Global Information Assurance Certification Paper

John F. Rastatter

Practical Assignment GIAC Level 2: Firewalls, Perimeter Protection and VPNs
Version 1.5 (as of 28 January 2001)

Assignment 1: Define a security architecture for GIAC Enterprises

1.1 Background:

GIAC Enterprises is a growing company with 700 employees (500 at the main headquarters location) that recently acquired their primary competitor in the market for fortune cookie sayings. GIAC expected earnings for the current fiscal year are $200 million. The company is converting their operations to e-commerce and have hired e-business consultants to find the best way to insure the security of their secretive fortune cookie sayings while utilizing the advantages of the Internet for communications with customers, suppliers and international partners.

In addition to generating fortune cookie sayings that reside in various locations on the Windows NT network, the company's employees use the network for e-mail, searching commercial databases, transfer files, and various other reasons. The company's managers would like to centralize much of their current computer operations. They feel that recent attempts by hackers to steal their intellectual property and otherwise disrupt their operations can be curtailed with proper security awareness and adherence to security safeguards.

1.2 Requirements:

One of GIAC Enterprises' young computer technicians recently attended Security Essentials at a SANS conference and convinced management to compile a list of company specific security requirements for the new network architecture. The requirements will also serve as a guide for the e-business consultants as well as for employees when the new architecture is implemented.

1) consolidate company sensitive information, especially fortune cookie sayings, onto as few protected servers as possible
2) provide strong protection (e.g. firewall) at the connection point to the Internet
3) provide additional protection for the research and development (R&D) department where new sayings and ideas germinate
4) provide a mechanism to implement and track the latest security patches for workstations, servers and network equipment
5) install a secure backup system for important servers
6) install a centralized log server for all network security devices and servers to use
7) enforce secure 6 letter/number passwords with changes every 4 months
8) install anti-virus software on all computers
9) provide confidential links to customers, suppliers and partners

10) perform testing and auditing of the network security system every 6 months

1.3 Security Architecture:

The e-business consultants made several recommendations to the GIAC managers and the following solution was accepted:
The company will upgrade its current 512 Kbps fractional T1 wide area circuit to a full T1 circuit with the option of purchasing additional or redundant wide area bandwidth if necessary. The company can currently afford to have periodic downtime (not to exceed 4 hours) of the T1 circuit or other network equipment because their business is not time sensitive. Their contracts with telecom equipment providers reflect this requirement.

The company will continue to use the local telephone company as its ISP due to a good deal it recently negotiated. The no-name border router that uses access filters is the only security device that the company currently utilizes for protection against malicious outsiders. This router will be upgraded to a Cisco model 3640 and other security devices will be implemented on their network (see figure 1).

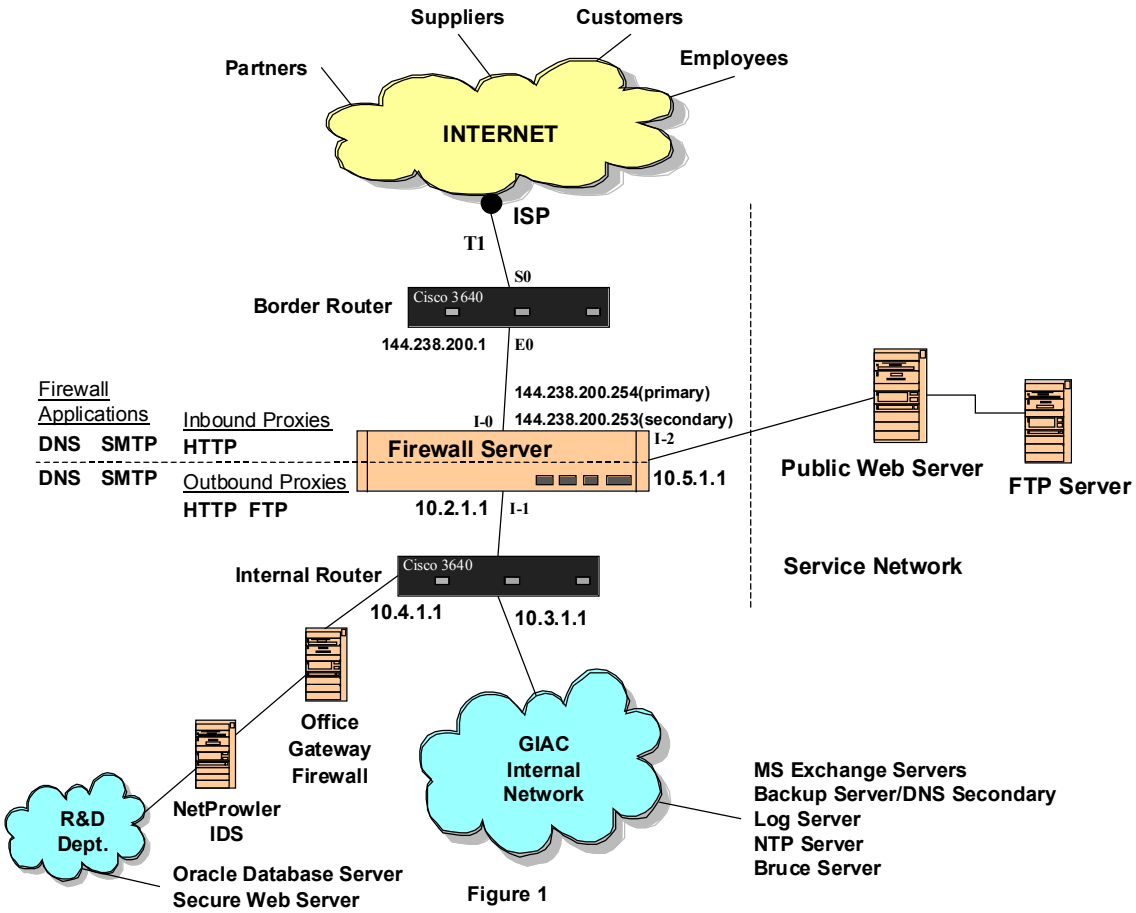

Figure 1

1.3.1 Border Router:

A Cisco 3640 with 4 available network module slots was selected since it is a medium range expandable router that should suit the needs of the company. GIAC will use only 2 of the network slots, a 4-port serial module and a 4-port ethernet module. Only one serial port will be used for the T1 WAN connection and one ethernet port will be used to connect to the primary firewall. The router will be used for initial screening of addresses and protocols as presented in the security policy. An internal Cisco 3640 router and several Cisco Catalyst 1912 Switches will be used on the internal network.

