GIAC Enterprises: Server Security Policy and Procedures for E-Commerce

GIAC Information Security Officer (GISO) Practical
Version 1.2
SANS Capitol Hill

By Ellen Roth

Assignment 1: Describe GIAC Enterprises

1.1 Description of GIAC Enterprises

GIAC Enterprises (GIAC) is a Washington D.C. e-commerce company that sells United States flags to consumers across the country. GIAC's inventory of products includes small desktop flags to very large flags that can be hung from the side of skyscrapers to demonstrate patriotism. The prices of GIAC's flags range from $1.00 to $2500, depending on size. There are no other known e-commerce sites in the United States that have such a wide, varied selection of flags to meet the needs and budget constraints of virtually every patriotic customer.

GIAC consists of four major departments: Operations, IT Services, Manufacturing, and Customer Service. Each of these departments has a Vice President, who is the most senior person and who reports directly to the GIAC Chief Executive Officer (CEO). The smallest group is Operations, which has a staff of five individuals. This group handles GIAC's administrative functions such as marketing and PR, internal human resources, and office management. The next smallest group is Customer Service, with eleven personnel. This group primarily handles product shipping and customer inquiries on the 24-hour hotline that is described in the Business Operations section of this document. The twenty-person Manufacturing Group produces the flags that GIAC sells. Finally, the IT Services Group, featured in this document, consists of fifteen individuals. These are the technical personnel who ensure that GIAC's e-commerce network is operational and ready to process orders, and that individual servers are able to perform their e-commerce function. These are also the individuals who assess and make security recommendations to the company.

Over the past year, GIAC's business has grown markedly due to world events. Average daily sales have risen from $5,000 to $25,000 a day, with no decline in sight. GIAC attributes its success to its ability to keep its web servers available on average 99% of the time. Since GIAC's success depends in part on impulse buying, GIAC must ensure that it is able to take orders twenty-four hours a day. In addition, GIAC must make sure it is able to accept a wide range of credit and debit cards, from Visa to Carte Blanche.

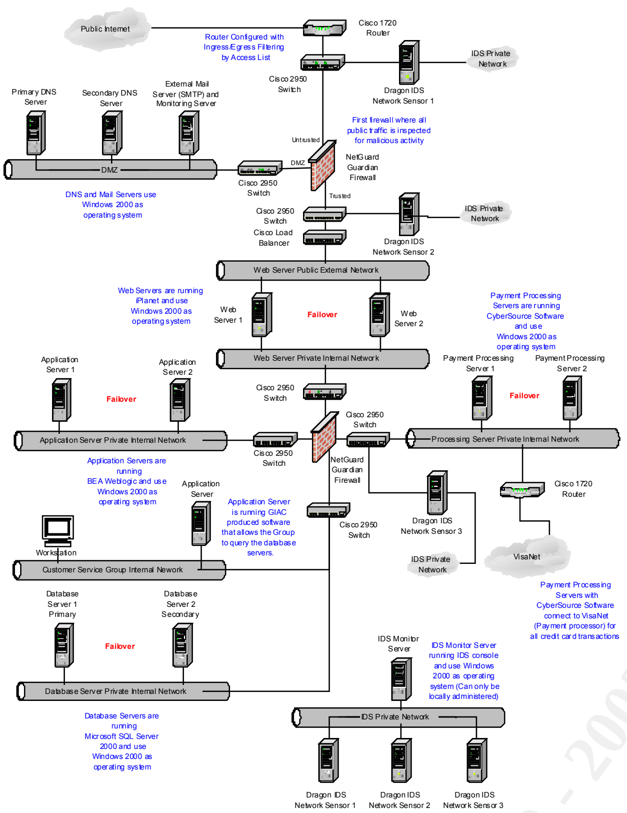
1.2 IT Infrastructure

GIAC's Information Technology (IT) infrastructure is shown in Figure 1-1 (An enlarged version is included as Appendix A of this document). The IT infrastructure is based on the Windows 2000 operating system. The design was created with e-commerce network architecture best practices and a defense-in-depth strategy in mind. The overall infrastructure meets the strict security requirements necessary to securely handle consumer credit card information. The infrastructure configuration will be discussed in the following sections.

Public Application Area

GIAC's first line of defense is a Cisco 1720 packet-filtering border router, which runs Cisco IOS Software version 12.2. This router is critical to the overall network design, because it is the first checkpoint encountered by inbound traffic, and the last checkpoint encountered by outbound traffic. Consequently, the router has been configured with ingress/egress filtering, according to guidance specified by the SANS Institute, which states that[1]:

1. Any packet coming into your network must not have a source address of your internal network
2. Any packet coming into your network must have a destination address of your internal network
3. Any packet leaving your network must have a source address of your internal network



Public Internet
Router Configured with Ingress/Egress Filtering by Access List
Cisco 1720 Router
Cisco 2950 Switch
IDS Private Network
Dragon IDS Network Sensor 1
Primary DNS Server
Secondary DNS Server
External Mail Server (SMTP) and Monitoring Server
First firewall where all public traffic is inspected for malicious activity
Untrusted
DMZ
NetGuard Guardian Firewall
DMZ
Cisco 2950 Switch
Trusted
DNS and Mail Servers use Windows 2000 as operating system
Cisco 2950 Switch
Cisco Load Balancer
IDS Private Network
Dragon IDS Network Sensor 2
Web Server Public External Network
Web Servers are running iPlanet and use Windows 2000 as operating system
Web Server 1
Failover
Web Server 2
Payment Processing Servers are running CyberSource Software and use Windows 2000 as operating system
Web Server Private Internal Network
Application Server 1
Application Server 2
Payment Processing Server 1
Payment Processing Server 2
Failover
Cisco 2950 Switch
Failover
Cisco 2950 Switch
Application Server Private Internal Network
Cisco 2950 Switch
Processing Server Private Internal Network
NetGuard Guardian Firewall
Application Servers are running BEA Weblogic and use Windows 2000 as operating system
Application Server
Application Server is running GIAC produced software that allows the Group to query the database servers.
Cisco 2950 Switch
Dragon IDS Network Sensor 3
Cisco 1720 Router
Workstation
IDS Private Network
VisaNet
Customer Service Group Internal Nework
Payment Processing Servers with CyberSource Software connect to VisaNet (Payment processor) for all credit card transactions
Database Server 1 Primary
Database Server 2 Secondary
Failover
IDS Monitor Server
IDS Monitor Server running IDS console and use Windows 2000 as operating system (Can only be locally administered)
Database Server Private Internal Network
IDS Private Network
Database Servers are running Microsoft SQL Server 2000 and use Windows 2000 as operating system
Dragon IDS Network Sensor 1
Dragon IDS Network Sensor 2
Dragon IDS Network Sensor 3

Figure 1-1 GIAC Enterprises Network Diagram

4. Any packet leaving your network must not have a destination address of your internal network.
5. Any packet coming into your network or leaving your network must not have a source or destination address of a private address or an address listed in RFC1918 reserved space. These include 10.x.x.x/8, 72.16.x.x/12 or 192.168.x.x/16 and the loopback network 127.0.0.0/8.
6. Any source routed packets or any packets with the IP options field set should be blocked.
7. Reserved, DHCP auto-configuration and Multicast addresses should also be blocked:

   0.0.0.0/8
   169.254.0.0/16
   192.0.2.0/24
   224.0.0.0/4
   240.0.0.0/4

This ingress/egress configuration makes the most of Cisco's Access Control List (ACL) feature on its routers, and prevents many common cyber attacks. By using this setup, GIAC is ensured that the Cisco 1720 router is truly operating as a first line of defense.

[1] *SANS Institute "The Twenty Most Critical Internet Security Vulnerabilities (Updated) The Experts' Consensus" Version 2.504 May 2, 2002* *http://www.sans.org/top20.htm* *(September 4, 2002).*

As demonstrated below, should the Cisco router fail and traffic reach the first Guardian firewall, a very similar firewall configuration will stop the types of traffic that the packet-filtering firewall was intended to extinguish before it reaches the innermost parts of GIAC's network.

