



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.

Auditing a Small Internet Business Hosted by an Internet Service Provider: an Auditor's Perspective

Auditing Networks, Perimeters, and Systems

GSNA Practical Assignment

Version 2.1- Option 1

Stephanie Frigon, October 2003

© SANS Institute 2003, Author retains full rights.

Abstract/Summary

This paper is a complete audit performed on a small internet business, which is hosted on an Internet Service Provider, from an auditor's perspective. The audit focuses on identifying risks associated with that of a small business, those associated with ISPs, as well as inherent risks of the systems software and applications. Sufficient research has been done to identify these risks and has been provided within the paper. The format of the audit is the following: identifies the system, lists risks associated with the system, creates a checklist of tests to identify the systems exposure to these risks, and provides the audit results. Additionally, this paper provides recommendations from the auditor's perspective of what this system/business can do to mitigate these risks. The content of this paper could be useful for other companies/applications/systems established in similar environments, and therefore, subject to similar risks.

© SANS Institute 2003, Author retains full rights

Assignment 1: Research in Audit, Measurement, Practice and Control

1.1 Introduction

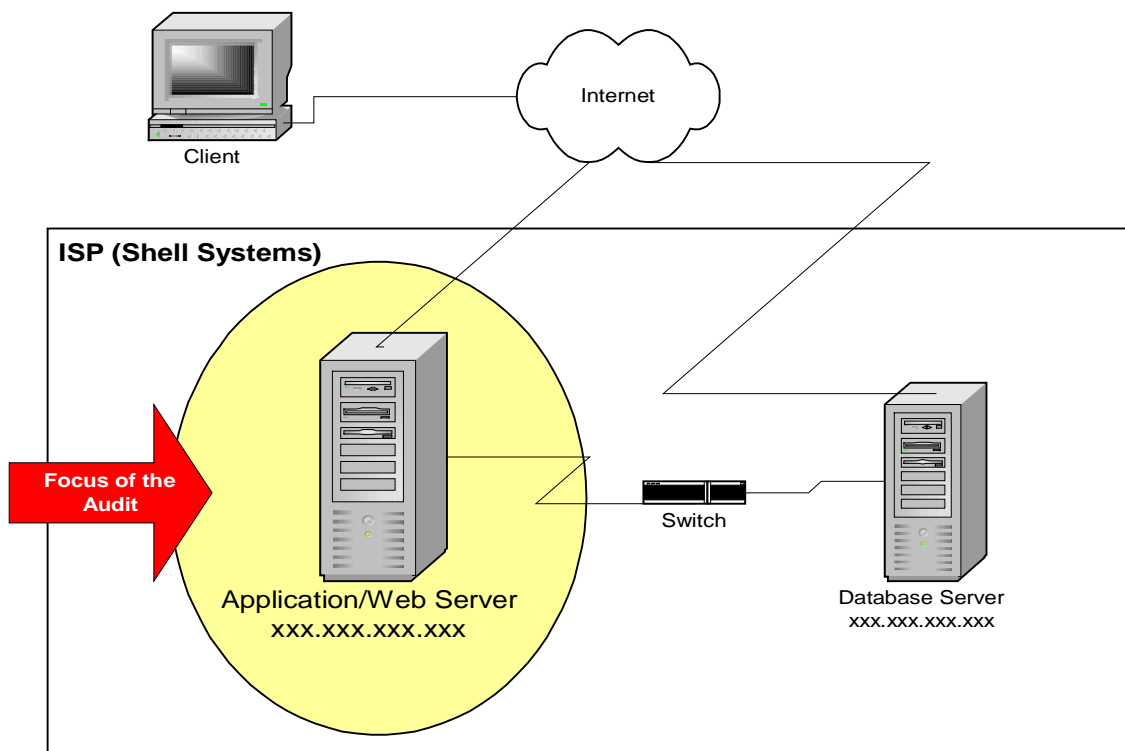
Site.example is a small online digital photo album business run by a single owner and administrator. *Site.example* outsources its technical infrastructure to a large Internet Service Provider and has recently experienced a series of external hacking attacks; thus interrupting business operations. *Site.example* would like an audit performed on its basic infrastructure components to determine areas of exposure and weaknesses within its technical environment. However, due to the nature of the business, this audit will not only need to focus on identifying the security risks and exposures from the technical standpoint, but it will also need to perform a more detailed analysis within its business operations. Because *Site.example* is a small business operated by one person and utilizes an outsourced service, additional security concerns and exposures need to be addressed. This audit will identify the risks and determine its associated vulnerabilities within *Site.example*'s technical and business operations environments. The audit will provide recommendations focused on maximizing the protection of its data while still maintaining functionality and usability for regular business operations.

1.2 Identify the System

1.2.1 System Environment

Site.example provides a website for users to store, share and network digital photographs. The overall environment of *Site.example* is composed of one database server and one web/application server. Each server runs Windows 2000 as the server operating system. The database runs SQL Server 2003 and stores data such as user details, photos and credit card information. This database is populated by user input from the Graphical User Interface that is supported by a separate web server. The web server is built on a Windows 2000 Server platform and runs Internet Information Services 5.0. This server is accessed on the front end from user input via the internet. On the backend, the server communicates with the database server to feed and retrieve requested data. These two servers are physically located at the Internet Service Provider in Atlanta, GA. Both servers are accessed and administered by the system owner, via terminal services, from the Administrator's home, New York City, NY, using a cable connection to the internet. The following diagram below depicts the environment for *Site.example*'s infrastructure.

© SANS Institute - Author retains full rights



1.2.2 Focus of the Audit

As identified in the above diagram, the focus of the audit will be the Application/Web Server. This is because of several reasons. The major application and service this server runs, Internet Information Services 5.0, has many known (and of course unknown) vulnerabilities associated with it. Because this system is accessed from the web, the system has many access points and is most exposed to external users. This system is housed at the Internet Service Provider, which can limit the control for the Administrator. The below table provides more detailed specifications for the Application/Web Server.

Web/Application Server xxx.xxx.xxx.xxx	
Hardware	
Make	• Dell
Model	• PowerEdge
Processor	• Dual 2.4 GHz Intel® Xeon
Memory	• 2 GB RAM and Two 36 GB 10K SCSI hard drive(s)
Software	
Operating System (including Service Pack Level)	• Windows 2000 Service Pack 4
Major Applications	• Internet Information Services 5.0
Access	
Internal Connections	<ul style="list-style-type: none"> • Connects to Client workstation via terminal services. • Connects to the internet • Connects to the Database server
Physical Location	• Atlanta, GA

Personnel Access	<ul style="list-style-type: none"> • Administrator • Shell Systems personnel
Functionality	
Business Purpose:	<ul style="list-style-type: none"> • Runs applications services and web service information

It should be noted that while this audit will focus on the Application/Web Server system, a complete audit should be performed on the other components identified within this environment.

1.3 Evaluating Risk

Risks can be defined as the potential impact of the system's exposure to a known or unknown vulnerability. Impacts of risk are evaluated through the potential loss to *confidentiality*, *integrity* and *availability* of the data. *Confidentiality* ensures that information resources are used only by those authorized to do so. *Integrity* indicates that the information should be protected from unauthorized or unintentional modification. Lastly, *Availability* ensures that information resources remain accessible whenever needed. This audit will focus on identifying risks that will pose potential threats to the loss of Confidentiality, Integrity and Availability to the data. It is important to remember that there must be a balance between security and business functionality. For example, solutions that address threats to confidentiality and integrity of data may also limit the availability of the data. Therefore, in responding to any potential threats, one must remember how this threat relates to the business functionality and needs.

There are two categories of risk which will be examined throughout this audit: procedural and technical risks. *Procedural risks* are associated with business operations, and its processes, and procedures. *Technical risks* are associated with the configurations and maintenance of the physical technical infrastructure. Due to the nature of *Site.example's* business, procedural and technical risks are identified as a function of the company's physical infrastructure, the principles of small business, and its outsourced arrangement with Internet Service Provider.

This audit will use the following criteria to evaluate the identified risks:

- **Control:** Describes how the given aspect of the business/system should exist and/or function. The "control" therefore is the definition of what *should* exist/occur.
- **Concern:** Identification of what could go wrong, both procedural and technical, with the control.
- **Likelihood:** Classification of how likely this could occur
- **Consequences:** Determination of the effects of an exploited risk and its impacts to confidentiality, integrity and availability of the data.

1.3.1 Business and Procedural Risk: *Site.example's* business is operated by one person. No established security processes, procedures nor checks and balances exist. As a small business, *Site.example* is confronted with concerns associated with limitations on budgets, resources, and functional expertise. Furthermore, *Site.example* uses an

Internet Service Provider, which therefore limits many physical as well as information security controls. These constraints create major obstacles to ensuring security best practices. The following table discusses these business and procedural risks.

1. Limited Resources		
	<i>Control:</i>	Organization should have skilled and available resources in order to effectively perform all necessary business operations.
	<i>Concern:</i>	Few and inexperienced resources are operating the <i>Site.example</i> business, and therefore, they cannot effectively manage all operations.
	<i>Likelihood:</i>	High- In small businesses, it is difficult to financially support many resources with specialized skills, such as security.
	<i>Consequences</i>	The number of resources working for <i>Site.example</i> is limited and they do not have the <u>time</u> or the <u>skills</u> to implement and follow appropriate security procedures and controls. An exploit can take advantage of this lack of knowledge and resources.
2. Budget Constraints		
	<i>Control:</i>	Industry best practice is to allocate 15% of the company's budget to Information Technology investment; this would include costs for addressing security.
	<i>Concern:</i>	Limited budgets will not be able to support the required hardware, tools, and resources required to securely operate the business.
	<i>Likelihood:</i>	High- In small and particularly start up businesses, funds are limited as they are funded by few investors. Therefore, operating budgets are at a minimum.
	<i>Consequences</i>	Budget does not exist to support the <u>hardware</u> , <u>tools</u> and <u>resources</u> required to support the existence of security processes and controls within the company. Therefore, in the case of an exploit, the appropriate tools and resources are not available to mitigate and remediate the incident.
3. Non-standardized security policies and procedures		
	<i>Control:</i>	A standardized set of processes should be implemented within any operation to ensure all security concerns are acknowledged and addressed. Examples of such processes would be the consistent monitoring of audit logs and verifying users/groups and permissions allowed into the systems.
	<i>Concern:</i>	Lack of these security processes indicates that neither attention nor efforts are made to address security needs. Furthermore, when a security incident does occur, there is no knowledge or guidance of what to do.
	<i>Likelihood:</i>	Medium- Basic business plans should include these standardized processes. Additionally, contracts with outsourcers should include these policies and procedures.
	<i>Consequences</i>	Business operates in an insecure environment with little awareness of what security vulnerabilities exist. In the event of an incident, business operations could cease as little knowledge exists on how to

		control it.
4.	Uncontrolled/monitored physical security and access control	
	<i>Control:</i>	The business should install physical security measures in order to protect both their physical and information assets. This would include appropriate locks to doors, desks and storage areas. Furthermore, there should be established controlled processes for people who wish to access them.
	<i>Concern:</i>	Without any physical security, there is no way of preventing or identifying unauthorized people from gaining access to proprietary and confidential data.
	<i>Likelihood:</i>	Medium- Most buildings and offices contain some form of physical security. However, the enforcement of this security is usually out of the business owner's control, as physical security is usually managed by an outsourced company.
	<i>Consequences</i>	Unauthorized people will gain access into physical areas and be able to gain access to proprietary and confidential data; thus compromising its confidentiality, integrity and availability.
5.	Nonexistent Backup and Storage procedures	
	<i>Control:</i>	Data stored in the system should be regularly backed up and stored in a secure place.
	<i>Concern:</i>	If data is not regularly backed up, compromises to the system could result in loss of all data which cannot be restored.
	<i>Likelihood:</i>	Medium- Back up of data should be a primary concern for the system administrator. In any system compromise, the data will certainly be altered if not lost.
	<i>Consequences</i>	If a system is compromised or mistakenly shut down and data is lost, <i>Site.example</i> potentially loses all information, which is detrimental to the operations of the company.

- 1.3.2 **Technical Risk:** From a technical perspective, risks are associated with known vulnerabilities and exploits. *Site.example*'s application and web server runs on Windows 2000 Server and IIS 5.0 which have known vulnerabilities and exploits associated with them. Without appropriate maintenance and knowledge of these vulnerabilities, *Site.example* runs a serious risk to external threats. The technical risks are outlined below:

1.	Default Installations of the Operating System	
	<i>Control:</i>	An "out of the box" installation of the operating system should never be trusted by system administrators. All operating systems should be uniquely configured according to the business requirements and appropriately hardened for security risks.
	<i>Concern:</i>	OS are running default installations which have many known security vulnerabilities/known exploits associated with them.
	<i>Likelihood:</i>	High- Many Administrators, particularly those with less security knowledge, trust the default installations.

	<i>Consequences</i>	It is easy for an attacker to determine probable vulnerabilities of the operating system when it is configured from the default settings. An attacker will attempt known attacks toward the system based on the default installation and compromise the system.
2. Default Installations of Major Application		
	<i>Control:</i>	The default “out of the box” installation of Internet Information Service 5.0 should be uniquely configured for business requirements and appropriately hardened for known security risks.
	<i>Concern:</i>	Applications which are running default installations have many known security vulnerabilities and exploits.
	<i>Likelihood:</i>	High- Many Administrators, particularly those with less security knowledge, trust the default installations.
	<i>Consequences</i>	An attacker will attempt known attacks toward the system based on the default installation and compromise the system.
3. Exposure to known Vulnerabilities/Exploits		
	<i>Control:</i>	Systems should be tested for and patched on a regular basis against known vulnerabilities.
	<i>Concern:</i>	Systems which are not hardened against known vulnerabilities can be easily compromised through known and frequent attacks, worms and viruses.
	<i>Likelihood:</i>	High- Regular maintenance/hardening of systems is often left to the responsibility of the administrator and seen as less important. Therefore, time is not spent toward understanding and learning old and new security vulnerabilities. This leaves the system unpatched and vulnerable.
	<i>Consequences</i>	Systems can be attacked by common/well known exploits such as buffer overflows, cross site scripting, and Denial of Service attacks.
4. Weak Perimeter Security		
	<i>Control:</i>	System should be protected by perimeter security controls such as a firewall to protect against external access and attacks.
	<i>Concern:</i>	If there is no layer of perimeter protection, access into systems are open to any and all external attacks.
	<i>Likelihood:</i>	Medium- A majority of ISPs enforce some form of perimeter protection. However, the strength of the firewall rules may be weak as they need to service a variety of needs.
	<i>Consequences</i>	Systems can be easily identified, accessed and compromised.
5. Insecure Data in Transit		
	<i>Control:</i>	Traffic between connected systems should not be seen to anyone eavesdropping on network. SSL should be used.
	<i>Concern:</i>	When the client machine (administrators console in NY) communicates with the servers stored at the ISP (Atlanta), information is sent in clear text.
	<i>Likelihood:</i>	High- Most Internet Service providers do not provide private connections.
	<i>Consequences</i>	Data is transferred in clear text across the internet. “Listeners” can capture, store or alter this data.