1.3.2 Primary Firewall:

A firewall was selected as part of a security package of services supplied and supported by a value-added reseller (VAR), Macro International. Macro will also supply and support the virtual private networks (VPNs) and the internal firewall.

The primary firewall will be the BorderWare Firewall Server version 6.1. It is a proxy/application level firewall built on a hardened operating system and running on a standard Intel platform. In our case, an Intel ISP 1100 1-GHz PC with 512 MB RAM and 20 GB hard drive was selected to host the firewall. The applications and proxies hosted here are memory and disk drive intensive more so than processor intensive. For this reason fast RAM access and a fast SCSI drive were selected with the Intel system.

Built on BorderWare's EAL4 certified, hardened operating system, the firewall is capable of running the following application servers: HTTP, DNS, SMTP/POP, and FTP. It can also run the following application proxies: HTTP, SHTTP, SSL, FTP, POP, Telnet, WHOIS, Gopher, AOL, Real Audio, NetShow multimedia, Oracle SQL and user defined proxies. It supports standard IP-Sec/IKE VPNs as well as a proprietary VPN called SmartGate.

SC Magazine in a 2000 review of the BorderWare firewall commented that "the secure OS that underpins BorderWare has resulted in performance improvements and a more flexible hardware requirement". The hardening process for the firewall OS, "removes risky processes such as IP forwarding, dangerous system calls and dynamic routing, as well as implementing such things as packet interface checks, random IP sequence numbers and packet filters". The magazine gave the firewall good grades (4 of 5 stars in all categories), did not mention a performance problem when several applications and proxies are running together on the same PC and was critical only of the lack of a server to server VPN, that was added in a subsequent release.

The primary firewall will be setup with the SMTP and DNS application servers running on both sides of the firewall. The following application proxies will be used: HTTP, and FTP. The fortune cookie sayings will reside on an Oracle database server in the R&D department. External VPN users will have access to the secure web server located in R&D and this department will be separated from the rest of the internal network by the internal router, a BorderWare Office Gateway firewall and a NetProwler intrusion

detection system (IDS). A publicly accessible web server along with an FTP server will be located on the service network. To differentiate web traffic to the secure web server (VPN users) versus the public web server on the service network, multiple address translation at the primary firewall will be used. A secondary IP address at the external interface of the firewall and a different name in DNS will be used for the secure web server for the VPN users. All other traffic is addressed to the primary IP address of the firewall external interface in accordance with network address translation (NAT).

The firewall will support 3 interfaces; interface I0 to the Internet (border router ethernet connection), I1 connection to the internal network, and I2 connection to the service subnet (also called the secure server net (SSN) by BorderWare). As mentioned above, network address translation (NAT) will occur at the firewall (internal network uses 10.2.0.0 / 255.255.0.0 network) and the firewall will host several virtual private network (VPN) implementations.

1.3.3 Virtual Private Networks

Two types of VPNs will be used for secure communications with the 4 primary external interface groups (customers, suppliers, partners and travelling employees).

GIAC has several outside suppliers (mostly in Taiwan) who supplement the internal R&D department in dreaming up new sayings and providing other raw materials for new sayings. This group will need the highest level of security and as such, will use the proprietary SmartGate client server VPN to connect to the firewall in order to access the web server on the service network. This solution is capable of utilizing smart cards and secure ID tokens but will not use them currently.

The suppliers will have access to special directories on the secure web server that are only accessible by them and the R&D staff. The customers and international partners will use a standard server to server (gateway to gateway) IPSec/IKE VPN. Employees who travel can use SmartGate configured laptops or a standard IPSec client server VPN. In each case, the primary firewall at GIAC will terminate the VPN connection.

1.3.4 Internal Firewall

A firewall will be setup to protect the small but extremely sensitive work in the R&D department where dreams become reality. A smaller and cheaper version of the BorderWare Firewall Server, called the Office Gateway, will be utilized here. Although the Office Gateway was design for small offices, it is sufficient for the extra security of the R&D group. The hardware selected to run the firewall is an Intel ISP 1100 750-MHz PC with 256 MB RAM and 7 GB hard drive. The additional protection afforded by this firewall will be discussed in the Security Policy section.

1.3.5 Servers

As mentioned previously, the DNS and SMTP (e-mail) servers will be located on the primary firewall. BorderWare has constructed a split DNS application and GIACs external addresses will reside on the outside of the firewall, with their internal addresses residing on the internal DNS part of the firewall. The firewall will act as the primary DNS for both internal and external addresses, and the ISP DNS server will be used as the secondary DNS for external addresses while an internal system will support the secondary DNS server. The SMTP application running on the firewall will feed one of 3 MS Exchange mail servers on the internal network. All e-mail users operate Windows NT but there are a few UNIX systems and Macs around that use the network only for web browsing.

The public web server is located on the service network along with the FTP server. The public web server will access the FTP server when necessary to send large non-sensitive corporate files. The secure web server is located behind the R&D firewall and the NetProwler IDS. It will access the secure Oracle database server for proprietary information when requested by VPN users (customers, suppliers, and partners). The database server has security safeguards including BlackICE defender firewall.

Assignment 2: Security Policy

2.1 Discussion:

The corporation has adopted a security policy of defense in depth. The defense in depth concept specifies concentric layers of protection for the internal corporate network much like a medieval castle with a moat, castle wall, defenders, and inside reserve force. Beginning at the Internet and proceeding through the Internet Service Provider (ISP), the outer boundary of this concentric defense perimeter is embodied in the border router. The next boundary of protection is the primary firewall. The third boundary is VPN protection afforded to trusted external users. The fourth boundary is the additional firewall protecting the R&D department. The fifth boundary is server and host level protections. In GIACs case, most of the servers are located outside of the R&D department firewall.

We will begin with a general corporate headquarters security policy that will be broken down to each of the defense in depth layer components.

2.2 General Security Policy

The management of GIAC has approved the following general policy.