Beyond the Cisco 1720 router, there is a Cisco 2950 switch that controls the direction of traffic between Dragon Intrusion Detection System (IDS) network sensor 1 and the first firewall[2]. When traffic reaches the IDS, it is evaluated to determine if it can be considered malicious traffic. Should the IDS detect anomalous traffic, the router may be configured to block a specific IP address. However, changing the router's configuration in this way is rare, and is only the result of the administrator being able to compile enough evidence to prove that a specific IP address appears to have malicious intentions. In general, the router is not configured with this level of granularity since GIAC processes orders from individuals all over country, and its customers change constantly. Blocking a specific IP address can potentially shut out business that is important to GIAC's livelihood. If the IDS does not register a problem[3], traffic is directed to the next layer of defense in the public application area--GIAC's NetGuard Guardian 2.0 stateful inspection firewall. Although Guardian 2.0 is relatively expensive, it integrates well with Microsoft 2000, which the operating system currently in use[4].

The stateful inspection firewall is able to keep track of the state of multiple, simultaneous TCP/IP based connections that are made to GIAC's network within its state table. As a result, it is nearly impossible for a potential attacker to launch a Denial of Service (DoS) attack on GIAC's network and consequently reduce its availability. The firewall has been configured overall to allow inbound secure web and unsecured web traffic to connect to the servers in the Web Server DMZ so that e-commerce orders can be placed. The firewall ruleset indicates that inbound connections are permitted as long as their destination port is high, generally above port 1023[5]. In addition, the ruleset always blocks the following traffic, consistent with the National Institute for Standards and Technology *Guidelines on Firewalls and Firewall Policy*:

- Inbound traffic from a non-authenticated source system with a destination address of the firewall system itself
- Inbound traffic containing ICMP, inbound or outbound traffic using a source address that falls within the address ranges set aside in RFC 1918 as being reserved for private networks
- Inbound traffic from a non-authenticated source system containing SNMP
- Inbound traffic containing IP Source Routing information

[2] *Cisco 2950 switches are also located throughout the entire GIAC architecture at each firewall interface.*

[3] *The IDS essentially attempts to compile "normal" patterns in network traffic over time, so inconsistencies can be detected and noted as anomalies.*

[4] *"Windows NT Firewalls Guardian Vs. Firewall/Plus Vs. Eagle NT Vs. AltaVista Firewall"* *http://www.pctoday.com/editorial/hth/970720.html*

[5] *Wack, J., Cutler K., and Pole, Jamie. Guidelines on Firewalls and Firewall Policy: Recommendations of the National Institute of Standards and Technology. p. 11 http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf*

- Inbound or outbound network traffic containing a source or destination address of 127.0.0.1
- Inbound or outbound network traffic containing a source or destination address of 0.0.0.0
- Inbound or outbound network traffic containing directed broadcast addresses

There are Cisco 2950 switches on either interface of the firewall, connecting to the DMZ network and the web server public external network.

Within the DMZ there are several publicly accessible servers. Two DNS servers, one primary and one secondary, allow all domain request information for GIAC's networks to be answered. This prevents GIAC from having to rely on third party service providers to make changes to their naming structures in a timely fashion. The DNS servers are configured so that if one DNS server fails, the other can immediately take over. The external mail server, also located in the DMZ, is running Microsoft Exchange Server 2000 to allow communications via email to GIAC's customers after they have successfully completed a transaction. As explained in *Section 1.3 Business Operations*, redundant email servers are not necessary for GIAC, as email is not an important part of daily operations or customer service.

Private Internal Networks

Web Server Internal Network

GIAC uses a Cisco load balancer to dynamically shift user requests to each web server within the web server internal network. The purpose of the load balancer is to ensure that neither web server is inundated with requests and therefore becomes overloaded and inaccessible to customers. Servers within this network segment are configured with Microsoft Windows 2000 Server SP3 and Sun iPlanet 6.0 web server.

The web server internal network is an air gapped network point that ensures that public internet traffic cannot traverse. As shown in Figure 1-1, the network is isolated from both the external/publicly accessible network segments including the DMZ with a firewall. It is also isolated from the internal network segments including the application server internal network with another firewall. The air gapped feature has been created by ensuring that there is a physical separation between the screened web server subnet and the DMZ external network.

The web servers in this segment, like the servers in the application server network and database server network, are clustered. This provides redundancy and a safeguard should one web server be compromised by an attack, or fail. The customer attempting a transaction is not cognizant that there are multiple web servers in the architecture, as the servers present themselves as a single virtual server[6]. The customer simply enjoys the high-availability and reliability of GIAC's ordering capability. For additional security,

[6] *McGeehe, Brad M. "An Introduction to SQL Server Clustering"* http://www.sql-server-performance.com/clustering_intro1.asp *(August 15, 2002)*

administrator accounts are not used on either web server, and extraneous users do not have web server accounts.

Application Server Internal Network

All business logic for the GIAC's web application resides on the application server internal network, which is protected by a NetGuard Guardian 2.0 stateful inspection firewall, similar to the firewall that separates the external network segments from the internal segments. The servers on this network segment are running BEA Weblogic 7.0 on Windows 2000 operating system. As with the web server network, the servers in this network segment are clustered to provide for reliability. BEA Weblogic 7.0 was chosen specifically because of its automatic failover capability, which promotes high availability overall for GIAC's network. In the event of a failure, another server in the cluster maintains current client session information, as multiple code instances have been set up on the individual servers[7].

The application servers are critical to the overall network architecture. Application servers allow the web servers to dynamically present web pages to GIAC's customers during a transaction. GIAC's application code is written in Java, which provides more scalability than other popular coding languages such as Cold Fusion. After a customer submits credit card and order information to GIAC, the application servers query the servers that reside in the database server internal network during a transaction. Consequently, the application server internal network servers are the center of GIAC's transaction processing capability.

Customer Service Group Internal Network

As described previously, the Customer Service Group is responsible for ensuring that GIAC's customers receive the flags that they have ordered. This requires Customer Service Group personnel to be able to access the database servers, which temporarily store credit card and other order information for a day's transactions before this information is backed up and removed from the databases.

The Customer Service Group Internal Network consists of a series of workstations, all using the Windows 2000 operating system, and an application server. The application server is running custom software that was designed by GIAC's IT Services Group software developers to allow Customer Service Group personnel to query the database to determine what items must be shipped, and to what address.

Database Server Internal Network

GIAC's Microsoft SQL Server 7.0 database servers are critical to operations, and their overall uptime is one of the most important factors to GIAC's success. Realizing this, the database servers in this network segment have been clustered in an Active/Passive configuration. In the event of the failure of one database server, the other server will be

[7] *BEA Weblogic Server 7.0 Overview "The Foundation for Enterprise Application Infrastructure"* *http://www.beasys.com/products/weblogic/server/wls_70_ov_wp_04021.pdf*

able to pick up the transaction session and complete a customer's transaction without the customer being aware of any problems. Unless there is a problem, one server is functioning as the database server and the other is waiting to take over if necessary. If the primary node fails, and failover to the secondary node occurs, the cluster will still retain the same SQL Server virtual name and TCP/IP address, although now a new physical server will be responding to client's requests[8]. This Active/Passive cluster functionality is facilitated by Windows 2000 Advanced Server, which has been installed on each database server. Credit card information is encrypted and stored within the database servers, and backed up daily. Backup tapes are stored securely in an off-site location, in a fireproof, secure box.

Processing Server Internal Network

The processing server internal network is the site within the network architecture where payment processing occurs. In short, it is here where GIAC connects to VisaNet so that VisaNet can confirm that a credit card number that a customer has presented for payment is valid. According to VisaNet rules, this part of the network is subnetted away from other parts of the network.

As specified in the diagram, GIAC's payment servers are running CyberSource software on Windows 2000 operating system. The CyberSource processing system works as follows during a transaction, according to CyberSource specifications[9]. A GIAC customer places an order for GIAC's flags, and hits the "submit" button on the order form that has been presented at the web server. This order form includes credit card information, which is supplied by the customer. GIAC transfers the credit card information using SCMP over the Internet to CyberSource, which formats the transaction detail and securely routes the transaction authorization request to the third-party processor. Then, the transaction is routed to the purchaser's bank to request authorization. The issuing bank either accepts or declines the transaction. Finally, CyberSource returns a message to GIAC indicating whether the transaction has been approved or not. This information generates an appropriate web page that is seen by the customer, telling the customer whether the transaction has completed or failed. CyberSource settles the transaction as well, charging the card and giving money to the account owner, which is GIAC.

