



# Global Information Assurance Certification Paper

Copyright SANS Institute  
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering  
"Auditing Systems, Applications, and the Cloud (Audit 507)"  
at <http://www.giac.org/registration/gсна>

# **Web Server Security Assessment**

## **an Independent Auditor's Perspective**

**GSNA Practical Assignment, v2.1**  
**By Derek Cheng**  
**November 9, 2003**

## Table of Contents

<b>Abstract.....</b>	<b>3</b>
<b>Assignment 1 – Research in Audit, Measurement Practice and Control .....</b>	<b>4</b>
Identify the System to Be Audited .....	4
Diagram 1: Basic Network Architecture .....	4
Evaluate the Risk to the System .....	5
Table 1: External Threat Analysis.....	6
What is the Current State of Practice? .....	7
<b>Assignment 2 – Create an Audit Checklist .....</b>	<b>9</b>
Planning and Administration.....	9
Security Operations Review .....	11
Vulnerability Testing.....	14
<b>Assignment 3 – Audit Evidence .....</b>	<b>19</b>
Security Operations Review .....	19
Audit Checklist #6 - Access Controls.....	19
Audit Checklist #7 - Patch Management Controls .....	19
Audit Checklist #8 - Security Logging Controls .....	20
Audit Checklist #9 - Security Monitoring Controls .....	20
Audit Checklist #10 - Incident Response Controls .....	20
Vulnerability Testing .....	21
Audit Checklist #12 - Audit of Password Policy .....	21
Audit Checklist #14 - Server Identification Verification, using Netcat .....	24
Audit Checklist #15 - Port Scanning, using Nmap .....	25
Audit Checklist #16 - Web and CGI Vulnerability Scanning, using Nikto .....	26
Audit Checklist #17 - Vulnerability Scanning, using Nessus.....	30
Measure Residual Risk .....	38
Is the System Audible?.....	38
<b>Assignment 4 – Audit Report .....</b>	<b>39</b>
Executive Summary .....	39
1.0 High Risk Findings .....	40
2.0 Medium Risk Findings .....	44
3.0 Low Risk Findings .....	44
References.....	46

## **Abstract**

The purpose of this practical is to demonstrate how to audit a web server by performing both a review of security operational procedures and an assessment of security vulnerabilities of a web server. This practical consists of four main phases which include researching, developing a formal and repeatable audit checklist, conducting the audit against live web servers, and developing a report targeted for management.

The audit checklist was developed by leveraging personal security experience, existing audit checklists, and freeware and open source security tools.

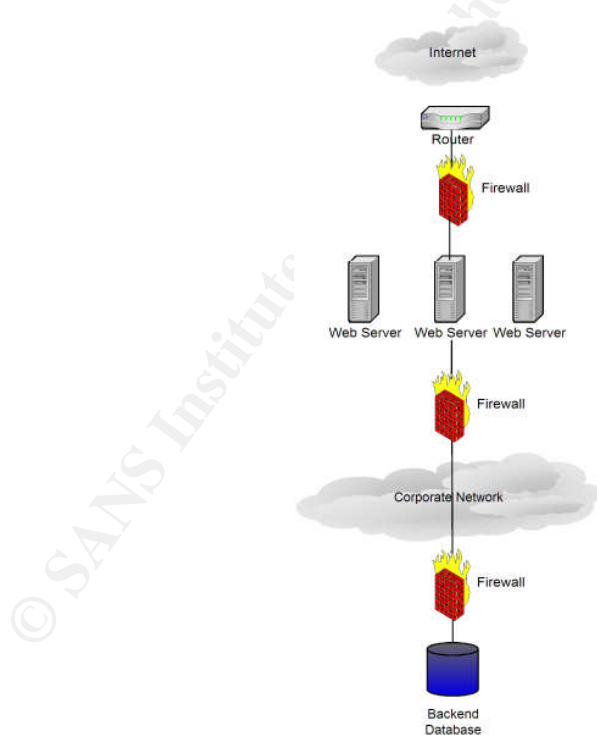
© SANS Institute 2004, Author retains full rights.

# Assignment 1 – Research in Audit, Measurement Practice and Control

## Identify the System to Be Audited

The client that I am auditing is a mid-size financial institution based in California. To protect the identity of the client, I will refer to them using the fictitious name “Acme” throughout this practical. At Acme’s request, I am auditing three business critical web servers are running critical applications such as their corporate website, business partner application, and Outlook Web Access (OWA) mail. These web servers are located in Acme’s demilitarized zone (DMZ) between two firewalls. There is also a border router in front of the external firewall to help offset some traffic from the external firewall to help protect against denial of service (DoS) attacks, mutated packets and unused ports (see Diagram 1: Basic Network Architecture)

**Diagram 1: Basic Network Architecture**



Acme has a heterogeneous operating system environment consisting of Windows NT, Windows 2000, Solaris 2.6 – 2.8. For network devices such as firewalls, routers, and switches, Acme is primarily using Cisco devices. Acme is also using Snort for intrusion detection and has both a network operations center

(NOC) monitoring traffic on a 24x7x365 basis and a computer incident response team (CIRT) to handle and investigate suspicious activity.

Acme's OWA server is running on a Windows 2000 server SP3 with IIS 5.0. This application provides email access to remote users. The business partner application is running on Sun Solaris with Netscape-Enterprise/3.5.1C. Business partners log into this system and enter and query customer information such as social security numbers, addresses, and financial information. The Acme corporate website is running on Sun Solaris with Netscape-Enterprise/3.5.1C. This website is primarily an informational website that has information about the Acme's services and products. Acme relies heavily on their corporate website for marketing purposes to promote their products and services.

A secure configuration of these systems will prevent unauthorized access to confidential data and will help protect against known security vulnerabilities such as buffer overflow attacks and misconfigurations of operating systems and web applications.

## **Evaluate the Risk to the System**

These web servers are hosting applications that are accessible by anyone on the Internet. Because external firewalls typically allow HTTP/HTTPS traffic through in order to communicate to web servers, web based attacks have become very ubiquitous. This creates extremely high risk and exposure for any company that relies on web applications to conduct business. The security threat also remains constant because thousands of users are on these web servers at any given time.

Since new vulnerabilities are discovered on a daily basis, there is no guarantee in security. What may appear to be secure today may be completely insecure tomorrow. It is important that companies make security a priority and continue to stay current with security patches and update policies and procedures as necessary. The overall security objective for these systems is to ensure that the operating system and application are configured securely and have up-to-date patches to protect against known security vulnerabilities.

Each of the three systems have different types of risks associated with them. Leveraging information from Acme's business continuity plan (BCP), Acme feels that these servers contain their most critical and high risk applications. The OWA server stores much of Acme's electronic mail, many of which contain information related to their business and clients. If this server were compromised, a malicious user would have access to Acme's corporate emails, and potentially sensitive and confidential information. This information could be used for social engineering, identity theft, and other concerted attacks against Acme.

If the Acme corporate website was defaced, Acme's business reputation may be jeopardized and Acme may lose confidence and trust with their customers and business partners. Acme may also suffer financial losses associated with lost ad revenue and negative publicity.

If the business partner application was compromised, a malicious user could potentially access the backend database that stores sensitive and confidential customer information such as client contact information, social security numbers, credit scores, and other personal financial information.

In addition, Acme may need to formally notify California residents if there is any breach of their personal information. This recent California Bill SB 1386 requires that "a state agency, or a person or business that conducts business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the data, as defined, to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The bill would permit the notifications required by its provisions to be delayed if a law enforcement agency determines that it would impede a criminal investigation. The bill would require an agency, person, or business that maintains computerized data that includes personal information owned by another to notify the owner or licensee of the information of any breach of security of the data, as specified." <sup>1</sup>

Working with Acme personnel, I developed the following table (Table 1: External Threat Analysis) which analyzes and identifies the various types of external threats that Acme could face and the motivation and likelihood of attack.

**Table 1: External Threat Analysis**

Identification	Description	Motivation/ Likelihood	Comments
Hackers	Individuals outside of the electronic perimeter that may attempt to penetrate and exploit the Acme network systems looking for computing resources, information, or financial gain.	Medium / Medium	Acme is a high profile financial institution that can be found easily on the Internet. Adequate perimeter defenses and escalation procedures help to mitigate this risk.
Malicious Code	Computer virus or program designed to disrupt computer operations.	Medium / High	Users have the ability to download files and executables from the Internet and to receive viruses via e-mail. Also, media may be brought in from an outside source that is infected.

<sup>1</sup> BILL NUMBER: SB 1386, [http://info.sen.ca.gov/pub/01-02/bill/sen/sb\\_1351-1400/sb\\_1386\\_bill\\_20020926\\_chaptered.html](http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html)

Competition	Other financial institutions in the same arena in search of valuable customer information or industry secrets.	High / High	Acme is one of the largest financial institutions in the world and could be a valuable information resource for competitors.
Former Employee(s)	Associates that may have had trouble within the corporation, or who may have recently left because of an internal conflict.	High / Medium	A current or former employee may have an immediate and lasting impact as a result of current or former access to critical systems and data. The impact is mitigated by the type and extent of access by the employee, as well as sound account maintenance.
Vendor Personnel/ Contractors	Vendors and contractors may provide system maintenance and/or be involved with administration. In some cases, services may be conducted remotely through dial-up or direct connect into the corporate network.	Medium / Medium	Vendor personnel and contractors typically have privileged access to systems and may inadvertently cause a disruption of service if not properly monitored. Specific guidelines and restrictions help to mitigate the opportunity for this type of event.

## What is the Current State of Practice?

I used the Google search engine <http://www.google.com> as the basis to look for audit related information for web servers. In addition, I searched the following audit checklist repositories and informational security websites:

- AuditNet (<http://www.auditnet.org>)
- Center for Internet Security (<http://www.cisecurity.org/index.html>)
- ISACA – Information Systems Audit and Control Association (<http://www.isaca.org>)
- OSSTMM - Open Source Security Testing Methodology Manual (<http://www.ideahamster.org/projects/osstmm.htm>)
- SANS Reading Room (<http://rr.sans.org>)
- SANS Posted Practicals for GIAC certifications (<http://www.giac.org/cert.php>)
- SANS Security Policy Project (<http://www.sans.org/resources/policies>)

I found that there are a number of resources that exist to audit web servers both from a security operational perspective and a vulnerability assessment perspective. However, during my research, I was unable to find a single resource which combines both into one audit.

For technical and configuration checks, I relied mostly on the security benchmarks developed by the Center for Internet Security and the Open Source Security Testing Methodology Manual. I felt that the combination of these two resources provided a strong methodology to both securely configure systems as well periodically audit them for security vulnerabilities.



In terms of processes or procedures that may affect the security of the system such as access control and patch management, I tailored many audit checklists from AuditNet. However, I did not find any checklists that I could simply use without heavy customization. For instance, I did not find any checklists or procedures for security patch management, so I customized a change management checklist to meet the needs of my security audit.

© SANS Institute 2004, Author retains full rights.

## Assignment 2 – Create an Audit Checklist

Acme has requested a security audit of the three of their business critical web servers. These servers are located in a DMZ between two firewalls and are physically located in a data center with limited access.

The following 20 step audit checklist is separated into three separate categories (1) Planning and Administration, (2) Security Operations Review, and (3) Vulnerability Testing. Planning and Administration and the Security Operations Review were conducted with key Acme IT personnel such as the Director of Security, Network Engineers, and System Administrators. Due to the sensitivity and potential impact of testing, Vulnerability Testing was conducted during off-peak business hours at the request of Acme.

The purpose of this audit is to identify known security configuration weaknesses and vulnerabilities with the identified web servers. In addition, the audit will review critical security operational procedures that should be in place to support security efforts and help protect the confidentiality, integrity, and availability of systems.

#	Ref.	Control Objective	Testing / Compliance	Risk	Obj/ Sub
<b>Planning and Administration</b>					
1.	Personal experience	Determine the scope of the vulnerability assessment project and identify the critical web servers that will be audited.	<p>Interview key personnel and review pertinent documents to gain a detailed understanding of the business objectives, risks to meeting those objectives, and controls that mitigate the risk.</p> <p>Business objectives and critical systems should be clearly defined and adequately documented.</p>	Understanding the client's business objectives, associated risks, and security controls is an integral component of the audit and will directly affect the results of the audit. Without clearly defining the scope of the project, it is possible the project may not be completed on time or that expectations are not fully met.	Sub

2.	Personal experience	Web server information such as application name (e.g. IIS, Apache, etc.), application version, IP address, domain name, related network diagrams, open ports, etc. should be documented.	<p>Conduct interview with key personnel to gather all relevant information about the web servers. Documentation should be provided whenever possible.</p> <p>Web server documentation such a network diagrams, open port information, IP addresses should be documented and up-to-date.</p>	Without validating that the IP addresses of the web servers that are being audited, it is possible that the vulnerability tests may inadvertently affect servers that are out of scope or belong to another organization.	Obj
3.	<p>SANS Security Policy Project, <a href="http://www.sans.org/resources/policies/">http://www.sans.org/resources/policies/</a>.</p> <p>Guel, Michele D., "A Short Primer for Developing Security Policies", <a href="http://www.sans.org/resources/policies/Policy_Primer.pdf">http://www.sans.org/resources/policies/Policy_Primer.pdf</a>, 2001.</p>	Security policies and procedures related to the systems being audited should be in place.	<p>Conduct interviews with the client to gather related policies and procedures.</p> <p>Identify that information security policies exist. For a list of commonly used security policies, please visit <a href="http://www.sans.org/resources/policies/">http://www.sans.org/resources/policies/</a>.</p> <p>Review the policies and verify that they are:</p> <ul style="list-style-type: none"> <li>• Implementable and enforceable</li> <li>• Concise and easy to understand</li> <li>• Balance protect with productivity</li> </ul> <p>The policies should also:</p> <ul style="list-style-type: none"> <li>• State reasons why the policy is needed</li> <li>• Describe what is covered by the policy</li> <li>• Define contacts and responsibilities</li> <li>• Discuss how violations will be handled<sup>2</sup></li> </ul>	Information security policies and procedures provide guidance to employees on how to protect the company's valuable information and technology resources and are a fundamental component of any information security program.	Sub

<sup>2</sup> Guel, Michele D., "A Short Primer for Developing Security Policies", [http://www.sans.org/resources/policies/Policy\\_Primer.pdf](http://www.sans.org/resources/policies/Policy_Primer.pdf), 2001.

4.	Personal experience	Time and date to perform network vulnerability testing should be determined and properly coordinated.	<p>Work with key personnel to coordinate time and date to perform network vulnerability testing that would be the least impact and interruption to business operations.</p> <p>An email should be used to validate the time and date of testing.</p>	<p>The client's web servers can be extremely sensitive depending of the type of business. Typically network vulnerability testing should be done at off-peak hours such as nights and weekends.</p> <p>An email should be kept a record of the approved time and date of the testing.</p>	Sub
5.	Personal experience	Other affected parties such as the incident response team, NOC, web server administrators, etc should be notified prior to testing.	<p>Provide advanced notice to affected parties such as the client's incident response team, system administrators, NOC, and intrusion detection analysts.</p> <p>Emails should be sent by the client's security contact to notify the appropriate parties of the testing.</p>	<p>Without providing advanced notice about the scheduled vulnerability tests, IT personnel may not be aware of the testing. Ample time may not be given in order to take the necessary precautions and safety measures.</p> <p>The emails should be kept a record in case any problems with the client's security teams arise.</p>	Sub
<b>Security Operations Review</b>					
6.	<p>Warigon, Slemo. "Access Control Audit Program", <a href="http://www.audit.net.org/docs/access.txt">http://www.audit.net.org/docs/access.txt</a>, Mar 9, 1995.</p> <p>Sikac, John. "Access Security Checklist", <a href="http://www.audit.net.org/docs/AccessSecurityChecklist.doc">http://www.audit.net.org/docs/AccessSecurityChecklist.doc</a>, Oct. 16, 2001.</p>	Policies and procedures should be in place to reasonably control and manage logical access to the systems	<p>Verify that an access control policy exists and includes the following:</p> <ul style="list-style-type: none"> <li>• Defines who is responsible for access control and account provisioning (e.g. new users, terminations, changes)</li> <li>• Defines how account provisioning is performed.</li> <li>• Requires that users are given minimum access level needed to do their job.</li> <li>• Requires that accounts are periodically audited for validity.</li> </ul>	Without a formal access control procedure, user accounts may not added, changed, or deleted in a timely manner. Outdated user accounts may be left active on the system indefinitely and can be used by unauthorized persons to access potentially sensitive and confidential information.	Sub

	Personal experience				
7.	Sutton, Virginia. "Change Management Audit Program", <a href="http://www.audit.net.org/docs/chn_gmgt.txt">http://www.audit.net.org/docs/chn_gmgt.txt</a> , Oct. 10, 1999.	Policies and procedures should be in place to timely monitor, test, and deploy security patches	<p>Verify that a patch management procedure exists and includes the following:</p> <ul style="list-style-type: none"> <li>• Defines who is responsible for patch management</li> <li>• Defines how patch availability is monitored and new patches are reviewed</li> <li>• Requires that patches are reviewed for criticality</li> <li>• Requires that an estimated time to completion is communicated</li> <li>• Defines how to coordinate and execute testing and deployment of patches, usually through the change management procedure</li> <li>• Requires that documentation is kept for patch management</li> <li>• Requires systems be polled on a regular basis to ensure that they have the latest patches applied to them.</li> </ul>	Without a formally documented patch management policy and procedure, critical security patches may not be applied in a timely manner, leaving systems vulnerable to known weaknesses that can lead to system compromise or loss of confidential information.	Sub
8.	Personal experience	Policies and procedures should be in place log suspicious activity for analysis.	<p>Verify that a logging policy and procedure exists and includes the following:</p> <ul style="list-style-type: none"> <li>• Requires that logging is enabled</li> <li>• Defines how logging is protected from unauthorized access</li> <li>• Defines how logging is stored and archived securely</li> </ul>	<p>Log files help keep track of activity occurring on systems at all times and can often provide early warning of an impending attack. Logs are also crucial when forensic investigations are occurring. Without logging, it may be difficult to detect potential intruders.</p> <p>Logs contain confidential information about the company's systems and should be adequately protected from authorized access.</p>	Sub

9.	Personal experience	Policies and procedures should be in place to monitor and detect suspicious activity.	<p>Verify that a monitoring policy and procedure exists and includes the following:</p> <ul style="list-style-type: none"> <li>• Defines who is responsible for monitoring</li> <li>• Defines how monitoring is performed</li> <li>• Requires that monitoring is performed on a 24x7x365 basis.</li> <li>• Requires that a mechanism is in place such as an intrusion detection system (IDS) or automated scripts to analyze the logs and send alerts of any suspicious activity</li> </ul>	Without formal server monitoring procedures in place, it is difficult to maintain consistent monitoring of the IT environment. It is also more likely that important security alerts are overlooked or misinterpreted.	Sub
10.	SANS: Computer Security Incident Handling: Step-by-Step	Policies and procedures should be in place to respond to and properly handle security incidents.	<p>Verify that an incident handling procedure exists and includes the following steps:</p> <ul style="list-style-type: none"> <li>• Identify the incident and assess the situation</li> <li>• Contact appropriate parties including management, incident response team, public relations, legal department and law enforcement authorities as appropriate</li> <li>• Contain the incident to avoid further damage</li> <li>• Maintain evidence by backing up the compromised system and maintaining other records</li> <li>• Eradicate the problem by removing the cause of the incident</li> <li>• Recover the incident by bringing systems and services back online</li> <li>• Analyze the incident to discover root causes and implement appropriate measures to protect against future similar incidents</li> <li>• Document the incident in a formal incident report</li> </ul>	<p>Without a formal security incident response plan in place to guide in the effective and efficient response to security incidents, disruptions to business operations can be prolonged and can possibly reoccur.</p> <p>Having a security incident response procedure in place can help reduce and limit the negative impact of a security incident, and can assist the organization in prosecuting the perpetrators of attacks. Because computer security incidents are on the rise, it is important to be prepared to respond to them efficiently and effectively in the event preventative security measures are circumvented. In addition, recent world events have underscored the need for effective incident response procedures.</p>	Sub

11.	Personal experience	Policies and procedures should be in place for reallocation or decommissioning of servers.	<p>Verify that a reallocation or decommissioning policy and procedure exists and includes the following:</p> <ul style="list-style-type: none"> <li>• Defines who is responsible for reallocation or decommissioning of servers</li> <li>• Criteria that defines what systems can be reallocated</li> <li>• Process to securely delete data from the servers or properly dispose of the hardware.</li> </ul>	Servers typically contain confidential and sensitive data and should be carefully handled. If information is not securely deleted or disposed of, an unauthorized individual may have access to the data.	Sub
<b>Vulnerability Testing</b>					
12.	Personal experience	The password policy on the Microsoft OWA server should be align with Acme's password policy.	<p>DumpSec</p> <ul style="list-style-type: none"> <li>• Download DumpSec from <a href="http://www.somarsoft.com/">http://www.somarsoft.com/</a> and install the program. This tool requires an established connection to the Windows server, so coordinate with the client's system administrator.</li> <li>• After the connection to the server is established, start DumpSec</li> <li>• Click "Report" → "Select Computer"</li> <li>• When prompted, enter the IP address of the computer being audited</li> <li>• Click "Report" → "Dump Policies"</li> </ul> <p>Note: DumpSec can also provide other useful information such as users, groups, and shares.</p>	If the password policy on the server does not meet or exceed the company's password policy, user accounts may have weak or easily guessed passwords.	Obj

13.	<p>SANS class, "Auditing Networks, Perimeters, and Systems Hands-On Workbook", 2003.</p> <p>Personal experience</p>	<p>Windows operating system should be configured securely and up to current patch levels.</p>	<p>Microsoft Security Baseline Analyzer (MSBA)</p> <ul style="list-style-type: none"> <li>Download MSBA from <a href="http://download.microsoft.com/download/8/e/e/8ee73487-4d36-4f7f-92f2-2bdc5c5385b3/mbsasetup.msi">http://download.microsoft.com/download/8/e/e/8ee73487-4d36-4f7f-92f2-2bdc5c5385b3/mbsasetup.msi</a> and install the program.</li> <li>This tool requires administrator access to the server, so coordinate with the client's system administrator.</li> <li>Start MSBA</li> <li>Click "Scan a computer"</li> <li>Enter the IP address or the hostname of the computer</li> <li>Click "Start scan"</li> </ul>	<p>Older versions of operating systems that have not been patched or are not configured properly are known to have a number of security vulnerabilities that can result in system compromise and denial of service attacks. If a malicious attacker exploits the vulnerabilities associated with misconfigurations and older hotfixes and services packs, the attacker may have complete control over a system, access to sensitive and confidential information, and potentially impact the availability of the system.</p>	Obj
14.	<p>Scambray, Joel. Shema, Mike, <u>Hacking Web Applications Exposed</u>, McGraw-Hill, New York, 2002.</p> <p>Personal experience</p>	<p>Server information such application name and version should correspond to information provided in step 2.</p>	<p>Netcat</p> <ul style="list-style-type: none"> <li>Download netcat from <a href="http://www.atstake.com/research/tools/network_utilities/">http://www.atstake.com/research/tools/network_utilities/</a>.</li> <li>In Windows, open a DOS prompt and change to the directory where netcat is installed.</li> <li>To grab the banner for a web server, type in the following: <ul style="list-style-type: none"> <li>nc -vv &lt;IP address&gt; 80 //this will connect to the web server at port 80 in verbose mode</li> <li>type in: HEAD / HTTP1.0</li> <li>[Hit the carriage return twice]</li> </ul> </li> </ul>	<p>If the web application type and version do not correspond with the information provided by the client, it is possible that the server is incorrect, the banner was altered, or the application has been changed without the client knowing.</p>	Obj



15.	<p>Scambray, Joel. Shema, Mike, <u>Hacking Web Applications Exposed</u>, McGraw-Hill, New York, 2002.</p> <p>Personal experience</p>	<p>Verify that only the necessary ports are listening on the target web servers.</p>	<p>Nmap</p> <ul style="list-style-type: none"> <li>• Download Nmap from <a href="http://www.insecure.org/nmap/">http://www.insecure.org/nmap/</a></li> <li>• In Windows, open a DOS prompt and change to the directory where nmap is installed.</li> <li>• To scan for open ports on the web server, type in the following: <ul style="list-style-type: none"> <li>◦ <code>nmap -sS -P0 -O -v -oN &lt;text file&gt; &lt;IP address&gt;</code> //this will perform a SYN scan, check for commonly used ports, scan even if ping (ICMP) is not enabled, attempt to identify the operating system of the web server, scan in verbose mode, and output the results to a text file.</li> </ul> </li> </ul>	<p>Unnecessary ports should never be open because it provides a malicious attacker additional opportunities to penetrate into the system and gain access to unauthorized data.</p>	Obj
16.	<p>Scambray, Joel. Shema, Mike, <u>Hacking Web Applications Exposed</u>, McGraw-Hill, New York, 2002.</p> <p>Personal experience</p>	<p>Test for web and CGI related vulnerabilities</p>	<p>Nikto</p> <ul style="list-style-type: none"> <li>• Download Nikto from <a href="http://www.cirt.net/code/nikto.shtml">http://www.cirt.net/code/nikto.shtml</a>.</li> <li>• In Windows, open a DOS prompt and change to the directory where Nikto is installed.</li> <li>• Type in the following: <ul style="list-style-type: none"> <li>◦ <code>nikto.pl -update</code> //this will download the latest Nikto vulnerability checks</li> <li>◦ <code>nikto.pl -allcgi -verbose -host &lt;IP address&gt; -output &lt;IP address&gt;.txt</code>  // this will scan the web server for all CGI vulnerabilities, in verbose mode, and will output the results to a text file.</li> </ul> </li> </ul>	<p>Vulnerabilities found on a web server may result in a number of leakage of information, unauthorized access to confidential and sensitive information, or unavailability of the server.</p>	Obj

17.	<p>SANS class, “Auditing Networks, Perimeters, and Systems Hands-On Workbook”, 2003.</p> <p>Personal experience</p>	<p>Test for operation system and configuration related vulnerabilities.</p>	<p>Nessus</p> <ul style="list-style-type: none"> <li>• Download Nessus from <a href="http://www.nessus.org">http://www.nessus.org</a></li> <li>• In Unix, open a terminal window</li> <li>• Type in the following: <ul style="list-style-type: none"> <li>○ <code>nessus-update-plugins</code> //automatically download the latest scripts</li> <li>○ <code>nessusD -D</code> //start the Nessus daemon</li> </ul> </li> <li>• Open a 2nd terminal window</li> <li>• Type in the following: <ul style="list-style-type: none"> <li>○ <code>nessus</code> // starts the Nessus application</li> </ul> </li> <li>• After you log into the Nessus application, click the “Plug-ins” tab.</li> <li>• Click “Enable all but dangerous plug-ins”. Dangerous plug-ins include denial of service attacks which could potentially take down or cause instability to the server.</li> <li>• For each web server that is being audited, configure the plug-ins so that they reflect your knowledge of the server. For instance, for an IIS server, enable all of the IIS plug-ins and disable the Apache plug-ins. If you know that FTP is not running, disable the FTP plug-ins, etc.</li> <li>• Click the “Scan options” tab</li> <li>• For the web server being audited, enter the ports that are open from the results of your Nmap scan (common delimited). There is no need to re-perform another entire port scan using Nessus.</li> <li>• Click the “Target selection” tab.</li> <li>• Enter the IP address of the web server(s) being audited (common delimited)</li> <li>• Click “Start the scan”</li> </ul>	<p>Vulnerabilities found on a web server may result in a number of leakage of information, unauthorized access to confidential and sensitive information, or unavailability of the server.</p>	<p>Obj</p>
-----	---	---	---	--	------------

18.	Personal experience	Analyze and correlate scan results	<p>Using the results from the scanners, perform a risk analysis on the potential vulnerabilities. Risk ratings should consider a number of factors such as the potential impact to the organization and likelihood of occurrence.</p> <p>Compare the results with the information that was provided by the client to verify if they appear accurate.</p>	Because security auditing tools and vulnerability scanners are known to generate false positives and insignificant information, it is important to carefully analyze the results for validity and accuracy.	Sub
19.	<p>Scambray, Joel. Shema, Mike, <u>Hacking Web Applications Exposed</u>, McGraw-Hill, New York, 2002.</p> <p>Personal experience</p>	Perform manual and non-intrusive tests to verify results	<p>Based on the results from the scanners, some simple manual verification tests can be performed using basics tools such a web browser, telnet, FTP, or netcat. For results related to exposed files and directories, verify them using a web browser by entering the IP address and the directory or file that is exposed in the address field. For instance, enter http://&lt;IP address&gt;/manual in the address field.</p> <p>For results related to open ports on the system, you can use telnet or netcat to connect to the IP address and port.</p> <p>For telnet, enter the following:</p> <ul style="list-style-type: none"> <li>• telnet &lt;IP address&gt; &lt;port number&gt;</li> </ul> <p>For netcat, enter the following:</p> <ul style="list-style-type: none"> <li>• netcat -v &lt;IP address&gt; &lt;port number&gt;</li> </ul> <p>You may also choose to meet with the client's system administrators and network engineers to review and verify the results.</p>	Because security auditing tools and vulnerability scanners are known to generate false positives and insignificant information, it is important to validate as many results as possible.	Obj
20.	Personal experience	Run appropriate exploits in a controlled environment to verify vulnerabilities.	With the client's written authorization, appropriate exploits such as buffer overflow appropriate exploits can be run from a controlled lab environment against the servers to verify if they are actually vulnerable.	Exploits have not been thoroughly tested and may cause instability to a system.	Obj

## Assignment 3 – Audit Evidence

The following 10 tests are the areas that I feel represent the most significant security concerns and support the findings in the audit report.

### Security Operations Review

The security operations review involved examining existing manual and automated procedures within Acme for adequate security administration activities and to verify that security operations are being conducted in accordance with stated policies and procedures.

The administrative controls established to support the network perimeter are a critical component to understanding the policies, procedures, and standards in place.

Audit Checklist #6 - Access Controls	FAIL
<b>Objective: Policies and procedures should be in place to reasonably control and manage logical access to the system.</b>	

Acme IT personnel provided a policy and procedure for user account provisioning and management. The process requires that a manager of the new or terminated user to submit a form through a web-based ticketing system. This process is used for all user accounts, including privileged level accounts such as administrator or root level access. Human Resources sends our weekly notifications of terminated employees to all managers and system administrators to delete accounts. In addition, accounts are periodically audited to verify the validity and appropriate allocation of rights. To test this control, I selected a judgmental sample of 5 system administrators and identified one user who did not have a documented ticket for his administrative access to the systems.

Audit Checklist #7 - Patch Management Controls	FAIL
<b>Objective: Policies and procedures should be in place to timely monitor, test, and deploy security patches .</b>	

Acme does not have a formal patch management procedure in place. The current informal process is to monitor several security advisories including CERT and SecurityFocus and deploy the patches if applicable to the Acme IT infrastructure.

Acme does not have a process to test the patches before deployment. From the results of my Nikto and Nessus scans, I found that several servers and applications are not running the latest version of patches.

<b>Audit Checklist #8 - Security Logging Controls</b>	<b>PASS</b>
---	-------------

**Objective: Policies and procedures should be in place log suspicious activity for analysis.**

Acme IT personnel provided a security logging policy and procedure which requires that security event logging is enabled for all network devices and servers. Logs are sent to a syslog server where Swatch is used monitor and alert the appropriate individuals via email of suspicious activity. After the vulnerability testing was performed, I verified that logs were captured of my port scans and vulnerability scans during the timeframe of the test. In addition, I had an administrator perform failed login attempts against the systems and verified that he was emailed a notice of these unsuccessful attempts.

<b>Audit Checklist #9 - Security Monitoring Controls</b>	<b>PASS</b>
--	-------------

**Objective: Policies and procedures should be in place to monitor and detect suspicious activity.**

Acme IT personnel provided a security monitoring policy and procedure which details the steps used to monitor the network and critical servers. Acme has a network operations center (NOC) that has staff monitoring the network and critical servers on a 24x7x365 basis. The procedure also references the Incident Response procedure (see Audit Checklist #10) in the event that an incident occurs.

Acme is currently using Cisco IDS for intrusion detection which is used to alert appropriate individuals of suspicious activity on the network. After the vulnerability testing was performed, I verified that alerts were generated (both email and pager alerts) of my port scans and vulnerability scans during the timeframe of my test.

<b>Audit Checklist #10 - Incident Response Controls</b>	<b>PASS</b>
---	-------------

**Objective: Policies and procedures should be in place to respond to and properly handle security incidents.**

Acme IT personnel provided an incident response policy and procedure. I reviewed this document and verified that it included all of the criteria that I was testing for in an incident response policy and procedure. The Acme incident response

team comprised of key IT personnel, HR, legal, and executive management. I also sampled 5 of the most recent security incidents and verified that they were adequately handled and documented in a report.

## Vulnerability Testing

Vulnerability testing was conducted in order to identify issues that may be exploitable from an external perspective. I performed vulnerability testing in an established controlled environment to test the identified critical web servers using known vulnerability tools and techniques. These measures were fully coordinated with the key Acme personnel and announced to other internal systems staff prior to the initiation of any testing. Due to the sensitivity of the systems, Acme requested that exploits were not used. Because exploitation could lead to operational problems or system instability, these potential vulnerabilities were identified and communicated to the Acme team and were not exploited.


Audit Checklist #12 - Audit of Password Policy	PASS
<b>Objective: The password policy on the Microsoft OWA server should be align with Acme's password policy.</b>	

Dumpsec is a free security auditing tool for Microsoft Windows NT/2000. It can be used to gather information such as users, groups, shares, and policy settings. I downloaded Dumpsec from <http://www.somarsoft.com/>. Because this tool required an established connection to the Windows server, I had the client's system administrator install and run this tool. I compared the results of Dumpsec with the Acme password policy (Audit Checklist #3) that was provided to me.

### Instructions performed:

- Start DumpSec
- Click "Report" → "Select Computer"
- When prompted, enter the IP address of the computer being audited.
- Click "Report" → "Dump Policies"

**Left Blank Intentionally**

Screenshot of DumpSec after a computer has been selected. The IP address of the system being audited should appear on the top bar of the window.	Results from DumpSec after selecting “Dump Policies”
	<p>10/02/2003 4:20 PM - Somarsoft DumpSec (formerly DumpAcl) - \\xxx.xxx.90.10 Policies</p> <p>Account Policies</p> <ul style="list-style-type: none"> <li>Min password len: 8 chars</li> <li>Max password age: 90 days</li> <li>Min password age: 0 days</li> <li>Password history: 5 passwords</li> <li>Do not force logoff when logon hours expire</li> <li>Lockout after 3 bad logon attempts</li> <li>Reset bad logon count after 30 minutes</li> <li>Lockout duration: 90 minutes</li> </ul>

Left Blank Intentionally

<b>Audit Checklist #13 - Audit of Service Packs, Hotfixes, and Patches, using MSBA</b>	<b>FAIL</b>
--	-------------

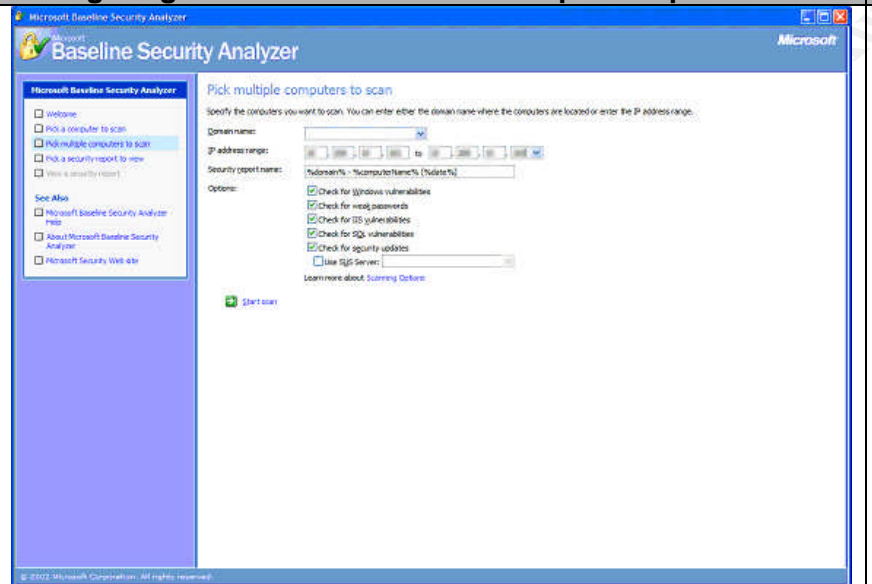
**Objective: The Windows server should be configured securely and up-to-date with security patches**

The Microsoft Security Baseline Analyzer MSBA is a free tool that is used to audit Windows systems to identify common security misconfigurations. I downloaded this tool from <http://download.microsoft.com/download/8/e/e/8ee73487-4d36-4f7f-92f2-2bdc5c5385b3/mbsasetup.msi>. Because this tool requires administrator access, I had the client's system administration install and run this tool.

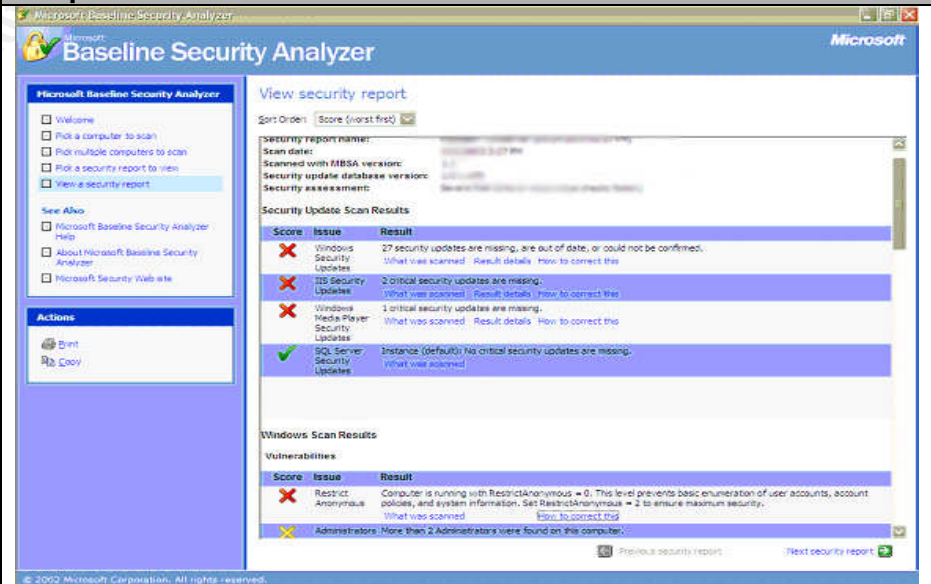
**Instructions performed:**

- Start Microsoft Security Baseline Analyzer
- Click “Scan a computer”
- Enter the IP address or the hostname of the computer
- Click “Start Scan”

## Configuring MSBA to scan one or multiple computers.



**Snapshot of the results from MSBA.**





## Audit Checklist #14 - Server Identification Verification, using Netcat

PASS

**Objective:** The password policy on the Microsoft OWA server should be align with Acme's password policy.

Netcat is known to be the "Swiss army knife" of security tools because of it's extreme versatility to do perform a number of useful

tasks such as outbound or inbound connections, TCP or UDP, to or from any ports, full DNS forward/reverse checking, and banner grabbing, just to name a few. Netcat is a command-line free tool and can be downloaded from [http://www.atstake.com/research/tools/network\\_utilities/](http://www.atstake.com/research/tools/network_utilities/). For the purposes of this audit, I used Netcat to grab the banners of the web servers. This typically will identify the type and version of the web server application.

### Instructions performed:

- In Windows, open a DOS prompt and change to the directory where netcat is installed.
- To grab the banner for a web server, type in the following:
  - o nc -vv <IP address> 80 //this will connect to the web server at port 80 in verbose mode
  - o type in: **HEAD / HTTP1.0**
  - o [Hit the carriage return twice]

Netcat results of the main website	Netcat results of the OWA server	Netcat results of the business partner website
C:\>nc -nv xxx.xxx.90.233 80 (UNKNOWN) [xxx.xxx.90.233] 80 (?) open HEAD / HTTP/1.0  HTTP/1.1 500 Server Error Server: Netscape-Enterprise/3.5.1C Date: Thu, 02 Oct 2003 03:43:38 GMT Content-length: 305 Content-type: text/html Connection: close  sent 17, rcvd 167: NOTSOCK	C:\>nc -nv xxx.xxx.90.10 80 (UNKNOWN) [xxx.xxx.90.10] 80 (?) open HEAD / HTTP/1.0  HTTP/1.1 401 Access Denied Server: Microsoft-IIS/5.0 Date: Thu, 02 Oct 2003 03:45:54 GMT WWW-Authenticate: Basic realm="10.4.3.156" Content-Length: 4431 Content-Type: text/html  sent 17, rcvd 185: NOTSOCK	C:\>nc -nv xxx.xxx.87.12 80 (UNKNOWN) [xxx.xxx.87.12] 80 (?) open HEAD / HTTP/1.0  HTTP/1.1 500 Server Error Server: Netscape-Enterprise/3.5.1C Date: Thu, 02 Oct 2003 03:46:59 GMT Content-length: 305 Content-type: text/html Connection: close  sent 17, rcvd 167: NOTSOCK

## Audit Checklist #15 - Port Scanning, using Nmap

FAIL

### Objective: Only necessary ports should be open

Nmap one of the most popular free port scanners and network exploration tools. It can be used to scan small to large IP address ranges, identify operating systems running, and check for open or closed ports. Nmap can be downloaded from <http://www.insecure.org/nmap/>. I verified that the results from Nmap correlated with the list of open ports that Acme provided to me refer to Audit Checklist #2).

### Instructions performed:

- In Windows, open a DOS prompt and change to the directory where nmap is installed.
- To scan for open ports on the web server, type in the following:
  - o `nmap -sS -P0 -O -v -oN <text file> <IP address>` //this will perform a SYN scan, check for commonly used ports, scan even if ping (ICMP) is not enabled, attempt to identify the operating system of the web server, scan in verbose mode, and output the results to a text file. Confidentiality

Nmap results of the main website	Nmap results of the OWA server	Nmap results of the business partner website
<pre># nmap (V. 3.00) scan initiated Thu Oct 2 17:30:13 2003 as: nmap -sS -P0 -O -v -oN nmap_www.xxx.90.233.txt www.xxx.90.233 Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port Interesting ports on (www.xxx.90.233): Port      State  Service 21/tcp    open   ftp 25/tcp    open   smtp 53/tcp    open   dns 80/tcp    open   http 135/tcp   filtered loc-srv 137/tcp   filtered netbios-ns 139/tcp   filtered netbios-ssn 8080/tcp  filtered http-proxy TCP/IP fingerprint: SInfo(V=3.00%P=i386-redhat-linux- gnu%D=5/16%Time=3EC582AE%O=21%C=-1)</pre>	<pre># nmap (V. 3.00) scan initiated Thu Oct 2 17:26:13 2003 as: nmap -sS -P0 -O -v -oN nmap_www.xxx.90.10.txt www.xxx.90.10 Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port Insufficient responses for TCP sequencing (0), OS detection may be less accurate Interesting ports on (www.xxx.90.10): Port      State  Service 21/tcp    filtered ftp 25/tcp    filtered smtp 80/tcp    open   http 135/tcp   filtered loc-srv 137/tcp   filtered netbios-ns 139/tcp   filtered netbios-ssn 443/tcp   open   https 8080/tcp  filtered http-proxy TCP/IP fingerprint:</pre>	<pre># nmap (V. 3.00) scan initiated Thu Oct 2 17:19:16 2003 as: nmap -sS -P0 -O -v -oN nmap_www.xxx.87.12.txt www.xxx.87.12 Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port Insufficient responses for TCP sequencing (0), OS detection may be less accurate Interesting ports on (www.xxx.87.12): Port      State  Service 21/tcp    filtered ftp 25/tcp    open   smtp 80/tcp    open   http 135/tcp   filtered loc-srv 137/tcp   filtered netbios-ns 139/tcp   filtered netbios-ssn 443/tcp   open   https 8080/tcp  filtered http-proxy TCP/IP fingerprint:</pre>

<b>Audit Checklist #16 - Web and CGI Vulnerability Scanning, using Nikto</b>	<b>FAIL</b>
<b>Objective: Check for Web and CGI configuration related vulnerabilities</b>	

Nikto is an open source web server scanner which performs comprehensive tests against web servers. It checks for several weaknesses, including over 2500 potentially dangerous files/CGIs, versions on over 375 servers, and version specific problems on over 230 servers. Because new vulnerabilities are discovered daily, it is very important to ensure that Nikto is using the latest database of vulnerabilities. Vulnerability checks and code can be automatically updated from the main distribution server by using the 'update' option. Nikto can be downloaded from <http://www.cirt.net/code/nikto.shtml>.

#### Instructions performed:

- In Windows, open a DOS prompt and change to the directory where Nikto is installed.
- Type in the following:
  - o nikto.pl -update //this will download the latest Nikto vulnerability checks
  - o nikto.pl -allcgi -verbose -host <IP address> -output <IP address>.txt// this will scan the web server for all CGI vulnerabilities, in verbose mode, and will output the results to a text file.

**NOTE: The following test results contain information from the Nikto reports that are relative to this audit. In interest of saving space, the entire reports were not included.**

<b>Nikto scan of the main website</b>
<pre> ----- - Nikto v1.23 - www.cirt.net - Thu Oct 2 15:52:52 2003 ----- + Target IP:    XXX.XXX.90.233 + Target Hostname: ?? (unable to resolve) + Target Port:  80 ----- - Scan is dependent on "Server" string which can be faked, use -g to override + Server: Netscape-Enterprise/3.5.1C + Netscape-Enterprise/3.5.1C appears to be outdated (current is at least 6.0), 4.1 and 3.6 are still considered secure and common. + / - TRACE option appears to allow XSS or credential theft. See http://www.cgisecurity.com/whitehat-mirror/WhitePaper_screen.pdf for details (TRACE) + /.sh_history - A user's home directory may be set to the web root, the shell history was retrieved. This should not be accessible via the web. (GET)           </pre>

```

+ /.ssh Redirects to 'http://xxx.xxx.90.233/.ssh/', A user's home directory may be set to the web root, an ssh file was retrieved. This should not be
accessible via the web.
+ /.ssh/authorized_keys - A user's home directory may be set to the web root, an ssh file was retrieved. This should not be accessible via the web.
(GET)
+ /admin/ Needs Auth: (realm "Enterprise Server")
+ /admin/admin_phpinfo.php4 Needs Auth: (realm "Enterprise Server")
+ /admin/contextAdmin/contextAdmin.html Needs Auth: (realm "Enterprise Server")
+ /admin/cplogfile.log Needs Auth: (realm "Enterprise Server")
+ /admin/login.php?action=insert&username=test&password=test Needs Auth: (realm "Enterprise Server")
+ /admin/phpinfo.php Needs Auth: (realm "Enterprise Server")
+ /admin/system_footer.php Needs Auth: (realm "Enterprise Server")
+ /help/ - Help directory should not be accessible (GET)
+ /cgi-bin/search.cgi - This might be interesting... (GET)
+ /help/home.html - Default Netscape manual found. All default pages should be removed. (GET)
+ /publisher/ - Netscape Publisher. May have ability to edit files on the server. May be able to list arbitrary directories via GET request.
http://icat.nist.gov/icat.cfm?cvename=CVE-2000-0237 (GET)
+ /search - Netscape search for iPlanet versions 4.1 lower than SP 10 and iPlanet 6 lower than SP 3 are vulnerable to a buffer overflow. Search is
enabled on this server but the BO could not be confirmed. (GET)
- 7992 items checked, 8 items found on remote host

```

```

CLI Options Executed: -allcgi -verbose -host xxx.xxx.90.233 -output xxx.xxx.90.233.txt
-----

```

### Nikto scan of the OWA server

```

- Nikto v1.23 - www.cirt.net - Thu Oct 2 15:26:03 2003
-----
+ Target IP:      xxx.xxx.90.10
+ Target Hostname: ?? (unable to resolve)
+ Target Port:    80
-----
- Scan is dependent on "Server" string which can be faked, use -g to override
+ Server: Microsoft-IIS/5.0
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK
+ HTTP method 'PROPFIND' may indicate DAV/WebDAV is installed. This may allow DAV authorized users to consume system memory via large
requests or fill disk quotas.

```

```

+ HTTP method 'TRACE' may allow client XSS or credential theft. See http://www.cgisecurity.com/whitehat-mirror/WhitePaper_screen.pdf for details.
+ / - TRACE option appears to allow XSS or credential theft. See http://www.cgisecurity.com/whitehat-mirror/WhitePaper_screen.pdf for details (TRACE)
+ / - TRACK option ('TRACE' alias) appears to allow XSS or credential theft. See http://www.cgisecurity.com/whitehat-mirror/WhitePaper_screen.pdf for details (TRACK)
+ /public/ Needs Auth: (realm "xxx.xxx.90.10")
+ /xxxxxxxxxabcd.html - The IIS server may be vulnerable to Cross Site Scripting (XSS) in error messages, see http://www.microsoft.com/technet/security/bulletin/MS02-018.asp, http://icat.nist.gov/icat.cfm?cvename=CVE-2002-0075, SNS-49, http://www.microsoft.com/technet/security/bulletin/MS02-018.asp, http://www.cert.org/advisories/CA-2002-09.html (GET)
+ /_vti_bin/fpcount.exe - Frontpage counter CGI has been found. FP Server version 97 allows remote users to execute arbitrary system commands, though a vulnerability in this version could not be confirmed. (GET)
+ /_vti_bin/shtml.dll/_vti_rpc?method=server+version%3a4%2e0%2e2%2e2611 - Gives info about server settings. http://icat.nist.gov/icat.cfm?cvename=CAN-2000-0413, http://icat.nist.gov/icat.cfm?cvename=CAN-2000-0709, http://icat.nist.gov/icat.cfm?cvename=CAN-2000-0710, http://www.securityfocus.com/bid/BID-1608, http://www.securityfocus.com/bid/BID-1174. (POST)
+ /_vti_bin/shtml.exe - Attackers may be able to crash FrontPage by requesting a DOS device, like shtml.exe/aux.htm -- a DoS was not attempted. http://icat.nist.gov/icat.cfm?cvename=CAN-2000-0413, http://icat.nist.gov/icat.cfm?cvename=CAN-2000-0709, http://icat.nist.gov/icat.cfm?cvename=CAN-2000-0710, http://www.securityfocus.com/bid/BID-1608, http://www.securityfocus.com/bid/BID-1174. (GET)
+ /_vti_bin/shtml.exe/_vti_rpc - FrontPage may be installed. (GET)
+ /_vti_bin/shtml.exe/_vti_rpc?method=server+version%3a4%2e0%2e2%2e2611 - Gives info about server settings. http://icat.nist.gov/icat.cfm?cvename=CAN-2000-0413, http://icat.nist.gov/icat.cfm?cvename=CAN-2000-0709, http://icat.nist.gov/icat.cfm?cvename=CAN-2000-0710, http://www.securityfocus.com/bid/BID-1608, http://www.securityfocus.com/bid/BID-1174. (POST)
+ /_vti_inf.html - FrontPage may be installed. (GET)
- 8551 items checked, 9 items found on remote host
CLI Options Executed: -allcgi -verbose -host xxx.xxx.90.10 -output xxx.xxx.90.10.txt
-----

```

#### Nikto scan of business partner website

```

-----
- Nikto v1.23 - www.cirt.net - Thu Oct 2 13:45:48 2003
-----

```

```

+ Target IP:    xxx.xxx.87.12

```

```
+ Target Hostname: ?? (unable to resolve)
+ Target Port: 80
-----
- Scan is dependent on "Server" string which can be faked, use -g to override
+ Server: Netscape-Enterprise/3.5.1C
+ Netscape-Enterprise/3.5.1C appears to be outdated (current is at least 6.0), 4.1 and 3.6 are still considered secure and common.
+ / - TRACE option appears to allow XSS or credential theft. See http://www.cgisecurity.com/whitehat-mirror/WhitePaper\_screen.pdf for details (TRACE)
+ /.sh_history - A user's home directory may be set to the web root, the shell history was retrieved. This should not be accessible via the web. (GET)
+ /.ssh Redirects to 'http://xxx.xxx.87.12/.ssh/', A user's home directory may be set to the web root, an ssh file was retrieved. This should not be accessible via the web.
+ /admin/ Needs Auth: (realm "Enterprise Server")
+ /admin/admin_phpinfo.php4 Needs Auth: (realm "Enterprise Server")
+ /admin/contextAdmin/contextAdmin.html Needs Auth: (realm "Enterprise Server")
+ /admin/cplogfile.log Needs Auth: (realm "Enterprise Server")
+ /admin/login.php?action=insert&username=test&password=test Needs Auth: (realm "Enterprise Server")
+ /admin/phpinfo.php Needs Auth: (realm "Enterprise Server")
+ /admin/system_footer.php Needs Auth: (realm "Enterprise Server")
+ /help/ - Help directory should not be accessible (GET)
+ /cgi-bin/search.cgi - This might be interesting... (GET)
+ /help/home.html - Default Netscape manual found. All default pages should be removed. (GET)
+ /publisher/ - Netscape Publisher. May have ability to edit files on the server. May be able to list arbitrary directories via GET request.
http://icat.nist.gov/icat.cfm?cvename=CVE-2000-0237 (GET)
+ /search - Netscape search for iPlanet versions 4.1 lower than SP 10 and iPlanet 6 lower than SP 3 are vulnerable to a buffer overflow. Search is enabled on this server but the BO could not be confirmed. (GET)
- 7992 items checked, 7 items found on remote host

CLI Options Executed: -allcgi -host xxx.xxx.87.12 -verbose -output xxx.xxx.87.12.txt
-----
```

## Audit Checklist #17 - Vulnerability Scanning, using Nessus

FAIL

### Objective: Check for vulnerabilities and configuration weaknesses

Nessus is a very popular open source network vulnerability scanner that can be used to scan remote systems and networks. Similar to Nikto, you should always download the latest scripts/plugin-ins to ensure that Nessus is scanning against the most recent vulnerabilities.

Nessus can be downloaded from <http://www.nessus.org>.

### Instructions performed:

- In Unix, open a terminal window.
- Type in the following:
  - o `nessus-update-plugins` //automatically download the latest scripts
  - o `nessusD -D` //start the Nessus daemon
- Open a 2nd terminal window.
- Type in the following:
  - o `nessus` // start the Nessus application
- For Nessus configuration instructions, please see the next page.

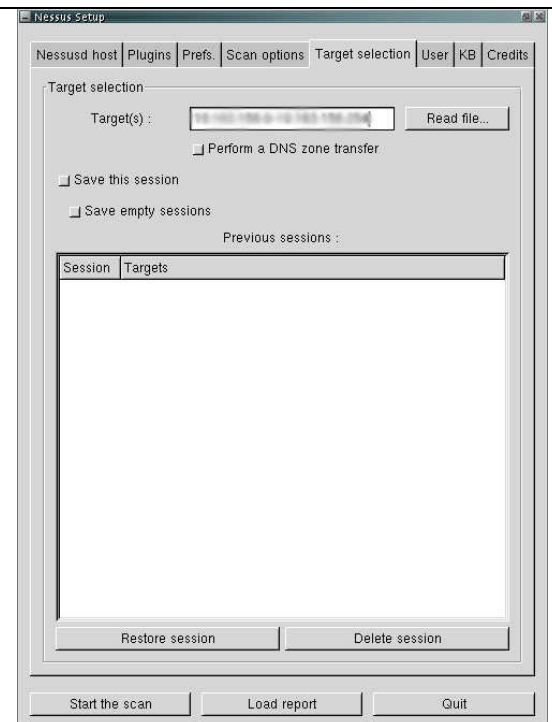
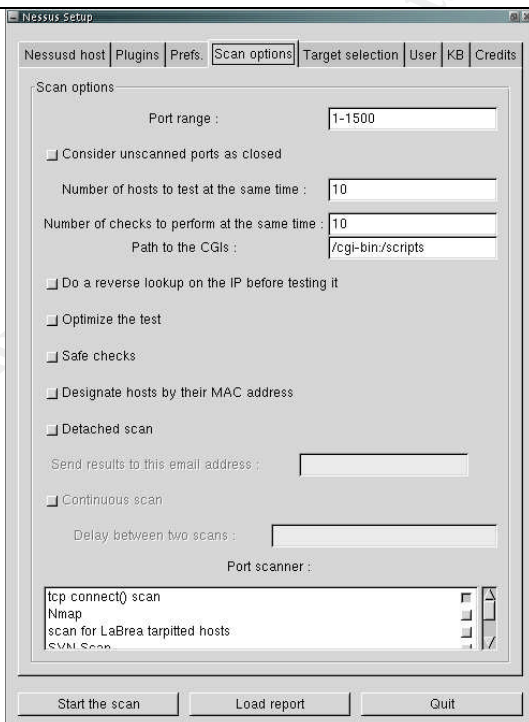
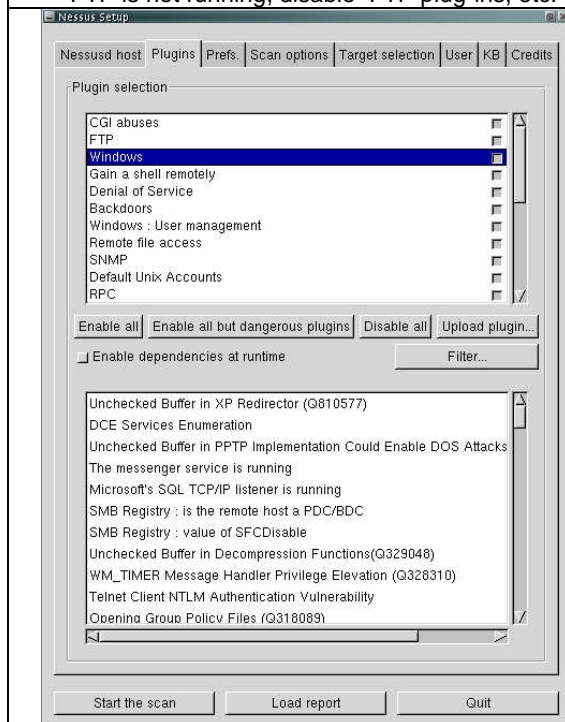
Left Blank Intentionally

## Nessus Configuration

- After you log into the Nessus application, click the “Plug-ins” tab.
- Click “Enable all but dangerous plug-ins”. Dangerous plug-ins include denial of service attacks which could potentially take down or cause instability to the server.
- For each web server that is being audited, configure the plug-ins so that they reflect your knowledge of the server. For instance, for an IIS server, enable all of the IIS plug-ins and disable the Apache plug-ins. If you know that FTP is not running, disable FTP plug-ins, etc.

- Click the “Scan options” tab
- For the web server being audited, enter the ports that are open from the results of your Nmap scan (common delimited). There is no need to re-perform another entire port scan using Nessus.

- Click the “Target selection” tab.
- Enter the IP address of the web server(s) being audited (common delimited)
- Click “Start the scan”





**NOTE: The following test results contain information from the Nessus reports that are relative to this audit. In interest of saving space, the entire reports were not included.**

#### **Nessus scan of the main website**

##### **+ xxx.xxx.90.233 :**

- . List of open ports :
  - o http (80/tcp) (Security warnings found)
  - o domain (53/tcp) (Security hole found)
  - o smtp (25/tcp) (Security notes found)
  - o ftp (21/tcp) (Security hole found)
  - o general/icmp (Security warnings found)
  - o ssh (22/tcp) (Security hole found)
  - o general/tcp (Security notes found)
  - o general/udp (Security notes found)
  - o domain (53/udp) (Security notes found)

- . Warning found on port http (80/tcp)

Your webserver supports the TRACE and/or TRACK methods. It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for 'Cross-Site-Tracing', when used in conjunction with various weaknesses in browsers.

An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Solution: Disable these methods.

If you are using Apache, add the following lines for each virtual host in your configuration file :

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]
```

If you are using Microsoft IIS, use the URLScan tool to deny HTTP TRACE requests or to permit only the methods needed to meet site requirements and policy.

See [http://www.whitehatsec.com/press\\_releases/WH-PR-20030120.pdf](http://www.whitehatsec.com/press_releases/WH-PR-20030120.pdf)  
<http://archives.neohapsis.com/archives/vulnwatch/2003-q1/0035.html>

Risk factor : Medium

. Information found on port http (80/tcp)

A web server is running on this port

. Information found on port http (80/tcp)

The remote web server type is :

Netscape-Enterprise/3.5.1C

Solution : We recommend that you configure (if possible) your web server to return a bogus Server header in order to not leak information.

. Vulnerability found on port domain (53/tcp) :

This is associated with three different vulnerabilities.

- 1) The remote BIND server, based on its version number, if running recursive DNS functionality, is vulnerable to a buffer overflow.
- 2) The remote BIND server is vulnerable to a denial of service (crash) via SIG RR elements with invalid expiry times.
- 3) The remote BIND server is vulnerable to a denial of service. When a DNS lookup is requested on a non-existent sub-domain of a valid domain and an OPT resource record with a large UDP payload is attached, the server may fail.

Solution : upgrade to at least bind 8.3.4

Risk factor : High

CVE : CAN-2002-1221, CAN-2002-1219, CAN-2002-1220

BID : 6159, 6160, 6161

## Nessus scan of the OWA server

### + xxx.xxx.90.10 :

- . List of open ports :
  - o https (443/tcp) (Security hole found)
  - o http (80/tcp) (Security hole found)
  - o general/icmp (Security warnings found)
  - o general/tcp (Security notes found)
  - o general/udp (Security notes found)

- . Vulnerability found on port https (443/tcp) :

The file /iisadmpwd/aexp2.htr is present. (or, aexp2b.htr, aexp3.htr, or aexp4.htr, search for aexp\*.htr)

An attacker may use it in a brute force attack to gain valid username/password.  
A valid user may also use it to change his password on a locked account.

Solution : Delete the file  
Risk factor : Serious  
CVE : CVE-1999-0407  
BID : 2110

- . Vulnerability found on port https (443/tcp) :

The remote host has FrontPage Server Extensions (FPSE) installed.

There is a denial of service / buffer overflow condition in the program 'shtml.exe' which comes with it. However, no public detail has been given regarding this issue yet, so it's not possible to remotely determine whether you are vulnerable to this flaw or not.

If you are, an attacker may use it to crash your web server FPSE 2000) or execute arbitrary code (FPSE 2002). Please see the Microsoft Security Bulletin MS02-053 to determine if you are vulnerable or not.

\*\*\* Nessus did not actually check for this flaw, so this  
\*\*\* might be a false positive

Solution : See <http://www.microsoft.com/technet/security/bulletin/ms02-053.asp>

Risk factor : High  
CVE : CAN-2002-0692  
BID : 5804

. Vulnerability found on port https (443/tcp) :

The IIS server appears to have the .HTR ISAPI filter mapped.

At least one remote vulnerability has been discovered for the .HTR filter. This is detailed in Microsoft Advisory MS02-018, 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 .HTR extension, and any other unused ISAPI extensions if they are not required for the operation of your site.

Solution:

To unmap the .HTR 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 .htr from the list.

Risk factor : High  
CVE : CAN-2002-0071  
BID : 4474

. Vulnerability found on port https (443/tcp) :

The remote WebDAV server may be vulnerable to a buffer overflow when it receives a too long request.

An attacker may use this flaw to execute arbitrary code within the LocalSystem security context.

\*\*\* As safe checks are enabled, Nessus did not actually test for this  
\*\*\* flaw, so this might be a false positive

Solution : See <http://www.microsoft.com/technet/security/bulletin/ms03-007.asp>

Risk Factor : High  
CVE : CAN-2003-0109  
BID : 7116

## Nessus scan of the business partner website

### + xxx.xxx.87.12 :

- . List of open ports :
  - o http (80/tcp) (Security warnings found)
  - o domain (53/tcp) (Security hole found)
  - o smtp (25/tcp) (Security notes found)
  - o general/icmp (Security warnings found)
  - o general/tcp (Security notes found)
  - o general/udp (Security notes found)
  - o domain (53/udp) (Security notes found)

- . Warning found on port http (80/tcp)

Your webserver supports the TRACE and/or TRACK methods. It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for 'Cross-Site-Tracing', when used in conjunction with various weaknesses in browsers.

An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Solution: Disable these methods.

If you are using Apache, add the following lines for each virtual host in your configuration file :

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]
```

If you are using Microsoft IIS, use the URLScan tool to deny HTTP TRACE requests or to permit only the methods needed to meet site requirements and policy.

See [http://www.whitehatsec.com/press\\_releases/WH-PR-20030120.pdf](http://www.whitehatsec.com/press_releases/WH-PR-20030120.pdf)  
<http://archives.neohapsis.com/archives/vulnwatch/2003-q1/0035.html>

Risk factor : Medium

. Information found on port http (80/tcp)

A web server is running on this port

. Information found on port http (80/tcp)

The remote web server type is :

Netscape-Enterprise/3.5.1C

Solution : We recommend that you configure (if possible) your web server to return a bogus Server header in order to not leak information.

. Vulnerability found on port domain (53/tcp) :

This is associated with three different vulnerabilities.

- 1) The remote BIND server, based on its version number, if running recursive DNS functionality, is vulnerable to a buffer overflow.
- 2) The remote BIND server is vulnerable to a denial of service (crash) via SIG RR elements with invalid expiry times.
- 3) The remote BIND server is vulnerable to a denial of service. When a DNS lookup is requested on a non-existent sub-domain of a valid domain and an OPT resource record with a large UDP payload is attached, the server may fail.

Solution : upgrade to at least bind 8.3.4

Risk factor : High

CVE : CAN-2002-1221, CAN-2002-1219, CAN-2002-1220

BID : 6159, 6160, 6161

## Measure Residual Risk

Given the audit checklist that I used, the business and security needs of the systems, and the results of the audit, there appears to be some residual risk that exists. All of the findings from my audit involved configuration issues or security operations procedural issues with the systems. The vulnerabilities that were discovered can be fixed with minimal to moderate amount of effort and cost. To help reduce the number of vulnerabilities in the future, I recommend that Acme perform quarterly vulnerability scans and before a new system is deployed.

Similar to my audit, Acme can utilize well-known freeware and open source security tools to help with this effort. Therefore, the estimated costs with making the web servers secure would be minimal, utilizing existing staff and resources. For the security operational procedures that do not exist or were deficient, Acme realizes the importance of these controls and has initiatives underway to create or refine the policies and procedures.

It is also important to note that even if all of the discovered vulnerabilities were remediated, it does not mean that the systems are secure. Because of systems being audited are web servers that can be accessed by anyone on the Internet, the threat and risk is always constant as new vulnerabilities are discovered daily.

## Is the System Audible?

There are some areas that can not be validated by the audit mainly because Acme was either unable to provide me the requested documentation or the information provided to me was from other analyses prior to my audit. For instance, Acme provided their security and business requirements which was the foundation of the audit. These security and business requirements were not tested, analyzed, or validated by the audit. In addition, prior to the audit, a business continuity plan was developed which included an exercise to rate Acme's critical systems by level of criticality. The web servers were selected from this plan and were not validated by the audit.

In meeting with Acme IT personnel, I discovered that they did not have standard documented procedure for security patch management. Because of this fact, this audit control is not auditable. However, to help support or warrant the need for a patch management procedure, I tested the version of patches and identified that they were inconsistent and not up-to-date.

## Assignment 4 – Audit Report

### Executive Summary

In general, it appears that Acme is taking proactive steps in understanding and managing information security risks. For those areas assessed during this project, there are both sound information security practices in place or under consideration, and security risks to Acme's information and systems. During the course of the project, several risk items were either addressed through longer-term initiatives or when possible mitigated immediately (e.g. removal of unnecessary services, use of SSH for Unix systems, and secured web server configuration). Currently, the overall security of the Acme IT infrastructure appears to be relatively stable with a few areas of weak controls. However, without having certain formalized security processes and procedures in place to control the IT environment, current weak areas can quickly escalate into major security issues for Acme in the face of a concerted attack against the IT infrastructure.

Based on this study, there were several opportunities identified for management to more clearly define their network security practices and strengthen the security environment. It is recommended that management address the following key observations:

- Servers are running older versions of applications with known vulnerabilities
- Servers have vulnerable file configurations or incorrect permissions
- Servers are running vulnerable services that if exploited could allow a malicious user to execute arbitrary code or gain complete control over the system
- A comprehensive set of formalized information security policies and procedures does not exist



#	Ref.	Risk Rating	Finding	Background/Risk	Recommendation	Costs / Compensating Controls
<b>1.0 High Risk Findings</b>						
1.1.	Audit Step #16	H	<p><b>Finding:</b> The Acme public website is running the Netscape's WebPublisher software. This software allows file uploads, downloads and provides the capability to change "permissions" on files. These features are accessible to any external user who can install a local copy of the Webpublisher on their own personal system and connect over the Internet and the Acme internal network to gain access to the system. The Webpublisher client can be downloaded directly from the Acme http:\\xxx.xxx.90.233\\publisher website. This vulnerability allows a user to navigate through the files and directories of the webserver.</p> <p><b>Details:</b> xxx.xxx.90.233 (<a href="http://www.acme.com">www.acme.com</a>)</p>	<p>The Webpublisher software allows you to upload, download, modify, delete and move files and directories. These requests have not yet been tested and may prompt the user for a password. However, password entry can be compromised by software through "brute force" techniques. If exploited, a malicious user could potentially perform numerous attacks such as uploading an executive arbitrary code or a malicious worm, removing or modifying files and content on the Acme website, or creating a backdoor into the system.</p>	<p>We recommend either uninstalling Webpublisher or setting directory permissions on the publisher directory. Alternatively, access control may be applied to WebPublisher through the access control module.</p> <p>To prevent similar problems in the future, a thorough review of web servers should be performed before deployment and periodically after deployment to identify configuration weaknesses such as unnecessary services and software running.</p>	<p>The cost to remove this vulnerability is minimal. Because the Webpublisher is not being used, the system administrator will simply need to uninstall the software.</p>

#	Ref.	Risk Rating	Finding	Background/Risk	Recommendation	Costs / Compensating Controls
1.2.	Audit Step #17	H	<p><b>Finding:</b> A remotely accessible directory, /IISADMPWD is mapped to c:\winnt\system32\inetrv\iisadmpwd, which contains a number of vulnerable .HTR files.</p> <p>These files were designed to provide system administrators the ability to provide HTTP based password change services to network users. The affected files, achg.htr, aexp*.htr, and anot*.htr can be used in this manner. Requesting one of the listed .htr files returns a form that requests the account name, current password, and changed password.</p> <p><b>Details:</b> xxx.xxx.90.10 (OWA Server)</p>	<p>These files can be used by a malicious user to determine whether or not the account requested exists on the host, as well as perform brute force attacks. If the account does not exist, the message "invalid domain" is returned. If the account exists, but the password change was unsuccessful, the malicious user is notified. This information can be used against the server and against other machines by preceding the account name with an IP address and a backslash. The server contacts the networked machine through the NetBIOS session port and attempts to change the password.</p>	<p>Configure Microsoft IIS to disable this feature and unmap the vulnerable directory. To unmap the .HTR extensions:</p> <ol style="list-style-type: none"> <li>1.Open Internet Services Manager.</li> <li>2.Right-click the Web server choose Properties from the context menu.</li> <li>3.Master Properties</li> <li>4.Select WWW Service -&gt; Edit -&gt; HomeDirectory -&gt; Configuration and remove the reference to .htr from the list.</li> </ol> <p>To prevent similar problems in the future, a thorough review of web servers should be performed before deployment and periodically after deployment to identify configuration weaknesses such as unnecessary services and software running.</p>	<p>It was determined that the .htr files are necessary in order for the web site to function properly. Therefore, the Microsoft IIS lockdown tool should be executed and .htr files be kept to preserve functionality.</p> <p>The cost is minimal because Acme has the existing staff and resources and IIS lockdown is a free tool.</p>
1.3.	Audit Step #17	H	<p><b>Finding:</b> IIS Server has .HTR ISAPI filter mapped. There is a buffer overflow in the HTR ISAPI extension.</p> <p><b>Details:</b> xxx.xxx.90.10 (OWA Server)</p>	<p>By submitting a malicious HTR request, a malicious user can exploit this buffer overflow. A malicious user could potentially interrupt the normal operation of the IIS server. In addition, s/he may be able to use this vulnerability to execute arbitrary code with the privileges of the HTR ISAPI extension. On IIS 5.0 and 5.1, this permits access with the privileges of the IWAM_computename account.</p>	<p>Apply the patch describe in: <a href="http://www.microsoft.com/technet/security/bulletin/ms02-018.asp">http://www.microsoft.com/technet/security/bulletin/ms02-018.asp</a></p> <p>In addition, we recommend unmapping the .HTR ISAPI extension. To unmap the .HTR extension:</p> <ol style="list-style-type: none"> <li>1.Open Internet Services Manager.</li> <li>2.Right-click the Web server choose Properties from the context menu.</li> <li>3.Master Properties</li> <li>4.Select WWW Service -&gt; Edit -&gt; HomeDirectory -&gt; Configuration and remove the reference to .htr from the list.</li> </ol> <p>By default, the IIS Lockdown Tool disable HTR support, by unmapping the HTR ISAPI extension. To prevent similar problems in the future, a thorough review of web servers should be performed before deployment and periodically after deployment to identify configuration weaknesses such as unnecessary services and software running.</p>	<p>It was determined that the .htr files are necessary in order for the web site to function properly. Therefore, the Microsoft IIS lockdown tool should be executed and .htr files be kept to preserve functionality.</p> <p>The cost is minimal because Acme has the existing staff and resources and IIS lockdown is a free tool.</p>

#	Ref.	Risk Rating	Finding	Background/Risk	Recommendation	Costs / Compensating Controls
1.4.	Audit Step #17	H	<p><b>Finding:</b> FrontPage Server Extensions (FPSE) are installed. A vulnerability has been reported in the SmartHTML (shtml) interpreter component of FrontPage Server Extensions.</p> <p><b>Details:</b> xxx.xxx.90.10 (OWA Server)</p>	<p>A malicious user could potentially exploit this vulnerability and cause consumption of CPU due to an infinite loop condition. This may adversely affect the server's ability to perform other functions. Because of the buffer overflow vulnerability, remote malicious users could also potentially execute arbitrary code on target hosts running FrontPage Server Extensions 2002.</p>	<p>We recommend uninstalling Frontpage Server Extensions until a patch has been installed.</p> <p>It is also possible to disable SmartHTML Interpreter by configuring the web server with "IIS Lockdown Tool". However, Acme has not been able to successfully run this tool in the past.</p> <p>Apply the appropriate patch from Microsoft: <a href="http://support.microsoft.com/default.aspx?scid=kb:en-us:Q324096">http://support.microsoft.com/default.aspx?scid=kb:en-us:Q324096</a></p> <p>To prevent similar problems in the future, a thorough review of web servers should be performed before deployment and periodically after deployment to identify configuration weaknesses such as unnecessary services and software running.</p>	<p>It was determined that the .htr files are necessary in order for the web site to function properly. Therefore, the Microsoft IIS lockdown tool should be executed and .htr files should be kept to preserve functionality.</p> <p>The cost is minimal because Acme has the existing staff and resources and IIS lockdown is a free tool.</p>
1.5.	Audit Step #17	H	<p><b>Finding:</b> A buffer overflow in ntdll.dll, as used by WebDAV on Windows 2000, allows remote malicious users to execute arbitrary code via a long request to IIS 5.0.</p> <p><b>Details:</b> xxx.xxx.90.10 (OWA Server)</p>	<p>A malicious user may use this flaw to execute arbitrary code within the LocalSystem security context. The Windows library ntdll.dll includes a function that does not perform sufficient bounds checking. The vulnerability is present in the function "RtlDosPathNameToNtPathName_U" and may be exploited through other programs that use the library if an attack vector permits it.</p> <p>One of these programs is the implementation of WebDAV that ships with IIS 5.0. The vector allows for the vulnerability in ntdll.dll to be exploited by a remote attacker.</p>	<p>Apply the patch from Microsoft: <a href="http://microsoft.com/downloads/details.aspx?FamilyId=C9A38D45-5145-4844-B62E-C69D32AC929B&amp;displaylang=en">http://microsoft.com/downloads/details.aspx?FamilyId=C9A38D45-5145-4844-B62E-C69D32AC929B&amp;displaylang=en</a></p> <p>Until a patch can be applied, you may wish to disable IIS: <a href="http://support.microsoft.com/default.aspx?scid=kb:en-us:321141">http://support.microsoft.com/default.aspx?scid=kb:en-us:321141</a></p> <p>If you cannot disable IIS, the IIS lockdown tool can be used to disable WebDAV.</p> <p>To prevent similar problems in the future, periodic vulnerability assessments should be performed to identify known security vulnerabilities.</p>	<p>The cost to fix this problem is minimal to moderate. The Microsoft patch should be downloaded and tested before deploying to production servers.</p> <p>If vulnerability assessments are performed, open source tools such as Nikto and Nessus may be used to reduce costs.</p>

#	Ref.	Risk Rating	Finding	Background/Risk	Recommendation	Costs / Compensating Controls
1.6.	Audit Step #17	H	<p><b>Finding:</b> 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.</p> <p><a href="http://www.securityfocus.com/archive/1/181109">http://www.securityfocus.com/archive/1/181109</a></p> <p><b>Details:</b> xxx.xxx.90.10 (OWA Server)</p>	By exploiting the vulnerability, a malicious user may be able to remotely execute arbitrary code against the server and potentially gain access to confidential information.	<p>To unmap the .printer extension:</p> <ol style="list-style-type: none"> <li>1.Open Internet Services Manager.</li> <li>2.Right-click the Web server choose Properties from the context menu.</li> <li>3.Master Properties</li> <li>4.Select WWW Service -&gt; Edit -&gt; HomeDirectory -&gt; Configuration and remove the reference to .printer from the list.</li> </ol> <p>To prevent similar problems in the future, a thorough review of web servers should be performed before deployment and periodically after deployment to identify configuration weaknesses such as unnecessary services and software running. In addition, removing support for IPP should be part of the Acme web server lockdown procedure.</p>	The cost to fix this problem is minimal. Instead of unmapping the .printer extension, the latest hotfix for this vulnerability was applied to mitigate the vulnerability.
1.7.	Audit Step #7, 13	H	<p><b>Finding:</b> A number of security updates are missing or out of date, including three critical security updates.</p> <p><b>Details:</b> xxx.xxx.90.10 (OWA Server)</p>	<p>These critical security updates will correct Windows vulnerabilities such as buffer overflow and flaws with applications and services.</p> <p>A malicious user may use these vulnerabilities to perform denial of service attacks or execute arbitrary commands and obtain a shell to the server.</p>	<p>Install the latest service packs and/or individual updates on the system. The Windows Update website <a href="http://v4.windowsupdate.microsoft.com/en/default.asp">http://v4.windowsupdate.microsoft.com/en/default.asp</a> has the latest service pack and security update releases to download.</p>	<p>The cost to fix this problem is minimal to moderate. The Microsoft patch should be downloaded and tested before deploying to production servers.</p> <p>Microsoft Security Baseline Analyzer should be used to audit the system on a periodic basis.</p>

#	Ref.	Risk Rating	Finding	Background/Risk	Recommendation	Costs / Compensating Controls
<b>2.0 Medium Risk Findings</b>						
2.1.	Audit Step #17	M	<p><b>Finding:</b> The FTP server is vulnerable to 'glob heap corruption' flaw.</p> <p><a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0249">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0249</a>  <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0550">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0550</a></p> <p><b>Details:</b> xxx.xxx.90.233 (<a href="http://www.acme.com">www.acme.com</a>)</p>	<p>A variety of FTP servers incorrectly manage buffers in a way that can lead to remote intruders executing arbitrary code on the FTP server. The incorrect management of buffers is centered around the return from the glob() function.</p> <p>A malicious user may use this problem to execute arbitrary commands and obtain a shell to the server.</p>	<p>If there is a valid business purpose for FTP, we recommend upgrading the FTP server software to the latest version.</p> <p>Otherwise, using a more secure file transfer solutions such as SCP or SFTP is recommended.</p> <p>To prevent similar problems in the future, a thorough review of web servers should be performed before deployment and periodically after deployment to identify configuration weaknesses such as unnecessary services and software running.</p>	<p>The cost to fix this problem is minimal. The FTP port should be blocked at the firewall because it is not in use.</p>
2.2.	Audit Step #17	M	<p><b>Finding:</b> The version of OpenSSH is older than 3.4 and has known vulnerabilities associated with it.</p> <p><a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0639">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0639</a>  <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0640">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0640</a></p> <p><b>Details:</b> xxx.xxx.90.233 (<a href="http://www.acme.com">www.acme.com</a>)</p>	<p>There is a flaw in older versions of OpenSSH that can be exploited remotely to give a malicious user a shell on this server.</p> <p>If a shell is obtained on the server, it is possible for a malicious user perform tasks such as create user accounts, upload Trojan files or malicious binaries, escalate privileges, modify data, and reduce the level of security of the system.</p>	<p>Upgrade to the latest version of OpenSSH and restrict access to the service or turn off the service.</p> <p>To prevent similar problems in the future, a thorough review of web servers should be performed before deployment and periodically after deployment to identify configuration weaknesses such as unnecessary services and software running. In addition, Acme should subscribe to a security mailing lists such as Buqtraq, SANS, CERT which will help identify older versions of software that are vulnerable.</p>	<p>The cost to fix this problem is minimal. The SSH port should be blocked at the firewall because it is not in use.</p>
<b>3.0 Low Risk Findings</b>						
3.1.	Audit Step #16	L	<p><b>Finding:</b> The /.sh_history of the root user is accessible and revealed the last commands performed by the root user.</p> <p><b>Details:</b> xxx.xxx.87.12 xxx.xxx.90.233 (<a href="http://www.acme.com">www.acme.com</a>)</p>	<p>This is leakage of information that a malicious user could potentially take advantage of to launch more educated and sophisticated attacks.</p>	<p>Configure the server so that the /.sh_history is not accessible. To prevent similar problems in the future, a thorough review of web servers should be performed before deployment and periodically after deployment. This will help identify configuration weaknesses such as exposing unnecessary directories and files to the Internet.</p>	<p>The cost to fix this problem is minimal. The web server should be configured to not allow read, write, or execute to this file or directory.</p>

#	Ref.	Risk Rating	Finding	Background/Risk	Recommendation	Costs / Compensating Controls
3.2.	Audit Step #16	L	<p><b>Finding:</b> The /help directory is accessible by an external user. In addition, the default Netscape Web Publisher Users Guide is also accessible at /help/home.html.</p> <p><b>Details:</b> xxx.xxx.87.12 xxx.xxx.90.233 (<a href="http://www.acme.com">www.acme.com</a>)</p>	This is leakage of information that a malicious user could potentially take advantage of to launch more educated and sophisticated attacks.	<p>Configure the server so that the /help and /help/home.html are not accessible.</p> <p>To prevent similar problems in the future, a thorough review of web servers should be performed before deployment and periodically after deployment. This will help identify configuration weaknesses such as exposing unnecessary directories and files to the Internet.</p>	The cost to fix this problem is minimal. The web server should be configured to not allow read, write, or execute to this file or directory.
3.3.	Audit Step #15, 16, 17	L	<p><b>Observation:</b> DNS port 53 is open.</p> <p><b>Details:</b> xxx.xxx.90.233 (<a href="http://www.acme.com">www.acme.com</a>)</p>	<p>Several vulnerabilities are associated with DNS which include buffer overflow denial of service attacks.</p> <p>According to Acme, DNS should not be allowed from the outside.</p>	<p>Apply the appropriate patches for DNS.</p> <p>To prevent similar problems in the future, a thorough review of web servers should be performed before deployment and periodically after deployment. This will help identify configuration weaknesses such as allowing unnecessary</p>	The cost to fix this problem is moderate. This problem will be resolved through migration away from Sendmail.
3.4.	Audit Step #13	L	<p><b>Finding:</b> Restrict Anonymous was found to being = 0.</p> <p><b>Details:</b> xxx.xxx.90.10 (OWA Server)</p>	Have restrict anonymous enabled allows enumeration of user accounts, account policies, and system information. This leakage of information can be used by malicious user who could potentially launch more educated and sophisticated attacks.	<p>To restrict anonymous connections from accessing this system information, change the RestrictAnonymous security settings to either 1 or 2.</p> <p>1 – Do not allow enumeration of Security Accounts Manager (SAM) accounts and names</p> <p>2 – No access without explicit anonymous permissions</p>	The cost to fix this problem is minimal and should be a simple configuration change.

## References

Bill Number 1386, [http://info.sen.ca.gov/pub/01-02/bill/sen/sb\\_1351-1400/sb\\_1386\\_bill\\_20020926\\_chaptered.html](http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html)

Center for Internet Security, Windows 2000 and Solaris Benchmarks, <http://www.cisecurity.org/>

Guel, Michele D., "A Short Primer for Developing Security Policies",  
[http://www.sans.org/resources/policies/Policy\\_Primer.pdf](http://www.sans.org/resources/policies/Policy_Primer.pdf),  
2001.

Institute for Security and Open Methodologies, "Open Source Security Testing Methodology Manual v2.1",  
<http://www.ideahamster.org/projects/osstmm.htm>

Scambray, Joel. Shema, Mike, Hacking Web Applications Exposed, McGraw-Hill, New York, 2002.

Sikac, John. "Access Security Checklist", <http://www.auditnet.org/docs/AccessSecurityChecklist.doc>, Oct. 16, 2001.

SANS class, "Auditing Networks, Perimeters, and Systems Hands-On Workbook", 2003.

SANS Security Policy Project, <http://www.sans.org/resources/policies/>.

Sutton, Virginia. "Change Management Audit Program", <http://www.auditnet.org/docs/chngmgmt.txt>, Oct. 10, 1999.

Warigon, Slemo. "Access Control Audit Program", <http://www.auditnet.org/docs/access.txt>, Mar 9, 1995.