Global Information Assurance Certification Paper

Security Audit of a Web Server Environment

GIAC Certified Security Consultant Version 1.0

By
Chris Bilger
March 21, 2005

Abstract
GIAC Enterprises works in an industry where security is a top priority. A breach of security on the company's public web site would be embarrassing and could cause a loss of revenue. It is critical that every measure is taken to secure the corporation's web server. GIAC Enterprises has decided to have a neutral company do a security assessment of the web environment. Security

Consultant Inc. (SCI) put together a detailed proposal to try to win the contract. The contract was awarded to SCI and detailed analysis will be done to determine the overall security posture of the web server. The information gathered will be reported to the senior management at GIAC Enterprises.

Part I: Methodology and Process

Security Consultants Inc.
Security Consultants Inc.(SCI) is a small IT security corporation. The company was founded in 1993 by Jim Flight. Before starting SCI, Jim Flight worked 10 years at the National Security Agency (NSA). SCI's main focus is providing customers with security solutions. Areas of expertise spans:

- Security Assessments
- Hardware and Software implementation and support
- Policy creation and review
- Disaster Recovery Plans
- Business Continuity Plans

SCI does work for the Department of Defense, the National Security Agency, FBI, and Department of Homeland Security. SCI aids in identifying and eliminating security risks in networking software and hardware. Strong ties with these organizations allow SCI to keep abreast of new technologies and threats.

The staff at SCI is the company's strongest asset. The staff is highly technical and extensively trained in IT security. The company is comprised of four technical and two administrative staff members. The knowledge base of SCI employees spans across multiple platforms and vendors. A brief description of each technical employee is described below:

Consultant A: Has been working with SCI for 12 years. He has 20 years of experience with networking and IT security. He holds a Top Secret Security Clearance with NSA.
Strengths: Windows server platforms, Microsoft applications, Cisco product line, and network security solutions
Certification: Cisco Certified Network Associate (CCNA), Cisco Certified Network Professional (CCNP), Cisco Certified Security Professional (CCSP), Cisco Certified Internetworking Expert (CCIE), InfoSEC, Certified Information System Security Professional (CISSP), Microsoft Certified Systems Engineer (MCSE) NT 4.0, 2000, 2003

Consultant B: 6 years as a security consultant for SCI. 15 years of experience in IT industry.

Strengths: UNIX OS, Intrusion Detection Systems, Firewalls
Certifications: Cisco Certified Network Associate (CCNA), Microsoft Certified Systems Engineer (MCSE) 2000, Red Hat Certified Engineer (RHCE), Sun Certified Network Administrator (SCNA)

Consultant C: 8 years of experience in writing and evaluating corporate policies for private and government organizations. Currently holds a Top Secret Security Clearance with NSA and FBI.
Strengths: Creating and reviewing policies, Disaster Recovery Plans, Business Continuity Plans
Certifications: Certified Information System Security Professional (CISSP), Information Systems Security Engineering Professional (ISSEP),

Consultant D: 15 years of experience with computer forensics, and incident handling.
Strengths: Intrusion Detection Systems, Linux OS, Forensics
Certification: GIAC Certified Incident Handler (GCIH), Certified Ethical Hacker (CEH), Certified Information Systems Security Professional (CISSP)

GIAC Enterprises
GIAC Enterprises is a small minority owned corporation that provides software development solutions to government and civilian organizations. The corporation's main headquarters is located in Greenbelt, MD. GIAC's major customers are government agencies located around the Maryland, Virginia, and Washington D.C. area. GIAC Enterprises was established in 1998 and has been growing rapidly over the last seven years.

GIAC Enterprises has a corporate web site that is used for recruiting and marketing. The web site was built by an employee of the company three years ago to give the corporation a web presence. The main concern of GIAC is securing the web server that is currently housing the company's public web site. It would be embarrassing if the company's web site was defaced due to the sensitive nature of the work they perform. A breach of the web server could cause a loss of business resulting from lack of trust from their customers. It may be viewed as a deficiency in security knowledge and lack of planning on the corporation's part.

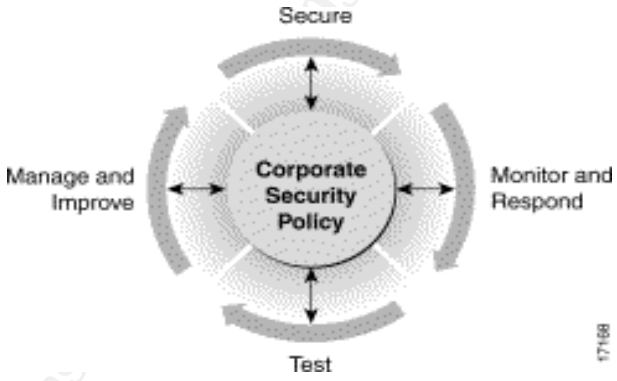
Methodology
SCI has determined that GIAC Enterprises is in need of assistance with the security posture of the web server environment. The opportunity exists for SCI to bid for the contract. SCI has processes in place to aid them in winning a customer's business.
The CEO has extensive training on sales and dealing with customers. The corporation's CEO will setup a brief meeting with the CEO of GIAC Enterprises to get a better understanding of the scope of the project. It is critical to listen closely to the GIAC CEO and fully understand everything they need during the

security audit. SCI will recite the client's needs back to them to ensure a firm understanding.
After the meeting we will cater a proposal and pitch to GIAC Enterprises. Information pertaining to our cleared security background and employee knowledge will be leveraged. SCI will reinforce our company's strong relationships with the government and a vast amount of IT vendors.
SCI's methodology for security is based on the Cisco security wheel. The wheel contains four main areas:

- Secure – Take steps to secure the network
- Monitor – Audit system and detect violations
- Test – Validate effectiveness (attempt hacking)
- Improve – Determine weaknesses that need to be changed

The security process is designed like a wheel because a corporation needs to continuously improve the networks security. Illustration 1-1 is a depiction of Cisco's security wheel.

Illustration 1-1 Cisco Security Wheel



SCI will monitor and test several key areas of the network that pertain to the web server environment. The areas are split into network, server, IIS components, policies and physical security. Each area is investigated against best practice guides developed by SCI, DOD and the product vendor.

Part II: Proposal and Pitch

Letter to CEO

March 21, 2005

John Stagger
4210 Red Branch Road
Greenbelt, MD 21992

Dear John Stagger,

As the CEO of an organization that deals heavily with government customers Security Consultants Inc. (SCI) understands the importance of security. Your organizations web site is your portal to the business community that you serve. The government community needs to be assured that the companies it relies on for IT development understand the importance of security and protects their data according.

John, you have decided wisely to outsource the auditing of the company's web server environment to a consulting firm. Hiring a consultant to perform this task takes away biases that may be created when in house IT staff performs the audit. It also ensures that billable employees remain focused on the contracts they support and are not pulled off to run the audit.

SCI is a consulting firm founded in 1993. The majority of our business deals with network security. Our mission is to provide our customers superior security services. Our staff is extensively trained with a vast amount of security knowledge. SCI does an abundance of work with government clients. Our experience makes us aware of the issues that are facing your organization. SCI has several staff members that hold top secret security clearances with Department of Defense organizations.

The following document outlines our proposed solution to the security needs facing your organization. I think you will find that SCI's solution will satisfy the requirements of your corporation. If given the opportunity SCI will live up to our outstanding reputation and provide GIAC Enterprises with an unmatched level of satisfaction.

Sincerely,

Jim Flight
CEO
Security Consultant Inc.
1-800-555-1212

Company Background
SCI is a small consulting firm that specializes in IT security. The company is located in Rockville, MD and does work in the government and private sector. SCI has been servicing large firms in the Baltimore, Washington and Virginia area and created a remarkable reputation.

We have provided high level IT solutions during the sixteen years the company has been operating. The SCI staff has a large body of knowledge in network security. Several employees of SCI hold clearances across multiple government sectors. The organization prides itself on delivering outstanding work to all customers. Services we provide include:

Security Assessments
- Security and Vulnerability Scans
- Physical Security
- Server Security
- Application Security
  - Web
  - E-mail
  - Database
  - Custom
- Firewalls
- Routers
- Switches
- IDS\IPS
- Enterprise Anti-virus

Hardware and Software Installation

Microsoft Products
- Windows 2000 Server
- Windows 2000 Server Clusters
- Windows 2003 Server
- Windows 2003 Server Clusters
- Microsoft Exchange 5.5, 2000, 2003
- Microsoft SQL 7.0, 2000
- Microsoft IIS 5.0, 6.0
- Group Policy and Active Directory
- DNS

Cisco Products
- Routers
- Switcher (layer 2 and 3)
- PIX firewall
- IDS
- HIDS
- IP Telephony
- VPN Concentrator
- Content Services Switch
- Secure Content Accelerator
- Access Server

Unix\Linux

- Solaris 9, 10 Tru64
- Red Hat 7, 9
- HP-Unix

Security Devices

- Enterprise Anti-virus
- Enterprise backup software
- URL filtering
- Spam filtering appliances

Project Timeline

The project is scheduled to last fifteen business days. There will be three individuals supporting the project. The project can start as early as the first week in April. The following is the sequence of the audit.