Provide Internet web access to all employees
Provide Internet e-mail functionality to all employees

Provide DNS services
Provide Internet file transfer (FTP) capability to all employees
Allow external users access to the public web server (the public web server accesses the FTP server on the service network, so the FTP protocol must be open to outside users who have a connection to the web server)
Provide access to the secure web server (in R&D) for VPN users
Block all other traffic

The company feels confident in allowing access to the public web server, located on the service network, by Internet users, due to the internal safeguards on the server. The web server can access the FTP server, also located on the service network, for non-sensitive company information files, if requested by external or internal users. The Security Policy allows VPN users access to company sensitive information such as the fortune cookie sayings via the secure web server located in the R&D department. The secure web server does not contain sensitive information but has access to the Oracle database server containing secure information. Macro International, the security consultants, has assisted the company with much of the network security implementation and the safeguarding of the Web servers (see Macro's document gateway at http:\\security.macroint.com (login: public, password: security).

2.3 Border Router Security Policy:

The border router is being used to filter "noise" such as source routing, IP spoofing, and ICMP redirects. It will block private addresses and some protocols that are unnecessary to reach the firewall. The router access control list (ACL) will help reduce the traffic level at the firewall, which is important since the firewall is running several applications and proxies. The internal log server will be setup to receive specified sys-logging from the border router. The following is the ACL for the border router, with comments:

! **beginning of access-list 101 (inbound on serial port from Internet)**
!
! deny private addresses
!
access-list 101 deny ip 192.168.0.0 0.0.255.255 any log
access-list 101 deny ip 172.16.0.0 0.15.255.255 any log
access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
!
! deny localhost, broadcast and multicast addresses
!
access-list 101 deny ip 127.0.0.0 0.255.255.255 any
access-list 101 deny ip 255.0.0.0 0.255.255.255 any
access-list 101 deny ip 224.0.0.0 7.255.255.255 any
!
! deny incoming addresses with our internal address – prevent spoofing
!
access-list 101 deny ip 144.238.200.0 0.0.0.255 any log

```
!

! apply access-list 101 to S0 port inbound on border router
!
ip access-group 101 in
!
! beginning of access-list 102 (outbound on E0 port from Internal Net)
! deny all addresses except those originating from our network (log all traffic from
! GIAC addresses other than primary firewall address)
access-list 102 permit  ip host 144.238.200.254 any
access-list 102 permit ip 144.238.200.0 0.0.0.255 any log
access-list 102 deny  ip any any log
!
! Don't allow internal hosts to send icmp
!
access-list 102 deny  icmp any any log
!
! Only allow packets from border firewall
!
!end of access list 102

! apply access-list 102 to E0 port outbound on border router
!
ip access-group 102 in
!

! miscellaneous items added to config in order to armor the router on all ports
no ip direct-broadcast  ! prevents malicious directed broadcasts causing DoS
no ip unreachables ! prevents router from giving network info based on ICMP errors
no service tcp-small-servers ! prevents exploitation of undiscovered vulnerabilities
no service udp-small-servers ! prevents exploitation of undiscovered vulnerabilities
no service finger ! prevents hacker exploits of logged in users info
no ip http ! disables router server HTTP service
no ip bootp ! disables router server bootp service
no ip source-route ! disables source routing potential for exploitation
no snmp ! snmp is not being used for monitoring the router at this time
service password encryption ! displays router passwords in encrypted format
Banner /
WARNING: authorized access only
/
logging 144.238.200.34 ! specifies address of the firewall, will redirect to log server
!
! secure vty and aux port
!
line aux 0
access class 2 in
```

```
transport input all
line vty 0 4
access class 1 in
password 7 xxxxxxxxxx
login
!
! allow specific host into router
!
access-list 1 permit 144.238.200.34
!
! block access to aux
!
access-list 2 deny 0.0.0.0 255.255.255.255
```

2.4 Primary Firewall Security Policy

This is the most important security system on the network and is expected to block all unwanted traffic. Since the BorderWare Firewall Server is an application/proxy firewall, it can also monitor acceptable traffic types to determine its validity. For example, the HTTP proxy not only opens the firewall to standard HTTP port 80 (as a packet filter does), but it knows what valid HTTP traffic looks like. It will reject traffic such as internet relay chat (IRC) that could be setup on an internal server using port 80.

From the company's general security policy, we know to accept HTTP web traffic into and out of the site (from both the public and secure web servers). The same is true for FTP traffic to and from the FTP server although external users cannot directly access the FTP server. The Email and DNS servers are located on the firewall, so these protocols will pass through in a secure manner provided they are setup properly. Telnet is needed to manage the border router from an internal administrator only. All other traffic will be blocked. It is important to log all traffic hitting the firewall except "chatty" broadcast traffic like NetBios.

The firewall proxies are setup directionally between 2 firewall ports only, therefore the setup is as follows:
External to Service – http
Internal to Service – http
Internal to Service – ftp
Internal to External – http
Internal to External – ftp

The following is the primary firewall rulebase:

Source	Destination	Service	Action	Track
F/W Admin	Firewall	Firewall	Accept	Long
Any	Firewall	NBT/ident	Reject	No

Any	Firewall	Any	Drop	Long
VPN	Secure Web Server	http	Accept	Long
Internal	Any	http	Accept	Long
Internal	Any	ftp	Accept	Long
Telnet station	Border Router	telnet	Accept	Long
External	Public Web Server	http	Accept	Long
Service	Any	Any	Drop	Alert
Any	Any	Any	Drop	Long

The first section of the rulebase above describes access to the firewall itself. Only the administrator is provided access and broadcasts reaching the firewall are rejected (RST sent) and not logged since this would quickly fill up the log space with unnecessary traffic entries. All other traffic directed to the firewall is dropped (timeout) and logged. Rulebase order is important here since if the third rule (drop and log any traffic to the firewall) had been issued first, the other 2 rules would have no effect. Thus we always list from the specific to the general.

The next sections involve accepting certain traffic types. VPN users coming from the Internet can be identified by their protocols and allowed access to the secure web server on the internal network. VPN users can send and receive smtp e-mail since the firewall hosts a smtp mail server. It's not necessary in this case to specifically open the firewall to smtp (or DNS) above since the applications take care of this. Additional VPN protection measures are discussed in the next section.

