# Global Information Assurance Certification Paper

# Assignment 1 – Security Architecture

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

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

**Background and Assumptions:**

The first step in designing security architecture is understanding and defining what you are trying to protect by establishing the boundaries and by determining the type of access. In addition, as boundaries are established and security measures developed, policies and procedures must be developed in order to provide guidelines for expected behavior and use of the GIAC Enterprises network.

As identified above, the startup Internet Company, GIAC Enterprises, is an Internet company with customers, suppliers (telecommuting workforce and some local workforce) and partners, which require access to data and telephony. The boundary of GIAC Enterprises network encompasses not only the LAN's (Local Area Network) Internet connection but must also address the telephony connections. Since, telephony connections are generally analog – due to cost of handsets and fax requirements, the risk of some analog modems being present on the local network is probable. Therefore, not only must the data be protected from the Internet connection, but the data must also be protected from dial-out and dial-in connections.

Telephony will be supplied via the GIAC Enterprises phone switch, which has a dedicated PRI (Primary Rate Interface) phone connection from the local area phone service central switch. The PRI line shall have a SecureLogix XXXX PRI Firewall installed in-line. This PRI Firewall will be configured to only allow fax, voice, video, and identified modems.

Due to the potential volume of Internet connectivity, GIAC Enterprises has contracted for a single T1 (1.544 Mbps) network line with upgrade potential to multiple T1's or a T3 (45 Mbps). The T1 line is identified as the WAN (Wide Area Network) connection provided by the upstream provider.

Customers are issuing purchasing information that can originate from any where in the world. This data needs to be protected from data hijacking and modification. Since on-line purchasing using Credit Card information will be the norm, authentication and encryption is required before and during a data transaction. Since the customers will be using any number of Operating Systems on different workstations, a common presentation interface is needed; such as an Internet browser using HTML (hyper text markup language) on a secure connection, TCP (Transmission Control Protocol) 443 utilizing a certificate mechanism on the GIAC Enterprise server.

Suppliers are technically the telecommuting work force, therefore; they need to be able to connect to GIAC Enterprises corporate resources in order to deal with management issues such as time cards, corporate policies, and the fortune saying database. The suppliers will require a more intimate connection with GIAC Enterprise because essentially the suppliers are the employees. VPN (Virtual Private Network) or RAS (Remote Access Server) connections with strong authentication and encryption can provide the necessary access.

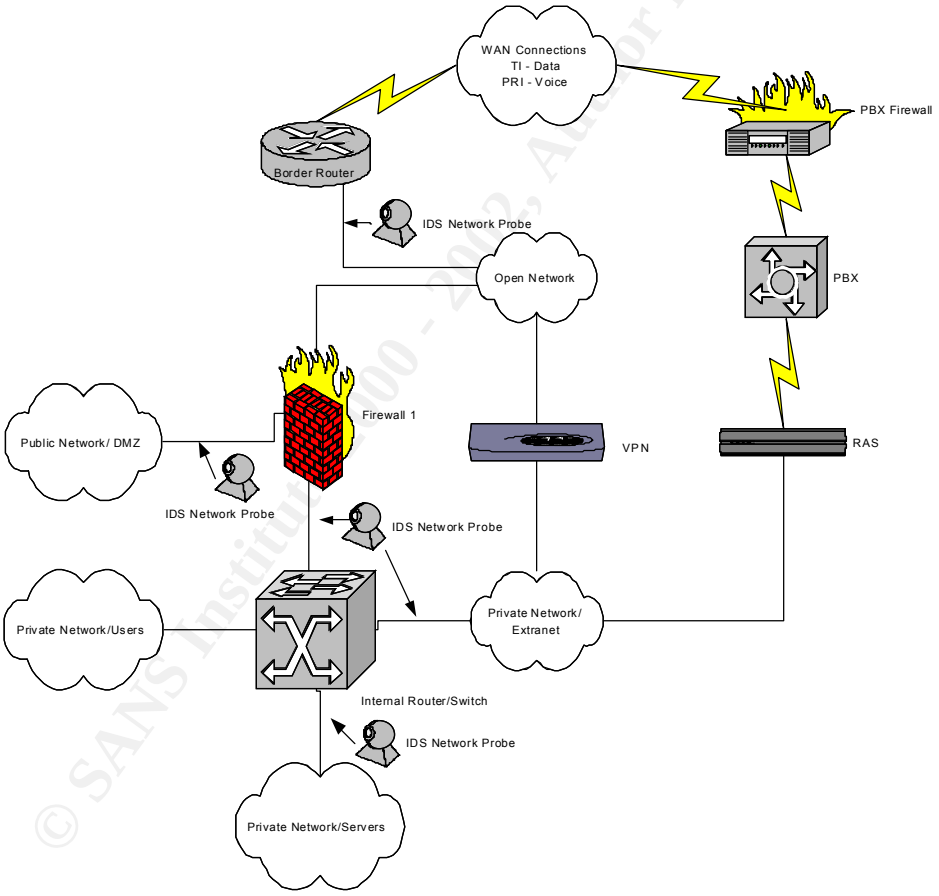
Partners, on the other hand, map into the reseller market, by reselling the fortunes after translating them into different languages. So Partners need access to the fortunes database in order to be able to extract fortune sayings. Partners must pay a fee for that access and a percentage of the reselling.

Since customers, suppliers, and partners must be able to access different datasets within GIAC Enterprises, it is necessary that the presentation of the datasets be via a common user interface, such as an Internet browser like Netscape or Internet Explorer.

**Network Design:**

Network security will be achieved by using a layered approach – the further in the access, the tighter the restrictions. Reference Drawing 1 for a logical network connectivity diagram. All network equipment; consisting of routers, firewalls, virtual private network appliances (VPNs) and Remote Access Servers (RAS); used in this model will be configured based on a default deny posture both inbound and outbound the network. Reference Table 1 for a description of the network equipment illustrated in Drawing 1. The network shall be broken into three major containers; the Open network, the Public network, and the Private network. Definitions of the network containers are found at the end of this section. Each network shall be separated by network device; such as a router or firewall programmed with appropriate access controls. Network security policies shall be posted on a Private network Web Server.

