1406
***A**** Seq: 0x7EB3EC2  Ack: 0xA9F2EA8  Win: 0x5D65  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS181]

[**] [1:0:0] IDS297/web-misc_http-directory-traversal1 [**]
[Classification: (null)] [Priority: 0]
08/16-11:33:42.173166 0:1:30:D7:31:0 -> 0:50:D1:59:90:60 type:0x800 len:0xA9
222.222.222.222:1607 -> 219.1.1.10:80 TCP TTL:173 TOS:0x0 ID:28048 IpLen:20 DgmLen:155
***A**** Seq: 0xA40DDE  Ack: 0x604B0E7  Win: 0x751D  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS297]

[**] [1:0:0] IDS211/web-cgi_http-cgi-w3-msql-solx86 [**]
[Classification: (null)] [Priority: 0]
08/16-11:33:42.423155 0:1:30:D7:31:0 -> 0:50:D1:59:90:60 type:0x800 len:0x1E2
222.222.222.222:30414 -> 219.1.1.10:80 TCP TTL:43 TOS:0x0 ID:12725 IpLen:20 DgmLen:468
***A**** Seq: 0x3391ED9  Ack: 0x5FC46C0  Win: 0x616A  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS211]

[**] [1:0:0] IDS292/web-frontpage_http-frontpage-shtml.dll [**]
[Classification: (null)] [Priority: 0]
08/16-11:33:42.923133 0:1:30:D7:31:0 -> 0:50:D1:59:90:60 type:0x800 len:0x572
222.222.222.222:30165 -> 219.1.1.10:80 TCP TTL:43 TOS:0x0 ID:5477 IpLen:20 DgmLen:1380
***A**** Seq: 0x34E1FE3  Ack: 0x73B525C  Win: 0x82D  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS292]

[**] [1:0:0] IDS552/web-iis_IIS ISAPI Overflow ida [**]
[Classification: (null)] [Priority: 0]
08/16-11:33:43.173122 0:1:30:D7:31:0 -> 0:50:D1:59:90:60 type:0x800 len:0x22F
222.222.222.222:32125 -> 219.1.1.10:80 TCP TTL:68 TOS:0x0 ID:6807 IpLen:20 DgmLen:545
***A**** Seq: 0x1DEC396  Ack: 0xA9A4  Win: 0x1300  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS552]

[**] [1:0:0] IDS292/web-frontpage_http-frontpage-shtml.dll [**]
[Classification: (null)] [Priority: 0]
08/16-11:33:43.423111 0:1:30:D7:31:0 -> 0:50:D1:59:90:60 type:0x800 len:0x4FC
222.222.222.222:14354 -> 219.1.1.10:80 TCP TTL:113 TOS:0x0 ID:29857 IpLen:20 DgmLen:1262
***A**** Seq: 0x80F6BC0  Ack: 0x4720EB1  Win: 0x1099  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS292]