1.4 Current State of Practice

Currently, *Site.example* has no regular security auditing, vulnerability assessment or baseline practices. Therefore, this will be the first audit to be conducted these systems. The following process and resources will be used to audit *Site.example*'s system

1.4.1 Research and Documentation: The following sources have been consulted.

- SANs InfoSec Reading room (www.sans.org/rr) Provides series of articles/whitepapers discussing security concerns associated with Small Businesses, using Internet Service Providers, as well as technical documentation on default installations
- Microsoft Knowledge Base (www.support.microsoft.com) Provides articles and tools for determining vulnerabilities associated with Microsoft products (OS, Applications)
- Google Searches: Useful search terms within the security sections included: Security of Small Business, Internet Service Providers, Default Installation, IIS, and Security Budgets.

Below is a specific list of articles related to the specific topics covered throughout this paper:

Windows 2000 Server Security

- <http://www.sans.org/top20/>
 - The Sans Top 20 identifies the top vulnerabilities known to date. This is important to be aware of when conducting any audit and should be used to identify what major risks could be on your system. IIS is the number one Windows vulnerabilities on the list.
- <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/mbsahome.asp>
 - This link brings you to information and the download Microsoft Baseline Security Analyzer tool, which is a very helpful tool to identify missing patches and configurations on major Microsoft products (Operations System, IIS, SQL).
- <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/chklist/w2ksvrcl.asp>
 - This checklist is provided by Microsoft to help secure default installation of Windows 2000 Server.
- <http://support.microsoft.com/default.aspx?scid=kb;en-us;246261>
 - Information on Anonymous Connections- default installation
- <http://www.eventid.net/search.asp>. This site provides helpful information for different event log IDs.
- Security Windows 2000- Resource and reference book which provides detailed explanations on services, policies, and registry entries for Windows 2000 Operating system.

Internet Information Services 5.0 Security

- <http://www.sans.org/rr/paper.php?id=275>
 - This article provides more detailed information on security concerns of web servers running IIS and how to lock it down.
- <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/iis5cl.asp>
 - This checklist is provided by Microsoft to help secure the installation of IIS. This should be used when first configuring any IIS system and should be used to check current configurations.

Small Business/Home office Security concerns

- <http://www.sans.org/rr/paper.php?id=615>
 - This article goes into more detail on a “free” option for *home security*, ZoneAlarm, a personal firewall. This is a helpful option for cost efficient ways to securing a system.
- <http://www.sans.org/rr/paper.php?id=617>
 - This article, as titled, lists and explains security problems *for small companies*. Some risks it identifies, which is included in this audit, are: lack of technical knowledge, default or ‘outdated’ installations (set up is done by independent consultants who do not regularly update the system), lack of perimeter security, no backup processes, no written security policies or processes.
- http://searchsecurity.techtarget.com/originalContent/0,289142,sid14••_gci932898,00.html
 - This search security article addresses issues of IT and security budgets
- <http://antivirus.about.com/cs/beforeyoubuy/tp/aatpavwin.htm>
 - Article provides information regarding popular antivirus software

Internet Service Providers and Physical Security

- http://www.giac.org/practical/gsec/Kim_Hughes_GSEC.pdf
 - This paper identifies security issues and concerns when storing data at an ISP
- <http://www.itsc.state.md.us/oldsite/info/InternetSecurity/BestPractices/PhysSecurity.htm>
 - Discusses information regarding importance of physical security. This reference article was found from another GIAC paper- Patrick Boismenu's GSNA paper (Sept 5th, 2003)
- http://www.microsoft.com/serviceproviders/columns/isp_security.asp
 - This article provides a security *checklist for Internet Service Providers*. Some checklist items which are included in this audit are: limiting user's rights (people who have access to certain files and directories as well as the number of users on a system), testing firewalls, policy security, and physical security.
- <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/5min/5min-203.asp>
 - Article discussing importance of physical security for businesses.

Perimeter Security

- <http://computer.howstuffworks.com/nat3.htm>. Provides information how Network Address Translation works.
- <http://www.chebucto.ns.ca/~rakerman/trojan-port-table.html>. This article provides lists of dangerous ports and associated Trojans. This is a helpful reference after you have run a port scan against the system to identify what ports should and should not be open.

1.4.2 Tools: The following security tools will be used to obtain information and identify security vulnerabilities associated with the system:

- Nessus- This is a free Vulnerability Assessment tool. Download is available at www.nessus.org. Nessus identifies running services and open ports within the system scanned and identifies known vulnerabilities and exploits associated with them. *Nessus relies heavily on banner information and therefore can result in many false positives. Careful attention and investigation has to be made on the results of this tool.*
- nMap- Free port scanning tool which can be run against the system to determine open ports/services running on the system. Download available at www.insecure.org
- Microsoft Baseline Security Analyzer: Scans system to determine missing security patches as well as default installation/mis-configurations in Microsoft operating systems and applications
- Snort Sniffer tool: www.snort.org. Snort is a free network traffic monitoring tool which will be used to collect traffic packets as the web/application server is accessed.

1.4.3 Process

1. Written approval will be obtained from both *Site.example* and the ISP to perform the audit and use of the tools identified
2. User Ids and passwords will be created for access to system
3. Baseline and back up of the systems to be audited will be taken. This will provide an accurate depiction of the current state of the environment.
4. All relevant documents will be obtained from the client to begin procedural audit
5. Technical audit will be performed using the listed tools above

Assignment 2: Create an Audit Checklist

In order to assess *Site.example*'s susceptibility to the above risks, the following checklists have been created. There is a one-to-many relationship between the identified risks and the tests which need to be performed associated with that risk.

Each item within the checklist includes the following information:

- Reference: Provides information regarding research, associated articles and knowledge associated with this check
- Control Objective: States the purpose of the check
- Risk: Identifies what risk this check addresses and its possible consequences

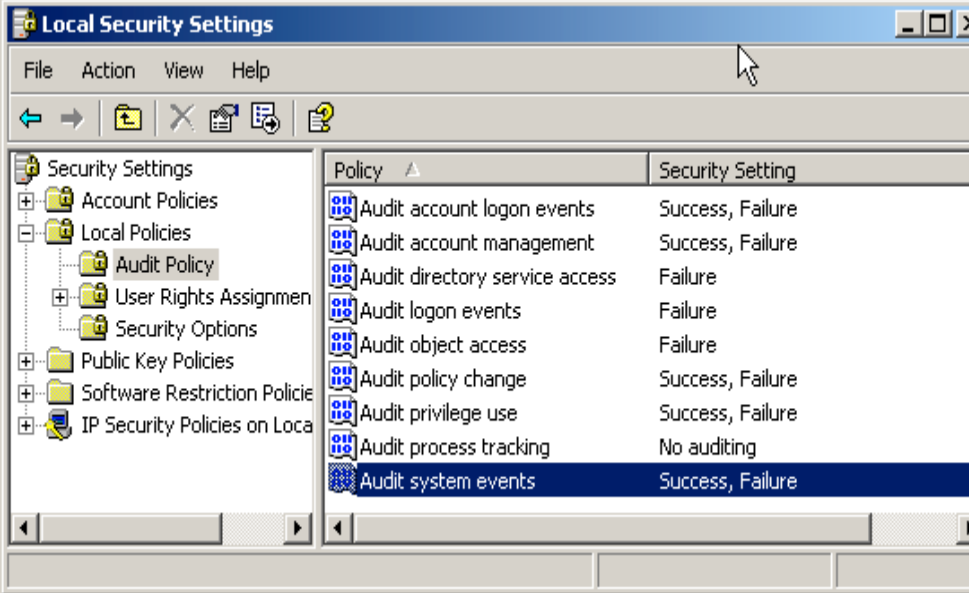
- **Compliance:** Determination if the system is compliant and under what conditions it is enabled or not enabled.
- **Testing:** Lists the tests, commands and tools that need to be used in order to perform the check
- **Objective/Subjective:** Identifies if this is a repeatable verifiable test (objective) or judgment or based on feedback

2.1 Technical Audit Checklist

The following checklists have been created to address each of the identified risks listed in section 1.3. Several checks and testing procedures will be performed in order to address each risk.

2.1.1 Technical Risk 1: Checklist for Default Installation of Operating Systems

Test 1	
Reference:	http://support.microsoft.com/default.aspx?scid=kb;en-us;246261 http://www.sans.org/top20/#W5
Control Objective	Verify that the system restricts anonymous connections.
Risk:	Null sessions can be used to display information about users, groups, shares and password policies. Default Installations of Windows 2000 Server does not protect against the ability to establish null sessions and to connect to the IPC\$ share.
Compliance	Response in the command line should be: "System error 5 has occurred. Access is denied." If you receive "System error 5 has occurred. Access is denied", then your system is not accepting null sessions. If you receive "The command completed successfully," then that means that your system is vulnerable.
Testing	1. On the server machine, open the command prompt locally 2. Enter the following command into the command prompt: >net use \\xxx.xxx.xxx.xxx\IPC\$ ""/user: "" 3. Press Enter
Objective/ Subjective	Objective test. Results are generated from a repeatable and verifiable process and/or tool.
<i>To be completed after the test:</i>	
Successful?	
Result Details:	
Stimulus/	Stimulus

Response																					
Test 2																					
Reference:	http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/chklist/w2ksvrcl.asp http://support.microsoft.com/default.aspx?scid=kb;en-us;300549 http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/entserver/sag_seconceptsaudit.asp																				
Control Objective	Verify that the system <u>has been configured</u> to collect security events.																				
Risk:	Out of the box installations of Windows 2000 Server does not enable security event logging. Without security event logging, there is no record of who has attempted and/or gained access to the system and files. This is important in the event of a system compromise.																				
Compliance	<p>The security event log policy should capture for success and failure according to the following (based on Microsoft best practices):</p>  <table border="1"> <thead> <tr> <th>Policy</th> <th>Security Setting</th> </tr> </thead> <tbody> <tr> <td>Audit account logon events</td> <td>Success, Failure</td> </tr> <tr> <td>Audit account management</td> <td>Success, Failure</td> </tr> <tr> <td>Audit directory service access</td> <td>Failure</td> </tr> <tr> <td>Audit logon events</td> <td>Failure</td> </tr> <tr> <td>Audit object access</td> <td>Failure</td> </tr> <tr> <td>Audit policy change</td> <td>Success, Failure</td> </tr> <tr> <td>Audit privilege use</td> <td>Success, Failure</td> </tr> <tr> <td>Audit process tracking</td> <td>No auditing</td> </tr> <tr> <td>Audit system events</td> <td>Success, Failure</td> </tr> </tbody> </table>	Policy	Security Setting	Audit account logon events	Success, Failure	Audit account management	Success, Failure	Audit directory service access	Failure	Audit logon events	Failure	Audit object access	Failure	Audit policy change	Success, Failure	Audit privilege use	Success, Failure	Audit process tracking	No auditing	Audit system events	Success, Failure
Policy	Security Setting																				
Audit account logon events	Success, Failure																				
Audit account management	Success, Failure																				
Audit directory service access	Failure																				
Audit logon events	Failure																				
Audit object access	Failure																				
Audit policy change	Success, Failure																				
Audit privilege use	Success, Failure																				
Audit process tracking	No auditing																				
Audit system events	Success, Failure																				
Testing	<ol style="list-style-type: none"> 1. Open the Control Panel on the server 2. Go to Administrative Tools -> Local Security Policy 3. Click on Local Policy-> Audit Policies 4. Compare settings with the above displayed settings 																				
Objective/ Subjective	Objective test. Results are generated from a repeatable and verifiable process and/or tool.																				
<i>To be completed after the test:</i>																					
Successful?																					