IDS Network and Security

As shown in Figure 1-1, GIAC's network includes three Dragon IDS Network Sensors, which connect to a Dragon 5 Intrusion Detection System running Dragon Server. The IDS sensors are located at key points in the network where incoming traffic should be monitored. One is located off the Cisco 2950 switch, just after (or before) traffic passes through the border router. The second is located inside the internal network, off the Cisco 2950 switch that is located just after (or before) traffic passes through the

[8] *McGeehe, Brad M. "An Introduction to SQL Server Clustering" http://www.sql-server-performance.com/clustering_intro1.asp (August 15, 2002)*

[9] *"How it Works – Credit Card Processing" http://www.cybersource.com/products_and_services/electronic_payments/credit_card_processing/howitworks.xml*

NetGuard Guardian Firewall that segments the DMZ and external network from the web server screened subnet and the rest of the internal networks. The third IDS sensor is located off the Cisco 2950 switch that is between the internal firewall and the processing server private internal network. At each of these locations, the IDS sensor examines traffic and determines whether it is anomalous or if it is part of a pattern that suggest malicious activity. The IDS network itself is located entirely separate from the rest of GIAC's network. The network is placed here because it makes it highly unlikely that a potential attacker could access and disable the IDS console. The IDS can only be administered locally.

Consistent with SANS IDS Sensor Placement guidance within *Inside Network Perimeter Security*, each Cisco switch's spanning ports are configured so that the IDS receives all traffic that is passing through the switch. Also consistent with SANS guidance, IDS sensor 1 monitors for scans, probes, or attacks from the Internet, IDS sensor 2 examines traffic that has made it past the firewall and into the public web server network, and IDS sensor 3 focuses on attacks that would be likely to be launched against the internal processing server network, where critical credit card data resides temporarily while a credit card is processed and authorized.

1.3 Business Operations

GIAC's primary concern as an e-commerce site is having high availability. GIAC's Information Technology (IT) services group is responsible for the availability and reliability of the network, as well as the security of its individual components. Consequently, the IT Services Group has focused on building an architecture that is fully-redundant, with clustered servers on every tier. Only necessary services are allowed to run on each of its servers. In addition, the IT Services Group has installed IDS sensors at key points of the network to monitor traffic. GIAC's key servers, particularly the database servers, are protected by multiple defensive layers to ensure that credit card information has a low chance of being stolen, altered, or misused. This way, GIAC provides peace of mind to its customers when they purchase products.

Customers must be able to connect to GIAC's external web server network, where they complete e-commerce transactions from their point of view (regardless of what is happening in the internal networks). Without high availability, GIAC's customers will not be able to purchase items, and GIAC will not be able to generate revenue. Although GIAC's selection of flags is better than any other e-commerce site that has been identified to date, flag purchases are generally impulse buys. If GIAC cannot meet a customer's need, GIAC's customers can generally find another place to buy merchandise. In addition, if GIAC's service is not available when a customer wants to make an impulse buy, GIAC loses out on new business and a new customer relationship that could be quite profitable. Because of the high availability requirement, GIAC has at least one technician on call and present in GIAC's building at all times.

A key part of GIAC's business is ensuring that GIAC is able to authorize the credit cards that customers provide for payment. Consistent with VisaNet rules, a frame relay line connects VisaNet to GIAC's network, so that no sensitive information is being transmitted in the clear, over the Internet. Once a transaction is complete, data is truncated and stored in the database server, which is password protected. Only the system administrators, each of whom has undergone a thorough background investigation, have the password to the server.

Once orders have been placed by the customer and the credit card transaction is successful, GIAC must ship its products. The Customer Service Group is responsible for shipping the goods that GIAC's Manufacturing Group produces. To accomplish this, Customer Service Group personnel have a separate network segment that consists of several workstations and an application server. Those responsible for shipping products are able to query the transaction database to find out what products need to be shipped to what address. The application server, which is located in this network segment, allows Customer Service Group staff to perform the query. The server is running custom software that has been written to only allow the Customer Service Group staff to view certain details of the transaction, and not allow staff to see highly sensitive data such as credit card numbers.

Besides making purchases on GIAC's site, the external customer world contacts GIAC personnel via email. However, email is not critical to GIAC's operations. Customers would only use the email customer contact option if the 24-hour customer service phone number, answered by a Customer Service Group staff member on duty, were not active. In either case, calls or emails that are sent to GIAC deal with problems the customer has completing transactions. Customers do not call GIAC to actually place orders. The "Contact Us" link on GIAC's webpage specifically states that email responses are returned within twelve hours, whereas customer phone calls can be answered immediately. Consequently, customers should not be surprised if they do not immediately receive an email response.

Assignment 2: Areas of Risk

The following three concerns are specific to GIAC's operations as an e-commerce site:

- Public Web Server Compromise
- Database Server Compromise
- Improper Implementation of Changes to GIAC Application Code

2.1 Methodology

Consistent with NIST risk management guidance[10], risk is characterized according to the following formula:

Risk = Impact x Likelihood

Impact for each risk has been assessed according to Table 2-1 below.

Impact	Description
High	May result in the *loss of significant* or major tangible assets, information, or information resources. May significantly disrupt or impede GIAC's mission or seriously harm its reputation or interest (e.g., loss of mission-critical system data by unauthorized users gaining access to GIAC's internal networks).
Medium	May result in the *loss of some* tangible assets, information, or information resources. May disrupt or harm GIAC's mission or harm its reputation or interest. For example, authorized users are not able to access mission-supportive data for several days.
Low	May result in the *loss of minimal* tangible assets, information, or information resources. May adversely affect GIAC's mission, reputation, or interest. For example, authorized users are not granted access to mission-supportive data for an hour.

Table 2-1 Impact Assessment

Likelihood for each risk has been assessed according to Table 2-2 below.

Likelihood	Description
High	The capability of the threat is significant, and/or countermeasures to reduce the probability of threat exploitation are insufficient.
Medium	The capability of the threat is medium, and implemented countermeasures lessen the probability of threat exploitation.
Low	The capability of the threat is limited, and countermeasures are in place that effectively reduces the probability of threat exploitation.

Table 2-2 Likelihood Assessment

[10] *Stoneburner, G., Goguen, A., Feringa, A. Risk Management Guide for IT Systems: Recommendations of the National Institute of Standards and Technology. p. 21-25. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf*

Finally, the overall risk level for each risk was determined according to Figure 2-3, the Risk Level Matrix:

	Likelihood		
Impact	***High***	***Medium***	***Low***
High	High	High	Medium
Medium	High	Medium	Low
Low	Medium	Low	Low

Table 2-3 Risk Level Matrix

2.2 Risk 1: Data Integrity Cannot be Ensured through End-to-End Encryption

Overview of Risk

Currently, GIAC has serious data integrity problems, centering around a lack of encryption. GIAC's customers, by doing business with GIAC, are trusting that the sensitive and personal data that they enter during a transaction is safe from being modified or compromised as it moves through the transaction life cycle. Unfortunately, as GIAC's network stands, since GIAC does not encrypt transaction data it is very possible that an attacker could be observing and capturing credit card data while it is being transmitted from the customer to GIAC over the Internet. In addition, it is also possible that an attacker could modify the order data entered so that the customer ends up "ordering" more products than he or she intended, or that perhaps no product order would be ordered at all. It is even possible that the customer's credit card could be charged for an amount much greater than the price of the products, such as being charged $1000 for a $5.00 flag. The following scenarios are all viable, and further explain the ideas presented above:

- Again, customers trust that the information they are sending to GIAC is the same information that will be used to process the transaction. In other words, if a customer trusts that the integrity of the information they submit is maintained throughout the transaction. If a customer orders five 3 x 5 flags for a total cost of $25.00, the customer expects that his or her credit card will be charged this amount and the correct type and number of products will arrive in the mail. It is critical that information the customer sends is the same as the information that is ultimately processed, or customers will have to return products to GIAC. Worse yet, if the products shipped or charged do not match what was ordered, customers will need to contact GIAC about erroneous credit card charges and spend time rectifying a GIAC error. Either scenario would make e-commerce a hassle, and would make customers less likely to return.
- A malicious malicious intruder could modify information sent from the customer and change order details, resulting in a scenario where the customer would have ordered X number of products, and receive and be charged for Y products, either to GIAC or the customer's disadvantage. If, for example, GIAC ended up losing profit in this scenario, GIAC would suffer monetarily. Over time this could be a serious problem. If the customer was charged too much for the products he or she ordered, or if the wrong products arrived, the customer would have to go

through the hassle of returning products and making phone calls to GIAC about erroneous charges. Naturally, the customer might think that GIAC was trying to take advantage of the customer by raising prices or overcharging for products.