Internal users (employees on site) are given access to the Internet and Service networks for http (web traffic) and FTP. Providing access to the Service network may be considered risky since it is unsecure, but with the BorderWare firewall running http and ftp proxies, the company currently feels comfortable allowing this to happen. Next, the telnet admin station is granted access to the border router on the outside of the firewall. Internet users are allowed access to the Web (http) server on the Service network. The public web server can access the FTP server located on the Service network (for large file transfer requests, etc.), but Internet users cannot access the FTP server directly.

The final sections of the rulebase drops traffic coming from the Service network and any traffic not explicitly accepted in the preceding rules. Since it would be very unusual under normal circumstances to see traffic originating from the Service network, this rule also issues an alert (to the firewall security admin) in addition to dropping it. Traffic originating from the Service network could indicate that hackers compromised one of the servers.

2.5 VPN Security Policy

As mentioned earlier, standard IPSec will be used to support GIAC customers and international partners, and the proprietary SmartGate VPN will be used by suppliers and

travelling employees (for example on their frequent trips to the Far East pursuing ancient sayings). SmartGate has several advantages over IPSec. During setup between the remote client (called SmartPass) and the SmartGate server, a software ID token is created. Together with the user's login and password, the token is needed to establish secure connections. The token is another security mechanism protecting against a compromised login and password. IPSec utilizes transport layer protocols (e.g. ip-protocol 50 or 51) that are often blocked by firewalls and routers. SmartGate on the other hand, uses the TCP transport and any available open TCP ports on the local firewall such as tcp port 80 (http). SmartPass users begin the setup using a shared secret password to initiate authentication with the SmartGate server.

Just as with the SmartGate users, the IPSec users require encryption per the company's security policy database (see below) and therefore will use the Encapsulating Security Payload (ESP) protocol. They begin their setup by exchanging shared secret authentication passwords and then security associations are setup using Internet Key Exchange (IKE) and Oakley main mode. In all VPN situations, except for travelling employees, a security gateway will be used on both sides of the VPN connection. Therefore tunnel mode security associations are used for IPSec setup.

The following is the Security Policy Database for GIAC VPN operations. Inbound and outbound policies are the same for each user category.

User group	**VPN Type**	**Classification**	
Customers	IPSec	Secret	
Partners	IPSec	Confidential	
Suppliers	SmartGate	Top Secret	
Employees	SmartGate	Top Secret	

The following is the Security Associations Database used in conjunction with the Security Policy Database above.

Classification	**Encryption**	**Authentication**	**Duration**
Confidential	DES 56-bit	None	300 minutes
Secret	3-DES 168-bit	HMAC MD5	240 minutes
Top Secret	Blowfish 448-bit	HMAC MD5	180 minutes

A major concern for GIAC or any company contemplating virtual private network connectivity with external networks (i.e. extranet), is the security of the external sites being given access to your internal network. For this reason, each site has agreed to limit VPN connectivity with GIAC to selected approved users on only one subnet at the site. Virtual LAN (VLAN) connectivity within the site will help insure each approved user can access the VPN regardless of their physical location. As part of the semi-annual GIAC network security audit, these concerns will be re-examined. The VPN users are controlled via IPSec and SmartGate application security plus only one application , http, is allowed via the VPN.

2.6 Internal Router, Firewall and Intrusion Detection System (IDS) security policy:

The purpose of the internal router, firewall and IDS are to add protection to the research and development department. The router provides a separate path for VPN traffic to access the secure web server by blocking this traffic from entering the internal 10.3.1 network. The router also segments the R&D department from the rest of the corporate network. The firewall is running the http inbound and outbound proxy (much like the BorderWare Firewall Server, a larger version of the Office Gateway firewall used here) and directs the VPN traffic only to the secure web server. The firewall will also block and log ftp and telnet traffic and will allow only smtp, http, and syslog traffic (R&D users have an NT Exchange mail server that communicates with the other mail servers using smtp). The Intrusion Detection System (IDS) is setup to detect malicious outsiders or insiders attempting to steal secret sayings or to otherwise disrupt the primary economic interests of this $200 million-per-year company. The IDS will alert the company security officer if it detects evidence of malicious activity such as a covert loki channel or some other effort that could penetrate the company's defense in depth.

Assignment 3: Audit Your Security Architecture:

3.1 Planning the Assessment:

A security consultant different form the company who helped design the security architecture, will be chosen to perform an audit of the new security architecture for GIAC Enterprises. The consultants were selected with a bid of $4,800 for 2 days of work by 2 SANS certified firewall analysts. A formal report will be delivered to the company within 2 weeks of the effort. The work will be performed on the first 2 days of a 3-day holiday weekend. The last day of the weekend (example Memorial Day weekend), will be used for GIAC employees to ensure the network is back and functioning after the anticipated network downtime as part of the audit. The audit will involve taking parts of the network offline and running port scans, password crackers, network reconnaissance tools, and the like. The audit will be conducted in several stages; first will be from the outside (i.e. Internet) looking into the security architecture, and second will be from inside the corporate network. The second stage will involve an examination of the VPN tunnels into the network (as mentioned above) since these users have certain insider access. GIAC employees will be alongside the security consultants at all times both as a security measure and for training opportunities on the audit procedures that will be conducted henceforth every 6 months by the employees.

The primary audit tool being utilized by the security consultants for both the exterior and interior audit stages, is Axent NetRecon. NetRecon is a network vulnerability assessment tool that will probe nearly all network devices (including servers and workstations) and will analyze and report on the security holes that it discovers. The company has not committed to purchasing NetRecon or any other network audit tool, but will wait until the

test is complete and the consultants make final recommendations. The consultants have expertise in many other network security tools as well and will explain their use to the GIAC network administrators as time permits.

3.2 Implementing the audit:

The first stage of the audit implementation will place the NetRecon on the Internet (at the consultant's office) on Saturday morning after securing the entire GIAC network for the 2-day testing period. The test will focus (and report) on the SANS consensus top ten network security vulnerabilities as listed on their web site (http://www.sans.org/topten.htm). These are the most commonly exploited network vulnerabilities and is a good place to start since most hacker types are not deep thinkers and will tend to follow the path of least resistance when looking for cool targets to exploit. The GIAC network security setup is unique and very restrictive in terms of applications and protocols allowed to penetrate their defenses nevertheless there are several areas of concern and these will be examined in depth.