<i>Result Details:</i>	
<i>Stimulus/ Response</i>	

Test 3	
Reference:	http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/chklist/w2ksvrcl.asp http://support.microsoft.com/default.aspx?scid=kb;en-us;300549 http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/entserver/sag_seconceptaudit.asp http://www.microsoft.com/windows2000/en/datacenter/help/default.asp?url=/windows2000/en/datacenter/help/els_use_logs_troubleshoot.htm http://www.eventid.net/search.asp
Control Objective	Verify the system's security event logs are being collected by the system.
Risk:	The security log can record security events such as valid and invalid logon attempts as well as events related to accessing resources. An administrator can specify what events are recorded in the security log. For example, if you have enabled logon auditing, attempts to log on to the system are recorded in the security log. Out of the box installations of Windows 2000 Server does not enable security event logging. Therefore, there is no evidence for when a user accesses or attempts to access the system.
Compliance	The Security log in the event viewer shows a success logon attempt was made by the user with the corresponding event ID 528.
Testing	<ol style="list-style-type: none"> 1. Log into the server system. 2. Go to Control Panel-> Event Viewer 3. Click on the Security Events 4. Sort according to Event ID number 5. Locate ID 528 and double-click. 6. Match "user" field with the credentials used to log into the system
Objective/ Subjective	Objective test. Results are generated from a repeatable and verifiable tool.
<i>To be completed after the test:</i>	
<i>Successful?</i>	
<i>Result Details:</i>	
<i>Stimulus/ Response</i>	<i>Stimulus</i>

Test 4	
Reference:	http://www.microsoft.com/technet/treeview/default.asp?url=/technet/

	security/tools/Tools/mbsahome.asp The Microsoft Baseline Security Analyzer tool scans a systems registry to determine what service packs and Microsoft patches the system is missing.
Control Objective	Verify that the system service pack and patch level is up to date.
Risk:	Out of the box installations of Windows 2000 Server does not include any updates and fixes to the OS since it has been developed. Exploit code is developed based on these known weaknesses of the OS. Therefore, worms and viruses and hacking attacks can easily compromise systems which are not patched. Viruses and hacking attacks can be developed as soon as two months, if not sooner, after a patch is released; therefore, the likelihood of being exploited is very high. An example of this would be the Blaster worm.
Compliance	System should be running service pack level 4 and with no additional patches missing. Note, there is a known issue documented in article (Q306460) in which the tool cannot pick up these patches for Win 2k Server: MS01-022, MS02-008, MS02-053, MS02-064, MS02-065, MS03-008. Therefore, this will be recorded in the report as "cannot be determined."
Testing	1. Open MBSA tool on the server system, select "Scan a Computer". 2. Select Scan local computer. Check the 'Windows Vulnerabilities' and 'Security Update' 3. Results will appear in a new window. 4. Determine what hotfixes are missing. 5. From the Microsoft website links provided in the results of MBSA, determine the file versions which are not compliant 6. Run a search in Windows to locate these files and verify the version is out of date.
Objective/ Subjective	Objective test. Results are generated from a repeatable and verifiable tool.
<i>To be completed after the test:</i>	
Successful?	
Result Details:	
Stimulus/ Response	

2.1.2 Technical Risk 2: Checklist for Default installation of ISS

Test 5:	
Reference:	http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/mbsahome.asp http://www.sans.org/rr/paper.php?id=275

	MSBA checks for hotfixes Microsoft applications such as IIS to determine appropriate updates and security configurations have been installed.
Control Objective	Verify that all Security Patches for IIS 5.0 are installed
Risk:	Exploit code exists for vulnerabilities identified in IIS 5.0. Without having these known vulnerabilities patched, the system can be easily exploitable through attacks and viruses. Examples of this would be Code Red.
Compliance	The tool should produce results that there are no missing patches related to IIS.
Testing	<ol style="list-style-type: none"> 1. Open MBSA tool on the server system, select "Scan a Computer". 2. Select Scan local computer. Check the 'ISS Vulnerabilities' 3. Results will appear in a new window. 4. Determine what hotfixes are missing. 5. From the Microsoft website links provided in the results of MBSA, determine the file versions which are not compliant 6. Run a search in Windows to locate these files and verify the version is out of date.
Objective/ Subjective	Objective test. Results are generated from a repeatable and verifiable tool.
<i>To be completed after the test:</i>	
Successful?	
Result Details:	
Stimulus/ Response	

Test 6:	
Reference:	http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/iis5cl.asp http://www.sans.org/rr/paper.php?id=275
Control Objective	Verify that access to IIS files is restricted by not allowing users with non-administrator privileges to delete IIS files.
Risk:	By not limiting access to directories and files, malicious users and attackers can access, add and remove files, affecting the confidentiality and integrity of system.
Compliance	<p>Permission should be denied when trying to access files with the following file types:</p> <p style="text-align: center;">File Type</p> <p>CGI (.exe, .dll, .cmd, .pl)</p> <p>Script files (.asp)</p>

	<p>Include files (.inc, .shtm, .shtml)</p> <p>Static content (.txt, .gif, .jpg, .html)</p>
Testing	<ol style="list-style-type: none"> 1. Log into the server machine using the non-administrator account. 2. Open to the following directory: C:\inetpub\wwwroot\ 3. Click on the following file: "mmc.gif" 4. Right click and press delete. 5. Click yes, send it to the recycle bin 6. Navigate to the recycle bin and locate the file
Objective/ Subjective	Objective test. Results can be viewed by repeatable process.
<i>To be completed after the test:</i>	
Successful?	
Result Details:	
Stimulus/ Response	Stimulus

Test 7:	
Reference:	http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/iis5cl.asp http://www.sans.org/rr/paper.php?id=275 http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-023.asp
Control Objective	Verify that unused script mappings are removed from the IIS configuration.
Risk:	Unknown services and files can be exploited. By turning off unnecessary features, you are reducing the attack surface available to attackers.
Compliance	<p>The following script extensions should not exist within the configuration menu of IIS :</p> <p style="text-align: center;">Site.Example does not use... Remove this entry:</p> <p>Web-based password reset .htr</p> <p>Internet Database Connector (all IIS 5 Web sites should use ADO or similar technology) .idc</p> <p>Server-side Includes</p>

	<p>.stm, .shtm, and .shtml</p> <p>Internet Printing .printer</p> <p>Index Server .htw, .ida and .idq</p>
Testing	<ol style="list-style-type: none"> 1. Open Internet Services Manager. 2. Right-click the Web server, and choose Properties. 3. Click Master Properties 4. Select WWW Service, click Edit, click HomeDirectory, and then click Configuration 5. Determine if any of the following script extensions exist: <ul style="list-style-type: none"> .htr .idc .stm, .shtm, and .shtml .printer .htw, .ida and .idq <p>http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/iis5cl.asp</p>
Objective/ Subjective	Objective test. Results are generated from a repeatable and verifiable tool.
To be completed after the test:	
Successful?	
Result Details:	
Stimulus/ Response	
Test 8:	
Reference:	<p>http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/iis5cl.asp</p> <p>http://www.sans.org/rr/paper.php?id=275</p> <p>http://xforce.iss.net/xforce/xfdb/2229</p>

Control Objective	Verify that no sample IIS sites or documentation are installed within the local directory.
Risk:	Sample IIS sites can cause hanging problems and are used in denial of service attacks.
Compliance	<p>No directories should be found holding sample sites as listed below.</p> <p style="text-align: center;">Sample Virtual Directory Location</p> <p>IIS Samples \IISamples c:\inetpub\iissamples</p> <p>IIS Documentation \IISHelp c:\winnt\help\iishelp</p>
Testing	<ol style="list-style-type: none"> 1. Right click on the Start Icon 2. Go to Search 3. Under "search for file or folders" type in "inetpub\iissamples" 4. Click Search 5. Again, type "winnt\help\iishelp" 6. Click Search 7. Attempt to navigate to the directories: <p>c:\inetpub\iissamples</p> <p>c:\winnt\help\iishelp</p>
Objective/ Subjective	Objective test. Results are generated from a repeatable and verifiable tool.
To be completed after the test:	
Successful?	
Result Details:	
Stimulus/ Response	

2.1.3 Technical Risk 3: Checklist for Exposure to Known Vulnerabilities and Exploits

Test 9:	
Reference:	http://www.sans.org/top20/
Control Objective	Verify that the system is protected against the following Sans Top

	<p>Windows vulnerabilities:</p> <p>W1 Internet Information Services (IIS)</p> <p>W2 Microsoft SQL Server (MSSQL)</p> <p>W3 Windows Authentication</p> <p>W4 Internet Explorer (IE)</p> <p>W5 Windows Remote Access Services</p> <p>W6 Microsoft Data Access Components (MDAC)</p> <p>W7 Windows Scripting Host (WSH)</p> <p>W8 Microsoft Outlook and Outlook Express</p> <p>W9 Windows Peer to Peer File Sharing (P2P)</p> <p>W10 Simple Network Management Protocol (SNMP)</p>
Risk:	As indicated by being on the Sans top 10 Windows vulnerabilities, existence of these holes on the system make the system extremely open to common attacks.
Compliance	The Nessus report should not show any security holes associated with the above listed vulnerabilities. Note, false positives result when the results of the scan indicate something is vulnerable, when in fact it is not. These will be accessed when reviewing all the results.
Testing	<ol style="list-style-type: none"> 1. Launch the Nessus GUI 2. From the Plugins tab, select "enable all but dangerous plugins" 3. From the Scan Options tab, check "Optimize the Test" and "Safe Checks" 4. In the target selection tab, enter the IP address. Then click Start Session
Objective/ Subjective	Objective test. Results are generated from a repeatable and verifiable tool.
<i>To be completed after the test:</i>	
<i>Successful?</i>	
<i>Result Details:</i>	
<i>Stimulus/ Response</i>	

Test 10:	
Reference:	http://www.sans.org/rr/paper.php?id=615 http://antivirus.about.com/cs/beforeyoubuy/tp/aatpavwin.htm
Control Objective	Verify that the system has antivirus software installed and it is running updates automatically.
Risk:	Systems not running this software cannot block against widely spread viruses and there is no way of determining if the system is infected. New updates and viruses are available almost weekly.
Compliance	An antivirus software such as Norton or McAfee (see http://antivirus.about.com/cs/beforeyoubuy/tp/aatpavwin.htm for a

	list of software) should be installed and running.
Testing	<ol style="list-style-type: none"> 1. Go to Start-> Control Panel-> Add/Remove Programs 2. Locate installation of Antivirus System 3. Open the Antivirus System software and go to properties 4. Determine the latest virus update received on the system
Objective/ Subjective	Objective test. Results are generated from a repeatable and verifiable process.
<i>To be completed after the test:</i>	
<i>Successful?</i>	
<i>Result Details:</i>	
<i>Stimulus/ Response</i>	

2.1.4 Technical Risk 4: Checklist for Weak Perimeter Security

Test 11:	
Reference:	http://www.microsoft.com/serviceproviders/columns/isp_security.asp http://www.giac.org/practical/gsec/Kim_Hughes_GSEC.pdf
Control Objective	Verify that the ISP provides documentation to its customers indicating whether or not there is a firewall that exists at the edge of the network.
Risk:	If there is no layer of perimeter protection, access into systems are open to any and all external attacks. Moreover, because the systems are housed at an ISP, there is a strong possibility that the perimeter protection will be very weak, as it needs to service many needs.
Compliance	Documentation is provided by the ISP which agrees to provide a level of perimeter security for the ISP network.
Testing	<ol style="list-style-type: none"> 1. Obtain Security documentation from ISP. 2. Locate firewall rules
Objective/ Subjective	Subjective- Based on input received from the business owner.
<i>To be completed after the test:</i>	
<i>Successful?</i>	
<i>Result Details:</i>	
<i>Stimulus/ Response</i>	

Test 12:	
Reference:	http://www.microsoft.com/serviceproviders/columns/isp_security.asp http://www.cyber.ust.hk/handbook4/04_hb4.html#What%20services

	%20should%20be%20monitored
Control Objective	Verify that the server does not reply to a ping request.
Risk:	A standard firewall configuration rule is to reject the return of an ICMP incoming request. This means that when sending an echo request from the outside the network, one should not receive an echo reply. Having echo reply enabled on firewalls allows hackers to obtain information about the server such as IP address, which attackers can then more specifically target their attacks.
Compliance	Echo request should not return an echo reply such as: Reply from: xxxx.xxx.xxx.xxx where xxx.xxx.xxx.xxx is the server IP address.
Testing	1. Open the command prompt (Start-> Run 'cmd') on a machine outside the ISP network. 2. In the command prompt type, "ping <i>www.site.example</i> " 3. Press Enter
Objective/ Subjective	Objective- Results are generated from a repeatable and verifiable tool.
<i>To be completed after the test:</i>	
<i>Successful?</i>	
<i>Result Details:</i>	
<i>Stimulus/ Response</i>	<i>Stimulus</i>

Test 13:	
Reference:	http://www.microsoft.com/serviceproviders/columns/isp_security.asp http://www.cyber.ust.hk/handbook4/04_hb4.html#What%20services%20should%20be%20monitored
Control Objective	Verify that when port scanned, only the http(s) (port 80 and 8080) is seen in the results.
Risk:	The ability to reach the targeted host using a port scanning tool and obtaining open ports and services would indicate that very weak, if any, perimeter security exists. Only port 80 (web) should be seen on a web server. The ability for an attack to obtain this information makes it easy for attackers to determine their targets. This is a common "first step" for hackers.
Compliance	The scan tool should return the results of "port 80/tcp open http".