- A malicious intruder could modify information sent from the customer and change order details, resulting in a scenario where the customer would have ordered X number of products, and receive and be charged for Y products, either to GIAC or the customer's disadvantage. If, for example, GIAC ended up losing profit in this scenario, GIAC would suffer monetarily. Over time this could be a serious problem. If the customer was charged too much for the products he or she ordered, or if the wrong products arrived, the customer would have to go through the hassle of returning products and making phone calls to GIAC about erroneous charges. Naturally, the customer might think that GIAC was trying to take advantage of the customer by raising prices or overcharging for products

This risk is very serious to GIAC's business, and data integrity and the confidence of customers in GIAC as a result is considered the "crown jewels."

Potential for Damage

Clearly, this risk has the potential to seriously impact both GIAC and its customers. In the short term, if credit card numbers or personal information (names and addresses) are observed and intercepted by a malicious attacker, the attacker could use the credit card number to purchase non-GIAC products for him or herself. In addition, an attacker could try to sabotage GIAC's reputation by changing data so that the customer ultimately receives the wrong products, or is charged too much for the products that are ordered. Another possibility is that an attacker could modify data so that GIAC ends up sending more products than the customer has paid for, leading to a loss for GIAC. Any number of scenarios could happen while data is in transit throughout GIAC's network and across the Internet.

Each of these scenarios could make GIAC appear sneaky, unrealiable, or negligent in the way it handles transactions and data. Although GIAC may not necessarily be guaranteeing the safety of transactions, the customer is putting some level of trust in GIAC by exposing him or herself to the risk of doing business via the Internet. In the long term, if GIAC's customer base erodes, this would mean GIAC's collapse. GIAC's collapse could even happen as a result of legal claims should attackers successfully use a customer's credit card for personal purposes, and the customer be able to track this issue back to GIAC. Flags are generally a luxury or convenience item rather than a necessity. GIAC must give customers a reason to purchase flags via the Internet rather than at a store, and even give a reason to spend money on a flag at all.

With the current set-up, GIAC is not compliant with VisaNet rules, which not only specify that "for stored data, the minimum account information that needs to be encrypted is the Visa account number and expiration date", but also that "strong encryption (128-bit) is a requirement for all communications on the public network (i.e., Internet), which includes any public communication between the merchant and the customer or between the merchant and Visa." Although GIAC complies with the requirement that no data between GIAC and the merchant is "in the clear" by providing a frame relay line, Visa could possibly penalize GIAC or opt not to do business with GIAC for not ensuring that the transaction is encrypted end-to-end (and not ensuring that customers are generally well-protected from this risk), as well as the fact that the data is not encrypted in the database once the transaction is complete (prior to settlement). If GIAC fails to fully comply with VisaNet rules and is caught, GIAC will no longer be able to use VisaNet and could possibly lose all customers with bad publicity.

Mitigation

The following mitigation items must be employed by GIAC in order to mitigate this risk:

- When the customer is transmitting credit card and personal information to GIAC at the beginning of the web transaction, all data should be sent using HTTPS so that it is encrypted as it travels to GIAC's web server.
- The IPlanet web server should be configured to only allow for 128-bit SSL transactions. If the user's browser is not able to support this level of encryption, the user will then be stepped up to 128-bit encryption, because GIAC will be using Global Server ID's. This will ensure that any customer around the world can purchase a flag securely.
- GIAC should Verisign to purchase SSL certificates. When the data reaches the processing server internal network, it will be encrypted as well.
- To be consistent with Visa's security requirements, the interior firewall should be configured so that only HTTP and SSL traffic can reach the processing server internal network[11].
- Data should be backed up nightly, and at that point the entire day's transaction information should be removed from the database server.

Complying with VisaNet rules, as well as providing data encryption, is critical for GIAC to remain in business long-term. Each item must be considered and implemented right away.

Overall Assessment

Given the potential for damage, the impact that exploitation could cause has been determined to be ***High***. The Likelihood that exploitation could occur is ***Low****,* should the risks be mitigated per the IT Services Group's recommendations. Therefore, the overall risk is considered **Medium**. The residual risk is dependent upon the number of items GIAC chooses to employ, which in this case should be ALL of the items, resulting in little residual risk.

[11] *"Cardholder Information Security Program"* http://usa.visa.com/business/merchants/cisp_tech_info.html

2.3 Risk 2: Public Web Server Compromise

Overview of Risk

GIAC's public web servers are the company's interface with its customers. The integrity of the web servers' information, and web server availability, are critical for GIAC for the following reasons:

- Customers enter credit card information and product details at the web server that are necessary to process a transaction. Should the web server not be available for use, the customer cannot order GIAC products.
- While conducting business, the customer learns subtle things about GIAC by the way content is displayed on the web pages and what is stated. For example, web content tells a customer about how detail-oriented the company is, and how much it values its image and perhaps even its customers. Ultimately, the customer knows he or she is trusting GIAC with sensitive credit card and personal information during a transaction. Consequently, incorrect or misspelled web content may make the customer uneasy about GIAC and less likely to repeat business. It may even make customers unlikely to conduct e-commerce at all, regardless of the company, if companies show carelessness about their image.
- GIAC depends on revenue to run its business. If product prices were to be changed maliciously by someone with legitimate or illegitimate access to GIAC's web servers, GIAC would lose either direct profit or business. For example, if GIAC's prices displayed on the web site were raised to a ridiculous premium, customers who would normally have bought GIAC flags might find another place to make purchases, resulting in lost opportunity for GIAC. Conversely, if prices were lowered, GIAC might receive a lot of business but would lose profit from each sale. If either scenario went on long enough, GIAC could possibly go out of business.

Overall, the web servers are the crucial part of GIAC's business for several reasons. First, they are the customer's primary interface with GIAC. The web servers are the place where product information is entered. If information cannot be entered due to web server unavailability, or if information entered is modified during transaction processing, GIAC will lose customers and their confidence. Second, GIAC counts on the accuracy of the information the web servers display, so that the company can realize expected profit. Finally, the customer's only source of an impression about GIAC as a business is the web server and its content. The web servers are GIAC's only way to communicate product offerings and prices to customers.

Potential for Damage

Several scenarios could happen during a web server compromise:

- First, and most devastatingly, the web server could be rendered unavailable via an attack such as DoS. If this were to happen, customers could not purchase products for a given period of time. GIAC sells approximately $25,000 worth of flags per day, so for each hour of web server unavailability, GIAC could use up to $1000. Although this seems to be a small amount of money, GIAC would begin to collapse quickly.

- Second, simple spelling or minor content changes could be made to GIAC's web server by internal sources or even by an external individual able to gain access to the servers. This would be embarrassing to the company, but not devastating. However, if an individual undertook a larger scale web defacement, which could include total takeover of the web server's content, this could badly damage public image and result in major customer losses. Depending on the magnitude of defacement, different amounts of damage could occur.
- Third, prices on the web servers could be changed by an internal or external source to impact GIAC profits. Either a customer could see overblown prices on GIAC's web site and be discouraged from buying, or the customer could see very low prices and buy, but to the detriment of GIAC's profit margin. Long term, this could be very damaging and ultimately put GIAC out of business.