3.2.1 SANS Top Ten Vulnerabilities

Since UNIX and LINUX systems are no longer used at GIAC (except in a few isolated cases), most of the SANS top ten are not applicable. Bind is used as part of the Split DNS architecture on the firewall but it has been updated (via CERT advisories at http://www.cert.org/advisories) to correct the nxt, quin, and named vulnerabilities. The public web server and the secure web server have removed all sample CGI programs and the secure web server does not run any CGI programs or Cold Fusion. The public web server may therefore be exploitable. RPC's, sendmail, mime, sadmind and mountd are not a problem since they affect UNIX and LINUX primarily but the Remote Data Services (RDS) vulnerability could be a problem since it is used on both of the company's web servers even though both web servers have the latest upgrades and patches. The company is concerned about file sharing vulnerabilities such as viruses and worms since the GIAC employees frequently use file transfers and email over the Internet. Keeping up to date on the latest OS patches and virus signatures will be a priority. NetBios over tcp/ip (NBT) is used throughout the company and the remote VPN sites for file transfers. In addition to the security of the remote VPN sites, the vulnerability of NetBios misuse is a major concern of GIAC management. The next item on the SANS top ten is none or weak password protection for administrator accounts on servers, network devices, etc. This will be resolved with NetRecon and through the use of L0pht Crack (http://www.l0pht.com), a password cracking tool, by the consultants. Finally, imap, pop and snmp are not used at GIAC but mobile code scripting holes within products such as ActiveX may present a problem on the IIS web servers and Internet Explorer browsers used inside the network.

3.2.2 Other Vulnerabilities:

Aside from the SANS top ten, most of GIAC's vulnerabilities are associated with the major protocols and applications allowed passed the firewall into the internal network.

Access into the internal network from the service network is a concern since a hacker could possibly compromise one of the servers on the service network and launch an attack from there. For this reason, the audit will test every segment from every other segment, and will take the service network offline, using its IP addresses to attempt access to the internal and external networks. Special attention will be paid to DNS, using Sam Spade (a sophisticated DNS query tool), if necessary to supplement NetRecon. Email access utilizing the smtp protocol will be examined , as will the other 2 major vulnerabilities FTP and HTTP. Telnet and logging from the border router are 2 other applications allowed passage through the firewall. Covert channels using one of the approved protocols (loki variants, smtp, etc.), and denial of service vulnerabilities (e.g. distributed DoS, SYN flood, etc.) are other concerns. A major concern is the network bottleneck and single point of failure located at the primary firewall. This could be the Achilles Heel of the network security architecture.
The list below summarizes the applications and protocols allowed to pass into and out of the GIAC network.

From where	To where	Protocol	Security note
External	Service	http	F/w proxy
	Through f/w	ESP ip proto 50	IPSec encryption
	Through f/w	ISAKMP udp/500	IPSec setup
	Through f/w	tcp/80	SmartGate port #
	R&D	http	VPN web traffic
	Internal	smtp	F/w application
		DNS	F/w application
Internal	Service	http	F/w proxy
		ftp	"
	External	http	"
		ftp	"
		telnet	Admin only to rtr.
		smtp	F/w application
		DNS	F/w application
Service	External	none	
	Internal	none	

This checklist will help the consultants to evaluate if some of the allowable protocols are contributing to vulnerabilities based upon the output of NetRecon and the other audit tools.

3.3 Results of the Audit:

The security consultants completed their audit work on Sunday afternoon and the network was reconnected and tested Sunday evening and Monday (holiday) in preparation for opening of business on Tuesday. The employees who accompanied the audit team learned quite a lot from the 2 SANS certified firewall analysts (several signed up for SANS training). The report was received within 2 weeks and a meeting was held

between corporate security, network administration and management to discuss the recommendations.

Below are several of the items taken from the NetRecon report on the network vulnerabilities observed during the audit. Notice the description, recommended solution and additional info on the subject vulnerability.

Vulnerability Name: **FTP access obtained**
Risk: 54
Description: NetRecon has successfully logged on to an FTP server either anonymously or by guessing the login name and password from a short list. FTP (file transfer protocol) is a protocol for transferring files between systems. The ftp service is used by many applications for data communications. Some systems also allow users to connect to an ftp server to upload and download files. ftp servers are vulnerable to a wide range of attacks designed to retrieve files without authorization (including password files) and execute commands on other parts of the server. Anonymous FTP means that anyone who can connect to the service can log in, greatly increasing the potential number of attackers and attacks. There are a number of other ways that anonymous FTP access can be abused, including using an anonymous FTP site as a drop zone for illegal files.
Solution: Obtain the latest patches from your vendor. Older versions of ftp on both UNIX and Windows NT contain security vulnerabilities. Don't allow anonymous ftp access unless it is absolutely necessary. Configure your system to log all ftp accesses and transfers and periodically check these logs for patterns of misuse. Make sure the home directory of your ftp server is not writable and disallow connections from system Ids (including root, uucp, nobody, and bin). Firewall FTP access where practical. Symantec's Intruder Alert can be used to monitor any connections to the ftp port.
Additional Information: http://www.cert.org/tech_tips/anonymous_ftp_abuses.txt (1)
Links: 1. http://www.cert.org/tech_tips/anonymous_ftp_abuses.txt
# of Network Resources: 1
Network Resource Aliases Network Resource Type Details
xxx, 10.1.xx, 00:00:f2:12:47:19 IP host, xxx Port = 21, Protocol = TCP, Service = ftp
Page 1 of 56

Vulnerability Name: **anonymous FTP access is enabled**
Risk: 53
Description: NetRecon has successfully logged on to an FTP server anonymously. FTP (file transfer protocol) is a protocol for transferring files between systems. The ftp service is used by many applications for data communications. Some systems also allow users to connect to an ftp server to upload and download files. ftp servers are vulnerable to a wide range of attacks designed to retrieve files without authorization (including password files) and execute commands on other parts of the server. Anonymous FTP means that anyone who can connect to the service can log in, greatly increasing the potential number of attackers and attacks. There are a number of other ways that anonymous FTP access can be abused, including using an anonymous FTP site as a drop zone for illegal files.
Solution: Don't allow anonymous ftp access unless it is absolutely necessary. Configure your system to log all ftp accesses and transfers and periodically check these logs for patterns of misuse.