Day 1–2:	Kickoff meeting and employee interviews
Day 3–7:	Network Audit
Day 8:	Internal and External Security Scan
Day 9-10:	Review of all data collected
Day 11-14:	Compile all data into a Report
Day 15:	Final Presentation and Deliverable

Upon completion of the contract the final deliverable will be given to the customer.

Project Scope

The main focus on this project will be to identify the security posture of the GIAC web server environment. The settings on the web server will be reviewed against lists of known security weaknesses to determine overall system security. The hardware devices that reside on the network between the external network and the web server will be checked for proper security. To get a better understanding of the services that are provided in the audit a list has been included below. The items that are not covered in the audit are considered separate projects. SCI can put together a proposal for any items in the list that GIAC deems necessary.

Items that are covered:

- Physical access to web server
- Security of the server and operating system: Check the patch levels of the server, scan for known vulnerabilities, group policy applied to servers, and web application software.
- Password strength
- Network Security: Look at routers, switches, firewalls and other network components that are unique to the web server system.

- Policies: A brief review of policies to make sure that they exist and are being kept current.

Items that are not covered

- Web Content: The actual web code will not be reviewed. Code vulnerability is considered a separate project that can be performed at the customer request Questions will be asked of the programmers of the site to determine if this type of audit should be performed.
- Hardware Configuration: Granular analysis of each hardware device will not be done. The device will be checked for correct security settings for the network environment.
- Detailed Policy Review – A detailed policy review is considered a task in itself. A detailed review can be purchased separately.

SCI understands the business environment that GIAC supports. SCI deals with government clients in the same industry. SCI is positive that after the security audit is completed GIAC Enterprises will have the tools to create a more secure network environment.

GIAC vs. SCI Responsibilities

There are key GIAC personnel that will need to be available during the audit. The employees required are the Security Officer, the System Administrators, the Network Manager and the web content Programmer. The SCI team will require the following items to perform the audit:

- User account and password information to logon
  - Firewall
  - Router
  - Switch
  - IDS monitor
  - Web Server
- Two network drops that attach to the DMZ switch
- Available IT policies
  - Risk Assessment
  - Business Continuity Plan
  - Disaster Recovery
  - Change Control

SCI ensures that all customer data remains highly secure. SCI personnel will bring two laptops per technician. One has wireless access to the Internet and the other is used for scanning and recording security data. No usernames or passwords will leave the GIAC facility. The corporate data will be stored on a laptop that has an encrypted hard drive. SCI will delete all information regarding the GIAC network once the information is reported. A non-disclosure agreement can also be drafted and signed by the SCI organization.

High-level Methodology

There are five phases that will be taking place during the audit of the corporate network. During each phase different tasks will be performed by the SCI staff. The phases of the project are:

Phase 1 – Meeting and Interviews

- Introductions to GIAC Enterprises and SCI staff.
- Interview GIAC employees to obtain pertinent security information.
- Record answers to question to be incorporated into the final review.

Phase 2 – Network Audit

- Hardware Audit – Log onto the router, switch, IDS and firewall and check security settings. Settings will be checked against best practice standards and security information suggested by the Department of Defense.
- Software Audit – The OS and web application will be check for security weaknesses. The server will be checked against best practice industry standards and security information outlined by the vendor and the Department of Defense.
- Physical Security – The physical security of the server will be checked. SCI will determine if proper physical measures have been taken to secure the server from possible unauthorized access.

Phase 3 – Security Scan

- A security scanner will be used to expose weaknesses of the web server. The scan will be done from inside the network and externally.

Phase 4 – Compile Date

- All the data obtained from the audit will be reviewed by several technicians. The review will cover in depth analysis of all data retrieved during the audit. The network scans will be reviewed to eliminate false positives that exist.
- The data will then be sent to the technical writer who will put all the information into a report. The report will cover all the security weakness found in the network.

Phase 5 – Final Presentation

- The final presentation will be given to GIAC Enterprises. The rest of the day will be allotted to question and answers sessions.

Project Deliverables

The proposed project will have three deliverables. The deliverables can be broken down into the following categories:

1) Project Plan – The project plan will be a breakdown of the phases,

duration and resources used in each step of the project. It will cover the approach SCI intends to use and the tasks being performed. The billing information will be included with the project plan. A non-disclosure form will be signed by our organization and given to GIAC.

2) Audit Document – The audit document covers all the information obtained during the security audit performed on GIAC's web server. An executive summary will outline what will be found in the audit. There will then be an extensive amount of technical information
3) Audit Presentation – A final presentation will be given to upper-management and IT staff. The presentation briefly touches on the network security problems that should be addressed.

Three hard copies of each deliverable and a soft copy will be provided to GIAC. The project plan will be delivered on the first day of the contract. The other deliverables will be presented to the customer on the closing day of the project.

Billing
The costs are broken down by labor category. The project will require three SCI technicians of varying skill levels. The bill has details about possible price savings and our billing phases. If you have any question please contact Jim Flight at 1-800-555-1212.

SCI Inc.
4332 Rockville Rd
Rockville MD, 21002
March 21, 2005

John Stagger
CEO
GIAC Enterprise
4210 Red Branch Road
Greenbelt, MD 21992

John Stagger:

The table outlines that pricing for the web server security audit:

Labor Category	Hourly Rate	Approx. Hours	Cost
Senior Security Engineer	$130.00	80	$10,400
Security Engineer	$110.00	120	$12,000
Technical Writer	$78.00	32	$2,496
		Total	$24,896.00

If you confirm this estimate within 15 days of March 21, 2005, we'll give you an 8% discount.

The billing of the work will take place in three phases.
30% is due at the signing of the contract
30% is due by the project start date
40% is due within 15 days of the project end date

SCI the consulting solution for your business.

Prepared by: Jim Flight
CEO, SCI Inc.
1-800-555-1212

Accepted by: _____

Date: _____

Pitch
Understanding the business of our customer is significant in pitching our proposed solution. The sales manager is required to do research on a firm that SCI is attempting to enter into business with. The manager will check the customer's public web site and review any recent public documents on the company. SCI feels an advantage is gained by obtaining extensive knowledge about prospective clients. It shows them that we consider them important. The information gathered before meeting with a potential customer can be leveraged by SCI to obtain their business.

SCI plans to use the similar customer background to help win the contract. Our organization has cleared individuals that have worked with the same companies that GIAC Enterprises works with. SCI understands the market that GIAC operates in and the regulations the government enforces. The fact that our employees are cleared at top secret levels assures that we understand the sensitive nature of GIAC's customers.

SCI is a small consulting firm that has a four person IT team. Each individual is highly trained in their security area. The size of the corporation can work to our advantage when bidding for contracts. GIAC Enterprises can be certain that our best employees will be working on this project. Our company does not win work with impressive resumes and then put less qualified individuals on the job site. Every company that SCI does business with gets our top notch IT staff.

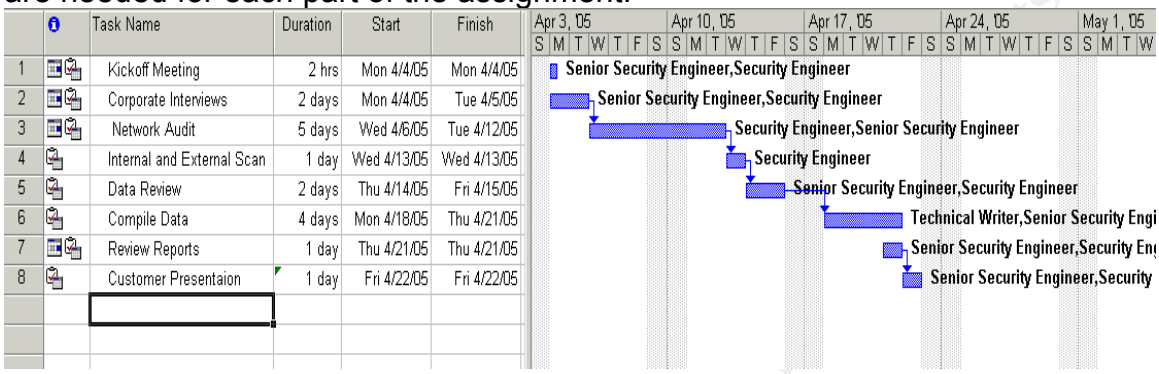
Part III: Project Performance

Project Plan
The goal of this project is to do a thorough audit of GIAC Enterprise's web server environment. All data obtained during this audit will be used to help GIAC Enterprises make the web server more secure. Two technicians will be onsite at GIAC headquarters performing the audit. The technicians will be on premises for eight days logging information about the systems.

After all the auditing has been completed SCI will compile the data into a report. A presentation will take place on the last day of the project that identifies our findings.
After the presentation GIAC Enterprises can setup question and answer sessions to go over all the data in the report. At the close of the contract all data pertaining to the project will be turned over to the CEO of GIAC Enterprises.

Project Schedule

The project will take fifteen work days to complete. The project plan will be outlined to detail what events occur on what days. It will show what resources are needed for each part of the assignment.



	Task Name	Duration	Start	Finish
1	Kickoff Meeting	2 hrs	Mon 4/4/05	Mon 4/4/05
2	Corporate Interviews	2 days	Mon 4/4/05	Tue 4/5/05
3	Network Audit	5 days	Wed 4/6/05	Tue 4/12/05
4	Internal and External Scan	1 day	Wed 4/13/05	Wed 4/13/05
5	Data Review	2 days	Thu 4/14/05	Fri 4/15/05
6	Compile Data	4 days	Mon 4/18/05	Thu 4/21/05
7	Review Reports	1 day	Thu 4/21/05	Thu 4/21/05
8	Customer Presentaion	1 day	Fri 4/22/05	Fri 4/22/05

Day 1 - Kickoff Meeting

Staff \Hours– Senior Security Engineer (2), Security Engineer (2)

Day 1 – 2 Corporate Interviews

Staff \Hours– Senior Security Engineer (10), Security Engineer (14)
Description – The interviews will be held with the organization's Security Officer, System Administrators, the Network Manager and the Programmer. Questions will help in determining security posture.

Day 3 – 7 Network Audit

Staff\Hours – Senior Security Engineer (30), Security Engineer (40)
Description – Log onto different network devices and check settings. Look into the security and application on the web server.

Day 8 Internal and External Security Scan

Staff\Hours – Security Engineer (8)
Description – The engineer will run a security scan against the web server. The scan will
take place both internally and externally.

Day 9 – 10 Data Review

Staff\Hours - Senior Security Engineer (16), Security Engineer (16)
Description – All the data collected from the audit will be reviewed. False positives will be determined and removed before the report is initiated.

Days 11 – 14 Compile Data\Review Reports

Technical Writer (32), Security Engineer (32), Senior Security Engineer (8)
Description – A report will be written covering all the aspects of the network uncovered in the audit. The Senior Security Engineer will review the final document for accuracy and sign off on it.

Day 15 – Customer Presentation

Staff\Hours – Senior Security Engineer (8), Security Engineer (8)
Description – A presentation will be given to GIAC on our findings. A question and answer session will follow the presentation.

Budget Breakdown

The project budget will determine the amount of money that the SCI will net from the project of auditing the web server. Pricing is determined by taking salary plus overhead costs associated with an employee. Overhead costs cover office space, benefits, and the organization's administrative staff. The table below breaks down the project's labor budget.

Labor Categories	Hourly Rate	Loaded Rates	Hours	Actual Rates	Billable Rates	
Senior Security Engineer	$76.00	$130.00	80	$6,080	$10,400	
Security Engineer	$30.00	$110.00	120	$3,600	$12,000	
Technical Writer	$28.00	$98.00	32	$896	$2,496	
				$10,576	**$24,896**	
					($10,576)	
				Net Profit	**$14,320**	

Some employees do not have a high profit margin due to their expertise. These individuals are usually senior level personnel with clearances. These individuals are offset by the profit margin on other employees.

Communication

The communication that will be taking place between the client and SCI will be limited to weekly status reports. The reports will be sent by e-mail and are not required to be formal. The purpose of the report is to state progress over the week and expected tasks for the following week. The report will have a section that covers difficulties and successes. The difficulties section can be helpful in providing upper management with a list of obstacles to the projects success. The weekly status reports will be sent to the CEO of GIAC Enterprises. The customer always has the ability to call brief impromptu meetings with the technician if there is a matter that needs immediate attention.

Meeting/Interview Process

On the first day of the project it is standard to have a kickoff meeting. The CEO

of GIAC Enterprises will briefly explain the purpose of the audit. The CEO will voice his support of the project. He will let the key members of the company know they will be playing an important role in the success of the audit. The floor will then be turned over to SCI's lead technician on the project.

SCI will take time to do introductions of our staff and the GIAC employees. Then we will present our project plan and timelines. Before the meeting is complete each individual will know what they are responsible for and when they will need to be available to our employees.

There are several employees that will need to be interviewed to obtain information about company security. The following questions have been written down to ask the employees.

1) (Network Manager) What are the backgrounds and knowledge base of the two data center system administrators? *This question will help to determine possible areas of weakness. If the two employees are highly trained in hardware devices a natural place to look may be the software on the network. Our technicians never make assumptions based on the answer to this question but use it as an aid. This question would be asked of the Network Manager since they would have the information on the two employees. Asking these questions may result in a negative response. It can come off as a threatening question because you may be inferring that they don't have knowledge in certain areas.*
2) (Network Manager, System Administrators) What are the policies that the IT department uses and when are they updated? *This question is trying to establish the policies that the IT department uses. This question is asked of both the Network Manager and the System Administrator to ensure the answers are the same. Many times there are policies in place that no one follows. By asking the question to all three employees we can better determine policy use.*
3) (Security Officer) What measures have been taken to physically secure the building? *The Security Officer would have information regarding facility physical security. This person may be the only individual that knows the true extent of the physical security.*
4) (System Administrators) – What is your process for installing patches? *The system administrators would be the professionals installing the patches on servers and hardware. The question seeks to find out how often patches are done, what are the means by which they are informed of patches and how they get installed on the production web server.*
5) (System Administrator/Programmer) What type of web content does the site have? *It is helpful for SCI to know what the site is used for and the content that exists. This will help us determine how it can be secured.*
6) (System Administrator) - Is there additional security measures you would like to see implemented on the web environment? *The question is*

asked to determine if the staff is interested in making the environment more secure. If they have a lot of great ideas it is important to find out why they are not being implemented.

7) (System Administrator) – Is there a budget for security training in the IT department? *The question is aimed at finding out the overall importance the organization places on IT security. There should be a certain budget allocated to sending staff both IT and employee to security training.*
8) (System Administrator) – What is the process for monitoring the IDS alerts? *The question enables SCI to figure out how the IDS is used. If an IDS is installed but not monitored it serves no purpose. IDS alerts need to be looked into to determine the impact of the threat. An action should be taken based on the threat level.*

The closing day of the project there will be a presentation given to upper-management and the IT department. The presentation will give an overview of the areas that need improvement. At the close of the meeting questions will be addressed and hard copy of the reports will be handed out.

Pitfalls

There are several issues that can arise during the life cycle of a project. It is critical to recognize these problems and correct them before they become detrimental to the project. Unresolved issues can cause a project to fail and the organization to lose a customers future business.

An area a consultant can encounter resistance is with the IT department. The IT department may feel that our organization is making them look bad or exposing problems they have not found yet. It is usually easy to spot these types of problems because the employees will avoid you or not give you enough information. The best way to address this problem is by reassuring the IT team that you are just here to observe and aid them in the process of improving the networks security. Make sure that they know all of the things that are currently being done well on the network in regards to security. Focusing on only the negative aspects of the network may spark defensiveness by the GIAC employees. As a last resort the CEO can be contacted if a problem continually stands in the way of SCI performing the job.

The employees that work for the organization are a critical part of the project's success. If a key individual is not going to be around when needed it can cause delays in the project. SCI will need to identify all key personnel and make sure they will be available during the audit. This can be done by setting appointments with key personnel ahead of time to make sure that their calendars are open. It may be necessary to identify two employees for each category so there is a backup if one is out for some unforeseen reason.

Value Added

Our corporation prides itself in adding value to the product we deliver. At the

closing of our security audit we will provide GIAC Enterprises with a written document covering the security audit. There will also be a presentation given to upper-management on the information obtained in the audit. The document and presentation will cover the positive aspects of the network's security and areas that need improvement.

It is hard for an organization's IT department to have a wide variety of networking knowledge. SCI provides our customers a two hour training lunch to cover an area of the client's choice. The topics can help to aid the customer in securing the network and carrying out the suggestions in the audit documentation.

A corporation's security posture continuously changes as new software and hardware are introduced to the environment. Vulnerabilities for software are released on a daily basis. It is critical to create a cycle where the system is being audited every year. As a valued customer, you will receive 10% off next years' audit if the audit is booked at the closing of this contract.

A network is only as strong as its weakest link. An entire audit of the GIAC network should be performed to ensure that a compromise of another system on the network won't adversely affect the corporate web server. SCI is trained to handle large scale entire network audits. As a valued customer SCI will take 10% off the cost of this service if booked within one month of the close of this contract.

SCI believes that after going over the security of the environment there may be another opportunity that presents itself. The audit that is performed is aimed at individuals that have a technical background. The purpose of our audit is not to give them a step by step guide to securing the GIAC Enterprise. The report will go into great detail on all the changes that need to be made to the network. The "how to" should be taken care of by the IT staff at the company. SCI can be hired to come in and assist with implementing the settings outlined in the report.

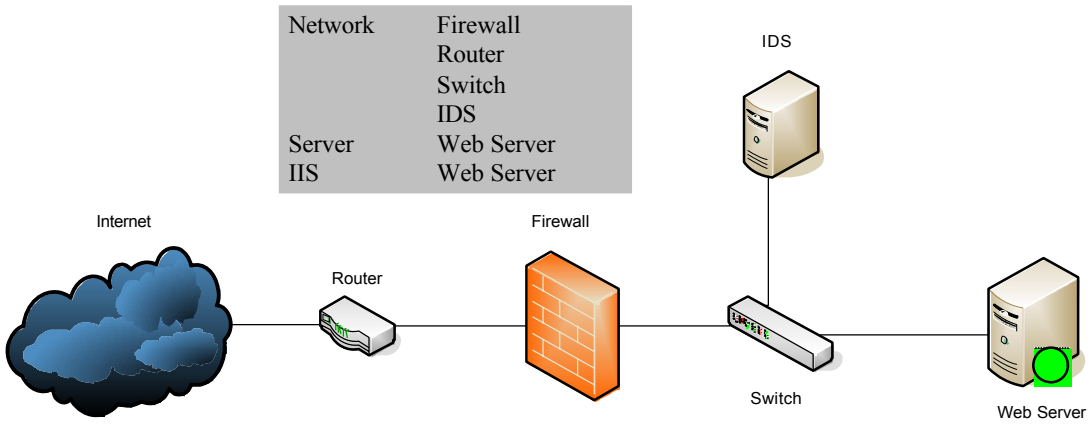
Part IV: Final Deliverables

Introduction

Information regarding the security audit of GIAC Enterprise's web server is covered in this document. The audit first outlines the positive information found when conducting the web server audit. The areas of concentration have been split into policies/documentation, network, server, IIS components and physical security. The next section of the audit will cover the areas that need improvement. The areas will be broken down into network, server, and IIS components. A summary of the positive and negative aspects will be outlined in this document followed by a more in-depth technical section.

An illustration of the GIAC web server network architecture and a list of what falls into each component have been placed below.

Illustration 1-1



After a full review is completed a security scan is performed on the web server from inside and outside the network. The results of the scan and solutions to the problems encountered will be outlined.

High Level Overview

There are several key areas in the network that SCI determined to have adequate security measures applied to protect against threats. Other areas need to be addressed to ensure the web server is not compromised

Secure Aspects

- Physical Security
- Router Security
- Switch Security
- Firewall Security
- IDS Security
- Policy Existence
- Patch Management
- Virus Scanning
- IIS Services Installed
- Users with Least Privilege

Unsecured Aspects

- Windows 2000 System Security
- Default User Accounts
- IPSec Policy
- TCP/IP Stack
- IIS Lockdown

Positive Attributes of Current Operating Environment

There are several security enhancements that have been done to the operating environment to guard against a security breach. This shows that the current IT administrators take security seriously and are making strides to protect valuable corporate data. The positive aspects will be covered briefly before describing areas that need attention.

Server

Server Setup

The corporate web server has been setup as a stand alone server. A stand alone server is not a member of the corporate domain. Servers that are part of a domain will have domain accounts with privileged access to the server. Creating a stand alone server ensures that the server can only be used by members that have an account on that server locally.

User Accounts

User accounts are setup for each employee that requires access to the server. The accounts have been added to groups and the groups are assigned permissions at different access levels. The administrators are applying the concept of least privilege to the web server. Only permissions that are required to accomplish tasks are given to the employee (the least amount of privilege).

Virus Scan

Mcafee Enterprise Virus Scan version 8.0 is installed on the server. The product is update weekly with new virus definitions. The administrative staff is on Mcafee's mailing list. When an e-mail is received by Mcafee listing a new threat

the server is updated immediately.

IIS

IIS Components

The current web environment is only running the components needed for IIS to server web pages. FTP, SMTP, NNTP and FrontPage server extensions have not been installed on the web server. The above protocols have known risks associated with them. The IT team has minimized the corporation's risk by not installing unused protocols.

Network

Router

There have been numerous amounts of security measures taken to lockdown the Internet router. The network administrator provided the team with running configurations, access-lists, and interface information from the router. The team also provided SCI technicians with limited logon capabilities to the router so the settings could be viewed. The routers have had unnecessary services disabled to guard against weaknesses. The service passwords have been encrypted on the router so they are not transmitted or stored in clear text. Remote administration of the router has been disabled and must be done through a console cable connected directly to the router. All other means of administering the router have been disabled. The overall security of the router was great.

Switch

The switch that is installed between the firewall and the web server has been properly secured by the network administrator. Unnecessary services and remote access have been disabled. All ports except for the IDS and web server ports have been disabled. The port that houses the web server has had port security enabled on it.

Firewall

A Cisco PIX firewall has been placed on the network between the web server and the Internet. The web server has been placed on a DMZ port of the firewall that is segregated from the internal network and external networks. The firewall has access lists that only allow port 80 to the web server from the external network. The interfaces have been setup correctly to ensure that traffic can only flow from higher to lower interfaces. This allows internal LAN users to access the internet and DMZ but these networks cannot access the internal network.

IDS

A network IDS is attached and monitoring inbound and outbound traffic on the DMZ. The IDS has several different categories for events that occur on the network. The IDS has been setup with thresholds. Administrative staff is paged and e-mailed based on the severity of the threat. All high level security events are investigated to determine source and type of event. A test was performed from outside the network to trigger high alarm IDS events. After a couple of minutes the IP was blocked at the firewall. The IT team at GIAC Enterprises is doing an exceptional job at staying on top of the IDS events.

Physical Access

The web server environment is kept in a data center. The room is secured with its own alarm system and cipher locks. The alarm system has motion sensors and a card access system that logs all employees entering and leaving the data center. There are currently only five people in the corporation that have full access to the data center. A sign in log is used to track individuals that are brought into the room under supervision.

The facility has a surveillance system in place to monitor corporate assets. The data center has one camera installed that monitors the room. The surveillance system uses a digital video recorder DVR to archive the data recorded. The system is reviewed every other day by the company's Security Officer.

Policies\Documentation

Policies

The IT staff has many policies in place to ensure that the web environment is secured and in working order. The scope of this audit does not cover detailed policy review. It checks to see if they exist and are kept updated. The following is a list of current policies the corporation has and regularly updates:

- Disaster Recovery Plan
- Change Control
- Business Continuity
- Patch Management
- Server Access
- Incident Handling and Response
- Acceptable Use
- Backup Procedures

Patch Management

The computer operations staff keeps on top of patch releases and makes sure the server environment is kept up to date with the latest patches. The IT staff is part of several online e-mailing lists that keep them abreast of new patches as they are released. Microsoft's Baseline Security Analyzer was run against the server and no missing patches were found. It is recommended that GIAC Enterprises takes advantage of the Microsoft tool on a regular basis to check patch levels. The software is free and can be obtained at: http://www.microsoft.com/downloads/details.aspx?familyid=b13ebd6b-e258-

4625-b0a3-64a4879f7798&displaylang=en

Negative Attributes of the current Environment

The next section covers the areas of the network that need to have security settings implemented. It is important to remember to test changes in a development environment first before putting them into production. After the audit is complete a security scan of the server will take place.

Server Security

Disable Unneeded Services

Any services that are running and are not needed create potential risk for a web server. A review of the services should be done and all unneeded services should be removed. A sample list has been provided below of services that are not usually needed on a stand alone web server:

- Alerter
- Browser
- ClipBook Server
- DHCP Client
- Distributed File System
- License Logging Service
- Logical Disk Administrator
- Messenger
- Netlogon
- Network DDE
- Network DDE DSDM
- Remote Registry Service
- Removable Storage
- RPC Locator
- RunAs Service
- Simple TCP/IP Services
- Spooler
- Task Scheduler
- TCP/IP NetBIOS helper
- Telephony

This list is just a sample and should be first applied to a development server and

tested before implemented in a production environment. Services that are not covered in the above list may still not be needed in your operating environment.

Disable Components

The server only needs TCP\IP to function as a web server on the GIAC network. The administrators of the web server need to disable protocols that are not used to safe guard the server from an attacker. The NetBIOS protocol has been the target for many network attacks. The NetBIOS protocol should be disabled on the network card.

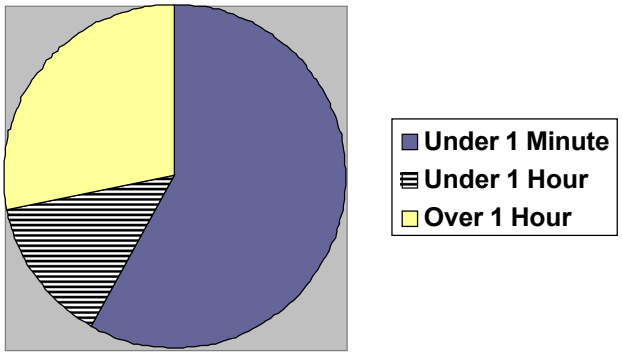
Hardening Server Security Settings

Windows Server 2000 gives an administrator the ability to harden the security settings on a server. There is a security configuration console that will allow administrators to change settings that are on the server. The settings that are installed by default are not secure and need to be addressed to prevent unauthorized access to the server. GAIC Enterprise's web server is currently running with the default installation of the security settings. The following list outlines the breakdown of the Security Configuration pieces:

- Account Policies – password policies
- Local Policies – Audit Policies, Rights Assignment, and Security Options
- Event Log – System Events
- Restricted Groups – memberships for groups
- System Services – configuration for services (auto, manual, disable)
- Registry – restrict access to registry
- File System – restrict access to files and directories

Account Policies

It is critical to make sure that users are creating passwords that are complex and changed frequently. When running a tool against your passwords 65% of the accounts passwords cracked in less than two minutes. The server Administrator account was included in the list of cracked passwords. Chart 1-1 illustrates the amount of time it took to crack the user account passwords.



The password policy for GIAC needs to be change to protect the server against password guessing and brute force attacks. The password policy outlined in table 1-1 is recommended by the National Security Agency.

Table 1-1 Account Policy Settings

Policy Options	**Recommended Settings**
Enforce Password History This feature ensures users are using different passwords each time a new one is entered. Range can be set from 0-24	24

Policy Options	Recommended Settings
Maximum Password Age The length of time before a password must be changed. Range can be from 1-999 days	90
Minimum Password Age The length of time a user must wait before he can change the password after it has just been changed. Ranges from 1-998 days	1
Minimum Password Length The amount of characters in each password	12
Passwords must meet complexity Requirements Forces an account to use upper and lowercase and a special character when creating a password. Complexity makes it more difficult for attackers to crack passwords	Enable
Store Password Using Reversible Encryption for all users in Domain Stores passwords using a two way hash. This option should not be used because it is similar to storing in clear-text	Disabled

Account Lockout Policy

There should be proper account lockdown policies implemented on the server to guard against password guessing. If no policy is enforced then an attacker can run brute force attacks until the password is cracked. Lockout policies provide an administrator a way to tell if someone has been trying to break into the company's system. If an account keeps getting locked out it is a red flag for IT staff to investigate why this is occurring. Table 1-2 outlines best practices for account lockout policies for a secure environment.

Table 1-2 Account Lockout Policy

Account Lockout Policy	Recommended Settings
Account lockout duration The amount of time that an account will be locked after threshold for wrong passwords entered is met. This ranges from 0-99999 minutes. 0 disables the account until an administrator unlocks it.	0
Account lockout threshold Number of invalid logons before the account gets locked	3
Reset account lockout counter after Number of minutes before the invalid logon account is reset	15 minutes

Local Policy Settings

Auditing Policy

A server should be audited to log events that occur. Audit logs are a way to track system use and pinpoint when a breach occurs. The audit logs are helpful in aiding with a forensic investigation. Table 1-3 lists the recommended settings for auditing the server.

Table 1-3 Audit Policy (Cox 394)

Audit Policy	**Recommended Settings**
Audit Account Logon Events Audits user logon/logoff events	Success and Failure
Audit Account Management Management of users or groups	Success and Failure
Audit Directory Service Access Only needed with Active Directory	No Auditing
Audit Logon Events Records users that have logged on and how they have logged on	Success and Failure
Audit Object Access Access to objects (files, directories and registry)	Failure
Audit Policy Change Changes to user rights policies, and trusts	Success and Failure
Audit Privilege Use Rights audits of user rights	Failure
Audit Process Tracking Tracks system processes	No Auditing
Audit System Events System events like restarting	Success and Failure

User Rights Assignment

The operating system comes with security options that enable an administrator to delegate certain rights to users of the system. The rights should be changed from the default settings to enhance security. Table 1-4 describes each right and the settings that should be changed on the web server.

Table 1-4 User Rights Assignments (Haney 33)

User Rights	**Current Settings**	**Recommended Settings**
Access this Computer from the Network Allows user to connect over the network to computer	Everyone, Administrators, Power Users	Administrator, Users
Act as part of the Operating System Allows a user or group to run a process as a trusted part of the OS	None	None

User Rights	Current Settings	Recommended Settings
Add workstation to domain Add a computer to the domain	None	None
Back up files and directories	Administrators, Backup Operators, Server Operators, Power Users	Administrators
Bypass traverse checking Allows user to access subdirectories even is user does not have access to the parent directory	Everyone, Administrators, Authenticated Users	Users
Change the system time Set the computer clock	Administrators, Server Operators, Power Users	Administrators
Create a pagefile Allows a user to create pagefiles used for virtual memory	None	Administrators
Create a token object Allows user to create an access token	Administrators	None
Create permanent shared object Allows a user to create special permanent directory objects	None	None
Debug programs Debug low level objects like threads	Administrators	Administrators
Deny access to this computer from the network Prevents users from accessing this server from the network	None	None
Deny logon as a batch job Prevents users from logging on as a batch job	None	None

User Rights	Current Settings	Recommended Settings
Deny logon as a service Prevents specific accounts from registering a process as a service	None	None
Deny logon locally Prevents user from logging on the server directly	None	None
Enable computer and user accounts to be trusted for delegation Allows user to set Trusted for Delegation on a user or computer object	Administrators	None
Force shutdown from a remote system Allows user to shutdown system of the network	Administrators, Server Operators, Power Users	Administrators
Generate security audits Allow process to generate security audit entries	None	None
Increase Quotas Allows user to increase processor quota assigned to a process	Administrators	Administrators
Increase scheduling priority Allows user to boost the priority of a process	Administrators	Administrators
Load and unload device drivers Right to install and remove device drivers	Administrators	Administrators
Lock pages in memory Right to lock pages in memory	None	None
Log on as a batch job Right to log on by using batch queue facility IUSR_*computername* does not need this right and can be removed	Administrators	None
Log on as a service Right for a process to register with the system as a service	Administrator, Account Operators, Backup Operators, Print Operators, Server Operators	None

Log on locally Right to log on at the system console	None	Administrators, IUSER_(machine name) IWAM_(machine name)

User Rights	Current Settings	Recommended Settings
Manage auditing and security log Right to view and clear the security log	Administrators	Administrators
Modify firmware environment variables Right to modify system environment variables	Administrators	Administrators
Profile single process Right to perform profiling on a process	Administrators	Administrators
Profile system performance Right to perform profiling on the system	Administrators	Administrators
Remove computer from docking stations Right to undock a laptop	Administrators	None
Replace a process-level token Right to modify a process's security access token	None	None
Restore files and directories Right to restore files that have been backed up	Administrators, Backup Operators, Server Operators, Power Users	Administrators
Shutdown the System Right to shutdown server	Administrators, Backup Operators, Account Operators, Server Operators, Print Operators, Power Users	Administrators
Synchronize directory service data No effect	None	None
Take ownership of files or other objects Right to take ownership of files, directories, printers and other objects	Administrators	Administrators

Security Attributes

The security attributes section of the security policy will determine security settings on the server. The default values in this area are set to ensure optimal functionality and not security. If the focus is being placed on security the changes outlined in Table 1-5 should be followed.

Table 1-5 Security Attributes (Henly38)

Security Attribute	**Recommended Settings**
Additional Restrictions for anonymous connections Puts restrictions on anonymous users	No access without explicit anonymous permission
Audit the access of global system objects Assigns a default SACL to system object which can then be audited	Enabled
Audit the use of backup and restore privilege	Enabled
Clear virtual memory pagefile when system shuts down Cleans out the pagefile at shut down	Enabled
Digitally sign server communications (when possible) Allows SMB server to perform digital packet signing when client also supports it	Enabled
Do not display last user name in logon screen	Enabled
LAN manager authentication level Determine the type of challenge and response to authenticate network logons	Send NTLMv2 response only\refuse LM & NTLM
Message text for users attempting to log on Banner displayed at log on	Configure a log on banner that states corporate policy against unauthorized access
Message title for users attempting to log on	Create a title for the banner

Security Attribute	Recommended Settings
Number of previous logons to cache Allows user to login when not connected to the network. If set to 0 the machine has to be connected	0 logons
Restrict CD-ROM access to locally logged on user only	Enabled
Restrict floppy access to locally logged on user only	Enabled

Settings for Event Logs

The event logs are an important part of investigating possible problems or intrusions on the network. It is key to have the settings for the event log set so an attacker cannot cover their trail. The settings outlined in table 1-6 are recommended settings to make sure the log size is big enough and the data is only manually archived.

Table 1-6 Event Log Settings

Event Log Settings	Recommended Settings
Maximum Application Log Size Security Log Size System Log Size	4194240 Kbytes
Restrict guest access to all logs	Enabled
Retain application log security log system log	Not defined
Retention method for all logs This defines how the logs will be deleted. Manually means the logs will have to be deleted by an administrator. The logs will not overwrite each other.	Manually
Shutdown the computer when the security log is full This setting is not recommend for a server that needs to have high availability	Disable

Registry

The registry is critical part of the Windows operating environment. It contains all the settings for the entire operating system. The security on a server's registry should be locked down to prevent users from changing critical settings. Table 1-7 outlines recommend setting changes. Under permissions Full Control = FC and Read = R. The values for Inherit are replace (all subkey regardless of permissions will reset to the new permissions set) and propagate (all subkeys that already inherit permissions will be changed to the new settings).

Table 1-7 Registry Security (Haney 76)

Key	Groups	Permissions	Inherit
HKey_LOCAL_MACHINE			
Software Information on software installed on the machine	Administrators Creator Owner System Users	FC FC (subkeys only) FC R	Replace
Software\Microsoft\NetDDE Settings for NetDDE	Administrators System	FC FC	Replace
Software\Microsoft\Windows NT\CurrentVersion\AsrCommands Automatic Recovery commands	Administrators Creator Owner System Users	FC FC (subkeys only) FC R	Replace
Software\Microsoft\Windows\ CurrentVersion\Group Policy Data for group policy settings	Administrators Authenticated Users System	FC R FC	Replace
Software\Microsoft\Windows\ CurrentVersion\Installer Configuration Information for the Windows installer	Administrators System Users	FC FC R	Propagate
Software\Microsoft\Windows\ CurrentVersion\Policies Stores registry entries managed by group policies	Administrators Authenticated Users System	FC R FC	Propagate
System Stores values for current control set or control sets that have been used before	Administrators Creator Owner System Users	FC FC (subkeys only) FC R	Replace
\Controlset001 \Controlset002 Control sets that may be used to install and run Windows	Administrators Creator Owner System Users	FC FC (subkeys only) FC R	Propagate

Key	Groups	Permissions	Inherit
\CurrentControlSet\Control\ SecurePipeServers\winreg Which users can use the remote registry	Administrators System	FC FC	Replace
\CurrentControlSet\Control\ Wmi\Security Security settings for Windows Management Instrumentation	Administrators Creator Owner System	FC FC FC	Replace
\CurrentControlSet\Hardware Profiles System hardware profiles	Administrators Creator Owner System Users	FC FC (subkeys only) FC R	Propagate
HKEY_USERS			
.Default	Administrators Creator Owner System Users	FC FC (subkeys only) FC R	Replace
.Default\Software\Microsoft\ NetDDE Settings for Network Dynamic Data Exchange	Administrators System	FC FC	Replace

File System

This section of the security policy defines permission for files and folders on the server. The default settings on Windows 2000 Server allows too much access to the Everyone group. In order to secure the server certain restriction should be made to these directories.

- Root
- System Directory - \winnt\system32
- System Drive – C:\

Table 1-8 list the changes that need to be made to the file system. The settings outlined in this table were established by the NSA. Under permissions Full Control = FC and Read = R. The values for Inherit are replace (all subfolders and files regardless of permissions will reset to the new permissions set) and propagate (all subfolders and files that already inherit permissions will be changed to the new settings).

Table 1-8 File System Permissions (Haney 88)

Folder\File	Groups	Recommended Permission	Inherit
Program Files Application installation directory	Administrators Creator Owner System Users	FC FC (subfolders and files) FC R,E	Replace

Folder\File	Groups	Recommended Permission	Inherit
C:\WINNT\system32\config Registry hive files	Administrators System	FC FC	Replace
C:\WINNT\system32\DTCLog Log file for MS Distributed Transaction Coordinator	Administrators Creator Owner System Users	FC FC (subfolders and files) FC R,E	Propagate
C:\WINNT\system32\ias Database for Internet Authentication Service	Administrators Creator Owner System	FC FC FC	Replace
C:\WINNT\system32\Ntbakup.exe Backup program	Administrators System	FC FC	Replace
C:\WINNT\system32\NtmsData Location for removable store database	Administrators System	FC FC	Propagate
C:\WINNT\system32\rcp.exe Remote copy command	Administrators System	FC FC	Replace
C:\WINNT\system32\regedt32.exe Registry editing tool	Administrators System	FC FC	Replace
C:\WINNT\system32\rexec.exe Program that executes remote calls	Administrators System	FC FC	Replace
C:\WINNT\system32\rsh.exe Program that executes remote shell	Administrators System	FC FC	Replace
C:\WINNT\system32\secedit.exe Security configuration and analysis tool	Administrators System	FC FC	Replace
C:\WINNT\system32\Setup	Administrators System Users	FC FC R,E	Propagate
C:\ Installation of Windows 2000 directory	Administrators Creator Owner System Users	FC FC (subfolders and files) FC R,E	Propagate
C:\autoexec.bat Initialization file for DOS apps	Administrators System Users	FC FC R,E	Replace
C:\boot.ini Boot Menu	Administrators System	FC FC	Replace
C:\config.sys Initialization file for DOS apps	Administrators System Users	FC FC R,E	Replace
C:\Documents and Settings Folder containing user profiles	Administrators System Users	FC FC R,E	Propagate

Folder\File	Groups	Recommended Permission	Inherit
C:\Documents and Settings\ Administrator Built-in administrator profile	Administrators System	FC FC	Replace
C:\Documents and Settings\ All Users Profiles for all users	Administrators System Users	FC FC R,E	Propagate
C:\Documents and Settings\ Default User Default desktop for users logging on for the first time	Administrators System Users	FC FC R,E	Replace
C:\WINNT Windows 2000 OS files are installed in this directory	Administrators Creator Owner System Users	FC FC (subfolders and files) FC R,E	Replace
C:\WINNT\$NtServicePackUninstall$ Older version of system files before SP was installed. Used for rollback	Administrators System	FC FC	Replace
C:\WINNT\$NtUninstall$ Uninstall for apps and hotfixes	Administrators System	FC FC	Replace
C:\WINNT\Debug System and Active Directory logs	Administrators Creator Owner System Users	FC FC (subfolders and files) FC R,E	Propagate
C:\WINNT\Debug\UserMode	Administrators System Users	FC FC Traverse folder, Create files (folder only) Create Files\Folders (Files only)	Propagate
C:\WINNT\security Security templates and analysis database	Administrators Creator Owner System	FC FC (subfolders and files) FC	Replace
C:\WINNT\regedit.exe Registry editing tool	Administrators System	FC FC	Replace

Folder\File	Groups	Recommended Permission	Inherit
C:\WINNT\Registration Contains Component Load Balancing files	Administrators System Users	FC FC R	Propagate
C:\WINNT\repair Backup files of SAM and important registry and system files	Administrators System	FC FC	Replace

The security settings to harden the Windows 2000 operating system can be configured by an .inf file. Using the Microsoft MMC console all the settings can be saved to a file. Saving the settings to a file make it easier to install them on multiple servers.

User Accounts

The administrator account has not had its name changed. It is important to change the name of the administrator account on the web server. The administrator account is a well known account in Windows 2000. Not renaming the administrator account provides an attacker with half the information they need to log onto a server. The attacker would only need the password to gain full access to the server. Once the administrator account has been changed a decoy administrator account should be created. The account should only be a member of the guest group.

The guest account has not had its name changed. It is important to change the name of the guest account on the web server. The guest account is a well known account in Windows 2000. By not renaming the guest account the attacker is provided with half the information they need to log onto a server. The attacker would only need the password to gain the same access as the guest account. Once the guest account has been renamed it is suggested that the account be disabled.

IPSec Policy

On a network layered defense against attacks is critical to protect corporate data. Each point in the network should have security implement to ensure data safety. An IPSec policy allows an administrator to determine what ports, protocols and IP addresses are allowed in and out of a server. Currently the only access that is needed from the external network is HTTP over port 80. An IPSec policy can be setup to limit access to only this port.

TCP/IP Stack

TCP/IP is the protocol used to communicate over the Internet. The protocol has certain vulnerabilities that exist. It's a good practice to harden the servers TCP/IP stack to guard against some of these weaknesses.

SYN attack is one of the weaknesses present in the TCP/IP stack. Registry settings will need to be changed to guard against the weaknesses. The changes will be made to the registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services:

Table 1-9 SYN Attack Protection Recommended Values (Microsoft 758)

Value	Recommended Setting
SynAttackProtect Connection response timeouts more quickly during SYN flood	2
TcpMaxPortsExhausted Threshold of TCP connections before SYN flood protection starts	5
TcpMaxHalfOpen Threshold of TCP connections in SYN_RCVD state	500
TcpMaxHalfOpenRetired Threshold of connections in SYN_RCVD state where 1 retransmission has been sent	400
TcpMaxConnectResponseRetransmissions How many times a SYN-ACK is sent before canceling attempt to respond	2
TcpMaxDataRetransmissions Number of time retransmission of data segment be for canceling connection	2
EnablePMTUDiscovery When set to one it force TCP to discover MTU over path to host. Attacker can use this to force packet fragmentation causing the stack to be overworked	0
KeepAliveTime How often TCP attempts to verify idle sessions	300000 (five minutes)
NoNameReleaseOnDemand Set to not release NETBIOS name when it is requested	1

Host Based Intrusion Detection

GIAC's network uses network based intrusion detection (NIDS). GIAC's NIDS logs traffic traveling across the network and reports suspicious activity based on signature sets. A further step can be taken to secure the corporate web server. Host based intrusion detection (HIDS) can be used to ensure changes are not made to the web server. HIDS is installed on the server and monitors access to the operating environment. It can be used to restrict access to critical directories so a malicious user can't make changes to the server. The HIDS can be used to lockdown the directory where the web content is so it cannot be changed.

IIS Lockdown

URL Scan\IIS Lockdown Tool

It is a good practice to lockdown the web server using Microsoft's IIS lockdown utility and URL scan. The IIS lockdown tool will secure the server by letting the administrator choose a server role. Once the server role is determined the IIS lockdown tool disables features that are not required for the specified server type.
In the case of GIAC Enterprises it is recommended that *Static Web Server* is selected. Once it has been selected the following extensions no longer work and are mapped to 404.dll: .asp, .asa, .cer, cdx, .htr, .idc, .shtm, shtml, .stm, and .printer. The 404.dll files when accessed will return a page not found message (Microsoft 457).

The IIS lockdown tool also creates two new groups one called Web Anonymous Users and Web Application Users. The IUSR_*computername* account is added to the Web Anonymous Users group and the IWAM_*computername* account is added to the Web Application group. During the lockdown of the server permissions to directories are based on these groups not to individual accounts.

During the installation of the IIS lockdown tool URL scan is installed. URL scan is used to filter HTTP requests. URL scan will block requests to the web server that contain unsafe characters (Microsoft 437). The URL scan tool can be manipulated by an administrator by opening the urlscan.ini file. Examples of values that can be added to the urlscan.ini file are:

- MaxAllowedContentLength
- MaxUrl
- MaxQueryString

The lockdown utilities can be found at the following URL:
http://www.microsoft.com/technet/security/tools/locktool.mspx

Default Directory Permissions

The permissions assigned to the default directory (*inetpub*) should be changed. The Everyone and Guest account should be deleted from having folder access. Allowing these groups to have access causes a threat to the security posture of the server. Attackers can place harmful code on the server to try and gain control.

Default Installation Directories

During the installation of IIS the software creates several directories that can be deleted from the server. The directories created have sample files, and features

that the GIAC organization does not need. These sample files and features can have vulnerabilities and should be deleted

- \inetpub\iissamples
- \inetpub\AdminScripts
- C:\program files\common files\system\msadc
- C:\winnt\web\printers
- C:\winnt\help\iishelp

The web\printer directory will automatically be restored after the server is restarted. Changes need to be made to the web folder to ensure the print folder is not recreated. The permissions on the folder should be

- Administrators, System – Full Control
- Web Anonymous Users – Deny Full Control

Once these changes are made the directory will not restore itself upon reboot (Walker 79).

The location of the company's web site is in the default inetpub\wwwroot folder. The corporate web site needs to be moved off the system partition. Moving the web site content to a different partition will protect the system against directory traversal attacks (Microsoft 453). The new directory can be placed on the partition labeled D:\. The new directory that will house the corporate web content should have the following permissions:

- Administrators, System – Full Control
- Authenticated Users, Web Anonymous Users – Read

Folder\File Permissions

There are certain files and folders that need to have the permission changed to protect the server. The changes that are outlined can be made part of the .inf file discussed under the server lockdown procedures. The purpose of this section is to deny full access to important files and directories to the Web Anonymous Users group.

Table 1-10 Directories to Deny Full Access to Web Anonymous Users (Walker 80)

Directory\Files	
C:\	Apply to directory only not files and subdirectories
C:\WINNT	Apply to directory only not files and subdirectories
C:\WINNT Explorer.exe, Regedit.exe, Poledit.exe, Taskman.exe	Apply to files listed
C:\WINNT\System	Apply to directory only not files and subdirectories

Directory\Files	
C:\WINNT\\debug	Apply to directory only not files and subdirectories
C:\WINNT\installer	Apply to directory only not files and subdirectories
C:\WINNT\repair	Apply to directory only not files and subdirectories
C:\WINNT\security	Apply to directory only not files and subdirectories
C:\WINNT system32	Apply to directory only not files and subdirectories
C:\WINNT\system32\ At.exe, cacls.exe, cmd.exe, command.com, cscript.exe, debug.exe, edlin.exe, finger.exe, ftp.exe, ipconfig.exe, krnl386.exe, nbstat.exe, net.exe, net1.exe, netsh.exe, posix.exe, rcp.exe, regedt.exe, regini.exe, regsvr.exe, rexec.exe, rsh.exe, runas.exe, runonce.exe, srvmgr.exe, sysedit.exe, syskey.exe, telnet.exe, tftp.exe, tracert.exe, usrmgr.exe, wscript.exe, xcopy.exe	Apply to files listed
C:\WINNT\system32\dllcache	Apply to directory only not files and subdirectories
C:\WINNT\system32\drivers	Apply to directory only not files and subdirectories
C:\WINNT\system32\inetsrv	Apply to directory only not files and subdirectories
C:\WINNT\system32\inetsrv iissync.exe	Apply to files listed
C:\WINNT\system32\os2	Apply to directory only not files and subdirectories
C:\WINNT\temp	Apply to directory only not files and subdirectories

Network Lockdown

Network Address Translation (NAT)

NAT is used to translate non-routable (internal) IP addresses to addresses that can be routed across the Internet. NAT is used for two reasons one to conserve Internet addresses and the other reason is for security purposes. NAT provides security by hiding the internal addresses from outside users (Benjamin 324). GIAC Enterprises is not currently using NAT for the corporate web server. The

web server address is a valid public address. It is suggested that the address be translated to add an additional layer of security. The firewall can be setup to statically map the external address to an internal one that is not known by outsiders.

Block Web Server Access

In most cases it is not a necessity for the web server to browse the Internet. Patches and virus updates can be downloaded on other workstations and then installed on the server. It is recommended that if you do not require Internet access you block it at your firewall. There are many viruses on the Internet that are spread though visiting a site with malicious content. In the event the server is compromised blocking external access guards against an attacker using the machine to attack other outside networks.

Ingress\Egress Filtering

Certain IP addresses should never be seen entering or leaving the network. Rules should be setup to block IP addresses. The network is comprised of one class C subnet of IP addresses. Only these addresses should be let out of the network. This will stop rogue device from exiting the network. Incoming traffic should never be sourced from non-routable IP addresses or address from the internal network. Examples of non-routable IP addresses are:

- 10.0.0.0
- 127.0.0.0
- 172.16.0.0
- 192.168.0.0

Internal Scan

The internal and external scans were performed using the Nessus auditing tool. Nessus will scan you network for known security weaknesses. It will report on any that it finds to be a risk. It places a value of either low, medium and high on the different issues. A section called *SCI Comment* has been added to some issues. It is to provide more information and to outline what issues are fixed by locking down the server as stated in the above audit documentation.

Type	Port	Issue and Fix
Vulnerability	www (80/tcp)	The remote Windows host has a ASN.1 library which is vulnerable to a flaw which could allow an attacker to execute arbitrary code on this host. To exploit this flaw, an attacker would need to send a specially crafted ASN.1 encoded packet with improperly advertised lengths. This particular check sent a malformed HTML authorization packet and determined that the remote host is not patched. Solution : http://www.microsoft.com/technet/security/bulletin/ms04-007.mspx SCI Comment: Install the patch that can be found at the above site. Risk factor : High CVE : CAN-2003-0818 BID : 9633, 9635, 9743 Other references : IAVA:2004-A-0001 Nessus ID : 12055
Warning	www (80/tcp)	The IIS server appears to have the .IDA ISAPI filter mapped. At least one remote vulnerability has been discovered for the .IDA (indexing service) filter. This is detailed in Microsoft Advisory MS01-033, and gives remote SYSTEM level access to the web server. It is recommended that even if you have patched this vulnerability that you unmap the .IDA extension, and any other unused ISAPI extensions if they are not required for the operation of your site. Solution: To unmap the .IDA extension: 1.Open Internet Services Manager. 2.Right-click the Web server choose Properties from the context menu. 3.Master Properties 4.Select WWW Service -> Edit -> HomeDirectory -> Configuration and remove the reference to .ida from the list. In addition, you may wish to download and install URLSCAN from the Microsoft Technet web site. URLSCAN, by default, blocks all .ida requests to the IIS server. SCI Comment: The need for URL SCAN and IIS lockdown tool has been discussed in the audit report. Risk factor : Medium CVE : CVE-2001-0500 BID : 2880 Nessus ID : 10695

Warning	www (80/tcp)	IIS 5 has support for the Internet Printing Protocol(IPP), which is enabled in a default install. The protocol is implemented in IIS5 as an ISAPI extension. At least one security problem (a buffer overflow) has been found with that extension in the past, so we recommend you disable it if you do not use this functionality. Solution: To unmap the .printer extension: 1.Open Internet Services Manager. 2.Right-click the Web server choose Properties from the context menu. 3.Master Properties 4.Select WWW Service -> Edit -> HomeDirectory -> Configuration and remove the reference to .printer from the list. SCI Comment: The need for URL SCAN and IIS lockdown tool has been discussed in the audit report. Installation of these tools will eliminate the warning. Reference : http://online.securityfocus.com/archive/1/181109 Risk factor : Low Nessus ID : 10661
Vulnerability	loc-srv (135/tcp)	The remote host is running a version of Windows which has a flaw in its RPC interface, which may allow an attacker to execute arbitrary code and gain SYSTEM privileges. An attacker or a worm could use it to gain the control of this host. Note that this is NOT the same bug as the one described in MS03-026 which fixes the flaw exploited by the 'MSBlast' (or LoveSan) worm. Solution: see http://www.microsoft.com/technet/security/bulletin/MS03-039.mspx SCI Comments: This firewall is currently blocking these ports from outside access. The IPSec policy would protect the server from internal attacks. Risk factor : High CVE : CAN-2003-0715, CAN-2003-0528, CAN-2003-0605 BID : 8458, 8460 Other references : IAVA:2003-A-0012 Nessus ID : 11835
Vulnerability	loc-srv (135/tcp)	The remote host is running a version of Windows which has a flaw in its RPC interface which may allow an attacker to execute arbitrary code and gain SYSTEM privileges. There is at least one Worm which is currently exploiting this vulnerability. Namely, the MsBlaster worm. Solution: see http://www.microsoft.com/technet/security/bulletin/MS03-026.mspx SCI Comments: This firewall is currently blocking these ports from outside access. The IPSec policy would protect the server from internal attacks. Risk factor : High CVE : CAN-2003-0352 BID : 8205 Other references : IAVA:2003-A-0011 Nessus ID : 11808

Vulnerability	microsoft-ds (445/tcp)	The remote Windows host has a ASN.1 library which is vulnerable to a flaw which could allow an attacker to execute arbitrary code on this host. To exploit this flaw, an attacker would need to send a specially crafted ASN.1 encoded packet with improperly advertised lengths. This particular check sent a malformed NTLM packet and determined that the remote host is not patched. Solution : http://www.microsoft.com/technet/security/bulletin/ms04-007.mspx SCI Comment: Install patch found at above site. Risk factor : High CVE : CAN-2003-0818 BID : 9633, 9635, 9743 Other references : IAVA:2004-A-0001 Nessus ID : 12054
Warning	microsoft-ds (445/tcp)	The host SID could be used to enumerate the names of the local users of this host. (we only enumerated users name whose ID is between 1000 and 1200 for performance reasons) This gives extra knowledge to an attacker, which is not a good thing : - Administrator account name : Administrator (id 500) - Guest account name : Guest (id 501) - TsInternetUser (id 1000) - IUSR_WEBSERVER (id 1001) - IWAM_WEBSERVER (id 1002) - jdrum (id 1003) - ajones (id 1004) - gmoney (id 1005) - jsmith (id 1006) - drucker (id 1007) SCI Comment: Once the IPSec policy has been created and installed on the server this port will be block. The enhanced security settings will not allow enumeration. Risk factor : Medium Solution : filter incoming connections this port CVE : CVE-2000-1200 BID : 959 Nessus ID : 10860
Warning	microsoft-ds (445/tcp)	The following local accounts have passwords which never expire : Administrator Guest TsInternetUser IUSR_WEBSERVER IWAM_WEBSERVER SCI Comment: This issue has been addressed on the audit. Password should have a limited lifetime Solution : disable password non-expiry Risk factor : Medium Nessus ID : 10916

Vulnerability	unknown (7436/tcp)	The remote Windows host has a ASN.1 library which is vulnerable to a flaw which could allow an attacker to execute arbitrary code on this host. To exploit this flaw, an attacker would need to send a specially crafted ASN.1 encoded packet with improperly advertised lengths. This particular check sent a malformed HTML authorization packet and determined that the remote host is not patched. Solution : http://www.microsoft.com/technet/security/bulletin/ms04-007.mspx Risk factor : High CVE : CAN-2003-0818 BID : 9633, 9635, 9743 Other references : IAVA:2004-A-0001 Nessus ID : 12055
Vulnerability	loc-srv (135/udp)	A security vulnerability exists in the Messenger Service that could allow arbitrary code execution on an affected system. An attacker who successfully exploited this vulnerability could be able to run code with Local System privileges on an affected system, or could cause the Messenger Service to fail. Disabling the Messenger Service will prevent the possibility of attack. This plugin actually checked for the presence of this flaw. Solution : see http://www.microsoft.com/technet/security/bulletin/ms03-043.mspx SCI Comment: This vulnerability only exist on machines that run NetBIOS while it is a good idea to install this patch NetBIOS should be disabled on the server. This vulnerability did not appear during an external audit because you firewall is blocking the ports that NetBIOS uses. Risk factor : High CVE : CAN-2003-0717 BID : 8826 Other references : IAVA:2003-A-0028 Nessus ID : 11890

External Scan

Type	Port	Issue and Fix
Warning	www (80/tcp)	The IIS server appears to have the .IDA ISAPI filter mapped. At least one remote vulnerability has been discovered for the .IDA (indexing service) filter. This is detailed in Microsoft Advisory MS01-033, and gives remote SYSTEM level access to the web server. It is recommended that even if you have patched this vulnerability that you unmap the .IDA extension, and any other unused ISAPI extensions if they are not required for the operation of your site. Solution: To unmap the .IDA extension: 1.Open Internet Services Manager. 2.Right-click the Web server choose Properties from the context menu. 3.Master Properties 4.Select WWW Service -> Edit -> HomeDirectory -> Configuration and remove the reference to .ida from the list. In addition, you may wish to download and install URLSCAN from the Microsoft Technet web site. URLSCAN, by default, blocks all .ida requests to the IIS server. Risk factor : Medium CVE : CVE-2001-0500 BID : 2880 Nessus ID : 10695
Warning	www (80/tcp)	The remote server is running with WebDAV enabled. WebDAV is an industry standard extension to the HTTP specification. It adds a capability for authorized users to remotely add and manage the content of a web server. If you do not use this extension, you should disable it. Solution : See http://support.microsoft.com/default.aspx?kbid=241520 Risk factor : Medium Nessus ID : 11424
Warning	www (80/tcp)	IIS 5 has support for the Internet Printing Protocol(IPP), which is enabled in a default install. The protocol is implemented in IIS5 as an ISAPI extension. At least one security problem (a buffer overflow) has been found with that extension in the past, so we recommend you disable it if you do not use this functionality. Solution: To unmap the .printer extension: 1.Open Internet Services Manager. 2.Right-click the Web server choose Properties from the context menu. 3.Master Properties 4.Select WWW Service -> Edit -> HomeDirectory -> Configuration and remove the reference to .printer from the list. Reference : http://online.securityfocus.com/archive/1/181109 Risk factor : Low Nessus ID : 10661

Conclusion

GIAC Enterprises current environment demonstrates that the System Administrators are performing tasks to safe guard the corporation's web server. The audit report reviews additional changes that can be made to further secure the network. It is important to remember that security is an ongoing process. Any features that are added to the environment should be researched and locked down. The web server environment needs to be analyzed on a regular basis to ensure it stays secure. SCI will be available to assist GIAC Enterprises with any future security needs.

Resources

Beale, Jay, HD Moore, and Noam Rathaus. Nessus Network Auditing. Rockland:
Syngress, 2004.

Benjamin, Henry. CCIE Security Exam Certification Guide. Indianapolis: Cisco Press,
2003.

Cox, Philip, and Tom Sheldon. Windows 2000 Security Handbook. Berkeley:
Mcgraw Hill, 2001.

Haney, J. Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set. Ft. Meade: National Security Agency, 2003.

Hipson, Peter. Mastering Windows 2000 Registry. Alameda: Sybex, 2000.

Lockhart, Andrew. Network Security Hacks. Sebastopol: O'Reilly, 2004.

Microsoft Corporation. Improving Web Application Security. June 2003
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/THCMCh16.asp

Minasi, Mark. Mastering Windows 2000 Server. Alameda: Sybex, 2000.

SANS Institute. Building a Consulting Practice. SANS: 2004.

SANS Institute. Delivering Results: Project Management & Soft Skills. SANS: 2004.

SANS Institute. Consulting with People and Organizations. SANS: 2004.

SANS Institute. Delivering Results: The Technical Skills. SANS: 2004.

Walker, William. Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0. Ft. Meade: National Security Agency, 2002.