Mitigation

Given the potential damage associated with a public web server compromise, GIAC's IT Services Group noted the following mitigation items, and has completed them:

- Web servers are single function servers—the only function of these servers is to provide web pages and content to customers
- Web servers are secured according to an established policy and in accordance with procedures, so that only specific services are allowed to run
- Web servers are clustered and configured for failover
- The web server internal network is an air gapped network point that ensures that public internet traffic can not traverse. The air-gapped feature has been created by ensuring that there is a physical separation between the screened web server subnet and the DMZ external network
- As shown in Figure 1-1, the network is isolated from both the external/publicly accessible network segments including the DMZ with a firewall. It is also isolated from the internal network segments including the application server internal network with another firewall
- Web servers only accept TCP connections on ports 443 and 80
- The exterior firewall that all traffic passes through before reaching the public web server tier has been configured to prevent many common types of attacks

The following mitigation items should be undertaken by GIAC to mitigate residual risk:

- The web servers themselves should be password protected. The passwords should change every seven days. Only the system administrators in charge of these servers and the VP for Information Assurance should know the passwords.
- Access controls for the web server should be set in a manner that limits resource use during a DoS attack against GIAC's web site, and that prevents disclosure of sensitive or restricted information upon compromise. According to NIST's publication "Guidelines on Securing Public Web Servers," the following files that should have access controls should be:

    - Application software and configuration files
    - Files related directly to security mechanisms (password hash files and other files used in authentication, files containing authorization information used in controlling access)
    - Server log and system audit files
    - System software and configuration files[12].
- GIAC should install an SSL certificate at the web server, so that customers accessing GIAC's e-commerce application can verify that GIAC is the organization with which the customer is about to conduct business prior to entering credit card data
- GIAC should encrypt all data as it passes from the web server and through the transaction life cycle. Data should be checked at each processing point to ensure that the data that was sent is the same as the data that was received by the server (see Risk 1)

Specific to web servers alone, GIAC must password protect the web servers so that content changes cannot be easily made by internal or external sources. At present, anyone internally with access to GIAC's network is able to access the web server to make changes. In addition, access controls are critical to ensuring that attackers are not able to use the web servers to their maximum potential for damage during a DoS attack. The items noted above as considerations from NIST regarding access controls and the files which should be protected require no financial commitment from GIAC, and can provide great benefit in future attack scenarios.

Perhaps most critical risk mitigation item yet to be employed that should definitely be established is encryption of the transaction data, which should be accomplished by mitigating Risk 1. This item is included to underscore the importance of encryption to GIAC's success and the safety of customer data. It is also included to underscore how important it is that GIAC undertakes these mitigation actions. Making these changes is absolutely critical to GIAC's continued operations. Not only could GIAC lose customers and profit from turning around incorrect orders, it GIAC's transaction data is modified by an attacker it also means that the attacker is able to steal credit card information while it is in transit. GIAC should quickly install an SSL certificate at the web server for their customers' peace of mind. This is not costly, and could increase the comfort customers have about doing business with GIAC over the Internet.

The IT Services Group has recommended that all of these actions be completed immediately due to the current vulnerability of the web servers.

Overall Assessment

Given the potential for damage, the impact that exploitation could cause has been determined to be *High*. The Likelihood that exploitation could occur is *Low,* should the mitigation items be addressed as indicated above, according to the recommendations of

[12] *Tracy, M., Jansen, W., McLarnon, M. Guidelines on Securing Public Web Servers: Recommendations of the National Institute for Standards and Technology. p. 28. http://csrc.nist.gov/publications/nistpubs/800-44/sp800-44.pdf*

the IT Services Group. Therefore, the overall risk is considered **Medium**. The residual risk is dependent upon the number of items GIAC chooses to employ. Even one item should mitigate the risk greatly. Using all of the recommendations may be somewhat costly, but using all of them should place GIAC in the best possible circumstance and in the best position to prevent damage. In any event, if the public web server's are compromised, this could cause very serious damage to GIAC's reputation and cash flow. Therefore, the potential for damage is always high.

2.3 Risk 3: Database Server Compromise

Overview of Risk

GIAC's database servers are the temporary storage location for credit card information after a transaction is complete. During a transaction, the application servers write critical information to the database, where it is stored until backup and removal.

GIAC's database servers must not be compromised at any cost. If they were compromised, one of two things could happen. First, the compromiser could steal credit card information and make purchases elsewhere, charging to GIAC's customers. If GIAC's customers found this out, they could in the worst case take legal action against GIAC. More likely, GIAC would lose individual customer business and any potential follow-on business that could have been gained through word-of-mouth. Second, the compromiser could modify credit card information and make it impossible for GIAC to correctly settle transactions. Since GIAC merchandise is sent from the shipping center every four hours, GIAC routinely sends products out before the transactions are settled. This is a necessary service feature that helps GIAC differentiate from its competitors. However, if credit card information is modified prior to settlement or is deleted from the database entirely, GIAC will lose money on the products it has shipped and cannot charge for anymore.

According to the network diagram (Figure 1-1), GIAC is exposing itself to internal risk in this area. The Customer Service Group Internal Network is not separated from the database servers by firewall. Instead, the Customer Service Group, which accesses transaction information to ship orders, could access information beyond what they are normally allowed to see (see Business Operations) by using the application server should they be able to find out the password to the database servers and compromise them. This is a very serious risk. This risk essentially makes it possible for internal Customer Service Group personnel to exploit all of the scenarios described in the paragraph above.

This risk is very serious, because it can be exploited by internal personnel as well as external individuals or entities.

Potential for Damage

There is potential for significant monetary damage to both GIAC and its individual customers if the database servers are compromised. This damage could range from a lost customers and loss of follow-on business, to major customer lawsuits. Because both internal and external groups or individual could cause damage as the network is currently established, the potential for damage is raised.

The damage that internal Customer Service Group personnel could cause if they were able to access credit card and other sensitive information is massive. Since GIAC does not have a log server, it could take a while for GIAC to notice that internal personnel are stealing credit card information. The earliest sign of a compromise of the database servers at all could turn up only when a customer receives his or her credit card statement and notices unknown line items, which the customer may or may not attribute to GIAC. Again, if these charges were somehow tracked to GIAC, there could be lawsuits and other debilitating events in GIAC's future. Should a disgruntled employee want to harm the company in another way, the employee could also modify product information before shipping details have been viewed by other GIAC Customer Services Group personnel. This could cause an increase in the number of incorrect orders that reach customers, and a decline in customer confidence similar to that described in Risk 1.

Mitigation

The following are GIAC's methods for mitigating this risk:

- Database servers are located in GIAC's internal network, beyond two well-configured firewalls
- Database servers are located on an entirely different network segment from any other parts of the network
- Servers in the DMZ cannot initiate connections to the database servers or anywhere else in the internal network
- Database servers are single-function servers. They are entirely separate from web servers and application servers. Application servers query the database servers during a transaction
- Customer credit card data is backed up every evening just after the batch file is settled. The day's data is then removed from the database servers

The following mitigation items have been proposed by GIAC's IT Services Group as additional steps that could be taken to prevent exploitation:

- The only individuals who have direct access to the database servers should be those responsible for administering the servers. The number of personnel with this responsibility must be as small as possible. The servers should be password protected, and the password should change every seven days.
- GIAC should require authentication to the application server that the Customer Service Group uses to look at information in the database, so that there is a clearer way to audit individual actions by user. Currently, there are two sign-in ID and two terminals for the entire group to use.
- GIAC should consider placing the Internal Customer Service Group network off the internal firewall rather than beyond the firewall.
- GIAC should consider having individuals working for the Customer Services Group undergo a background investigation prior to being hired. This

investigation would not need to be as extensive as what various IT Services Group personnel undergo, but should include a basic credit check at minimum.

Risk mitigation item #1 should be applied immediately, without delay. Although it requires some procedural changes, it is extremely important that personnel only have access to the database servers if necessary. Another important mitigation item to employ is requiring authentication when using parts of the Internal Customer Services Group network to retrieve purchase and shipping information. This should not be a very costly item to put in place. The last two items are also important. GIAC should not allow the Internal Customer Services Group network to be beyond the firewall and with relatively direct access to the database servers. Finally, GIAC should not neglect personnel security measures when hiring personnel. Though it is not highly likely that the individuals working in the Customer Services Group would be technically competent enough to be able to compromise the database servers, this measure would not be costly, and is similar to what other non-e-commerce companies (companies that for example do government contracting) have asked their future employees to do.