**Drawing 1: GIAC Enterprise Network Perimeter**




**Description of Data Route:** As the Wide Area Network connection enters the network perimeter, the first device encountered is the border router. The data then traverses the Open network and encounters the Firewall or the VPN appliance. From the Firewall, the data can be directed only into the Public network, which is also known as the DMZ (Demilitarized Zone). The Public network will service all customers, both current and potential, and the partners. The Firewall also connects to the Private network through the internal router. Meanwhile, an alternate path through the VPN will provide connectivity to the Private network through the Extranet network. The Extranet network is separated from the Private network by the

internal router with appropriate access restrictions. Intrusion Detection Systems (IDS) be placed appropriately through out the network in order to effectively monitor and detect potential problems.

**Description of Network Equipment:**

| Network Component | Manufacturer and Description | Rationale |
|---|---|---|
| Border Router | Cisco 3662-AC; Dual 10/100E Cisco 3660, 6-slot multiservice platform with IP software, 8 Mb of flash, 32 Mb SDRAM, two AC power supplies; NM-1FE2CT1-CSU module two port Channelized T1/ISDN-PRI with CSU network module and one Fast Ethernet Port, Running Cisco IOS 12.0 (11) | Supports IPsec tunneling protocols; hot swappable power supplies; compatible parts interchangeable with RAS thus reducing spare part inventory; capable of supporting high speed WAN connectivity and aggregating multiple connections Fast Ethernet to provide more bandwidth as needed |
| Firewall 1 | Sun SPARC Ultra 2 with 400 MHz dual processors and 512 Mb RAM, 10/100 Ethernet connections; disk mirroring on primary partition housing OS and Checkpoint software; Sun Solaris 2.7 patched; Checkpoint Firewall I 4.1 software with service patch 3 | Sun system hardening techniques are well known and document – reference SANS, NIST, or NSA documentation; chassis is capable of supporting higher speed connectivity via Gigabit connections |
| Internal Router/Switch | Cisco 6506; dual power supplies; Supervisor Engine 2 running CISCO IOS Software Layer 3 services, multiple 10/100 Mbps Ethernet | Supports MultiLayer Switch Feature card; wide range of interface types and densities; hot swappable power supplies; six slot expansion chassis so have room to grow; support of VLANs and ACLs; capable of aggregating Ethernet connections to achieve higher bandwidth at the desktop; supports integrated IDDS module on back plane of switching fabric; supports flow accounting using Net Flow switching software; can be configured with redundant switching fabrics |
| VPN | Cisco 5002 Concentrator | Support IPsec tunneling protocols; provides client software for Windows suite (95, 98, 98 second edition, NT 4.0 SP3-SP6, 2000, ME), MacOS, Sun Solaris (Intel and SPARC) and Linux; supports RADIUS authentication and accounting |
| RAS | Cisco 3642; Dual 10/100E Cisco 3640, 4-slot multiservice platform with IP software, 8 Mb of flash, 32 Mb SDRAM, two AC power supplies; NM-2CT1-CSU module two port Channelized T1/ISDN-PRI with CSU network module, | Supports Encryption; TACAS+ and RADIUS authentication and SecureID Tokens; hot swappable power supplies; Up to 48 analog modems; four FastEthernet ports; integrated CSU/DSU; supports up to 8 PRI lines; supports hardware |

| | | |
|---|---|---|
| | Running Cisco IOS 12.0 (11) | and software compression |
| PBX Firewall | SecureLogix TeleWall | Logs call progress; distinguishes inbound and outbound traffic by call type – voice, fax, modem, video, and STU-III; sends real-time alerts to system administrators |
| IDS and Monitoring | Cisco NetRanger Module;<br>ISS RealSecure IDS;<br>Checkpoint Firewall Logs;<br>Cisco Net Flow Product;<br>TeleWall Logs;<br>Network Associates Sniffer | IDS systems tend to compliment one another giving a particular view of how the manufacturer implemented their product. So complimentary tools are required to determine network activity. |

**Description of Network Containers:**

The Open network shall contain IT resources that need to be freely accessible via the Internet and cannot adhere to any of the restrictions placed upon the Public or Private network. IT resources located here will be available to the public-at-large and are not protected by the Firewall; thus the resources shall be protected by whatever measures that can be placed on the hosts by the system administrators. Any device located here will have to obtain a waiver from the GIAC network security officer with the system owner acknowledging and accepting all risks for existing in this container. Access originating from the Open network to the Private network shall be forbidden. Access originating from the Private network to the Open network shall be restricted and must use an acceptable form of authenticated and encrypted access.

The Public network shall contain IT resources that need to be accessed from the Internet but are protected by the Firewall or VPN. Access into the Public network shall be restricted based on service port required to the Public system. Access originating from the Public network into the Private network shall be restricted. Access originating from the Private Network to the Public network shall be restricted and must use an acceptable form of authenticated and encrypted access. GIAC user systems shall not exist in the Public network. Public network examples are the DMZ (Demilitarized zone) and the Extranet.

The Private network shall contain IT resources that need to access the Public, Private and Internet resources and will be located behind the Firewall. The Private network will contain both user systems and servers. Access originating from the Private network shall be restricted. Access originating from outside the Private network will also be tightly controlled.

## Assignment 2 – Security Policy

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

Border Router
Primary Firewall
VPN

Common commands for the Border Router, and Internal Router/Switch

Since the network is small and manageable, IP routes advertisements will be done using static routes. This prevents anyone from sniffing inside the network, from gleaning network configuration information by intercepting broadcast route advertisements. Comments included as appropriate per line of version marked by # sign.

```
version 12.1
service timestamps log uptime
service password-encryption          # encrypts passwords saved to configuration file
no service udp-small services        # disables chargen, echo, and discard
```

```
no service tcp-small services                    # disables chargen, echo, and discard
no service finger                                # disables finger service
no ip source-route                               # allows the software to discard any IP datagrams
                                                 containing source-route option
no ip http server                                # disables http configuration capability
ip cef                                           # Cisco Express Forwarding enabled
schedular interval 500                           # Reduces the effect from fast packet floods
no cdp running                                   # disables Cisco Discovery Protocol (CDP)
no ip bootp server                               # disables bootp server
logging buffered 16384                           # keeps contents of buffer when router reloaded
logging trap debugging
logging 111.222.123.201                          # address of remote logger
ip subnet-zero                                   # allows use of
ip classless                                     # allows subnetting of Class A, B and C addresses
!
aaa new-model
aaa authentication login default tacacs+ enable  # tacacs+ should be used for login
aaa authentication enable default tacacs+ enable # tacacs+ should be used for enable mode
aaa accounting exec start-stop tacacs+ enable    # tacacs+ logging is enabled
!
ip tacacs source-interface Loopback0             # loopback interface is the source of tacacs+ request
tacacs-server host 111.222.123.202               # primary tacacs server
tacacs-server key CKr3t#
!
username GIAC1 password 7 1101811051B13
enable secret <removed>
no enable password
!
```