Make sure the home directory of your ftp server is not writable and disallow connections from system Ids (including root, uucp, nobody, and bin). If practical, deny FTP access using a firewall. Symantec's Intruder Alert can be used to monitor any connections to the ftp port.
Additional Information: http://www.cert.org/tech_tips/anonymous_ftp_abuses.txt (1)
Links: 1. http://www.cert.org/tech_tips/anonymous_ftp_abuses.txt
# of Network Resources: 1
Network Resource Aliases Network Resource Type Details
xxx, 10.1.xx, 00:00:f2:12:47:19 IP host, xxx Port = 21, Protocol = TCP, Service = ftp
Page 2 of 56

Vulnerability Name: **passwd file obtained**
Risk: 49
Description: NetRecon has obtained a password file called passwd . This is the file used to store passwords on some network resources. If an attacker can gain access to this file using other vulnerabilities, and if shadow passwords are not implemented, there is a high probability that some passwords can be cracked using widely distributed password-cracking tools for Windows.
Solution: Implement shadow passwords, which prevent an attacker from gaining access to passwords.
Additional Information:
Links:
# of Network Resources: 1
Network Resource Aliases Network Resource Type Details
xxx, 10.1.xx, 00:00:f2:12:47:19 IP host, xxx
Page 6 of 56

Vulnerability Name: **smtp service enabled**
Risk: 45
Description: The smtp service uses the Simple Mail Transfer Protocol (SMTP) to send electronic messages. The smtp service may be used to obtain information about valid user names and other systems in the network. The smtp service is vulnerable to a variety of attacks.
Solution: Disable this service if it isn't necessary.
Additional Information:
Links:
# of Network Resources: 1
Network Resource Aliases Network Resource Type Details
xxx, 10.1.xx, 00:00:f2:12:47:19 IP host, xxx Protocol = TCP, Port = 25, Service = smtp
Page 9 of 56

There were many security problems that were identified and corrected, such as weak passwords, Windows server and workstation updates, etc. The consultants however gave GIAC network security a very good grade based upon the firewall security, split DNS and E-mail services. The VPNs were very secure for the most part provided the remote sites were audited properly. The web servers had some setup problems that were corrected but were being managed well. The border router was setup very well as were the internal router and switches. The employees were apparently well aware of proper

computer security particularly the R&D department where the company secrets were located.

The major architectural vulnerabilities reported by the consultants fell into several areas as listed in the table below:

Application/System	Vulnerability	Recommended action
FTP	Weak protocol security	Remove from network
telnet	Vulnerable outside firewall	Authenticate and/or encrypt
Primary firewall	Susceptible to overload and/or dDoS attack	Move some functions to alternate firewall
VPN	Internal access not restricted	Provide direct route to web server

Hacker types frequently use file transfer protocol since it is inherently weak from the security standpoint. The company provides information files to potential customers such as previously used fortune cookie sayings and negative information on their competitors. Perhaps this info can be incorporated into the public web server without keeping the FTP protocol vulnerability. Telnet is used to access the border router outside the firewall and the company will look into using an encryption capability like Layer 2 Forwarding protocol to access their Cisco router.

The primary firewall is the big area of concern expressed by the consultants. It is susceptible to becoming overloaded due to its multiple functionality and slows down processing when traffic gets heavy. Because it is single threaded and heavily loaded, it is also susceptible to distributed denial of service attacks (syn floods and the like). The consultants recommend providing an alternate firewall and offload some of the functionality. This will reduce the load on the primary firewall and provide a redundant path into the network if needed.

Finally, the VPN traffic could enter the internal network since it is using http (tcp/80) that is open on all workstations and many servers. Although this is not such a big concern if the remote extranet sites (customers, partners and suppliers) are properly secure, it is something worth considering if network changes are undertaken.

3.4 Recommended solution

Based upon the report from the consultants and the suggestions and comments of the network administrators, network security employees have submitted a new architecture to management for approval. As shown in figure 2, the new architecture employs an additional firewall (not necessarily a BorderWare Firewall Server) and connects the R&D department directly to the redundant firewall. Email and DNS traffic will have to travel from one firewall to the other but this can be done with a connection between the firewalls. Management will decide shortly if this proposed network architecture change is approved.