C:\>
```

Fig 5: Snort log generated by Snot probe

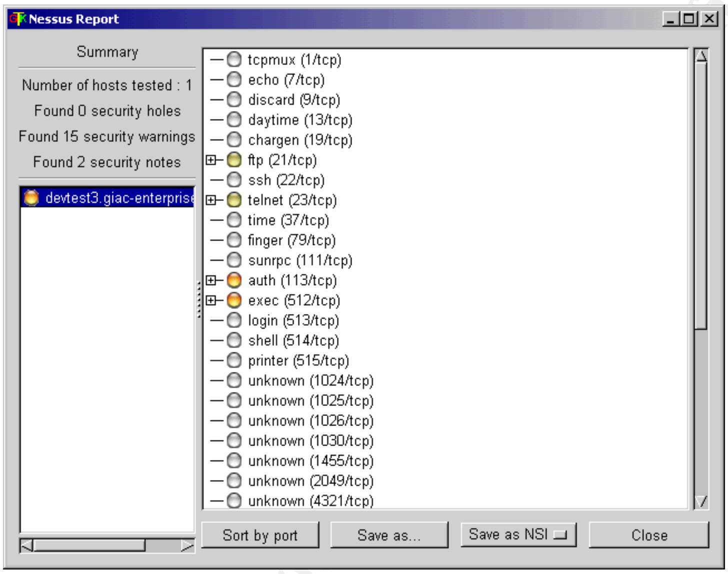
There seems to have been a problem with the first packet not being picked up by Snort, but on the whole, the performance seems to have been respectable. To better test that the vulnerability is picked up safely, an exploit would have to be found, which makes use of the Chameleon SMTPD vulnerability. However, since this product is not used in GIAC Enterprises, this is not a major concern.

Internal Audit

Once the external audit has been completed, the internal audit of the network is undertaken. It will consist of a vulnerability scanning exercise, again, using Nessus, and a password-cracking exercise, using the John the Ripper and L0phtcrack password cracking tools.

Vulnerability Scan

The internal Nessus scan included the publicly accessible servers in the DMZ. A large number of systems were scanned, and so the output shown below has been truncated, to display only serious security issues:



Summary

Number of hosts tested : 1
Found 0 security holes
Found 15 security warnings
Found 2 security notes

devtest3.giac-enterpris

```
— tcpmux (1/tcp)
— echo (7/tcp)
— discard (9/tcp)
— daytime (13/tcp)
— chargen (19/tcp)
⊞ ftp (21/tcp)
— ssh (22/tcp)
⊞ telnet (23/tcp)
— time (37/tcp)
— finger (79/tcp)
— sunrpc (111/tcp)
⊞ auth (113/tcp)
⊞ exec (512/tcp)
— login (513/tcp)
— shell (514/tcp)
— printer (515/tcp)
— unknown (1024/tcp)
— unknown (1025/tcp)
— unknown (1026/tcp)
— unknown (1030/tcp)
— unknown (1455/tcp)
— unknown (2049/tcp)
— unknown (4321/tcp)
```

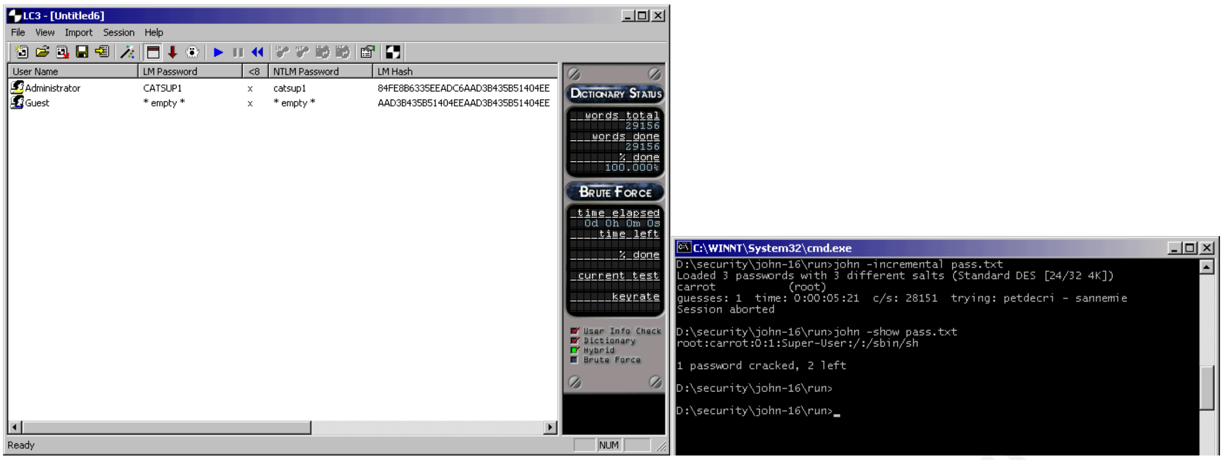
Fig6:Nessus scan of internal network

As the results show, a development system has not been locked down. This was the only unexpected result encountered.

Password Cracking

Having completed the network vulnerability scan, the IT Security department move onto the final phase of the audit: password auditing. As highlighted in the previous section, GIAC Enterprises has a clear policy governing the choice of passwords, and so to test that employees have been following these guidelines, the audit included the corporate Windows NT domain, which is used to administer employees' passwords, and the root passwords of the various Unix-based systems in use throughout the organisation.

The LC3 (formerly L0phtcrack) tool was used to crack the NT passwords, and the John the Ripper tool was used to crack passwords on Unix systems. Sample output is shown over:



User Name	LM Password	<8	NTLM Password	LM Hash
Administrator	CATSUP1	x	catsup1	84FE8B6335EEADC6AAD3B435B51404EE
Guest	* empty *	x	* empty *	AAD3B435B51404EEAAD3B435B51404EE