The password encryption service uses a simple Vigenere cipher; which is reversible; however, the encryption does prevent the casual observer from reading passwords that are printed or displayed on the terminal screen. The above removes services that are started up automaticallyin the CISCO IOS. The chargen, echo and discard services can be used to create a denial of service against the router or another device. The finger service is used to find out which users are logged into a network device; the information could be useful to an attacker. The disabled source-route option prevents the sender of the IP datagram from controlling the route that a datagram would take toward its destination. If http isn't being used to manage or monitor the router, then the service must be disabled. The CEF option enables a routing cache to be mirrored from the entire system routing table, which can result in better performance when under a SYN attack. The schedular interval prevents fast packet floods from causing the router to spend too much time dealing with interrupts. Another service to turn off if not used is CDP. The CDP service advertises what Cisco IOS software version is being run. The aaa accounting has been enabled on the router where a tacacs server is used to authenticate and record activities of network administrators. If the TACACS+ server fails, then the router falls back on the conventional authentication.

Per each routed interface activated on the VPN, RAS, Border Router and Internal Router/Switch, place the following commands.

```
!
interface xxxxxxxxx                              #xxxxxx signifies which interface like Serial0 or
                                                 Ethernet0
        no ip directed-broadcast                 #prevents attackers from using the router as a smurf
                                                 amplifier
        ip split-horizon                         #disables the re-broadcasting of ip routes out the
                                                 interface which generated it. When using secondary
                                                 interface IP, this is necessary in order to prevent
                                                 unnecessary network traffic
no ip proxy-arp                                  # disables the routers capability to proxy arps
```

```
!
```

Secure the vty interfaces on Border router, RAS, VPN, and Internal router/switch by applying an access list which will define what can connect on what service. Individual user name and passwords need to be identified. The service ssh can also be incorporated with the systems identified.

```
!
Access-list 1 permit 111.222.126.10 0.0.0.255
Access-list 1 permit 111.222.126.11 0.0.0.255
Access-list 1 permit 111.222.125.11 0.0.0.255
!
line vty 0 4
        access-class 1 in
        exec-timeout 5 0
        transport input ssh
        transport output none
        transport preferred none
        login authentication GIAC1
        history size 256
!
```

IP routes as stated earlier will not be advertised but will be placed in each individual router in order to reduce the gleaning information a potential hacker could learn and to reduce the network noise associated with repetitive route announcements.

```
!
ip route 0.0.0.0    0.0.0.0   111.222.xxx.xxx              #
ip route 111.222.xxx.0  0.0.0.255  111.222.xxx.xxx  # xxx must reflect the proper network and gateway
ip flow-export destination 111.222.125.200  9995     # address of net flow gatherer and port number
!
```

The first ip route statement illustrates the default route, where 111.222.xxx.xxx would represent the IP address of the far end router upstream from the current router. This address would vary from router to router. Additional route statements will also be required in order to address the connections on the GIAC network that was more than one hop away.

Generic External Interface ACL for RAS and Border router:

In order to secure IP routing, anti-spoofing needs to be address. This can be done by applying an access list that would prevent IP addresses from entering the GIAC Enterprises network. The following is an access list that would address ingress filtering on RFC1918, default, and multicast networks which would be applied to interfaces exposed to external networks. The access list also deals with the ICMP discovery scans. In this case the access list shown below would be applied to the border router WAN interface, VPN external interface, and RAS WAN interface.

```
!
access-list 101 deny icmp any any redirect                  # filters out ICMP redirects
access-list 101 deny icmp any any echo-request              # filters out ICMP discoveries
access-list 101 deny ip host 0.0.0.0 any                    # filters out BOOTP/DHCP clients
access-list 101 deny ip 10.0.0.0 0.255.255.255 any          # reserved RFC1918 private address space
access-list 101 deny ip 127.0.0.0 0.255.255.255 any         # reserved for loopback address
access-list 101 deny ip 169.254.0.0 0.0.255.255 any         # reserved RFC1918 private address space
access-list 101 deny ip 172.16.0.0 0.15.255.255 any         # reserved RFC1918 private address space
access-list 101 deny ip 192.0.2.0 0.0.0.255 any             # reserved address space
access-list 101 deny ip 192.168.0.0 0.0.255.255 any         # reserved RFC1918 private address space
access-list 101 deny ip 224.0.0.0 31.255.255.255 any        # reserved multicast address
access-list 101 deny ip 111.222.0.0 0.0.255.255 any         # internal IP address for GIAC Enterprises
access-list 101 deny ip any 255.255.255.128 0.0.0.127       # inverse of loopback reserved address
```

```
access-list 101 permit ip any any                    # allow all other ip packets
!
```

Specific ACLs for Internal router/switch:

For the internal router/switch, additional anti-spoofing can be addressed by applying an access list which contains the internal network address and deny all other IP. Example, if the DMZ has the subnet of 111.222.124.0, then the access list would be:

```
!
access-list 102 permit ip 111.222.124.0 0.0.0.255 any
access-list 102 deny ip any any
!
```

But the above anti-spoofing will not be needed when a more detailed access-list is written. For example if the DMZ contains the public DNS (Domain Name Server) and a web server running both http and secure http. The public DNS will get zone updates from the private DNS when the private DNS initiates the zone transfer. The DMZ also hosts a NTP server, which is access by all systems in the GIAC Enterprise network. Then the access list on the DMZ ingress interface would be:

```
!
access-list 102 permit udp host 111.222.124.2 eq 53 any gt 1023
access-list 102 permit tcp host 111.222.124.2 gt 1023 host 111.222.125.2 eq 53
access-list 102 permit tcp host 111.222.124.3 eq www any gt 1023
access-list 102 permit tcp host 111.222.124.3 eq 443 any gt 1023
access-list 102 permit tcp host 111.222.124.4 eq ntp 111.222.0.0 0.0.255.255 gt 1023
access-list 102 permit tcp host 111.222.124.5 eq ftp any gt 1023
access-list 102 permit tcp host 111.222.124.5 eq ftp-data any gt 1023
access-list 102 deny ip any any
!
```