Overall Assessment

Given the potential for damage, the impact that exploitation could cause has been determined to be *High*. The Likelihood that exploitation could occur is *Low,* should the risks be mitigated per the IT Services Group's recommendations. Therefore, the overall risk is considered **Medium**. The residual risk is dependent upon the number of items GIAC chooses to employ. Even one item should mitigate the risk somewhat, but using all of them should place GIAC in the best possible circumstance given the cost and benefits of applying each control. In any event, if the database server's critical information is modified, stolen, or otherwise compromised, the damage potential is always high.

Assignment 3: Evaluate and Develop Security Policy

The example policy that is included as Appendix B of this practical was obtained from http://www.sans.org/newlook/resources/policies/Server_Security_Policy.pdf. It has been amended to list "GIAC Enterprises" as the company.

3.1 Evaluation of Security Policy

Overall, GIAC's Server Security Policy is well written. It generally follows SANS guidelines on effective policy. However, the organization and contents of the policy could be improved to make the policy stronger and easier for the layperson, as well as the system administrator, to understand.

Purpose

The Purpose section of the Server Security Policy is concise. It is evident that the policy has been established as a standard for secure server configuration. The issue that the policy is intended to address is minimizing the risk of unauthorized access to proprietary information and technology. However, the policy does not specifically identify that the policy intends to prevent individuals with malicious intent from gaining access to and compromising GIAC's servers. This may be implied in the policy statement. However, the issue might make more of an impression on users and those involved with server configuration activities if the purpose more clearly spells out "why" the policy is necessary.

Background

A Background section has not been included in this policy. However, this section is optional and its absence does not impair the policy.

Scope

The Scope section of the policy generally well written and concise. It very clearly delineates that the policy "applies to server equipment owned and/or operated by GIAC Enterprises, and to servers registered under any GIAC Enterprises-owned internal network domain." However, the text continues to state that the policy applies to the internal network rather than DMZ servers, and that DMZ guidance can be found in a separate document. Since the DMZ designated in the diagram includes only DNS and an email server, I would not necessarily create separate policy for this, but rather develop a procedure should there be any specifics that need to be considered for the DMZ servers. The statements written in this policy should all apply to the DMZ.

Responsibility

Again, this section of the policy is well written and is to-the-point. The first statement, "all internal servers deployed at GIAC Enterprises must be owned by an operational group that is responsible for system administration" makes it absolutely evident that all systems must be owned by a specific group. This provision establishes accountability for policy implementation with an identifiable group or individual. The actions that groups that own systems must take are clearly delineated.

Although the Responsibility section should state who has the authority to review, approve, and modify policy, this policy does not talk about revisions to this document. The only references to change refer to modifications that the system administrator would make to the actual server's configuration or to "exception" policies that each owner group should write. The policy may be ambiguously written here, but it appears that this means that the Server Security Policy will not change, and only the individual exception policies will be modified. Eventually, the base policy will need to change, regardless of what is implied. This policy provides no guidance about who would perform and approve revisions, which is a deficiency. The Server Security Policy should only be revised by the VP for Information Assurance, with concurrence from the Configuration Control Board.

In addition, the document refers to "an operational group that is responsible for system administration." At GIAC, there is only one group that has this responsibility—the IT Services Group. Since this is the case, it would be clearer to change references to "an operational group" to specify the IT Services Group. Since there is only one group, it is important to call out exactly who is responsible within the IT Services Group for audits. In GIAC's case, this individual is the Chief Auditor. Calling this out specifically, it would set the Chief Auditor apart from other individuals within the group, and begin to address conflict of interest issues that could result from the IT Services Group auditing its own work.

Action/Policy Statements

Sections 3.2 and 3.3 both detail the specific actions required to implement this policy. For example, *Section 3.2 General Configuration Guidelines* includes statements such as "services and applications that will not be used must be disabled where practical." However, this section is not as tailored to GIAC as it could be. For instance, it would be helpful to mention VisaNet rules when discussing trust relationships, as trust relationships is one element that VisaNet's guidelines specifically addresses. In addition, there should be language stating that patches must not only be installed, but must be tested prior to installation. If a patch is applied that may affect other parts of GIAC's network, this could lead to lost profits. Instead of stating that servers must not be stored in cubicles, this policy must specify that servers (particularly the database servers) must be stored in a secure area that uses biometric authentication for access. None of GIAC's servers are stored in unsecured areas. In addition, I would recommend breaking the bullets in this section into several subsections to aid in comprehension. As it stands, the bullets are an unordered collection, and some key information might get lost.

Section 3.3 Monitoring very specifically identifies how logs for sensitive systems will be maintained and how long backups must be stored. This section manages to provide a detailed, comprehensive list of what must occur without being redundant or verbose. This adds to the accessibility of this policy and its overall usefulness. Since GIAC stores critical customer data, and since it is imperative that this data remain secure for the public to be confident in GIAC's services, it is important to modify the time specifications in the *Monitoring* section. Timeframes that logs should be maintained and backups be retained should be lengthened considerably. As stated in the risk portion of this document, should a compromise of the database server or web server occur and credit card data be stolen, this can result is legal action against GIAC. It will be important to have logs as forensic evidence. In addition, it is important to maintain these logs and backups long-term in case of a disputed order.

Another problem with the action-related sections of this policy is that they do not identify the date by which compliance must be achieved. The compliance portion of the document only discusses how frequently compliance audits will be performed, and by whom. Although including specifics here might "date" the policy, they would be beneficial in making sure the IT Services Group completes necessary actions quickly. Consequences for noncompliance can only be applied if a compliance date is documented. In addition, the compliance section states that auditing will be performed by an internal organization. Instead, GIAC should have an outside, unbiased audit performed so as to prevent either a conflict of interest or the possibility that inside abuses of power are not reported.

Revision History

To address the lack of guidance on revisions to this policy, as described under "Responsibility," it would be helpful to divide the section "Revision" history into two distinct sections. These sections would be "Revisions" and "Revision History" within a revised policy. In addition, since the "Revisions" section will include a mention of the Configuration Control Board, this body should be added as a definition. Finally, since this policy requires compliance and action from server administrators especially, and mentions responsibilities of various parties, the policy should be signed upon receipt by individuals for accountability.

3.2 Revised Server Security Policy

The following is a revision of the Server Security Policy that was included as Appendix B of this practical. Revisions are based on the critique and recommendations that were generated during this assignment.

Server Security Policy

1.0 Purpose

The purpose of this policy is to establish standards for the base configuration of server equipment that is owned and/or operated by GIAC Enterprises. Effective implementation of this policy will minimize unauthorized access by both internal and external users to GIAC Enterprises' servers, which house sensitive customer data. Compromise or exploitation of sensitive data by either internal or external sources could lead to loss of public confidence, loss of profit, or legal action against the company.

2.0 Scope

This policy applies to server equipment owned and/or operated by GIAC Enterprises, and to servers registered under any GIAC Enterprises-owned network domain.

This policy is specifically for equipment on the internal GIAC Enterprises network. For additional specifications concerning the secure configuration of equipment external to GIAC Enterprises on the DMZ, refer to the Internet DMZ Equipment Configuration Procedure.

3.0 Policy

3.1 Ownership and Responsibilities

All servers deployed at GIAC Enterprises are owned, and must be registered by, the appropriate server administrator from the IT Services Group. They must be registered according to the following specifications:

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
  - Server contact(s) and location, and a backup contact
  - Hardware and Operating System/Version
  - Main functions and applications, if applicable
- Upon registration, each server administrator must submit an approved server configuration guide. This guide must be maintained by the server administrator, and entered into the corporate enterprise management system.
- Any configuration changes that are suggested due to business needs must be approved by the Configuration Control Board.
- Information in the corporate enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures.

3.2 General Configuration Guidelines

- Operating System configuration should be in accordance with approved IT Services Group guidelines.
- Services and applications that will not be used must be disabled where practical.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do. VisaNet security requirements regarding trust relationships must be complied with.

Patching

- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Security patches must be tested prior to being applied uniformly to GIAC servers.