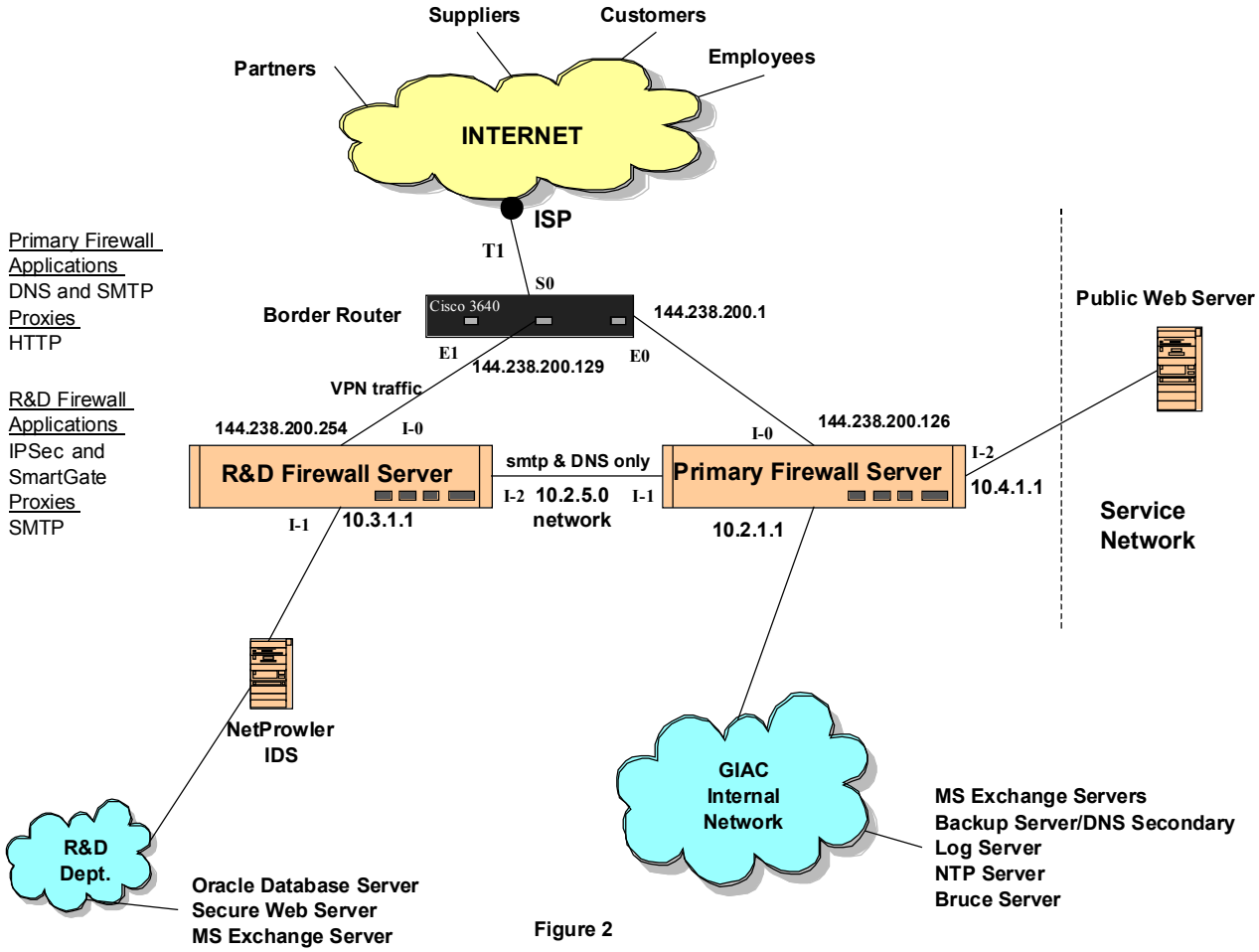

Figure 2

Assignment 4: Design Under Fire:

The network design chosen for this assignment was taken from Jeff Stevenson's practical at http://www.sans.org/y2k/practical/jeff_stevenson_gcfw.doc. Figures 3 and 4 contain Jeff's network design. The routers are Cisco 4700 and the firewalls are Firewall-1 (version 4.1 SP2) from Check Point, and CyberWall Plus-IP (version 6.03) from Netguard-1. Both firewall types are running on Windows NT server 4.0 (SP6a). The VPN used in his design is Ravlin 10 VPN from Red Creek.

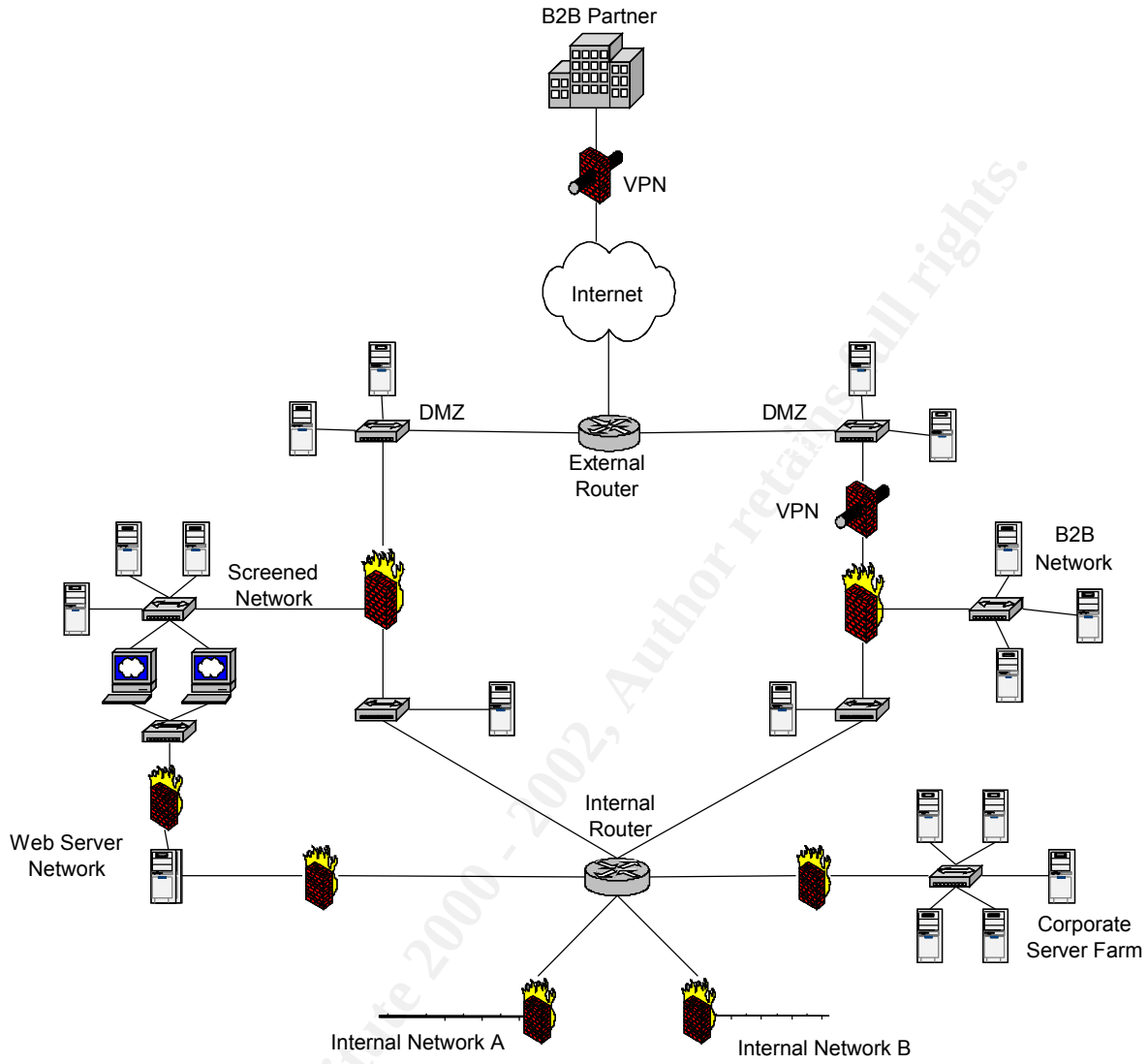

figure 3

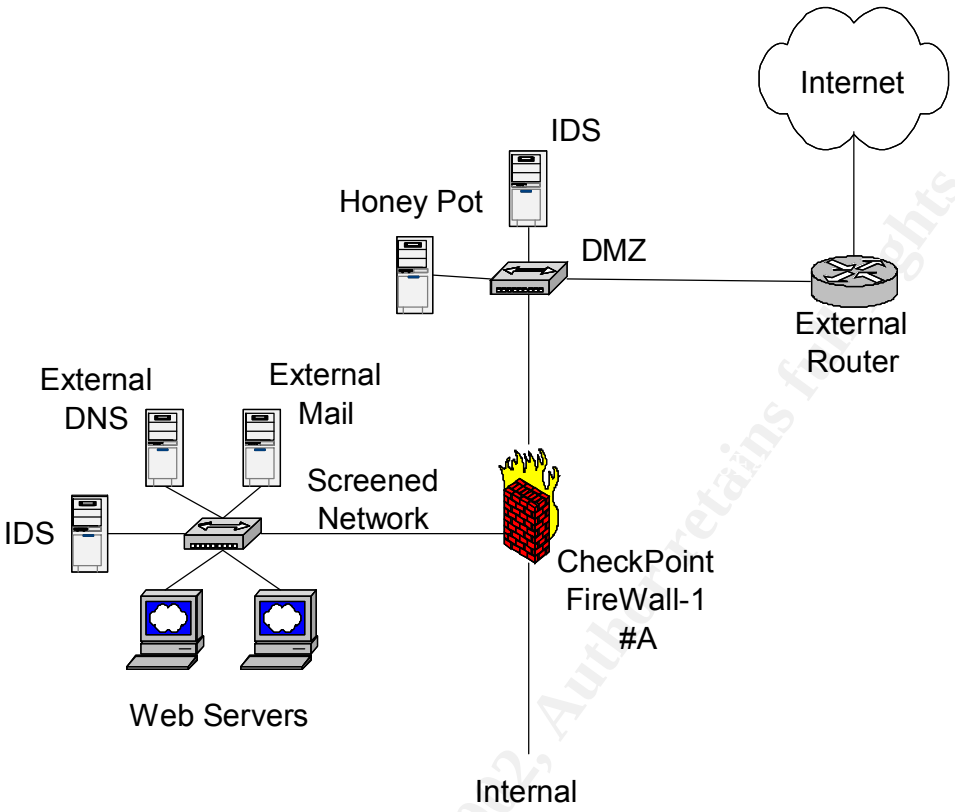

figure 4

4.1 Firewall Attack:

Mr. Stevenson's network design is very thorough and probably expensive (to purchase and maintain), however it is based on standard commercial products with known exploits. At http://www.securityfocus.com are listings of vulnerabilities by product (BorderWare used above is not included however). The recently posted vulnerabilities for CheckPoint Firewall-1 are applicable vulnerabilities of Mr. Stevenson's network solution.

Firewall-1 has a vulnerability (2000-11-01 valid username vulnerability) such that an attacker can determine a valid firewall username by the response given to an authentication request (firewall port 259) from a remote client. I would attempt connection to the firewall IP address on port 259 by entering a username and password. If the username is invalid, the firewall will respond with "<username> not found". If the username is valid and the password is incorrect, the firewall will respond with "Access denied by Firewall-1 authentication". Eventually a valid username will be found and then by using a password cracker with the valid username, access can be gained into the firewall using the compromised the user's privileges.

Once access is gained to the firewall, changes can be made to open the network to vulnerable protocols, such as an nmap or NetRecon scan of available services, followed by host or server intrusions, introduction of malicious code (trojans, viruses, etc.), or a denial of service.

4.2 Denial of Service Attack:

For the denial of service attack on Mr. Stevenson's design, I have chosen to attack the primary border router using tribal flood network 2000 (TFN2K). Info regarding the capabilities of TFN2K can be found at http://www2.axent.com/swat/News/TFN2k_Analysis.htm, and at http://www.angelfire.com/rock/nsi/. To download TFN2K (and other hacker tools) visit ftp://ftp.ntua.gr/pub/security/technotronic/denial/.

The border router is a Cisco 4700 model. It is a good medium scale router (133 MHz RISC processor) that should hold up well under many denial of service attacks. Unfortunately the wide area bandwidth connecting the router to the Internet is only a T1 (1.54 Mbps bandwidth) and should become saturated as the router is flooded with millions of packets per second from 50 cable modems. Even if the router can keep up with processing this large a quantity of packets, normal traffic will probably slow to a crawl. Since the router in question is outside the firewalls, there is really no good way to defend against this attack.

TFN2K can be identified on host systems (TFN2K can be identified since the Base 64 encoding leaves a telltale fingerprint at the end of every packet). The attack can then be traced back and possibly thwarted. TFN2K can also be blocked using egress filtering at the origination "agent" sites. However once the agent computers are compromised and their site is not performing egress filtering, there is not much that can be done to stop an attack in progress. Prevention and detection is the key for DDoS attacks.

4.3 Internal System Compromise:

Malicious code such as the Wscript.KakWormB http://www.sarc.com/avcenter/venc/data/wscript.kakworm.b.html or its predecessor, Wscript KakWorm, could be used to penetrate the network defenses when addressed to an internal user. The worm affects Microsoft Outlook and Outlook Express clients of the Microsoft Exchange Server used in Jeff's network design. This, and most, networks allow properly formatted e-mail through its defenses with the malicious code being carried in the body of the e-mail in most cases. Although there are patches to Outlook and virus detection signatures to prevent this attack, most sites do not keep up to date on all the latest patches and virus signatures. A custom designed worm (without detection signatures, etc.) would certainly get through all internal defenses. The worm could be used to setup a covert channel using ActiveX (for example) on the victim's PC without anyone's knowledge. The black hats would have easy access to the fortune cookie sayings at this point.

References

Print Media

Anonymous, Maximum Security, 2nd Edition. Sams Publishing 1998.

Axent Technologies, Inc., NetRecon – Installation and Getting Started Guide. 2000.

Fowler, Dennis, Virtual Private Networks. Morgan Kaufmann Publishers, Inc. 1999.

Lewis, Chris, Cisco TCP/IP Routing. McGraw-Hill Series on Computer Communications, 1998.

Stevens, W. Richard, TCP/IP Illustrated, Volume 1. Addison-Wesley, Boston, MA. 1994.

On-Line Sites

www.axent.com

www.borderware.com

www.cert.org

www.checkpoint.com

www.cisco.com

www.l0pht.com

security.macroint.com

www.microsoft.com

www.samspade.org/ssw/

www.sans.org

www.securityfocus.com