On the inbound interface of the private network for users, services that users need can be clearly identified. In this case, GIAC Enterprises allows users to access anywhere http, https, and ftp. The users also connect to a SQL database located in the private network for servers.

```
!
access-list 103 permit tcp 111.222.126.0 0.0.0.255 gt 1023 any eq ssh
access-list 103 permit tcp 111.222.126.0 0.0.0.255 gt 1023 any eq www
access-list 103 permit tcp 111.222.126.0 0.0.0.255 gt 1023 any eq 443
access-list 103 permit tcp 111.222.126.0 0.0.0.255 gt 1023 any eq ftp
access-list 103 permit tcp 111.222.126.0 0.0.0.255 gt 1023 any eq ftp-data
access-list 103 permit tcp 111.222.126.0 0.0.0.255 gt 1023 host 111.222.125.5 eq 1433
access-list 103 permit udp 111.222.126.0 0.0.0.255 gt 1023 host 111.222.125.2 eq 53
access-list 103 permit tcp 111.222.126.0 0.0.0.255 gt 1023 host 111.222.124.4 eq ntp
access-list 103 deny ip any any
!
```

On the inbound interface of the private network for the extranet, due to the fact that a Citrix server was established in the Extranet, the number of ports required for access to the database located in the private network for servers is reduced. The Citrix server, however, does require a Citrix client to be loaded on the Suppliers desktop in addition to the client application to support the VPN.

```
!
access-list 104 permit tcp 111.222.127.0 0.0.0.255 gt 1023 any eq www
access-list 104 permit tcp 111.222.127.0 0.0.0.255 gt 1023 any eq 443
access-list 104 permit tcp 111.222.127.0 0.0.0.255 gt 1023 any eq ftp
access-list 104 permit tcp 111.222.127.0 0.0.0.255 gt 1023 any eq ftp-data
access-list 104 permit tcp 111.222.127.0 0.0.0.255 gt 1023 host 111.222.125.2 eq 53
access-list 104 permit tcp 111.222.127.0 0.0.0.255 gt 1023 host 111.222.125.4 eq ntp
access-list 104 permit tcp host 111.222.127.2 gt 1023 host 111.222.125.5 eq 1433
access-list 104 deny ip any any
!
```

Security Configuration for the VPN appliance

The client and the VPN Concentrator will be using IPsec negotiations, which occur on UDP 500 for ISAKMP, the key exchange. The tunnel created will be using the Encapsulated Security Payload (ESP), which is IP protocol 50. The VPN Concentrator will be authenticating the user with a RADIUS server located in the Extranet. A shared secret will be exchanged between the VPN Concentrator and the client. The client will pass a user ID and password to the RADIUS server in an encrypted tunnel using the

The VPN clients will be negotiating a tunnel peer using the Internet Key Exchange (IKE) protocol. The IKE policy's authentication algorithm will use the Secure Hash Algorithm (SHA), which is more secure than message-digest 5 hash algorithm. The encryption algorithm will use triple Data Encryption Standard (3DES). The last piece used for the key exchange will be the Diffie-Hellman Group2 (G2), which is a 1024-bit algorithm. Commands are as follows:

!
Configure IKE Policy
Protection={SHA_3DES_G2}
!

Access lists for the VPN's WAN interface will address the same anti-spoofing issues as noted in an earlier section.

!
[IP Filter WAN-ACL]

```
deny 0.0.0.0 0.0.0.0 icmp type echo-requests                  # filters out ICMP echo requests
deny 0.0.0.0 0.0.0.0 icmp type redirect                       # filters out ICMP echo redirect
deny 10.0.0.0/8 0.0.0.0 ip                                    # reserved RFC1918 private address space
deny 127.0.0.0/8 0.0.0.0 ip                                   # reserved for loopback address
deny 169.254.0.0/16 0.0.0.0 ip                                # reserved RFC1918 private address space
deny 172.16.0.0/12 0.0.0.0 ip                                 # reserved RFC1918 private address space
deny 192.0.2.0/24 0.0.0.0 ip                                  # reserved address space
deny 192.168.0.0/16 0.0.0.0 ip                                # reserved RFC1918 private address space
deny 224.0.0.0/1 0.0.0.0 ip                                   # reserved multicast address
permit 111.222.1.0/24 111.222.1.10/32 udp src 500 dst 500     # allow open network addresses ISAKMP
permit 111.222.1.0/24 111.222.1.10/32 esp                     # allow open network address space ESP
deny 111.222.0.0/16 0.0.0.0 ip                                # internal IP address for GIAC Enterprises
deny 0.0.0.0 0.0.0.127/32 ip                                  # inverse of loopback reserved address
permit  0.0.0.0 111.222.1.10/32 udp src 500 dst 500           # allow ISAKMP packets
permit 0.0.0.0 111.222.1.10/32 esp                            # allow ESP packets
```

!

Primary Firewall Access –

| No | Source | Destination | Service | Action | Track | Install On | Time | Comment |
|---|---|---|---|---|---|---|---|---|
| 1 | Adminstation1<br>Adminstation2 | Fw-1 | Firewall1-services<br>Icmp-protocol | Accept | Long | Fw-1 | Any | 4/1/01 dkr |
| 2 | Fw-1 | PublicDNS | UDP 53 | Accept | account | Fw-1 | Any | 4/1/01 dkr |
| 3 | Fw-1 | PublicNTP | TCP 123 | Accept | Account | Fw-1 | Any | 4/1/01 dkr |
| 3 | Any | Fw-1 | Any | Drop | Long | Fw-1 | Any | 4/1/01 dkr |
| 4 | Any | PublicDNS | UDP 53 | Accept | Account | Fw-1 | Any | 4/1/01 dkr |
| 5 | Any | PublicWeb | Tcp 80; tcp 443 | Accept | Account | Fw-1 | Any | 4/1/01 dkr |
| 6 | Any | PublicFTP | Tcp 21 | Accept | Account | Fw-1 | Any | 4/1/01 dkr |
| 7 | Any | GIACmailgtwy | Tcp 25 | Accept | Account | Fw-1 | Any | 4/1/01 dkr |
| 8 | GIACprivatenet | Any | Tcp 80; tcp 443; tcp 21 | Accept | Account | Fw-1 | Any | 4/1/01 dkr |
| 9 | GIACmailgtwy | Any | Tcp 25 | Accept | Account | Fw-1 | Any | 4/1/01 dkr |
| 10 | Any | Any | Icmp-protocol | Drop | Long | Fw-1 | Any | 4/1/01 dkr |
| 11 | Any | Any | Any | Drop | Long | Fw-1 | Any | 4/1/01 dkr |