Access

- Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.
- Always use standard security principles of least required access to perform a function. Requests for additional access must be approved and submitted using the GIAC-specified request procedure.
- Server administrators must not use root accounts when using a non-privileged account will do.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).

Physical Security

- Servers housing critical data (SQL database servers in particular) should be physically located in an access-controlled environment within GIAC Enterprises. Physical access controls must include biometric authentication.

3.3 Monitoring

- Due to the nature of information that housed on GIAC's database servers in particular, all security-related events on critical or sensitive systems must be logged and audit trails saved and monitored as follows:
  - All security related logs will be kept online for a minimum of 2 week.
  - Daily incremental tape backups will be retained for at least 6 month.
  - Weekly full tape backups of logs will be retained for at least 1 year.
  - Monthly full backups will be retained for a minimum of 2 years.
- Security-related events will be reported to the VP for IT Services, who will review logs and report incidents to the Configuration Control Board for action. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
  - Port-scan attacks
  - Evidence of unauthorized access to privileged accounts
  - Evidence of unauthorized access to web servers and database servers specifically
  - Internal attempts to connect directly to web or database servers
  - Anomalous occurrences that are not related to specific applications on the host.

3.4 Compliance

This policy must be implemented in full by November 1, 2002.

- Audits will be performed on a regular basis by an external company engaged by GIAC Enterprises.
- Audits will be managed in conjunction with the VP for IT Services, in accordance with the Audit Policy. The VP for IT Services will present the findings to the Configuration Control Board, and then to appropriate support staff within the IT Services Group for remediation or justification.

- Every effort will be made to prevent audits from causing operational failures or disruptions.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	**Definition**
DMZ	De-militarized Zone. A network segment external to the corporate production network.
Server	For purposes of this policy, a Server is defined as any internal or external GIAC Enterprises Server. Desktop machines and Lab equipment are not relevant to the scope of this policy.
Configuration Control Board	Comprised of Vice Presidents of each of GIAC's divisions. Meets biannually (or more frequently as necessary) to review this policy and recommend revisions.

6.0 Revisions

This Server Security Policy may only be revised by the VP for IT Services, with concurrence from Configuration Control Board.

7.0 Revision History

______________________________ ______________________________

VP, IT Services Group

Assignment 4: Develop Security Procedures

The following procedure has been developed to support the revised Server Security Policy that is included in Assignment 3 of this practical.

4.1 Procedure for Secure Installation of GIAC Enterprises Web Servers

Purpose

The following procedure is designed to assist in the implementation of the GIAC Enterprises' Server Security Policy. It provides specific steps involved in installing the web server, based on industry guidelines prepared by the National Institute for Standards and Technology (NIST), and best practices.

The purpose of this procedure is to ensure that the minimum best practices in web server installation are followed, to minimize the chance of web server compromise, including compromise of web server content and discovery of components of GIAC's network architecture.

Responsibility

Server administrators, or their designated representative, are responsible for the web tier of GIAC's network architecture are primarily responsible for following this procedure. While this procedure presents the minimum security considerations for the web tier, additional security measures, when applicable and viable, may be proposed to GIAC's Configuration Control Board for review and consideration. Refer to GIAC's Configuration/Change Management Procedure for further guidance.

Procedure

Step 1: Ensure that the minimum system requirements for installing iPlanet 6.0 web server with Windows 2000 are met. The following requirements apply:

Memory: 512 MB minimum for Windows 2000
Disk Space: 2 GB minimum for Windows 2000

Step 2: Ensure Operating System recent security patches and hotfixes have been applied and tested.

Step 3: Uninstall any previous web server installations, including any IIS installation that may exist.

Step 4: If installation media is not on CD, install the minimum network services required to transfer iPlanet software and patches from a local server to the server of the iPlanet installation.

Step 5: Install the most current stable version of iPlanet 6.0 server software on a dedicated host, using iPlanet 6.0 documentation and release notes. Server must be installed consistent with GIAC's policy on Server Security, which includes creating a separate non-privileged user for the web server to run as, which file access only to files related to web server activity.

Step 6: Apply any patches or upgrades to correct known vulnerabilities after testing to ensure that patches or upgrades will not affect other parts of GIAC's network architecture. Known vulnerabilities and patches are identified on at the following location: http://docs.iplanet.com/docs/manuals/enterprise.html.

Step 7: Create a logical partition (separate from operating system and server application) for Web content and log files and ensure it has sufficient space.

Step 8: Remove or disable all services installed by the Web server application but not required (e.g., gopher, FTP, and remote administration). Refer to the SANS Security Consensus for Windows 2000 for more information on services that may be disabled.

Step 9: From the web server application root directory, remove all files that are not part of the web site.

Step 10: Remove all sample documents, scripts, and executable code.

Step 11: Remove all vendor documentation from server.

Step 12: Remove any file editors or code compilers from the server.

Step 13: Alter the audit policy, local security policy, and registry settings according to the specifications in the SANS Consensus Guideline entitled Security Windows 2000: Step-by-Step, and apply any additional security template or hardening script to server.

Step 14: Reconfigure HTTP service banner NOT to report Web server and operating system type and version.

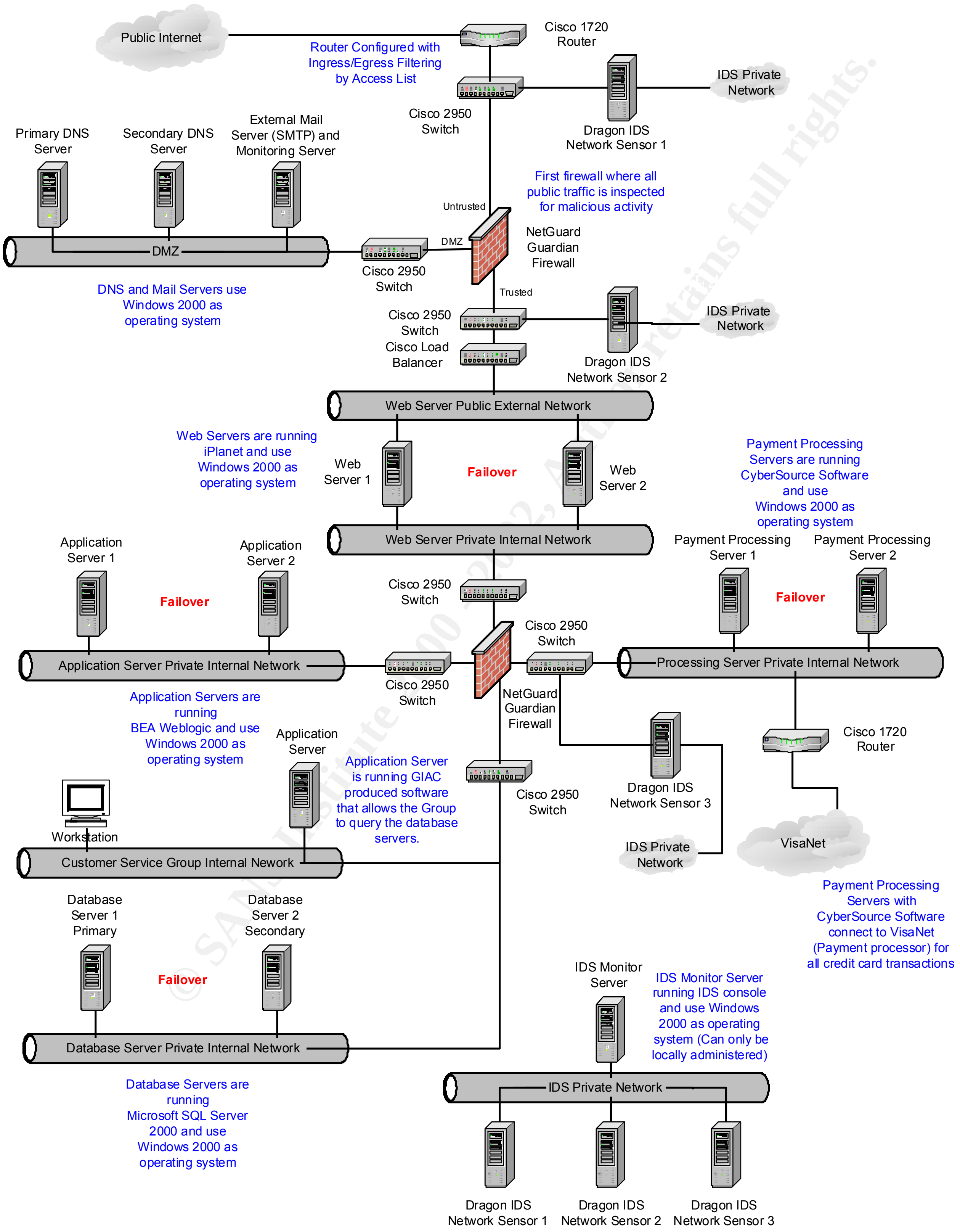
Step 15: If not already connected, connect server to the local network for IDS installation and vulnerability scanning. If the web server is open to the public Internet, it should be installed in a DMZ or a part of the network that is separated by a firewall from databases or servers that contain sensitive information.