```
D:\security\john-16\run>john -incremental pass.txt
Loaded 3 passwords with 3 different salts (Standard DES [24/32 4K])
carrot           (root)
guesses: 1  time: 0:00:05:21  c/s: 28151  trying: petdecri - sannemie
Session aborted

D:\security\john-16\run>john -show pass.txt
root:carrot:0:1:Super-User:/:/sbin/sh

1 password cracked, 2 left

D:\security\john-16\run>

D:\security\john-16\run>_
```

Fig7:Output from LC3 and John the Ripper password cracking tools

The results of the password cracking exercise were rather worrying. On average, around 10% of employees' passwords were found to be vulnerable to either name-based, or dictionary attacks. In addition, a number of Unix systems' root passwords were cracked using John. This presented the largest problem of all and highlighted a real need for better employee education.

Conclusion and Recommendations

The security audit revealed a number of security problems within GIAC Enterprises, with the most worrying being the prevalent use of poor passwords within the organisation. Although the IT Security department makes efforts to educate employees to choose strong passwords, it is obvious that this measure is not proving entirely effective. To augment this, a password policy engine could be introduced into the organisation, which checked passwords as they were changed, to ensure that weak passwords could not be chosen. A product such as the Password Policy Enforcer (http://www.tpis.com.au) could be used to accomplish this.

The only other area, in which weaknesses were found, was the enumeration phase of the audit. Too much information relating to company employees could be obtained from the web. This could possibly be used in social engineering scenarios, to gain unauthorised access to systems. Although employees have been warned about social engineering, it would be prudent to replace public registration information with generic network manager details, and email address. Also, technical employees should be discouraged from posting information to newsgroups which could identify them as an employee of GIAC Enterprises.

On the whole, the perimeter defences performed well against attacks, with access controls successfully limiting access to the critical publicly accessible systems on the DMZ network. The Snort IDS also successfully identified many of the most popular attacks currently being used by hackers.

The real success of the audit will only be seen in subsequent scans, when improvements in vulnerable areas can be noted, and security awareness throughout GIAC Enterprises continually improves.

Assignment 4 – Design Under Fire

Objectives

To demonstrate the possibility of weaknesses in any security architecture design, this report will attempt to show how a successful malicious attack could be implemented on Gale Slentz's proposed architecture, shown below:

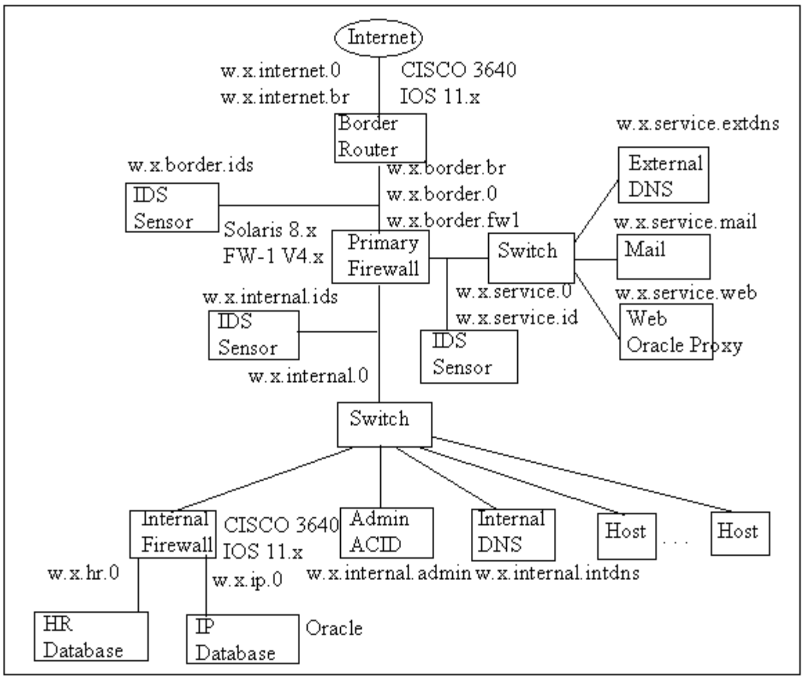


Fig8:Gale Slentz's proposed network architecture design

The attack will make use of network enumeration techniques, as well as exploiting known vulnerabilities with the security systems that Gale Slentz has chosen in her design.

The first step of the intrusion attempt will be to gain as much information about the security architecture as possible. In a similar approach to the audit exercise in the previous section, I first enumerate the network address space used by GIAC Enterprises, so that I can probe this range of addresses for information.

Disguising the Attack

Before probing the network for vulnerabilities, we will attempt to obscure my attacks by sending spoofed packets to GIAC Enterprises' public IP addresses. These spoofed packets will either be blocked by access control restrictions on the router and firewall, or cause the Snort IDS systems to trigger alert events. Their purpose is to create as much false information about my attacks as possible; to hide the network scans being performed at the same time.

To ensure that the spoofed traffic is a great an irritant as possible, we will use the Snot tool (http://www.sec33.com/sniph/) to generate packets which are designed to trigger alerts on Snort

IDS systems. Using a rule-set, such as the arachNIDS rules, Snot will generate a stream of packets with options and content specifically designed to match the rules file. The tool adds some degree of randomness to the packets, to make them more difficult to identify as Snot-generated traffic. A possible set of options would be:

```
snot –r vision.conf –d 219.1.1.0/24
```

For illustrative purposes, it has been assumed that GIAC Enterprises is still using the public address space 219.1.1.0/24.

Network Enumeration

Having obtained the domain registration information for GIAC Enterprises, the next step is to use a scanning tool, to see which systems and services can be accessed remotely. To do this, we will use the hping2 tool (http://freshmeat.net/projects/hping2/), which is an excellent tool for crafting arbitrary packets, and TCP-scanning systems.

From Gale Slentz's report, we can see that she has used nmap to test that the access control restrictions implemented on the router and firewall, are working as expected. However, only TCP connect, and SYN scans were used in this exercise. It is possible that the TCP stack implementation does not behave in an expected fashion on some of the exposed systems. To attempt to exploit this, we will use hping2 to perform a scan with only the ACK flag set, which may circumvent access controls on the router or firewall, and cause a publicly addressable system to respond. For example, this hping2 scan would scan the public web server for open ports:

```
hping2 www.giac-enterprises.com -A --frag -p ++
```

If any unexpected response was received from the public address space, this could be further investigated, to ascertain which services were available and whether they could be exploited.

Enumerating public services

Once the network scan has been completed, and assuming that the scan yields no successful connections, other than perhaps to public-facing services, the next phase of the attack will be to test these public services for weaknesses.

By connecting to the mail, web, and DNS servers, it is possible to gain a great deal of information about what platform they are running on, and in many cases the version of the software being used. Again, in a similar manner to the security audit, we connect to the public systems using telnet for the mail and web servers, looking for banner information to provide the version of software being used. For example:

```
[root@rottweiler /root]# telnet mail.giac-enterprises.com 25
Trying 155.198.34.10...
Connected to mail.giac-enterprises.com (219.1.1.5).
Escape character is '^]'.
220 mail.giac-enterprises.com ESMTP Exim 2.12 #1 Sun, 19 Aug 2001 09:01:49 +0100
```

```
quit
QUIT
Connection closed by foreign host.
```

In the case of the DNS server, dig will be used to attempt to gain the version of BIND being used. In any of these cases, if the version of the service running is not current, it may well be possible to exploit it. This is particularly the case with BIND, and the web services, which have recently been prone to several security vulnerabilities.

The SecurityFocus site (www.securityfocus.com) provides a good resource for searching for security vulnerabilities in any given software. Possible exploits for out-of-date services running might include:

BIND
TSIG Buffer Overflow
(BugTraq ID: 2302, this only affects version 8 of BIND).

ISC Bind 4 nslookupComplain() Buffer Overflow Vulnerability
(BugTraq ID: 2307, affects 4.9.x versions of BIND)

SendMail
Sendmail Unsafe Signal Handling Race Condition Vulnerability
(BugTraq ID: 2794, affects versions of sendmail older than 8.11.3)

Web
Oracle Internet Application Server (iAS) Listener and modplsql Vulnerabilities
(http://www.securityfocus.com/archive/1/153010)

The web server presents itself as a particular target, since there have been a number of vulnerabilities affecting the Oracle Application Server, and Internet Application Server products. Also, it might be possible to infer that the web server was running these products by nature of the particular structure of URL's used on the site, even if the web server's banner did not give away this information.

Circumventing Access Controls

If the public servers can be compromised, then this provides an obvious point from which the internal network can be penetrated. The firewall still protects the internal network, but if a weakness or exploit can be found, then we have bypassed the access controls in place on the router.

An alternative approach to gaining access to the internal network would be to circumvent the access controls in place on the router. Gale Slentz has specified in her design that Cisco IOS 11.1 will be used on the border router. Assuming that this has router not been patched, a vulnerability was announced that will allow a malicious user to arbitrarily gain administrative access to the HTTP administration interface on the router (BugTraq ID: 2936). Obviously, this would mean that access controls could be modified to allow access to the network.

Whether the access controls on the border router have been circumvented by compromising a system on the DMZ, or by exploiting the IOS vulnerability, we are still faced with the task of gaining access to the internal network, by circumventing the firewall.

As Gale Slentz specified, the firewall will be CheckPoint FW-1 4.x, running on a Solaris 8 system. This setup presents two areas we can explore for weaknesses.

The first approach would be to look for weaknesses in the Solaris system running FW-1. If any of the interfaces are not protected by the firewall, it might be possible to connect to the Solaris system, and attempt to exploit vulnerabilities in the operating system. Although the system has been bastion hardened, to prevent buffer overflows, this has not been proven to be effective in all situations. It would be worth attempting to exploit the following recent vulnerabilities:

Solaris Print Protocol Daemon Remote Buffer Overflow Vulnerability
(BugTraq ID: 2894)

Solaris rpc.yppasswdd Buffer Overflow Vulnerability
(BugTraq ID: 2763)

Both of these vulnerabilities would allow remote escalation of privileges to root level.

The other possibility is to make use of vulnerability in CheckPoint FW-1 to bypass the access control restrictions in place. The obvious vulnerability, which would allow me access to the internal network, would be the RDP protocol vulnerability, which was discovered in July 2001 (http://www.checkpoint.com/techsupport/alerts/rdp.html). This vulnerability allows RDP packets to pass through the firewall gateway, without being compared to the firewall rule-set. If RDP packets could be properly constructed, this would provide an undetected communication channel to the internal network.