Testing	<ol style="list-style-type: none"> 1. Set up the scanning machine outside the internal ISP network. 2. Open the command prompt (Start-> Run 'cmd') 3. Type 'nmap -sS xxx.xxx.xxx.xxx.' (where -sS is syn stealth mode 'xxx.xxx.xxx.xxx' is the target host) 3. Enter 4. Results of the port scan will show in the command prompt screen.
Objective/ Subjective	Objective- Results are generated from a repeatable and verifiable tool.
<i>To be completed after the test:</i>	
Successful?	
Result Details:	
Stimulus/ Response	Stimulus

Test 14:	
Reference:	http://computer.howstuffworks.com/nat3.htm
Control Objective	Verify that Network Address translation (NAT) occurs when attempting to access site.example.
Risk:	NAT is used to protect specific IP addresses (machine information) from leaving the internal network. If attackers can determine a specific machine's IP address, they can run more targeted attacks against the system. NAT should occur at the firewall.
Compliance	When attempting to ping the website URL, the actual internal reserved IP address is not displayed.
Testing	<p>From the server system:</p> <ol style="list-style-type: none"> 1. Log into the server system 2. Open the command prompt, type "IPConfig" <p>From outside the internal network (not on the server machine):</p> <ol style="list-style-type: none"> 1. Open the command prompt 2. Type "ping www.site.example" 3. Determine if the reply IP address matched that of the IP address obtained from the server system
Objective/ Subjective	Objective- Results are generated from a repeatable and verifiable tool.
<i>To be completed after the test:</i>	
Successful?	
Result Details:	
Stimulus/ Response	Stimulus

2.1.5 Technical Risk 5: Checklist for InSecure Data in Transit

Test 15:	
-----------------	--

Reference:	http://www.giac.org/practical/gsec/Kim_Hughes_GSEC.pdf
Control Objective	Verify that the only way to remotely administer the server at the ISP is through a secure (encrypted) connection.
Risk:	All traffic and sensitive data sent by the remote administrator to the server at the ISP should be sent via a protected channel. If it is not, this data can be picked up and viewed by an attacker sniffing the network
Compliance	Secure (encrypted) means of communication is used to log into the system.
Testing	<ol style="list-style-type: none"> 1. Obtain information from the administrator how he accesses the server located at the ISP. 2. What services does he use?
Objective/ Subjective	Subjective test. Based on results received from an interview.
<i>To be completed after the test:</i>	
Successful?	
Result Details:	
Stimulus/ Response	

Test 16:	
Reference:	http://www.giac.org/practical/gsec/Kim_Hughes_GSEC.pdf
Control Objective	Verify that someone cannot remotely log into the system to perform administrative activities (such as connections through terminal services) through an insecure connection.
Risk:	All traffic and sensitive data sent from the administrator to the remote system at the ISP could be seen and captured by eavesdroppers sitting on the internet; therefore, compromising integrity and confidentiality of the data.
Compliance	Connection is denied when attempting to log into the system via terminal services without strong credentials.
Testing	<ol style="list-style-type: none"> 1. Launch terminal services 2. Connect to: XXX.XXX.XXX.XXX 3. Log in with User ID and Password
Objective/ Subjective	Objective test. Results are generated from a repeatable and verifiable tool.
<i>To be completed after the test:</i>	

<i>Successful?</i>	
<i>Result Details:</i>	
<i>Stimulus/ Response</i>	<i>Stimulus</i>

Test 17:	
Reference:	http://www.giac.org/practical/gsec/Kim_Hughes_GSEC.pdf
Control Objective	Verify that the data entered into <i>site.example</i> is not sent in clear text, such as user ID and password.
Risk:	When sending sensitive data across the Internet, there is a very high risk that hackers are sniffing the HTTP connection. There is a risk that the hacker will capture your data in transit to the ISP if the connection is not encrypted between the client and the ISP. User names and passwords can be obtained.
Compliance	The user ID and password used to log into the website will not be seen in the log files.
Testing	<ol style="list-style-type: none"> 1. From outside the ISP network, run snort using the following commands: 2. In the command prompt, navigate to the snort executable folder and type: snort -vde -l ./log. Press enter. This will begin the packet sniffing tool. 3. Launch Internet Explorer and enter the website. 4. Enter user ID and password and log into the site. 5. Click control-C in the command prompt and search the data for sensitive information.
Objective/ Subjective	Objective test. Results are generated from a repeatable and verifiable tool.
<i>To be completed after the test:</i>	
<i>Successful?</i>	
<i>Result Details:</i>	
<i>Stimulus/ Response</i>	

2.2 Procedural and Business Audit Checklists

2.2.1 Procedural Risk 1: Budget Constraints

Test 18:	
Reference:	http://www.sans.org/rr/paper.php?id=617 http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci932898,00.html

Control Objective	Verify that <i>Site.example</i> has allocated 15% (industry average) of the companies' budget to IT and 5% of this toward security needs.
Risk:	Lack of budget means lack of security equipment and ability to address security problems. This leaves business with no security mechanisms.
Compliance	Business plan will show that a 5% of the IT budget is specifically allocated to security administration.
Testing	1. Locate Business Plan and Budget numbers 2. Request information to CFO 3. Obtain receipts of security related purchases
Objective/ Subjective	Objective- A business plan will be available which will demonstrate how the budget is allocated as well as evidence for purchases.
<i>To be completed after the test:</i>	
<i>Pass/Fail?</i>	
<i>Result Details:</i>	
<i>Stimulus/ Response</i>	

2.2.2 Procedural Risk 2: Limited Resources

Test 19	
Reference:	http://www.sans.org/rr/paper.php?id=617
Control Objective	Verify that an Administrator or employee has been allocated to administer security needs. Employee should be appropriately trained and experienced.
Risk:	Lack of staff and resources allocated to administering security makes it easier to target attacks on small businesses.
Compliance	Credentials of employee(s) should indicate the person has experience and/or training for administering security to the network.
Testing	1. Interview Employees 2. Obtain employee credentials
Objective/ Subjective	Subjective- Based upon feedback from personnel and documentation. Security personnel should be available to interview and supply you their credentials.
<i>To be completed after the test:</i>	
<i>Successful?</i>	
<i>Result Details:</i>	
<i>Stimulus/ Response</i>	

2.2.3 Procedural Risk 3: Non-standardized security policies and procedures

Test 20:	
Reference:	http://www.microsoft.com/technet/treeview/default.asp?url=/technet/

	security/chklist/w2ksvrcl.asp http://support.microsoft.com/default.aspx?scid=kb;en-us;300549 http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/entserver/sag_seconceptaudit.asp http://www.microsoft.com/windows2000/en/datacenter/help/default.asp?url=/windows2000/en/datacenter/help/els_use_logs_troubleshoot.htm http://www.eventid.net/search.asp
Control Objective	Verify the system's security event logs are being collected by the system.
Risk:	The security log can record security events such as valid and invalid logon attempts as well as events related to accessing resources. An administrator can specify what events are recorded in the security log. For example, if you have enabled logon auditing, attempts to log on to the system are recorded in the security log. Out of the box installations of Windows 2000 Server does not enable security event logging. Therefore, there is no evidence for when a user accesses or attempts to access the system.
Compliance	The Security log in the event viewer shows a success logon attempt was made by the user with the corresponding event ID 528.
Testing	<ol style="list-style-type: none"> 1. Log into the server system. 2. Go to Control Panel-> Administrative Tools -> Event Viewer 3. Click on the Security Events 4. Sort according to Event ID number 5. Locate ID 528 and double-click. 6. Match "user" field with the credentials used to log into the system
Objective/ Subjective	Objective test. Results are generated from a repeatable and verifiable tool.
<i>To be completed after the test:</i>	
Successful?	
Result Details:	
Stimulus/ Response	Stimulus

Test 21:	
Reference:	http://www.sans.org/rr/paper.php?id=617
Control Objective	Verify that system access (users and groups) are monitored and controlled.
Risk:	Addition of users and groups to the system provide an extended means to gain access to the system and should be regularly reviewed for changes.
Compliance	Users and Groups are maintained in a systematic process.

	Documentation should exist which would demonstrate that users and groups are reviewed regularly. Such documentation could include snap shots of the 'user and groups' or a spreadsheet which compares users and groups on routine basis.
Testing	<ol style="list-style-type: none"> 1. Interview Employees 2. Obtain documentation/evidence of past audit logs 3. Obtain Security policies/procedures document
Objective/ Subjective	Subjective/Objective- Interviews with personnel should demonstrate that this process is followed. Furthermore, physical evidence (files/documentation) should exist which lists these users and groups.
<i>To be completed after the test:</i>	
<i>Pass/Fail?</i>	
<i>Result Details:</i>	
<i>Stimulus/ Response</i>	

Test 22:	
Reference:	http://www.sans.org/rr/paper.php?id=617
Control Objective	Verify that systems undergo regular security vulnerability assessments.
Risk:	Systems are unpatched and vulnerable to known attacks.
Compliance	There is evidence of regular vulnerability assessments.
Testing	<ol style="list-style-type: none"> 1. Interview Employees 2. Obtain documentation/evidence of vulnerability assessments 3. Obtain Security policies/procedures document
Objective/ Subjective	Subjective- Based upon feedback from personnel
<i>To be completed after the test:</i>	
<i>Pass/Fail?</i>	
<i>Result Details:</i>	
<i>Stimulus/ Response</i>	

2.2.4 Procedural Risk 4: Uncontrolled/monitored physical security and access control

Test 23:	
Reference:	http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/5min/5min-203.asp http://www.itsc.state.md.us/oldsite/info/InternetSecurity/BestPractices/PhysSecurity.htm

Control Objective	Verify that all rooms at the ISP should be locked and access is only available to a small and known number of people.
Risk:	Systems which are not physically protected are available for anyone to gain physical access, attempt to log into the server and even physically steal this system. Thus, system and system information is compromised.
Compliance	Policy and process is followed which limits who has access to the system physically and it is appropriately secured.
Testing	<ol style="list-style-type: none"> 1. Obtain physical access policy and process from contract 2. Review the list of personnel that has been able to access the system
Objective/ Subjective	Objective- Based upon feedback from personnel and documentation received
<i>To be completed after the test:</i>	
<i>Pass/Fail?</i>	
<i>Result Details:</i>	
<i>Stimulus/ Response</i>	

Test 24:	
Reference:	http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/5min/5min-203.asp http://www.itsc.state.md.us/oldsite/info/InternetSecurity/BestPractices/PhysSecurity.htm
Control Objective	Verify that all rooms at the administrator's site (NY) should be locked and access is only available to a small and known number of people.
Risk:	Systems which are not physically protected are available for anyone to gain physical access, attempt to log into the server and even physically steal this system. Thus, the system and system information is compromised.
Compliance	Policy and process is followed which limits who has access to the system physically and it is appropriately secured.
Testing	<ol style="list-style-type: none"> 1. Obtain physical access policy and process from contract 2. Review the list of personnel that has been able to access the system
Objective/ Subjective	Objective- Based upon feedback from personnel and documentation received
<i>To be completed after the test:</i>	
<i>Pass/Fail?</i>	
<i>Result Details:</i>	
<i>Stimulus/ Response</i>	

2.2.5 Procedural Risk 5: Absent Backup and Storage procedures

Test 25:	
Reference:	http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/maintain/opsguide/secadmog.asp
Control Objective	Verify that regular backup procedures are followed.
Risk:	In the event of a system compromise, information will be lost and unable to restore.
Compliance	Backup procedures and files exist and are stored securely in an off site location.
Testing	1. Locate physical backups 2. Obtain documentation for the back up process
Objective/ Subjective	Objective- locate physical backups on the system.
<i>To be completed after the test:</i>	
Pass/fail?	
Result Details:	
Stimulus/ Response	

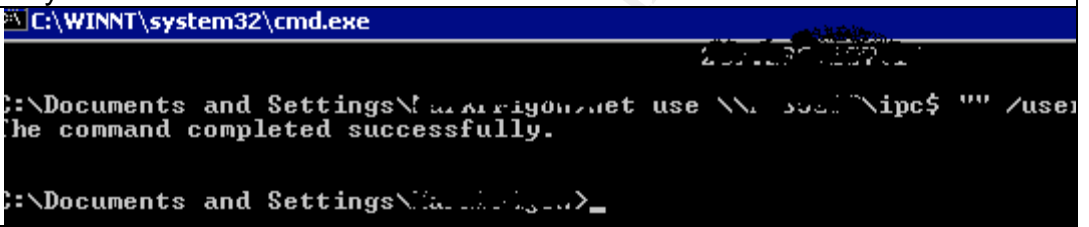
Assignment 3- Audit Evidence

3.1 Conduct the Audit

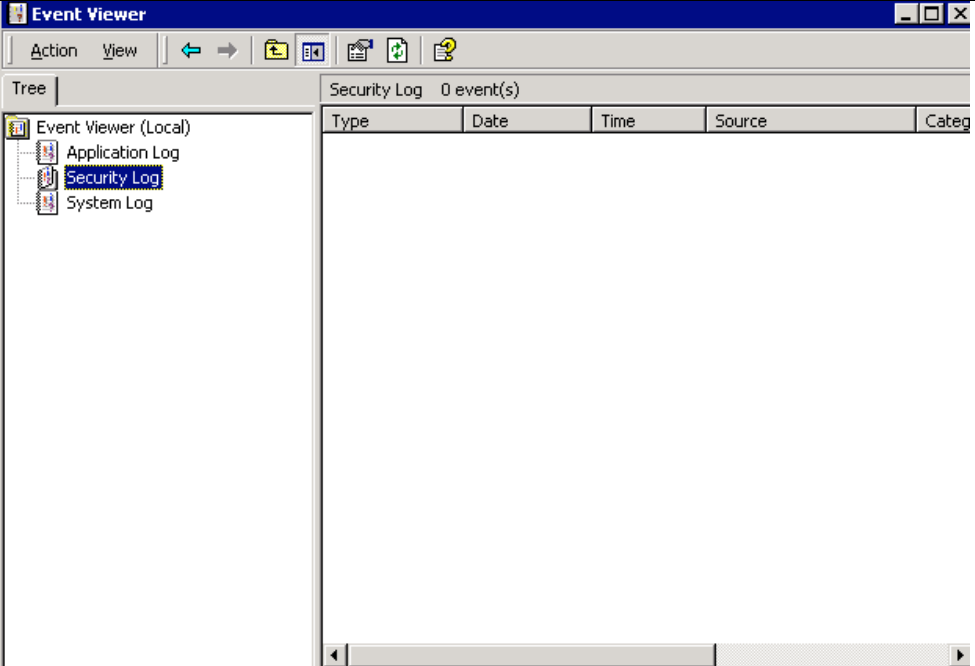
The following 10 items have been chosen to from the above checklist and the results shown.

1- 2.1.1 Technical Risk 1: Check for Default installation of Operating Systems

Test 1	
Reference:	http://support.microsoft.com/default.aspx?scid=kb;en-us;246261 http://www.sans.org/top20/#W5
Control Objective	Verify that the system restricts anonymous connections.
Risk:	Null sessions can be used to display information about users, groups, shares and password policies. Default Installations of Windows 2000 Server does not protect against the ability to establish null sessions and to connect to the IPC\$ share.
Compliance	Response in the command line should be: "System error 5 has occurred. Access is denied." If you receive "System error 5 has occurred. Access is denied", then your

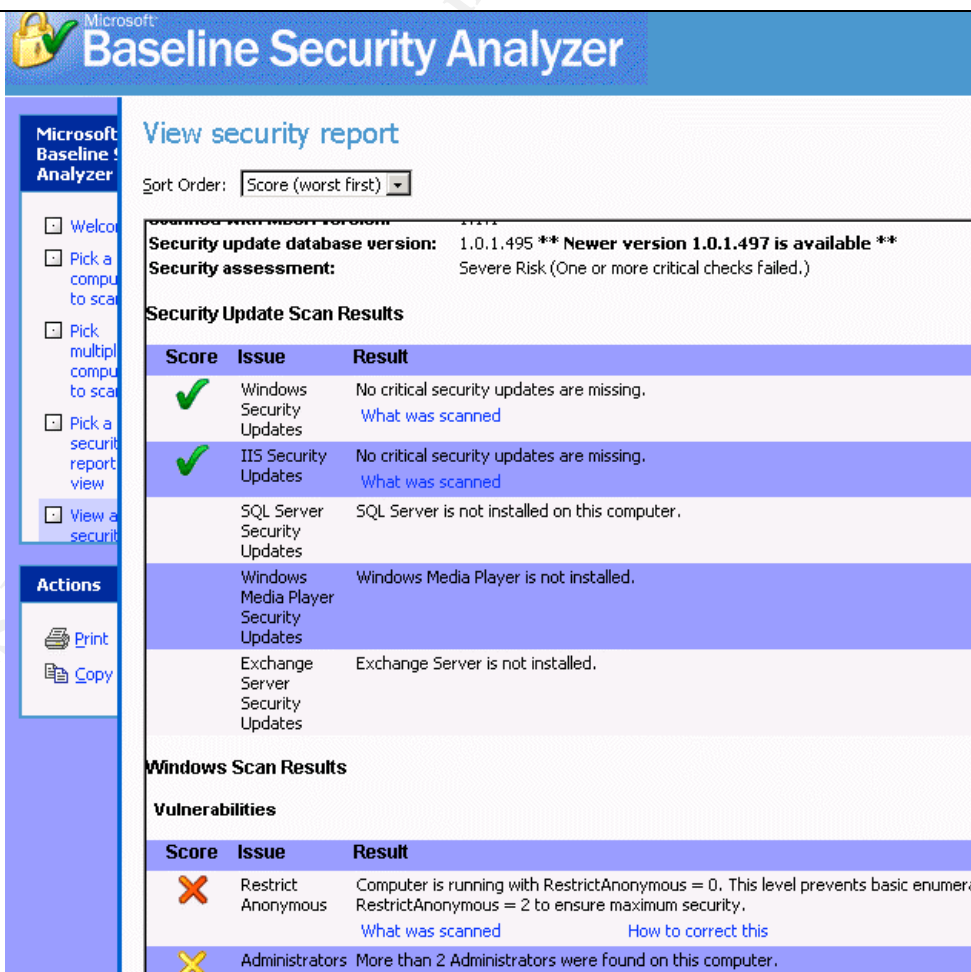
	<p>system is not accepting null sessions.</p> <p>If you receive "The command completed successfully." Then that means that your system is vulnerable.</p>
Testing	<ol style="list-style-type: none"> 1. On the server machine, open the command prompt locally 2. Enter the following command into the command prompt: >net use \\xxx.xxx.xxx.xxx \IPC\$ "" /user: "" 3. Press Enter
Objective/ Subjective	Objective test. Results are generated from a repeatable and verifiable process and/or tool.
To be completed after the test:	
Successful ?	Fail. Was not able to reach the actual system. This does not tell you either way if null sessions can be established.
Result Details:	
Stimulus/ Response	Stimulus

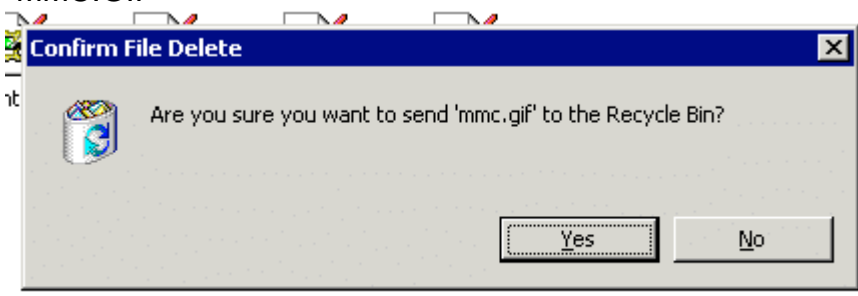
Test 3	
Reference:	http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/chklist/w2ksvrcl.asp http://support.microsoft.com/default.aspx?scid=kb;en-us;300549 http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/entserver/sag_seconceptaudit.asp http://www.microsoft.com/windows2000/en/datacenter/help/default.asp?url=/windows2000/en/datacenter/help/els_use_logs_troubleshoot.htm http://www.eventid.net/search.asp
Control Objective	Verify the system's security event logs are being collected by the system.
Risk:	The security log can record security events such as valid and invalid logon attempts as well as events related to accessing resources. An administrator can specify what events are recorded in the security log. For example, if you have enabled logon auditing, attempts to log on to the system are recorded in the security log. Out of the box installations of Windows 2000 Server does not enable security event logging. Therefore, there is no evidence for when a user accesses or attempts to access the system.
Compliance	The Security log in the event viewer shows a success logon attempt was made by the user with the corresponding event ID 528.

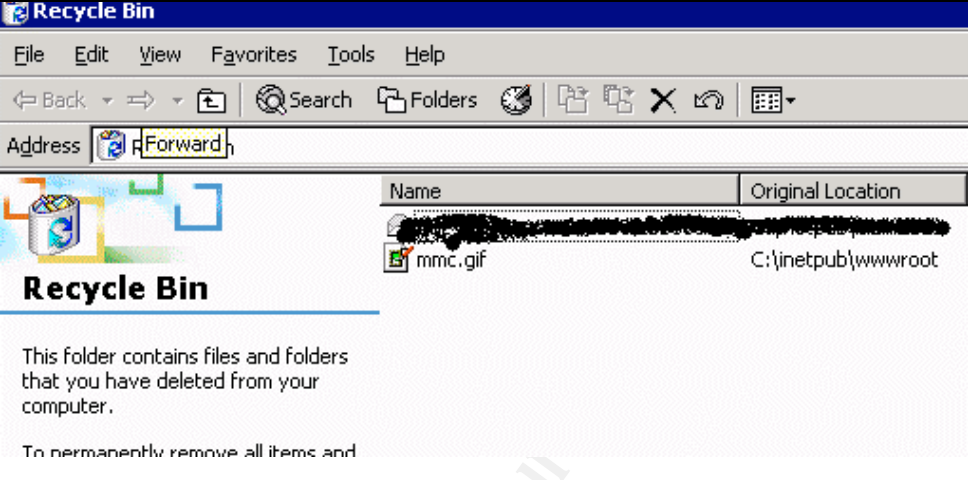
Testing	<ol style="list-style-type: none"> 1. Log into the server system. 2. Go to Control Panel-> Administrative Tools -> Event Viewer 3. Click on the Security Events 4. Sort according to Event ID number 5. Locate ID 528 and double-click. 6. Match "user" field with the credentials used to log into the system
Objective/ Subjective	Objective test. Results are generated from a repeatable and verifiable tool.
To be completed after the test:	
Successful?	Failed. The system is not configured to log security events.
Result Details:	 <p>The screenshot shows the Windows Event Viewer application. The 'Tree' pane on the left shows 'Event Viewer (Local)' expanded, with 'Security Log' selected. The 'Details' pane on the right shows 'Security Log' with '0 event(s)'. The table headers are 'Type', 'Date', 'Time', 'Source', and 'Category'.</p>
Stimulus/ Response	Stimulus

2.1.2 Technical Risk 2: Checklist for Default installation of ISS

Test 5:	
Reference:	http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/mbsahome.asp http://www.sans.org/rr/paper.php?id=275 MSBA checks for hotfixes for Microsoft applications such as IIS to determine appropriate updates and security configurations have been installed.
Control Objective	Verify that all Security Patches for IIS 5.0 are installed
Risk:	Exploit code exists for vulnerabilities identified in IIS 5.0. Without having these known vulnerabilities patched, the system can be easily exploitable through attacks and viruses. An example of this would be Code Red.

Compliance	The tool should produce results that there are no missing patches related to IIS.
Testing	<ol style="list-style-type: none"> 1. Open MBSA tool on the server system, select "Scan a Computer". 2. Select Scan local computer. Check the 'ISS Vulnerabilities' 3. Results will appear in a new window. 4. Determine what hotfixes are missing. 5. From the Microsoft website links provided in the results of MBSA, determine the file versions which are not compliant 6. Run a search in Windows to locate these files and verify the version is in compliance with the current patch level.
Objective/ Subjective	Objective test. Results are generated from a repeatable and verifiable tool.
To be completed after the test:	
Successful?	Pass. The system is appropriately patched for IIS security updates.
Result Details:	 <p>The screenshot displays the Microsoft Baseline Security Analyzer (MBSA) interface. The main window shows a 'View security report' for a local computer. The report indicates that the security update database version is 1.0.1.495, and a newer version (1.0.1.497) is available. The security assessment is 'Severe Risk (One or more critical checks failed.)'. The 'Security Update Scan Results' table shows that Windows Security Updates and IIS Security Updates are up to date, but SQL Server Security Updates, Windows Media Player Security Updates, and Exchange Server Security Updates are missing. The 'Windows Scan Results' section shows vulnerabilities: 'Restrict Anonymous' is set to 0, and 'Administrators' are found on the computer.</p>
Stimulus/ Response	

Test 6:	
Reference:	http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/iis5cl.asp http://www.sans.org/rr/paper.php?id=275
Control Objective	Verify that access to IIS files is restricted by not allowing users with non-administrator privileges to delete IIS files.
Risk:	By not limiting access to directories and files, malicious users and attackers can access, add and remove files, affecting the confidentiality and integrity of system.
Compliance	<p>Permission should be denied when trying to access files with the following file types:</p> <p style="text-align: center;">File Type</p> <p>CGI (.exe, .dll, .cmd, .pl)</p> <p>Script files (.asp)</p> <p>Include files (.inc, .shtm, .shtml)</p> <p>Static content (.txt, .gif, .jpg, .html)</p>
Testing	<ol style="list-style-type: none"> 1. Log into the server machine using the non-administrator account. 2. Open to the following directory: C:\inetpub\wwwroot\ 3. Click on the following file: "mmc.gif" 4. Right click and press delete. 5. Click yes, send it to the recycle bin 6. Navigate to the recycle bin and locate the file
Objective/ Subjective	Objective test. Results can be viewed by repeatable process.
To be completed after the test:	
Successful?	Failed. Able to delete the file.
Result Details:	<p>"MMC.GIF"</p> 

	
Stimulus/ Response	Stimulus

2.1.3 Technical Risk 3: Checklist for Exposure to Known Vulnerabilities and Exploits

Test 9:	
Reference:	http://www.sans.org/top20/
Control Objective	<p>Verify that the system is protected against the following Sans Top Windows Vulnerabilities:</p> <ul style="list-style-type: none"> W1 Internet Information Services (IIS) W2 Microsoft SQL Server (MSSQL) W3 Windows Authentication W4 Internet Explorer (IE) W5 Windows Remote Access Services W6 Microsoft Data Access Components (MDAC) W7 Windows Scripting Host (WSH) W8 Microsoft Outlook and Outlook Express W9 Windows Peer to Peer File Sharing (P2P) W10 Simple Network Management Protocol (SNMP)
Risk:	As indicated by being on the Sans top 10 Windows Vulnerabilities, existence of these holes on the system make the system extremely open to common attacks.
Compliance	The Nessus report should not show any security holes associated with the above listed vulnerabilities. Note, false positives result when the results of the scan indicate something is vulnerable, when in fact it is not. These will be assessed when reviewing all the results.
Testing	<ol style="list-style-type: none"> 1. Launch the Nessus GUI 2. From the Plugins tab, select "enable all but dangerous plugins" 3. From the Scan Options tab, check "Optimize the Test" and "Safe Checks"

	4. In the target selection tab, enter the IP address. Then click Start Session 5. Research the holes and manually verify possible false positives.										
Objective/ Subjective	Objective test. Results are generated from a repeatable and verifiable tool.										
To be completed after the test:											
Successful?	Failed. Numerous vulnerabilities were found on port 80 associated with IIS (no. 1 on the SANS top list).										
Result Details:	<div><div>Nessus Scan Report</div><div><p>This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these threats.</p><div>Scan Details</div><p>Hosts which were alive and responding during test 1</p><p>Number of security holes found 9</p><p>Number of security warnings found 29</p><div>Host List</div><table><thead><tr><th>Host(s)</th><th>Possible Issue</th></tr></thead><tbody><tr><td>xxx.xxx.xxx.xxx</td><td>Security hole(s) found</td></tr></tbody></table><p>[return to top]</p><div>Analysis of Host</div><table><thead><tr><th>Address of Host</th><th>Port/Service</th><th>Issue regarding Port</th></tr></thead><tbody><tr><td>xxx.xxx.xxx.xxx</td><td>ftp (21/tcp)</td><td>Security hole found</td></tr></tbody></table></div></div>	Host(s)	Possible Issue	xxx.xxx.xxx.xxx	Security hole(s) found	Address of Host	Port/Service	Issue regarding Port	xxx.xxx.xxx.xxx	ftp (21/tcp)	Security hole found
Host(s)	Possible Issue										
xxx.xxx.xxx.xxx	Security hole(s) found										
Address of Host	Port/Service	Issue regarding Port									
xxx.xxx.xxx.xxx	ftp (21/tcp)	Security hole found									

	<p>xxx.xxx.xxx.xxx http (80/tcp) Security hole found</p> <p>xxx.xxx.xxx.xxx msrdp (3389/tcp) Security warning(s) found</p> <p>xxx.xxx.xxx.xxx general/udp Security notes found</p> <p>xxx.xxx.xxx.xxx smtp (25/tcp) Security notes found</p> <p style="text-align: right;">Security Issues and Fixes: 216.205.74.162</p> <p>Type Port Issue and Fix</p> <p>Vulnerability ftp (21/tcp) It may be possible to make the remote FTP server crash by sending the command 'STAT *?AAA...AAA.'</p> <p>An attacker may use this flaw to prevent your site from distributing files</p> <p>*** Warning : we could not verify this vulnerability. *** Nessus solely relied on the banner of this server</p> <p>Solution : Apply the relevant hotfix from Microsoft</p> <p>See:http://www.microsoft.com/technet/security/bulletin/ms02-018.asp</p> <p>Risk factor : High CVE : CVE-2002-0073 BID : 4482 Nessus ID : 10934</p> <p>Informational ftp (21/tcp) Remote FTP server banner : 220 DHS5060 Microsoft FTP Service (Version 5.0).</p> <p>Nessus ID : 10092</p> <p>Vulnerability http (80/tcp) IIS comes with the sample site 'ExAir'. Unfortunately, one of its pages, namely /iissamples/exair/search/advsearch.asp, may be used to make IIS hang, thus preventing it from answering legitimate client requests.</p> <p>Solution : Delete the 'ExAir' sample IIS site.</p>
--	--

	<p>Risk factor : Medium/High CVE : CVE-1999-0449 BID : 193 Nessus ID : 10002</p> <p>Vulnerability http (80/tcp)</p> <p>IIS comes with the sample site 'ExAir'. Unfortunately, one of its pages, namely /iissamples/exair/search/search.asp, may be used to make IIS hang, thus preventing it from answering legitimate client requests.</p> <p>Solution : Delete the 'ExAir' sample IIS site.</p> <p>Risk factor : Medium CVE : CVE-1999-0449 BID : 193 Nessus ID : 10004</p> <p>Vulnerability http (80/tcp)</p> <p>The 'ping.asp' CGI is installed. Some versions allows a cracker to launch a ping flood against your machine or another by entering '127.0.0.1 -l 65000 -t' in the Address field.</p> <p>Solution : remove it.</p> <p>Reference : http://online.securityfocus.com/archive/82/275088</p> <p>Risk factor : Serious Nessus ID : 10968</p> <p>Vulnerability http (80/tcp)</p> <p>Allaire JRun 3.0/3.1 under a Microsoft IIS 4.0/5.0 platform has a problem handling malformed URLs. This allows a remote user to browse the file system under the web root (normally \inetpub\wwwroot).</p> <p>Under Windows NT/2000(any service pack) and IIS 4.0/5.0: - JRun 3.0 (all editions) - JRun 3.1 (all editions)</p> <p>Upon sending a specially formed request to the web server, containing a '.jsp' extension makes the JRun handle the request. Example:</p> <p>http://www.victim.com/%3f.jsp</p> <p>This vulnerability allows anyone with remote access to the web server to browse it and any directory within the web root.</p> <p>Solution: >From Macromedia Product Security Bulletin (MPSB01-13) http://www.allaire.com/handlers/index.cfm?ID=22236&Method=Full</p> <p>Macromedia recommends, as a best practice, turning off directory browsing for the JRun Default Server in the following applications:</p> <ul style="list-style-type: none"> - Default Application (the application with '/' mapping that causes the security problem) - Demo Application
--	---

	<p>Also, make sure any newly created web application that uses the '/' mapping has directory browsing off.</p> <p>The changes that need to be made in the JRun Management Console or JMC:</p> <ul style="list-style-type: none"> - JRun Default Server/Web Applications/Default User Application/File Settings/Directory Browsing Allowed set to FALSE. - JRun Default Server/Web Applications/JRun Demo/File Settings/Directory Browsing Allowed set to FALSE. <p>Restart the servers after making the changes and the %3f.jsp request should now return a 403 forbidden. When this bug is fixed, the request (regardless of directory browsing setting) should return a '404 page not found'.</p> <p>The directory browsing property is called [file.browsedirs]. Changing the property via the JMC will cause the following changes: JRun 3.0 will write [file.browsedirs=false] in the local.properties file. (server-wide change) JRun 3.1 will write [file.browsedirs=false] in the webapp.properties of the application.</p> <p>Risk factor : Medium BID : 3592 Nessus ID : 10814</p> <p>Vulnerability http (80/tcp)</p> <p>IIS comes with the sample site 'ExAir'. Unfortunately, one of its pages, namely /iissamples/exair/search/query.asp, may be used to make IIS hang, thus preventing it from answering legitimate client requests.</p> <p>Solution : Delete the 'ExAir' sample IIS site.</p> <p>Risk factor : Medium CVE : CVE-1999-0449 BID : 193 Nessus ID : 10003</p> <p>Vulnerability http (80/tcp)</p> <p>The dll '/_vti_bin/_vti_aut/dwssr.dll' seems to be present.</p> <p>This dll contains a bug which allows anyone with authoring web permissions on this system to alter the files of other users.</p> <p>In addition to this, this file is subject to a buffer overflow which allows anyone to execute arbitrary commands on the server and/or disable it</p> <p>Solution : delete /_vti_bin/_vti_aut/dwssr.dll Risk factor : High See also : http://www.wiretrip.net/rfp/p/doc.asp?id=45&iface=1 CVE : CVE-2000-0260 BID : 1109 Nessus ID : 10369</p> <p>Vulnerability http (80/tcp)</p> <p>It is possible to get the source code of the remote ASP scripts by appending %20 at the end</p>
--	---

	<p>of the request (like GET /default.asp%20)</p> <p>ASP source code usually contains sensitive information such as logins and passwords.</p> <p>Solution : install all the latest security patches</p> <p>Risk factor : Serious CVE : CAN-2001-1248 BID : 2975 Nessus ID : 11071</p> <p>Vulnerability http (80/tcp)</p> <p>The remote host is running Microsoft Content Management Server.</p> <p>There is a buffer overflow in the Profile Service which may allow an attacker to execute arbitrary code on this host.</p> <p>*** Since safe checks are enabled, Nessus did not actually *** test for this flaw but relied on the presence of *** /NR/System/Access/ManualLoginSubmit.asp to issue this *** warning.</p> <p>Solution : See http://www.microsoft.com/technet/security/bulletin/ms02-041.asp Risk factor : High CVE : CAN-2002-0620, CVE-2002-0621, CVE-2002-0622, CVE-2002-0623, CVE-2002-0050 Nessus ID : 11313</p> <p>Warning http (80/tcp)</p> <p>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.</p> <p>An attacker may use this flaw to trick your legitimate web users to give him their credentials.</p> <p>Solution: Disable these methods.</p> <p>If you are using Apache, add the following lines for each virtual host in your configuration file :</p> <pre>RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE TRACK) RewriteRule .* - [F]</pre> <p>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.</p> <p>See http://www.whitehatsec.com/press_releases/WH-PR-20030120.pdf http://archives.neohapsis.com/archives/vulnwatch/2003-q1/0035.html</p> <p>Risk factor : Medium Nessus ID : 11213</p>
--	--

	<p>Warning http (80/tcp)</p> <p>The remote web server seems to be vulnerable to the Cross Site Scripting vulnerability (XSS). The vulnerability is caused by the result returned to the user when a non-existing file is requested (e.g. the result contains the JavaScript provided in the request). The vulnerability would allow an attacker to make the server present the user with the attacker's JavaScript/HTML code. Since the content is presented by the server, the user will give it the trust level of the server (for example, the trust level of banks, shopping centers, etc. would usually be high).</p> <p>Risk factor : Medium</p> <p>Solutions:</p> <ul style="list-style-type: none"> . Allaire/Macromedia Jrun: <ul style="list-style-type: none"> - http://www.macromedia.com/software/jrun/download/update/ - http://www.securiteam.com/windowsntfocus/Allaire_fixes_Cross-Site_Scripting_security_vulnerability.html . Microsoft IIS: <ul style="list-style-type: none"> - http://www.securiteam.com/windowsntfocus/IIS_Cross-Site_scripting_vulnerability_Patch_available_.html . Apache: <ul style="list-style-type: none"> - http://httpd.apache.org/info/css-security/ . ColdFusion: <ul style="list-style-type: none"> - http://www.macromedia.com/v1/handlers/index.cfm?ID=23047 . General: <ul style="list-style-type: none"> - http://www.securiteam.com/exploits/Security_concerns_when_developing_a_dynamically_generated_web_site.html - http://www.cert.org/advisories/CA-2000-02.html <p>BID : 5305, 7353, 7344, 8037 Nessus ID : 10815</p> <p>Warning http (80/tcp)</p> <p>Mambo Site Server is an open source Web Content Management System. An attacker may use it to perform a cross site scripting attack on this host.</p> <p>Solution: Upgrade to a newer version. Risk factor : Medium BID : 7135 Nessus ID : 11441</p> <p>Warning http (80/tcp)</p> <p>Basit cms 1.0 has a cross site scripting bug. An attacker may use it to perform a cross site scripting attack on this host.</p> <p>In addition to this, it is vulnerable to a SQL insertion attack which may allow an attacker to get the control of your database.</p> <p>Solution : Upgrade to a newer version. Risk factor : Medium BID : 7139 Nessus ID : 11445</p> <p>Warning http (80/tcp)</p>
--	---

	<p>The remote web server is running P-Synch, a password management system running over HTTP.</p> <p>There is a flaw in the CGIs nph-psa.exe and nph-psf.exe which may allow an attacker to make this host include remote files, disclose the path to the p-synch installation or produce arbitrary HTML code (cross-site scripting).</p> <p>Solution : Upgrade to the latest version of P-Synch Risk factor : Low BID : 7740, 7745, 7747 Nessus ID : 11694</p> <p>Warning http (80/tcp)</p> <p>Siteframe 2.2.4 has a cross site scripting bug. An attacker may use it to perform a cross site scripting attack on this host.</p> <p>In addition to this, another flaw in this package may allow an attacker to obtain the physical path to the remote web root.</p> <p>Solution : Upgrade to a newer version. Risk factor : Medium BID : 7140, 7143 Nessus ID : 11448</p> <p>Warning http (80/tcp)</p> <p>DCP-Portal v5.3.1 has a cross site scripting bug. An attacker may use it to perform a cross site scripting attack on this host.</p> <p>Solution : Upgrade to a newer version. Risk factor : Medium BID : 7144, 7141 Nessus ID : 11446</p> <p>Warning http (80/tcp) A sample application shipped with IIS 5.0 discloses the physical path of the web root. An attacker can use this information to make more focused attacks.</p> <p>Solution: Always remove sample applications from productions servers. In this case, remove the entire /iissamples folder. Risk factor : Low Nessus ID : 10573</p> <p>Warning http (80/tcp)</p> <p>ezPublish 2.2.7 has a cross site scripting bug. An attacker may use it to perform a cross site scripting attack on this host.</p> <p>In addition to this, another flaw may allow an attacker store hostile HTML code on the server side, which will be executed by the browser of the administrative user when he looks at the server logs.</p> <p>Solution : Upgrade to a newer version. Risk factor : Medium CVE : CAN-2003-0310 BID : 7137, 7138 Nessus ID : 11449</p>
--	---

	<p>Warning http (80/tcp)</p> <p>The remote host seems to be vulnerable to a security problem in SquirrelMail. Its read_body.php didn't filter out user input for 'filter_dir' and 'mailbox', making a xss attack possible.</p> <p>Solution: Upgrade to a newer version.</p> <p>Risk factor : Medium CVE : CAN-2002-1276, CAN-2002-1341 BID : 7019, 6302 Nessus ID : 11415</p> <p>Warning http (80/tcp)</p> <p>The remote Auction Deluxe server is vulnerable to a cross site scripting attack.</p> <p>As a result, a user could easily steal the cookies of your legitimate users and impersonate them.</p> <p>Solution : Upgrade to Auction Deluxe 3.30 or newer Risk factor : Medium CVE : CAN-2002-0257 BID : 4069 Nessus ID : 11365</p> <p>Warning http (80/tcp)</p> <p>The remote server is vulnerable to Cross-Site-Scripting (XSS) when the FrontPage CGI /_vti_bin/shtml.dll is fed with improper arguments.</p> <p>Solution : See http://www.microsoft.com/technet/security/bulletin/ms00-060.asp Risk factor : Medium CVE : CAN-2000-0746 BID : 1594, 1595 Nessus ID : 11395</p> <p>Warning http (80/tcp)</p> <p>The remote host is hosting the Pod.Board CGI suite, a set of PHP scripts designed to manage online forums.</p> <p>There is a cross site scripting issue in this suite which may allow an attacker to steal the cookies of your legitimate users, by luring them into clicking on a rogue URL.</p> <p>Solution : None at this time Risk Factor : Low/Medium BID : 7933 Nessus ID : 11760</p> <p>Warning http (80/tcp)</p> <p>The remote host is using XMB Forum.</p> <p>This set of CGI is vulnerable to a cross-site-scripting issue that may allow attackers to steal the cookies of your</p>
--	--

	<p>users.</p> <p>Solution: Upgrade to a newer version. Risk factor : Medium CVE : CAN-2002-0316, CAN-2003-0375 BID : 4944, 8013 Nessus ID : 11527</p> <p>Warning http (80/tcp)</p> <p>The IIS server appears to have the .IDA ISAPI filter mapped.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Risk factor : Medium CVE : CVE-2001-0500 BID : 2880 Nessus ID : 10695</p> <p>Warning http (80/tcp)</p> <p>The remote host has a CGI called 'testcgi.exe' installed under /cgi-bin which is vulnerable to a cross site scripting issue.</p> <p>Solution: Upgrade to a newer version. Risk factor : Low BID : 7214 Nessus ID : 11610</p> <p>Warning http (80/tcp)</p> <p>The remote pafiledb.php is vulnerable to a cross site scripting attack.</p> <p>An attacker may use this flaw to steal the cookies of your users</p> <p>Solution : Upgrade to paFileDB 3.0 Risk factor : Medium BID : 6021 Nessus ID : 11479</p> <p>Warning http (80/tcp)</p> <p>osCommerce is a widely installed open source shopping e-commerce solution.</p>
--	---

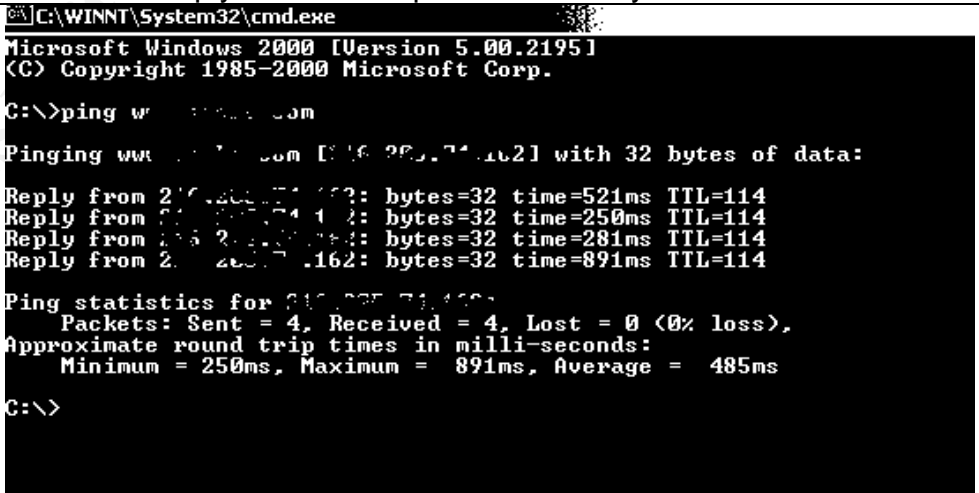
	<p>An attacker may use it to perform a cross site scripting attack on this host.</p> <p>Solution : Upgrade to a newer version. Risk factor : Medium BID : 7156, 7151, 7153, 7158, 7155 Nessus ID : 11437</p> <p>Warning http (80/tcp)</p> <p>The remote host is using ezPublish, a content management system.</p> <p>There is a flaw in the remote ezPublish which lets an attacker perform a cross site scripting attack. An attacker may use this flaw to steal the cookies of your legitimate users.</p> <p>Solution : Upgrade to ezPublish 3 Risk factor : Low/Medium BID : 7616 Nessus ID : 11644</p> <p>Warning http (80/tcp)</p> <p>Nuked-klan 1.3b has a cross site scripting bug. An attacker may use it to perform a cross site scripting attack on this host.</p> <p>In addition to this, another flaw may allow an attacker to obtain the physical path of the remote CGI directory.</p> <p>Solution : Upgrade to a newer version. Risk factor : Medium BID : 6916, 6917 Nessus ID : 11447</p> <p>Warning http (80/tcp)</p> <p>The remote host seems to be running MyAbraCadaWeb. An attacker may use it to perform a cross site scripting attack on this host, or to reveal the full path to its physical location.</p> <p>Solution: Upgrade to a newer version. Risk factor : Medium BID : 7126, 7127 Nessus ID : 11417</p> <p>Warning http (80/tcp)</p> <p>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.</p> <p>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</p>
--	--

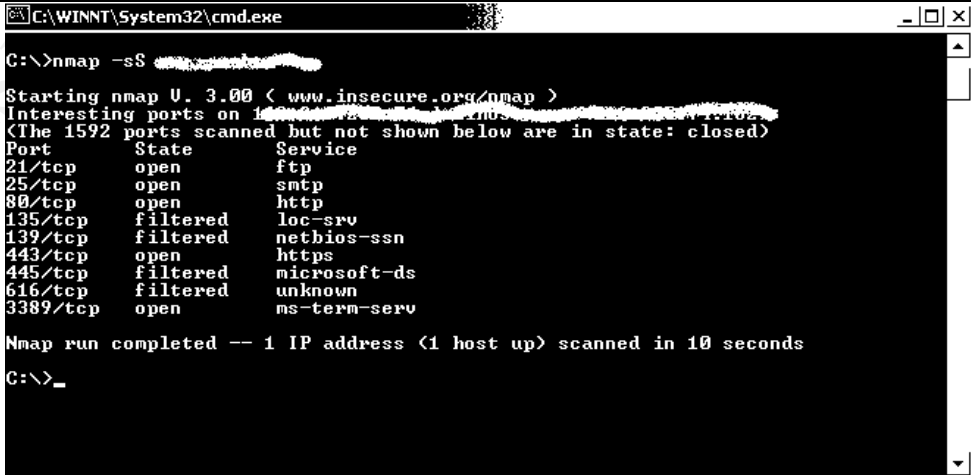
	<p>and remove the reference to .printer from the list.</p> <p>Reference : http://online.securityfocus.com/archive/1/181109</p> <p>Risk factor : Low Nessus ID : 10661</p> <p>Warning http (80/tcp)</p> <p>The following Sambar default CGIs are vulnerable to a cross-site scripting attack. An attacker may use this flaw to steal the cookies of your users :</p> <pre>/isapi/testisa.dll?check1=<script>code</script> /cgi-bin/envIRON.pl?param1=<script>code</script> /samples/search.dll?login=AND&query=<script>code</script> /cgi-bin/testcgi.exe?<script>code</script></pre> <p>Solution : Delete these CGIs. Risk factor : Medium BID : 7209 Nessus ID : 11492</p> <p>Warning http (80/tcp)</p> <p>The script /iissamples/sdk/asp/interaction/Form_JScript.asp (or Form_VBScript.asp) allows you to insert information into a form field and once submitted re-displays the page, printing the text you entered. This .asp doesn't perform any input validation, and hence you can input a string like: <SCRIPT>alert(document.domain)</SCRIPT>.</p> <p>More information on cross-site scripting attacks can be found at: http://www.cert.org/advisories/CA-2000-02.html</p> <p>Solution: Always remove sample applications from productions servers. In this case, remove the entire /iissamples folder. Risk factor : Low Nessus ID : 10572</p> <p>Warning http (80/tcp)</p> <p>The remote host is running the Xoops CGI suite.</p> <p>There is a cross site scripting issue in this suite which may allow an attacker to steal your users cookies.</p> <p>The flaw lies in the cgi glossaire-aff.php.</p> <p>You are advised to remove this CGI.</p> <p>Solution : None at this time Risk factor : Medium BID : 7356 Nessus ID : 11508</p> <p>Warning http (80/tcp)</p> <p>The remote host is running a version of pMachine which is vulnerable</p>
--	---

	<p>to two flaws :</p> <ul style="list-style-type: none"> - It is vulnerable to a path disclosure problem which may allow an attacker to gain more knowledge about this host - It is vulnerable to a cross-site-scripting attack which may allow an attacker to steal the cookies of the legitimates users of this service <p>Solution : None at this time. Disable this CGI suite Risk Factor : Low/Medium BID : 7980, 7981 Nessus ID : 11766</p> <p>Warning http (80/tcp)</p> <p>The remote host is running the Neoteris IVE.</p> <p>There is a cross site scripting issue in this server (in the CGI swsrv.cgi) which may allow an attacker to perform a session hijacking.</p> <p>Solution : Upgrade to version 3.1 or Neoteris IVE Risk factor : Medium CVE : CAN-2003-0217 Nessus ID : 11608</p> <p>Warning http (80/tcp)</p> <p>The remote host is running the Bandmin CGI suite.</p> <p>There is a cross site scripting issue in this suite which may allow an attacker to steal your users cookies.</p> <p>The flaw lies in the cgi bandwidth/index.php</p> <p>You are advised to remove this CGI.</p> <p>Solution : None at this time Risk factor : Medium CVE : CAN-2003-0416 BID : 7729 Nessus ID : 11672</p> <p>Informational http (80/tcp) The following CGI have been discovered :</p> <p>Syntax : cginame (arguments [default value])</p> <p>/default.aspx (pu [] uu [])</p> <p>Nessus ID : 10662</p> <p>Informational http (80/tcp)</p> <p>The remote web servers is [mis]configured in that it does not return '404 Not Found' error codes when a non-existent file is requested, perhaps returning a site map or search page instead.</p> <p>Nessus enabled some counter measures for that, however</p>
--	---

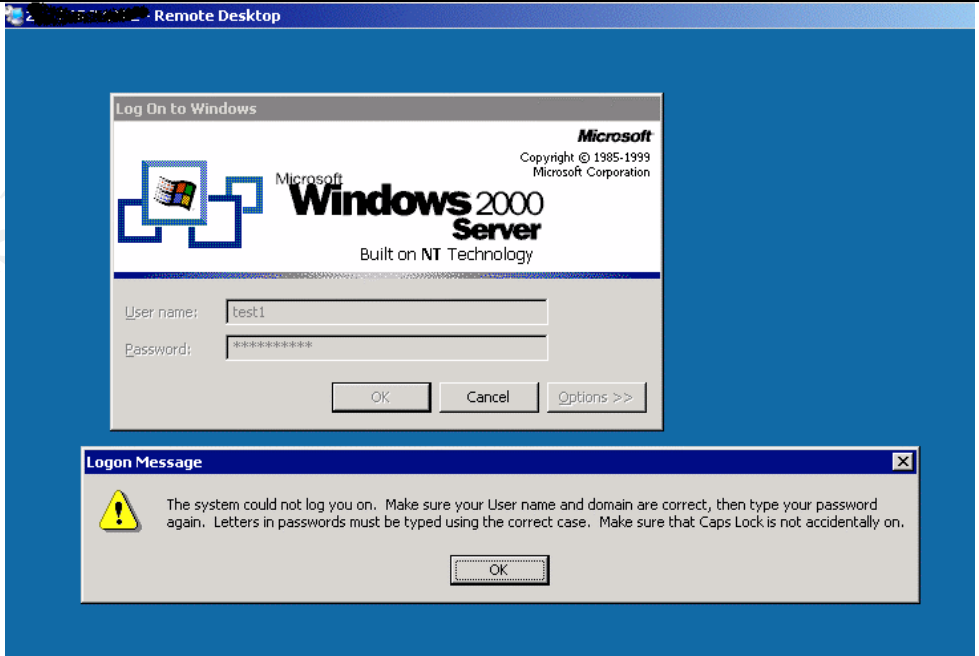
	<p>they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate Nessus ID : 10386</p> <p>Informational http (80/tcp) The remote web server type is :</p> <p>Microsoft-IIS/5.0</p> <p>Solution : You can use urlscan to change reported server for IIS. Nessus ID : 10107</p> <p>Warning msrdp (3389/tcp)</p> <p>The Terminal Services are enabled on the remote host.</p> <p>Terminal Services allow a Windows user to remotely obtain a graphical login (and therefore act as a local user on the remote host).</p> <p>If an attacker gains a valid login and password, he may be able to use this service to gain further access on the remote host.</p> <p>Note that RDP (the Remote Desktop Protocol) is vulnerable to Man-in-the-middle attacks, making it easy for attackers to steal the credentials of legitimates users by impersonating the Windows server.</p> <p>Solution : Disable the Terminal Services if you do not use them, and do not allow this service to run across the internet</p> <p>Risk factor : Medium BID : 7258 Nessus ID : 10940</p> <p>Informational general/udp For your information, here is the traceroute to xxx.xxx.xxx.xxx : 10.30.188.126 10.2.30.189 ? xxx.xxx.xxx.xxx</p> <p>Nessus ID : 10287</p> <p>Informational smtp (25/tcp) For some reason, we could not send the EICAR test string to this MTA Nessus ID : 11034</p> <hr/> <p>This file was generated by Nessus, the open-sourced security scanner.</p>
Stimulus/ Response	

2.1.4 Technical Risk 4: Checklist for Weak Perimeter Security

Test 12:	
Reference:	http://www.microsoft.com/serviceproviders/columns/isp_security.asp http://www.cyber.ust.hk/handbook4/04_hb4.html#What%20services%20should%20be%20monitored
Control Objective	Verify that a ping request to the server system is denied.
Risk:	A standard firewall configuration rule is to reject the return of an ICMP incoming request. This means that when sending an echo request (type code 8) from the outside the network, one should not receive an echo reply. Having echo reply enabled on firewalls allows hackers to obtain information about the server such as IP address, which attackers can then more specifically target their attacks.
Compliance	Echo request should not return an echo reply such as: Reply from: xxxx.xxx.xxx.xxx where xxx.xxx.xxx.xxx is the server IP address.
Testing	1. Open the command prompt (Start-> Run 'cmd') on a machine outside the ISP network. 2. In the command prompt type, "ping <i>www.site.example</i> " 3. Press Enter
Objective/ Subjective	Objective- Results are generated from a repeatable and verifiable tool.
To be completed after the test:	
Successful?	Fail. Echo reply returned request from the system IP address.
Result Details:	 <pre> C:\WINNT\System32\cmd.exe Microsoft Windows 2000 [Version 5.00.2195] (C) Copyright 1985-2000 Microsoft Corp. C:\>ping www.microsoft.com Pinging www.microsoft.com [66.253.71.162] with 32 bytes of data: Reply from 216.239.37.162: bytes=32 time=521ms TTL=114 Reply from 66.253.71.162: bytes=32 time=250ms TTL=114 Reply from 66.253.71.162: bytes=32 time=281ms TTL=114 Reply from 66.253.71.162: bytes=32 time=891ms TTL=114 Ping statistics for 66.253.71.162: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 250ms, Maximum = 891ms, Average = 485ms C:\> </pre>
Stimulus/ Response	Stimulus

Test 13:	
Reference:	http://www.microsoft.com/serviceproviders/columns/isp_security.asp http://www.cyber.ust.hk/handbook4/04_hb4.html#What%20services%20should%20be%20monitored
Control Objective	Verify that when port scanned, only the http (port 80) is seen in the results.
Risk:	The ability to reach the targeted host using a port scanning tool and obtaining open ports and services would indicate that very weak, if any, perimeter security exists. Only port 80 (web) should be seen on a web server. The ability for an attack to obtain this information makes it easy for attackers to determine their targets. This is a common “first step” for hackers.
Compliance	The scan tool should return the results of “port 80/tcp open http”.
Testing	<ol style="list-style-type: none"> 1. Set up the scanning machine outside the internal ISP network. 2. Open the command prompt (Start-> Run ‘cmd’) 3. Type ‘nmap -sS xxx.xxx.xxx.xxx.’ (where -sS is syn stealth mode and ‘xxx.xxx.xxx.xxx’ is the target host) 3. Enter 4. Results of the port scan will show in the command prompt screen.
Objective/ Subjective	Objective- Results are generated from a repeatable and verifiable tool.
To be completed after the test:	
Successful?	Fail. The port scan was able to obtain multiple ports which are open, not just port 80. These ports should be hidden from the public.
Result Details:	 <pre> C:\WINNT\System32\cmd.exe C:\>nmap -sS 192.168.1.102 Starting nmap U. 3.00 (www.insecure.org/nmap) Interesting ports on 192.168.1.102: (The 1592 ports scanned but not shown below are in state: closed) Port State Service 21/tcp open ftp 25/tcp open smtp 80/tcp open http 135/tcp filtered loc-srv 139/tcp filtered netbios-ssn 443/tcp open https 445/tcp filtered microsoft-ds 616/tcp filtered unknown 3389/tcp open ms-term-serv Nmap run completed -- 1 IP address (1 host up) scanned in 10 seconds C:\>_ </pre>
Stimulus/ Response	Stimulus

2.1.5 Technical Risk 5: Checklist for InSecure Data in Transit

Test 16:	
Reference:	http://www.giac.org/practical/gsec/Kim_Hughes_GSEC.pdf
Control Objective	Verify that someone cannot remotely log into the system to perform administrative activities (such as connections through terminal services) through an insecure connection.
Risk:	All traffic and sensitive data sent from the administrator to the remote system at the ISP could be seen and captured by eavesdroppers sitting on the internet; therefore, compromising integrity and confidentiality of the data.
Compliance	Connection is denied when attempting to log into the system via terminal services without strong credentials.
Testing	4. Launch terminal services 5. Connect to: XXX.XXX.XXX.XXX 6. Log in with any User ID and Password
Objective/ Subjective	Objective test. Results are generated from a repeatable and verifiable tool.
To be completed after the test:	
Successful?	Pass. Only a user with verified log in credentials on the system can log in using terminal services.
Result Details:	
Stimulus/ Response	Stimulus

2.2.1 Procedural Risk 1: Budget Constraints

Test 18:	
Reference:	http://www.sans.org/rr/paper.php?id=617 http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci932898,00.html
Control Objective	Verify that <i>Site.example</i> has allocated 15% (industry average) of the companies' budget to IT and 5% of this toward security needs.
Risk:	Lack of budget means lack of security equipment and ability to address security problems. This leaves business with no security mechanisms.
Compliance	Business plan will show that a 5% of the IT budget is specifically allocated to security administration.
Testing	1. Locate Business Plan and Budget numbers 2. Request information from CFO. 3. Obtain receipts of security related purchases
Objective/ Subjective	Objective- A business plan will be available which will demonstrate how the budget is allocated as well as evidence for purchases.
To be completed after the test:	
Successful?	Fail. No documentation was able to be provided. Therefore, results were based solely on input received from the CFO. Subjective results.
Result Details:	CFO has stated that he has not receipts or documentation of a budget for IT and security expenditures. He stated that purchases and investments made toward IT and security is on an as needed basis. There is no way to tell based on this information if that equates to 15% or not.
Stimulus/ Response	

2.2.5 Procedural Risk 5: Absent Backup and Storage procedures

Test 25:	
Reference:	http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/maintain/opsguide/secadmog.asp
Control Objective	Verify that regular backup procedures are followed.
Risk:	In the event of a system compromise, information will be lost and unable to restore.
Compliance	Backup procedures and files exist and are stored securely in an off site location.
Testing	1. Locate physical backups 2. Obtain documentation for the back up process

Objective/ Subjective	Objective- locate physical backups on the system.
To be completed after the test:	
Pass/fail?	Fail. Results were based in input received from speaking with the business owner (sole operator of the business). He did not have any documentation which explicitly details his back up procedures. However, based on this subjective feedback, there are backup and storage procedures.
Result Details:	Sole business owner assured that backups are created for the SQL database only by himself. However, these backups are stored on the system itself. He stated that the ISP offers routine back up services (at a price); however, the business has decided not to pay for this service.
Stimulus/ Response	

3.2 Measure Residual Risk

Residual Risk can be measured by examining the exposure or value of the system to the company minus the security controls which exist. As indicated above, this system's value to the company is crucial as it provides all the functionality to the company's operations. It operates as the interface for users to access and input their data. The results of the audit however, indicate that there are few security controls (such as firewalls, security auditing or monitoring) applied to this system. Therefore, the amount of residual risk which exists is very high.

This audit focused on testing for default installations of software, weaknesses of Internet Service Providers and weaknesses with administering a small start up company. Many procedural vulnerabilities which were identified, such as limited budgets, resources and security skills cannot be fixed simply due to the nature of this small, start up business. Furthermore, some other vulnerabilities, such as weak perimeter and physical security, cannot be fixed because that is up to the implementation of the service provider. However, some workarounds can be suggested in order to mitigate these risks. Firewalls and port filtering can be implemented on the system itself. Additionally, while budgets and resources may not be available to fully implement commercial products, some free and many "suites" of reasonable cost tools are easy to learn and will help to mitigate some of the risks.

3.3 Is the System Auditable?

The objectives of this audit were met through technical testing, observation, and data and information gathering through interviews and documentation. The technical testing portions of the audit were able to produce concrete results which lead to the determination of many weaknesses within the systems environment.

However in some cases, particularly on the procedural side, it was difficult to obtain clear and defining evidence for many of the control objectives. This is mainly due to the subjective nature of the tests performed in order to audit this type of information. No objective sources of

information, for example documentation, exists for the policies and processes operated within the business. Instead, information gathered from interviews with the sole business owner has to suffice in answering these questions. Therefore, these controls could not be examined objectively. Furthermore, because the system is physically located at the Internet Service Provider, audit objectives such as physical security had to rely on information within contracts and from interviews. There was not a way to physically see the system in person.

Assignment 4- Audit Report

4.1 Executive Summary

The audit's focus was to identify both technical and procedural weaknesses which can be associated with running small businesses and using outsourced providers. Furthermore, it's goal was to identify how these risks pose potential threats to the loss of Confidentiality, Integrity and Availability of data within this system. The results indicate that this system is vulnerable to many of the risks identified and that significant attention should be made to remediation. This report will identify these risks and propose solutions which can help protect against them. However, it is further revealed throughout this audit that some of the risks simply cannot be resolved due to environmental and business constraints. For these risks, the report will simply have to identify and accept until changes can be made to improve their security.

4.2. Audit Findings

Before detailing the findings, we will first summarize and explain the categories of risk which were identified and examined throughout this audit. The risks can be grouped into 3 categories: (1) those associated with running a small business, (2) those associated with using outsourced service providers, and (3) those associated with the application and services running on the system.

Many risks associated with Small Business focus on process and procedural concerns. Small businesses generally operated on limited funds and with limited resources. Budgets are often constrained and appropriate allocation to investing in technical infrastructures is deferred to an "as needed" basis. Furthermore, the knowledge and skills of resources are limited due to small number of employees, and little ability to send to appropriate training. These two concerns coupled together result in operations which cannot be securely run both because the infrastructure is not there and there are no resources which can support it. Therefore, appropriate security processes, both physical and technical, cannot be enforced.

Due to these limited resources and budgets, small businesses often look to outsourcing. In this case, *Site.example* is outsourcing its hardware network environment to a service provider. Security processes and procedures for the technical infrastructure now become at the hands of the service provider, and therefore, cannot be tailored to meet a specific business need. A major weakness identified is weak perimeter security. Service providers do not provide firewalls or perimeter filtering, or if they do, it is very weak seeing as they need to be able to service a variety of needs. Furthermore, service providers often do not offer encrypted communications between the server and client. Lastly, physical security is at the discretion of

the provider and the business owner has no control over whom and how their system is accessed. It soon becomes very clear how outsourcing limits the control for the business owner and these risks need to be addressed.

The last category of risks which were examined are those associated with the applications and services running on the system. It was identified that the server examined is running on Windows 2000 Server operating system and runs Internet Information Services 5.0. These software applications by default have many known weaknesses and holes associated with them, which, if not properly patched and addressed, can open itself to known wild attacks.

Based on these risks, the tables below outline the final results and recommendations of this audit. These recommendations include associated costs as well as compensating controls for each. Please note that the recommendations provided are based both on the criticality of the identified vulnerabilities as well as the feasibility for *Site.examples* to implement. Because Site.example is operated and run by one person, the amount of time and resources required for the implementation is supplied in each recommendation.

1) Operating System and Application Exposures:

Finding:	<p>Tests 1, 3, 5, 6, and 9 were used to determine the following finding:</p> <p>The application/web server for <i>Site.example's</i> is still running on default configurations of the operating system (Windows 2000 Server) and the Major Application (Internet Information Services 5.0). Although both were up-to-date on patches, other configurations such as no security event logging and the existence of IIS sample files on the system indicated that many default configurations still exist. Nessus identified five security holes on port 80, which are a result of this default installation.</p>
Risk:	<p>Attackers use commonly known holes first to attempt to break into a system. Knowledge of default installations of both the OS and IIS allows him/her to identify specifically where the system is vulnerable and what type of attack to use.</p>
Recommendation:	<p><u>Securely configure OS and applications:</u> Eliminate vulnerabilities by changing default installation configurations and adding additional security controls to the system</p> <ul style="list-style-type: none"> • Run tools such as IIS lockdown tool to change default settings • Remove sample applications and files on IIS • Establish and enforce security policy settings to the system (enable password policy, security event logs) • Have antivirus software running
Cost:	<ul style="list-style-type: none"> • IIS lockdown tool is a free tool and will cost 2 man hours to run and implement changes • Setting security policy settings is also free (done via the

	<p>registry of the system). Simply enabling security event logs would take .5 man hours to complete.</p> <ul style="list-style-type: none"> • Norton Antivirus and Personal Firewall software: \$69.95 and 2 man hours to install • McAfee VirusScan and Personal Firewall \$59.90 and 2 man hours to install • Microsoft Security Baseline Analyzer- free system configuration and patch checking tool and 2 man hours/month ongoing • Nessus is another free vulnerability assessment tool and will cost 3 man hours/month ongoing
Compensating Control:	<p>Many of these recommendations are simple configuration changes that any administrator could implement. If the administrator does not have the time to implement these changes, he/she would have to consider hiring a security resource. In New York City and in Atlanta, GA, a full time security resource costs approximately \$64,000. However, ad hoc changes and scans could be completed by hiring outsourced services from the ISP.</p>

Finding:	<p>Tests 9 was used to determine the following finding:</p> <p>The application/web server for <i>Site.example's</i> contains security vulnerabilities from the code that the site is using to operate. For example, the Nessus scan was able to detect a method in which one could obtain the source code of the website by entering a certain script into the URL.</p>
Risk:	<p>Source code usually contains sensitive information such as logins and passwords.</p>
Recommendation:	<p><u>Securely configure the application:</u> Establish tighter controls within the source code to prevent from cross site scripting attackers.</p> <ul style="list-style-type: none"> • Establish a Host Based Intrusion detection system to monitor and capture web attacks • Perform regular Vulnerability Assessments to identify weaknesses within the source code that could be susceptible to attacks
Cost:	<ul style="list-style-type: none"> • Snort is a free tool which can be used as a host based intrusion detection tool. It would require a detected resource to implement and monitor the event logs. However, it can also be a helpful forensics tool in gathering information after an attack has occurred. Implementing the tool would require one day for a skilled and trained Snort professional. • Use additional Vulnerability assessment tools to identify possible web attack vulnerabilities. Qualys Intranet Scanner costs \$1000 for one IP address. They will perform the scan and provide results. However, an additional 8 man hours a month should be allocated to reviewing and remediating

	these results.
Compensating Control:	The recommendations offer outsourced Vulnerability assessment services. However, consideration is going to have to be made on the remediation part. That is, resources will be needed to research and implement the changes provided by the Vulnerability assessment report.

2) Outsourced Internet Service Provider

Finding:	<p>Tests 12, 13 were used to determine the following finding:</p> <p>A very weak perimeter security exists within the environment that <i>Site.example</i>'s application/web server sits in. The audit was able to obtain a ping reply from the server as well as successfully port scan the system (obtain a list of services and ports open on the system).</p>
Risk:	Without any kind of perimeter security, which would helps to monitor and block malicious traffic, the system is vulnerable to a variety of internet attacks and viruses and worms, thus compromising confidentiality, integrity and availability of the data.
Recommendation:	<p><u>Establish blocking, monitoring and collecting mechanisms:</u></p> <p>Processes to collect and monitor system events can help identify and determine when systems are compromised</p> <ul style="list-style-type: none"> • Install a host based Personal Firewall that will collect logs. • Enable Audit security Event logs (system configuration) • Install Host based intrusion detection system which monitors and stores all traffic coming into the system • Establish a review process
Cost:	<ul style="list-style-type: none"> • Norton Antivirus and Personal Firewall software: \$69.95 and 2 man hours to install • McAfee VirusScan and Personal Firewall \$59.90 and 2 man hours to install • Other free personal Firewall solutions (ZoneAlarm, Sygate) at: www.webattack.com and 3 man hours to install • Snort- Free host based intrusion detection system. This could take up to 8 hours to install. • Hire a full time resource to ensure regular review and security processes are followed (\$64,000/yr www.salary.com)
Compensating Control:	Many of these recommendations will require the purchase of software system and hours for the administrator to spend on installation. However, if the administrator cannot take the time nor hire a new full time security resource, these services could be

	outsourced as well.
--	---------------------

3) Small Business

Finding:	Tests 12, 13 were used to determine the following finding: There is limited number of security resources, budget and processes.
Risk:	Once an attack is completed and the system is compromised, there are neither resources nor tools available remediate against this attack. Furthermore, in the event that the system crashes, all the data is lost because there are no back up procedures being followed.
Recommendation:	<u>Establish consistent Security processes and assessments</u> <ul style="list-style-type: none"> • Perform quarterly vulnerability scans • Consistently check patches • Monitor event logs • Perform backups • Monitor user access and permissions
Cost:	<ul style="list-style-type: none"> • Microsoft Security Baseline Analyzer- free system configuration and patch checking tool and 2 man hours/month ongoing • Nessus is another free vulnerability assessment tool and will cost 3 man hours/month ongoing • A full time security resource in New York City or Atlanta, GA will cost approximately \$64,000 (www.salary.com) • Man hours to consistently view event logs, perform backups, monitor users etc. is 8 hours/ week.
Compensating Control:	If hiring a full time security resource is not applicable, consider outsourcing these services to your ISP. The ISP provides back up procedures. If the ISP does not provide vulnerability assessment, try looking into services such as Qualys.

© SANS

References

See Sections 1.4.1 for complete listing of all references

© SANS Institute 2003, Author retains full rights.