The above rules illustrate the basics required to protect the Primary firewall while also addressing internal to external and external to internal traffic. Note that no VPN traffic is allowed to cross the Primary Firewall; instead the VPN gateway is connected in parallel. The listing below defines the names in the used in the above policy:

Administration1 GIAC Enterprise system

| | |
|---|---|
| Adminsitration2 | GIAC Enterprise system |
| PublicDNS | DNS server located in public network, 111.222.124.2 |
| PublicWeb | Web server located in Public network, 111.222.124.3 |
| PublicNTP | NTP server located in Public network, 111.222.124.4 |
| PublicFTP | FTP server located in Public network, 111.222.124.5 |
| GIACmailgtwy | Mail gateway server located private network, 111.222.127.6 |
| GIACprivatenet | all networks located behind GIAC Primary firewall |
| ICMP-protocol | represents all icmp protocol |
| Fw-1 | Primary Firewall includes all the interfaces, External, Internal and DMZ |
| Firewall1-services | A grouping of services needed to communicate with the Firewall predefined with Checkpoint Firewall 1 |

Additional configuration to the Primary firewall is addressed under the properties section on the Checkpoint Policy Editor. The following is the tab selection under each window:

- Security Policy
  - Apply rules to interface direction - inbound
  - Accept UDP replies
  - Deselect all implied rules
  - Check implied rules
- Services
  - Deselect the RSH/REXEC reverse stderr connections
- Log and Alert
  - Under tracking section
    - Select IP options drop as log
    - Log established TCP packets
    - Log IKE negotiations
    - Log encryption kernel events
- Access lists
  - Deselect accept RIP
  - Deselect accept Domain Name Over TCP
  - Deselect accept ICMP
- SYNDefender
  - Select passive SYN gateway
  - Select display warning messages

## Assignment 3 – Audit Your Security Architecture

Requirement is to audit the Primary Firewall described in assignments 1 and 2. The assignment must include:

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

<u>The Assessment Plan</u>

First decide where to be when the audit the Primary Firewall and when the audit should take place. The ideal place is to be node in the Open Network. Typically an audit would be done outside of peak networking hours, but since the goal is to audit what the Primary Firewall is protecting, the audit needs to be able to find as many alive systems as possible. No Denial of Service test is expected to be used during normal working hours. So to sum up the plan:

1. Locate audit tools on Open Network
2. Conduct audit during normal business hours but outside of peak network activity

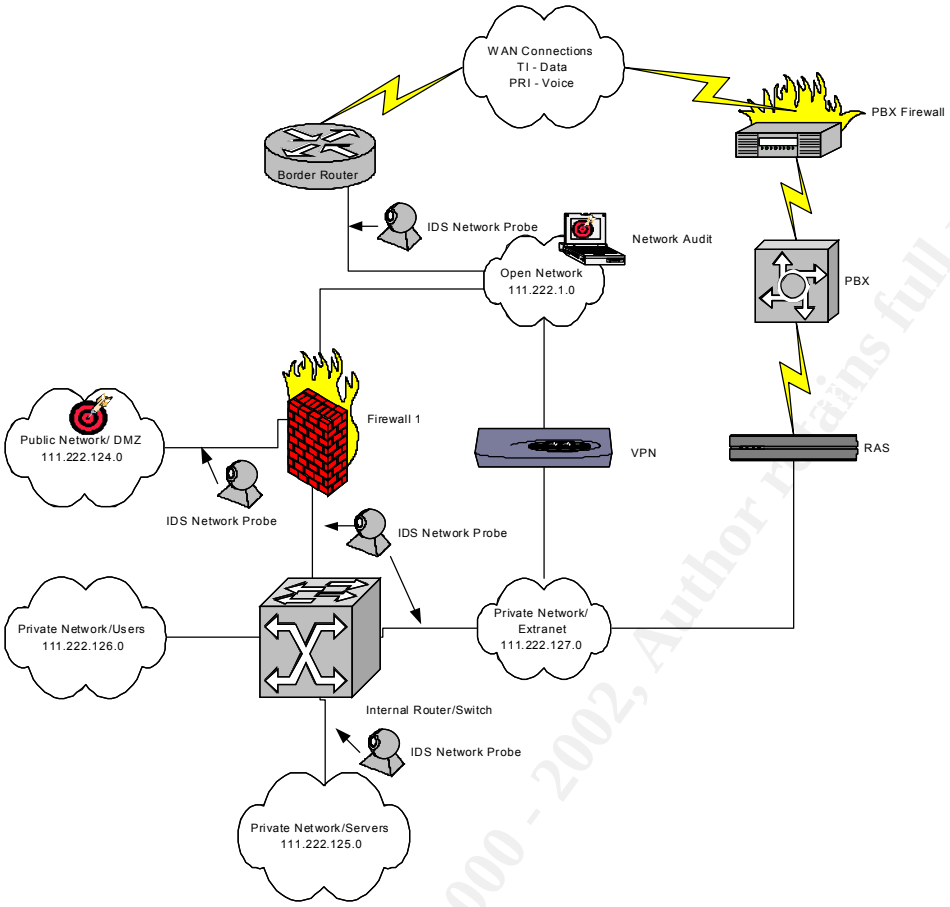
3. Using a variety of network tools
    a. Perform a network ping sweep
    b. If no response, perform a brute force stealth sweep on a well known tcp ports
        i. 80 (http)
        ii. 21 (ftp)
        iii. 139 (netbios)
        iv. 111 (rpc)
        v. 143 (imap)
        vi. 23 (telnet)
        vii. 53 (dns)
        viii. 25 (smtp)
    c. Perform stealth port scan on above discovered IPs
    d. Conduct Operating System fingerprinting
    e. Conduct a banner capture on open ports
    f. Check Internet sites for possible vulnerabilities in OS's and open ports

Estimated cost to conduct would consist of only time to perform scan and analysis; worst case it would take approximately 3 days at $250 per day for a Class B network. Depending on the network tool used a Class B network can have a ping sweep completed in 30 minutes or less. The software required to do the checks are available on the Internet for little or no cost. The computer used to do the scan would be an existing system re-allocated for this audit purpose. Estimated risk would be little to none as long as a Denial of Service wasn't attempted. Any DOS against the Primary Firewall would have to be scheduled after normal working hours.

Implement the Assessment

For this assessment, the following tools will be used: SuperScan a Windows Tool available from http://kier.net/software.html, but this is limited to a Class C address. This tool can also export out to a flat file for analysis and will retrieve banners. Another tool to used is based a Unix platform, called nmap (network mapper) available at http://www.insecure.org/nmap. The results are as follows from nmap. Below is the diagram depicting were the scanning system was located.

**Drawing 2: GIAC Enterprise Network Audit Diagram**




Step 1: Perform a ping sweep on a the DMZ

```
# ./nmap -sS -o class 111.222.124.1-254

Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Note: Host seems down. If it is really up, but blocking our ping probes, try -P0
Nmap run completed -- 254 IP address (0 hosts up) scanned in 31 seconds
```

Step2: Ping sweep failed to detect, so try brute force scan against tcp 80, http.

```
# ./nmap -sS –P0 class 111.222.124.1-254

Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )

Interesting ports on publicweb.giac.com (111.222.124.3):
Port       State       Service
80/tcp     open        http
443/tcp    open        https

Nmap run completed – 254 IP address (1 host up) scanned in 31 seconds
```

Step 3: Perform a banner capture and an OS finger print in order to determine vulnerabilities

```
# ./nmap -sS -P0 -O 111.222.124.3

Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Interesting ports on publicweb.giac.com (111.222.124.3):
```

(The 1521 ports scanned but not shown below are in state: closed)
Port State Service
80/tcp open http
443/tcp open https

TCP Sequence Prediction: Class=random positive increments
Difficulty=8325 (Worthy challenge)
Remote operating system guess: Microsoft NT 4.0 Server SP5 + 2047 Hotfixes

Nmap run completed -- 1 IP address (1 host up) scanned in 2 seconds

Banner grabbed using SuperScan – results were:

HTTP/1.1 200 OK..Server: Microsoft-IIS/4.0..Date: Wed, 04 Apr 2001 13:31:19 GMT..Content-Type: text/html..Set-Cookie: ASPSESSION

Step 4: Compile data and illustrate weaknesses found by doing the vulnerability assessment. Run ISS scans against hosts and apply appropriate patches.

Perimeter Analyis

The perimeter access points are through the Border router, the RAS and the phone system. The Border router and RAS have ACLs specifically written to deflect ping sweeps and deny other services. Most of the discovery tools that rely on either ping or snmp sweeps will not provide the desired result. The only discovery attacks that won't be fended off is the brute force scan on specific ports. The specific ports that will be mapped will logically exist in the DMZ. So network mapping will result in only a partial picture of the GIAC Enterprise network.

The phone system has a firewall in place that will not allow internal modems to map out on non-sanctioned analog lines nor will external modems be allowed to connect other than the identified RAS. Therefore, the modem risk has been mitigated.

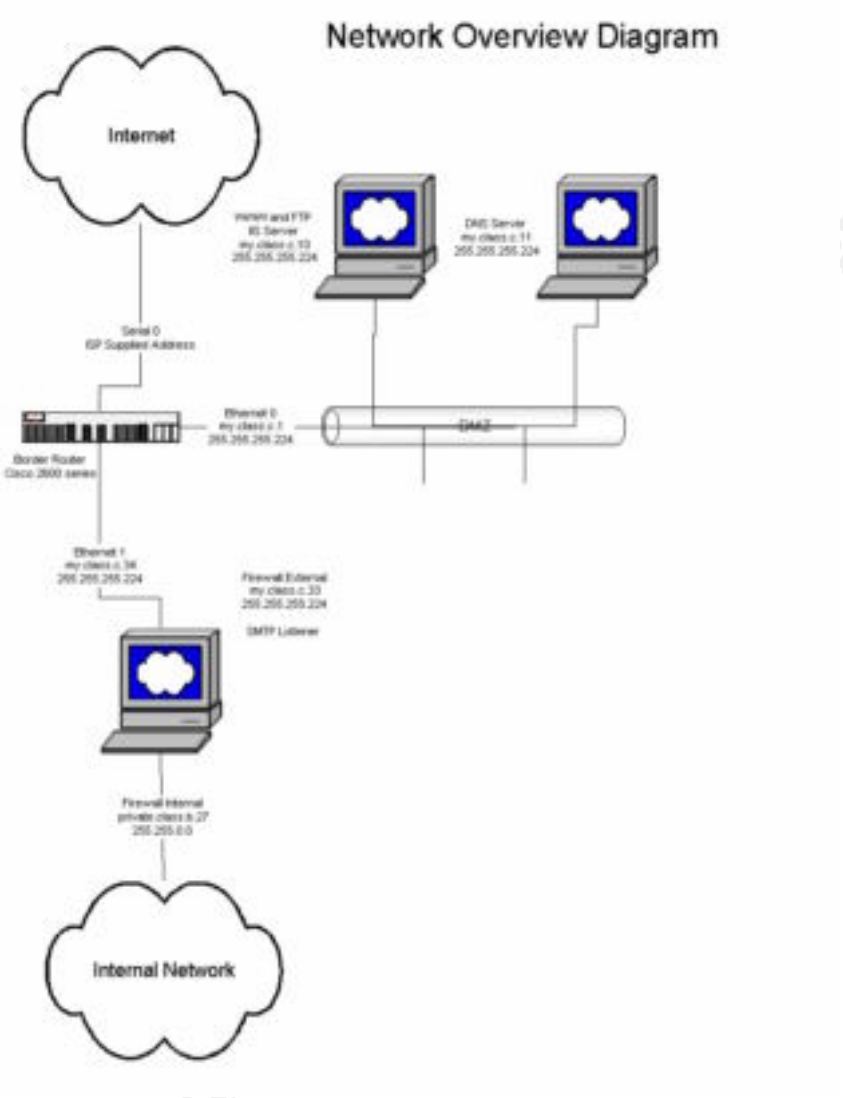
The improvements to the network architecture could include an additional Firewall between the Internal Router/Switch and the Extranet. Also, the private and public servers could benefit by having personal firewall and intrusion detection software installed. Other improvements would be to design the GIAC Enterprise network with a more fault tolerant network design; utilizing a secondary WAN connection through a different WAN supplier; providing redundancy at the Border router, Primary Firewall, and VPN appliance. See Drawing 2 below.

## Assignment 4 – Design Under Fire

Select a network design from any previously posted GCFW practical and paste the graphic into your submission. Be certain to list the URL of the practical you are using. Design the following three attacks against the architecture:

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

The Target network lifted from http://www.sans.org/y2k/practical/Jay_Landry.doc.




Part 1: Attack against the firewall

Since the firewall is not clearly identified as to the make or model, the following assumptions will be made: System is Sun SPARC Ultra 2 running Sun Solaris 2.7 and Checkpoint Firewall I 4.1 software. Researching the vulnerabilities on Solaris 2.7 and Checkpoint Firewall 1 4.1 software resulted in the following:

Starting at http://xforce.iss.net and search on Platform Solaris. Here were listed several potential exploits one of which was:

| Exploit | URL | Brief description |
|---|---|---|
| at-bo | http://xforce.iss.net/static/447.php | at(1) program on many systems contains an exploitable buffer overflow |
| bind-inverse-query-disclosure | http://xforce.iss.net/static/6018.php | ISC BIND versions 4.x prior to 4.9.8 and 8.2.x prior to 8.2.3 could allow a remote attacker to read environment variables from the stack. |
| cactus-shell-lock-root-privs | http://xforce.iss.net/static/3358.php | Shell-lock program allows any user to execute commands with root privileges. |
| canna-uum-bo | http://xforce.iss.net/static/3424.php | The Canna subsystem uum and canuum programs contain a buffer overflow |
| Multiple vulnerabilities on all platforms and versions of Check Point | http://xforce.iss.net/alerts/advise62.php | following security holes in Check Point FireWall-1:<br><br>1. One-way Connection Enforcement Bypass |

| | | |
|---|---|---|
| FireWall-1 | | 2. Improper stderr Handling for RSH/REXEC<br>3. FTP Connection Enforcement Bypass<br>4. Retransmission of Encapsulated Packets<br>5. FWA1 Authentication Mechanism Hole<br>6. OPSEC Authentication Spoof<br>7. S/Key Password Authentication Brute Force Vulnerability<br>8. GetKey Buffer Overflow |

Given that different services could be left open at the OS level and denied by the Checkpoint Security policy, the best mode of attack is to scan for open ports as outlined in Assignment 3 and then researching the what is available against that service.

```
# ./nmap -sS -p 1-65000 -v firewall

Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Host  (fireall) appears to be down, skipping it.
Note: Host seems down. If it is really up, but blocking our ping probes, try -P0
Nmap run completed -- 1 IP address (0 hosts up) scanned in 30 seconds
```

However, system did not respond to either the ping scan or with the option of no Ping. So the only attack left to do is trying the vulnerabilities shown with the Checkpoint software.

Part 2. Denial of Service Attack

In order to mitigate an ICMP DOS, depending on the network requirement for ICMP, the following are two options:

1. Deny all ICMP packets into and out of the network at the Border router.
2. Deny most ICMP and allow only a few types to enter and exit the network.
   a. Type 3 – destination unreachable
   b. Type 11 – Time exceeded

Access list additions for the Cisco 2600 shown in the diagram above would include the following statements and would be applied to both the external and internal interfaces inbound:

```
!
access-list xxx permit icmp any any 3
access-list xxx permit icmp any any 11
access-list xxx deny icmp any any
!
```

Additionally, a rate limit can be imposed on those icmp's that are coming in so that the Border router can drop the packet from processing should it exceed the rate. The caveat is that the Border router must be running at least IOS 12.0. The following is an example that would rate limit the ICMP identified above to 256 kbps at the interface identified.

```
! interface xxxxx
        rate-limit input access-group xxx 256000 8000 8000 conform-action transmit exceed-action drop
```

This will limit the ICMP type 3 and type 11 traffic to 256 Kpbs with a small burst rate. The rate limit command can be applied to other traffic also.

Part 3. Attack Plan

Since every major network usually requires a DNS server and there have been a lot of vulnerabilities associated with BIND, the target device will be a system with tcp or udp port 53 open. So a scan will be conducted against tcp/udp port 53. If that fails, a network scan will be done targeting the sendmail daemon, tcp 25, and the http daemon, tcp 80. After scanning the network for systems with open ports, tcp/udp 53, tcp 25, and tcp 80 (this required two separate scans), Nmap was targeted toward the specific IPs. That scan then returned the following:

For the DNS server:

```
Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Interesting ports on dns.someone.com (xxx.xxx.xxx.xxx):
```

```
(The 1521 ports scanned but not shown below are in state: closed)
Port      State      Service
53/udp    open       DNS

TCP Sequence Prediction: Class=truly random
                   Difficulty=9999999 (Good luck!)
No OS matches for host (If you know what OS is running on it, see http://www.ins
ecure.org/cgi-bin/nmap-submit.cgi).

Nmap run completed -- 1 IP address (1 host up) scanned in 2 seconds
```

For the mail server:

```
Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Interesting ports on mail.someone.com (xxx.xxx.xxx.xxx):
(The 1521 ports scanned but not shown below are in state: closed)
Port      State      Service
25/tcp    open       smtp

TCP Sequence Prediction: Class=truly random
                   Difficulty=9999999 (Good luck!)
No OS matches for host (If you know what OS is running on it, see http://www.ins
ecure.org/cgi-bin/nmap-submit.cgi).

Nmap run completed -- 1 IP address (1 host up) scanned in 2 seconds
```

For the Web server:

```
Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Interesting ports on web.someone.com (xxx.xxx.xxx.xxx):
(The 1521 ports scanned but not shown below are in state: closed)
Port      State      Service
80/tcp    open       http
443/tcp   open       https

TCP Sequence Prediction: Class=truly random
                   Difficulty=9999999 (Good luck!)
No OS matches for host (If you know what OS is running on it, see http://www.ins
ecure.org/cgi-bin/nmap-submit.cgi).

Nmap run completed -- 1 IP address (1 host up) scanned in 2 seconds
```

The banner was retrieved using SuperScanner and by issuing the Telnet command and the designated port. Example: mysystem# telnet xxx.xxx.xxx.xxx port# where port number is either 25, 80 or 53. The banner information indicated the following:

For DNS server, the banner information didn't reveal anything.

53 Domain Name Server

For the mail server, the banner information is shown below.

25 Simple Mail Transfer

220 mailserver (Mail*Hub TurboSendmail) ESMTP Service ready..

For the Web server, the banner information is shown below.

80 World Wide Web HTTP

HTTP/1.1 200 OK..Server: Microsoft-IIS/4.0..Date: Wed, 04 Apr 2001 13:32:28 GMT..Content-Type: text/html..Set-Cookie: ASPSESSION

Since the Web server look promising, the alert databases. Performed searches against each of the above banners at: **http://www.microsoft.com/technet/security/**

- MS01-004 : Malformed .HTR Request Allows Reading of File Fragments
- MS00-100 : Malformed Web Form Submission Vulnerability
- MS00-086 : Web Server File Request Parsing Vulnerability
- MS00-080 : Session ID Cookie Marking Vulnerability
- MS00-078 : Web Server Folder Traversal Vulnerability
- MS00-063 : Invalid URL Vulnerability
- MS00-060 : IIS Cross-Site Scripting Vulnerabilities
- MS00-057 : File Permission Canonicalization Vulnerability
- MS00-044 : Absent Directory Browser Argument Vulnerability
- MS00-030 : Malformed Extension Data in URL Vulnerability
- MS00-031 : Undelimited .HTR Request and File Fragment Reading via .HTR Vulnerabilities

**http://xforce.iss.net/**

Serious flaw in Microsoft IIS Unicode translation (Oct 26, 2000) http://xforce.iss.net/alerts/advise68.php

**http://www.securityfocus.com/**

2001-03-16: Microsoft IIS WebDAV 'Search' Denial of Service Vulnerability
2001-03-08: Microsoft IIS WebDAV Denial of Service Vulnerability
2001-03-01: Microsoft IIS Multiple Invalid URL Request DoS Vulnerability
2001-01-29: Microsoft IIS File Fragment Disclosure Vulnerability
2000-12-22: Microsoft IIS Front Page Server Extension DoS Vulnerability
2000-11-06: Microsoft IIS 4.0 ISAPI Buffer Overflow Vulnerability
2000-11-06: Microsoft IIS Executable File Parsing Vulnerability
2000-10-23: Microsoft IIS 4.0/5.0 Session ID Cookie Disclosure Vulnerability
2000-10-17: Microsoft IIS and PWS Extended Unicode Directory Traversal Vulnerability
2000-10-04: Microsoft IIS 5.0 Indexed Directory Disclosure Vulnerability
2000-09-05: Microsoft NT 4.0 and IIS 4.0 Invalid URL Request DoS Vulnerability
2000-08-21: Microsoft IIS Cross Site Scripting .shtml Vulnerability
2000-08-21: Microsoft FrontPage/IIS Cross Site Scripting shtml.dll Vulnerability
2000-08-14: Microsoft IIS 5.0 "Translate: f" Source Disclosure Vulnerability
2000-08-10: Microsoft IIS 4.0/5.0 File Permission Canonicalization Vulnerability
2000-07-17: Microsoft IIS 4.0/5.0 Source Fragment Disclosure Vulnerability
2000-07-14: Microsoft IIS 3.0 .htr Missing Variable Denial of Service Vulnerability
2000-07-13: Microsoft IIS Internal IP Address Disclosure Vulnerability
2000-05-11: Microsoft IIS 4.0/5.0 Malformed Filename Request Vulnerability
2000-05-11: Microsoft IIS 4.0/5.0 Malformed File Extension DoS Vulnerability
2000-05-10: Microsoft IIS 4.0/5.0 Malformed .htr Request Vulnerability
2000-05-06: Microsoft Frontpage Server Extensions Path Disclosure Vulnerability
2000-04-12: Microsoft IIS 4.0/5.0 Escaped Characters Vulnerability
2000-03-31: Microsoft Index Server Webhits.dll ASP Source Disclosure Vulnerability
2000-03-31: MS Index Server '%20' ASP Source Disclosure Vulnerability
2000-03-30: Microsoft IIS UNC Mapped Virtual Host Vulnerability
2000-03-20: Microsoft IIS 4.0 Chunked Transfer Encoding Buffer Overflow Vulnerability
2000-03-08: Microsoft IIS UNC Path Disclosure Vulnerability
2000-02-15: Microsoft IIS 4.0 Pickup Directory DoS Vulnerability
2000-02-09: NT IIS ASP VBScript Runtime Error Viewable Source Vulnerability
2000-02-02: NT IIS idq.dll Directory Traversal Vulnerability
2000-01-26: NT Index Server Directory Traversal Vulnerability

http://www.cert.org/

http://www.kb.cert.org/vuls/id/111677

The last flaw has code that is available for compiling in order to exploit the vulnerability. Description of vulnerability was taken from the Cert page indicated above: "A vulnerability exists in Microsoft IIS 4 and 5 such that an attacker visiting an IIS web site can execute arbitrary code with the privileges of the IUSR_machinename account. This vulnerability is referred to as the "Web Server Folder Directory Traversal" vulnerability. This vulnerability has characteristics similar to vulnerabilities that have been widely exploited in the past. Unless remedial action is taken, we believe it is likely that systems with this vulnerability will be compromised. "

Attached is a sample of the code that can be modified to cause harm or harvest information. The code is available on the Internet and was supplied by another bulletin:

"Exploit:
Attached is a unicode exploit that was used to assess the vulnerability. The code is written in C code, and can be compiled on any Unix box. (the exploit was found on the Internet). Once compiled, the program will spawn an "a.out" file. By running the command:
../a.out -t 123.123.123.123 -p 80 –i (-t is the option for target, -p for port, and -c followed by the command or in this case -i to give us a prompt)
If the command:
C>dir C:\ lists the contents of C:\, then the system is vulnerable, and needs corrective action immediately. If the web service is not absolutely needed, we recommend disabling the service. If the service is needed, install the patch.
Microsoft released patches for this vulnerability on October 17, 2000.
http://www.microsoft.com/technet/security/bulletin/ms00-078.asp "

The code was compiled and ran against the targeted system. Targeted system did not respond with a directory listing, therefore target was not vulnerable to this particular exploit. But as seen above, target could be vulnerable to an array of other opportunities.