Exploiting the Foothold

Now that a route into the internal network has been established, we can use this to further probe for an access point into the databases holding valuable information. Either we can repeat the process of looking for vulnerabilities in the firewall, or perhaps more simply, try to take control of user systems on the internal network, which might have access to the database systems.

Conclusion

This exercise shows that typical network architecture can be best exploited using vulnerabilities in the hosts exposed directly to the Internet. In Gale Slentz's design, she has allowed Internet users to connect directly to the web server. This puts the emphasis on bastion hardening the system adequately. Making use of proxy servers, or gateway intrusion detection systems would reduce this risk.

The other obvious entry point was to exploit the systems enforcing the access control restrictions

– namely the border router, and the firewall. If these systems are not patched against vulnerabilities in a timely fashion, it is inevitable that these vulnerabilities will be exploited. A strongly enforced policy is required, to ensure that systems and network administrators patch their systems when new vulnerabilities are discovered.

Appendix A – Nessus vulnerability scan output

Nessus Scan Report

Number of hosts which were alive during the test : 4
Number of security holes found : 1
Number of security warnings found : 2
Number of security notes found : 3

List of the tested hosts :

- mail.giac-enterprises.com**(Security holes found)**
- www.giac-enterprises.com **(Security notes found)**
- commerce.giac-enterprises.com **(Security notes found)**
- nameit.giac-enterprises.com (no noticeable problem found)

[Back to the top]

mail.giac-enterprises.com :

List of open ports :

- *smtp (25/tcp) (Security hole found)*

[back to the list of ports]

Vulnerability found on port smtp (25/tcp)

The remote SMTP server did not complain when issued the
command :
MAIL FROM: |testing

This probably means that it is possible to send mail
that will be bounced to a program, which is
a serious threat, since this allows anyone to execute
arbitrary command on this host.

NOTE : ** This security hole might be a false positive, since
some MTAs will not complain to this test, but instead
just drop the message silently **

Solution : upgrade your MTA or change it.

Risk factor : High
CVE : CAN-1999-0203

[back to the list of ports]

Warning found on port smtp (25/tcp)

The remote SMTP server
answers to the EXPN and/or VRFY commands.

The EXPN command can be used to find
the delivery address of mail aliases, or
even the full name of the recipients, and
the VRFY command may be used to check the
validity of an account.

Your mailer should not allow remote users to
use any of these commands, because it gives
them too much informations.

Solution : if you are using sendmail, add the
option
O PrivacyOptions=goaway
in /etc/sendmail.cf.

Risk factor : Low
CVE : CAN-1999-0531

[back to the list of ports]

Warning found on port smtp (25/tcp)

The remote SMTP server allows the relaying. This means that
it allows spammers to use your mail server to send their mails to
the world, thus wasting your network bandwidth.

Risk factor : Low/Medium

Solution : configure your SMTP server so that it can't be used as a relay
any more.
CVE : CAN-1999-0512

[back to the list of ports]

Information found on port smtp (25/tcp)

Remote SMTP server banner :
0
0

[Back to the top]

www.giac-enterprises.com :

List of open ports :

- *www (80/tcp)*
- *general/tcp (Security notes found)*

[back to the list of ports]

Information found on port general/tcp

> Nmap found that this host is running Windows NT 5 Beta2 or Beta3, Windows 2000 RC1 through final release, MS Windows2000 Professional RC1/W2K Advance Server Beta3

[Back to the top]

commerce.giac-enterprises.com :

List of open ports :

- *https (443/tcp)*
- *general/tcp (Security notes found)*

[back to the list of ports]

Information found on port general/tcp

> Nmap found that this host is running Windows NT 5 Beta2 or Beta3, Windows 2000 RC1 through final release, MS Windows2000 Professional RC1/W2K Advance Server Beta3

[Back to the top]

nameit.giac-enterprises.com :

List of open ports :

- *domain (53/tcp)*

This file was generated by Nessus, the open-sourced security scanner.

References

Printed Material

The SANS Institute, Firewalls, Perimeter Protection, and VPNs Course Reference. The SANS Institute, 2001.

Stuart McClure, Joel Scambray, George Kurtz, Hacking Exposed. Berkeley: Osborne / McGraw-Hill, 1999.

Stephen Northcutt, Judy Novak, Network Intrusion Detection: An Analyst's Handbook. Indianapolis: New Riders Publishing, 2000.

Simson Garfinkel, Gene Spafford, Practical Unix & Internet Security. Sebastopol: O'Reilly and Associates Inc., 1996.

Scott M. Ballew, Managing IP Networks with Cisco Routers. Sebastopol: O'Reilly and Associates Inc., 1997.

Online Resources

NetScreen Technologies Inc., "NetScreen Concepts & Examples User's Guide, version 2.6.1", 2001. URL: http://www.netscreen.com/support/downloads/C&E.pdf

NetScreen Technologies Inc., "NetScreen-1000 Users Manual, version 2.6", 2001.
URL: http://www.netscreen.com/support/downloads/NS-1000_Installation_Manual_260.pdf

Cisco Systems Inc., "Cisco 7513 Documentation", 2001.
URL: http://www.cisco.com/univercd/cc/td/doc/product/core/cis7513/index.htm

Extreme Networks, Inc., "Summit 1i Technical Specifications", 2001.
URL: http://www.extremenetworks.com/products/datasheets/Summit1i.asp?anchor=techspecs

Extreme Networks, Inc., "TechBrief: Leveraging Redundancy to Build Fault-Tolerant Networks", 2001. URL: http://www.extremenetworks.com/technology/how/esrp.asp

SecurityFocus.com, "Vulnerabilities", 2001. URL: http://www.securityfocus.com

Volera, "Excelerator", 2001. URL: http://www.volera.com/Products/Excelerator/

National Security Agency, "Windows 2000 Security Recommendation Guides", 2001.
URL: http://nsa1.www.conxion.com/win2k/index.html

Elise Gerich, "RFC 1466: Guidelines for Management of IP Address Space", 1993.
URL: http://rfc.net/rfc1466.html

SecurityFocus.com, “ARIS Predictor”, URL: Not Public

Software Tools

RedHat, Inc., “RedHat Linux 7.1”,
URL: http://www.redhat.com/products/software/linux/7-1_standard.html

Marty Roesch, “Snort”, URL: http://www.snort.org

Whitehats, Inc., “arachNIDS”, URL: http://www.whitehats.com/ids/index.html

Bastille Linux Project, “Bastille Hardening System”, URL: http://www.bastille-linux.org/

Tripwire Inc., “Tripwire Open Source, Linux Edition”, URL: http://www.tripwire.org/

Argus Systems Group, Inc., “PitBull LX”,
URL: http://www.argus-systems.com/product/overview/lx/

Microsoft Corporation, “Microsoft Windows 2000 Server”,
URL: http://www.microsoft.com/windows2000/server/default.asp

Microsoft Corporation, “Microsoft Internet Information Services 5.0”,
URL: http://www.microsoft.com/windows2000/technologies/web/default.asp

Neil Timm, “Guardian for Snort”, URL: http://home.golden.net/~elim/

eEye Digital Security, “SecureIIS”,
URL: http://www.eeye.com/html/Products/SecureIIS/index.html

Microsoft Corporation, “Microsoft Exchange Server 2000”,
URL: http://www.microsoft.com/exchange/default.asp

Fyodor, “Nmap”, URL: http://www.insecure.org/nmap/

Renaud Deraison, “Nessus”, URL: http://www.nessus.org/

eEye Digital Security, “Retina”, URL: http://www.eeye.com/html/Products/Retina/

sniph00, “Snot”, URL: http://www.sec33.com/sniph/

@stake, Inc., “LC3” (formerly L0phtCrack), URL: http://www.atstake.com/research/lc3/

Solar Designer, “John the Ripper”, URL: http://www.openwall.com/john/

TP Information Systems Pty Ltd., “Password Policy Enforcer”, URL: http://www.tpis.com.au/

Salvatore Sanfilippo, “hping2”, URL: http://www.hping.org/