Step 16: Install any host-based IDS sensors that may be required by GIAC's Server Security Policy.

Step 17: Run a vulnerability scanner, such as Nessus or ISS Internet Scanner to check for any misconfigurations or vulnerabilities that have been missed.

Step 18: Configure server or routers to permit web traffic from the Internet to the server, consistent with existing GIAC procedures and policy.

Appendix A: GIAC Enterprises Network Diagram


Public Internet
Cisco 1720 Router
Cisco 2950 Switch
Dragon IDS Network Sensor 1
IDS Private Network
Primary DNS Server
Secondary DNS Server
External Mail Server (SMTP) and Monitoring Server
DMZ
Cisco 2950 Switch
Untrusted
DMZ
Trusted
NetGuard Guardian Firewall
Cisco 2950 Switch
Cisco Load Balancer
Dragon IDS Network Sensor 2
IDS Private Network
Web Server Public External Network
Web Server 1
Failover
Web Server 2
Web Server Private Internal Network
Application Server 1
Failover
Application Server 2
Cisco 2950 Switch
Payment Processing Server 1
Failover
Payment Processing Server 2
Cisco 2950 Switch
Application Server Private Internal Network
Cisco 2950 Switch
NetGuard Guardian Firewall
Processing Server Private Internal Network
Cisco 1720 Router
Dragon IDS Network Sensor 3
Application Server
Cisco 2950 Switch
IDS Private Network
VisaNet
Workstation
Customer Service Group Internal Nework
Database Server 1 Primary
Failover
Database Server 2 Secondary
IDS Monitor Server
Database Server Private Internal Network
IDS Private Network
Dragon IDS Network Sensor 1
Dragon IDS Network Sensor 2
Dragon IDS Network Sensor 3

Router Configured with Ingress/Egress Filtering by Access List

First firewall where all public traffic is inspected for malicious activity

DNS and Mail Servers use Windows 2000 as operating system

Web Servers are running iPlanet and use Windows 2000 as operating system

Payment Processing Servers are running CyberSource Software and use Windows 2000 as operating system

Application Servers are running BEA Weblogic and use Windows 2000 as operating system

Application Server is running GIAC produced software that allows the Group to query the database servers.

Payment Processing Servers with CyberSource Software connect to VisaNet (Payment processor) for all credit card transactions

IDS Monitor Server running IDS console and use Windows 2000 as operating system (Can only be locally administered)

Database Servers are running Microsoft SQL Server 2000 and use Windows 2000 as operating system

Appendix B: Example Policy

Server Security Policy

1.0 Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by GIAC Enterprises. Effective implementation of this policy will minimize unauthorized access to GIAC Enterprises proprietary information and technology.

2.0 Scope

This policy applies to server equipment owned and/or operated by GIAC Enterprises, and to servers registered under any GIAC Enterprises-owned internal network domain.

This policy is specifically for equipment on the internal GIAC Enterprises network. For secure configuration of equipment external to GIAC Enterprises on the DMZ, refer to the Internet DMZ Equipment Policy.

3.0 Policy

3.1 Ownership and Responsibilities

All internal servers deployed at GIAC Enterprises must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by InfoSec. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by InfoSec.

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
  - Server contact(s) and location, and a backup contact
  - Hardware and Operating System/Version
  - Main functions and applications, if applicable
- Information in the corporate enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures.

3.2 General Configuration Guidelines

- Operating System configuration should be in accordance with approved GIAC Enterprises IT Services Group guidelines, which have been approved by the Configuration Control Board.
- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.

- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
- Always use standard security principles of least required access to perform a function.
- Do not use root when a non-privileged account will do.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.

3.3 Monitoring

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
  - All security related logs will be kept online for a minimum of 1 week.
  - Daily incremental tape backups will be retained for at least 1 month.
  - Weekly full tape backups of logs will be retained for at least 1 month.
  - Monthly full backups will be retained for a minimum of 2 years.
- Security-related events will be reported to InfoSec, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
  - Port-scan attacks
  - Evidence of unauthorized access to privileged accounts
  - Anomalous occurrences that are not related to specific applications on the host.

3.4 Compliance

- Audits will be performed on a regular basis by authorized organizations within GIAC Enterprises.
- Audits will be managed by the internal audit group or InfoSec, in accordance with the Audit Policy. InfoSec will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.
- Every effort will be made to prevent audits from causing operational failures or disruptions.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	Definition
DMZ	De-militarized Zone. A network segment external to the corporate production network.
Server	For purposes of this policy, a Server is defined as an internal GIAC Enterprises Server. Desktop machines and Lab equipment are not relevant to the scope of this policy.

6.0 Revision History

References

Allen, Julia. The CERT Guide to System and Network Security Practices. New York: Addison Wesley, Inc., 2001. 79-88.

BEA Weblogic Server 7.0 Overview "The Foundation for Enterprise Application Infrastructure"
http://www.beasys.com/products/weblogic/server/wls_70_ov_wp_04021.pdf

"Cardholder Information Security Program"
http://usa.visa.com/business/merchants/cisp_tech_info.html

Enterasys Networks "Dragon Server for Dragon 5 Intrusion Detection System"
http://www.enterasys.com/products/items/DS004/

Dillard, Clayton T. "eCommerce and Defense in Depth." October 24, 2001.
http://rr.sans.org/ecommerce/defense_indepth.php (August 15, 2002).

Flanagan, Heather L. "Egress Filtering – Keeping the Internet Safe from Your Systems." April 30, 2001. http://rr.sans.org/sysadmin/egress.php (August 15, 2002).

"How it Works – Credit Card Processing"
http://www.cybersource.com/products_and_services/electronic_payments/credit_card_processing/howitworks.xml

Maiwald, Eric. Network Security: A Beginner's Guide. New York: Addison Wesley, Inc., 2001.

McGeehe, Brad M. "An Introduction to SQL Server Clustering"
http://www.sql-server-performance.com/clustering_intro1.asp (August 15, 2002)

Northcutt, S., Zeltser, L., Winters, S., Frederick Karen K., Ritchey, Ronald W. Inside Network Perimeter Security. New York: New Riders, 2003.

SANS Institute "The Twenty Most Critical Internet Security Vulnerabilities (Updated) The Experts' Consensus" Version 2.504 May 2, 2002 http://www.sans.org/top20.htm (September 4, 2002).

Sun[tm] ONE Web Server
http://wwws.sun.com/software/products/web_srvr/home_web_srvr.html

Stoneburner, G., Goguen, A., Feringa, A. Risk Management Guide for IT Systems: Recommendations of the National Institute of Standards and Technology. p. 21-25.
http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Tracy, M., Jansen, W., McLarnon, M. Guidelines on Securing Public Web Servers Recommendations of the National Institute of Standards and Technology. p. 20-22.
http://csrc.nist.gov/publications/nistpubs/800-44/sp800-44.pdf.

"Windows NT Firewalls Guardian Vs. Firewall/Plus Vs. Eagle NT Vs. AltaVista Firewall"
http://www.pctoday.com/editorial/hth/970720.html

Wack, J., Cutler K., and Pole, Jamie. Guidelines on Firewalls and Firewall Policy: Recommendations of the National Institute of Standards and Technology. p. 11
http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf