

Auditing Windows Web server IIS5.0 with free tools

An auditor's perspective

By Serge Krasavin
CITES
University of Illinois
skrasavi@uiuc.edu

Table of contents:

1	Research in Audit	4
1.1	Risk to the system	4
1.2	System evaluation	8
1.2.1	Structured approach	9
1.2.2	Audit standards	10
1.3	Compliance with written policies and procedures	10
1.3.1	Current state of practice	10
1.3.2	Need for Improvement.....	14
2	Audit Checklist	16
2.1	Internet Information Server Security Checklist.....	16
2.1.1	Policies and procedures	16
2.1.2	Server Administration	16
2.1.3	Physical security.....	17
2.1.4	Business continuity.....	17
2.1.5	Server configuration	17
2.1.6	Unauthorized Access to resources.....	18
2.1.7	System Auditing	19
2.1.8	File System Configuration.....	19
2.1.9	Accounts.....	20
2.1.10	Services required.....	20
2.1.11	Backup	21
2.1.12	Monitoring/Intrusion detection procedure	21
2.1.13	Malicious Code	22
2.1.14	Vulnerability testing	22
2.1.15	System Modifications.....	23
2.1.16	Information posting and disclosure	23
2.1.17	Web specific	23
2.1.18	Web Audit trails	24
3	Audit of the server.....	26
3.1	Tools.....	26
3.2	Conduct an audit	27
3.2.1	Test 1 Policies and procedures	27
3.2.2	Test 2 Server configuration	27
3.2.3	Test 3 Monitoring/Intrusion detection procedure	33
3.2.4	Test 4 System Auditing.....	34
3.2.5	Test 5 Services required.....	39
3.2.6	Test 6 Web Audit trails	41
3.2.7	Test 7 System Modifications.....	43
3.2.8	Test 8 Vulnerability testing	46
3.2.9	Test 9 Malicious Code	51
3.2.10	Test 10 Web specific	52
3.3	Is the system auditable?	52
4	Follow up Report.....	54
4.1.1	Executive summary	54

4.1.2	Audit Results	54
4.1.3	Additional control objectives	59
4.1.4	Report Distribution.....	59
5	Conclusion	61
6	Appendix.....	62

Abstract

For the system auditor who is limited on resources, methodologies and tools described below can help to substantially narrow the gap between insecure and secure systems and perform a major goal of auditing process – compliance with the baseline.

1 Research in Audit

A Windows IIS 5.0 web server. The web server acts as an internet/intranet server providing administrative information to internal users as well publicly available information to external users.

General info	OS Name	Microsoft Windows 2000 Server
	Version	5.0.2195 Service Pack 3 Build 2195
	OS Manufacturer	Microsoft Corporation
	System Type	X86-based PC
Role	Web Server	
Software type	SYSTEM, IIS 5.0, Web Server Extensions	
	Source Path	D:\i386
	System Root	C:\WINNT

1.1 Risk to the system

Based on the company policies and procedures an auditor ought to consider what risks are present to the system. According to the IS Risk Assessment procedure “Risk is the possibility of an act or event occurring that would have an adverse effect on the organization and its information systems.”¹

A risk to the Web system can result in destruction, disclosure, or modification of data, mis-delivery of data, or denial of service, whether inadvertent or purposeful. The result from such a breach includes loss of customer confidence, financial loss, and the loss of productivity.

The Web server security audit is based on risk hunting approach to identify and analyze controlled and uncontrolled risks and define critical controls.

There are two basic methods of the web server risk evaluation.

One way to determine the risks is to rank various categories based on the nature of risk that the server is exposed to. Under each category, major risk components are enumerated. Depending on the type of risk a weight is assigned to each risk element. Each risk element is then further subdivided and is given a score. This risk score of a particular risk element is the product of the score and its weight. The total risk score of the function is the sum of the scores of all risk elements associated with a system. For ease of comparison, the risk score is measured on a scale of 100. Separate risk assessment sheets can be prepared for each of the auditable unit. Finally the scores obtained for each of the auditable units are consolidated and audits prioritized².

For example the business risk to the server at my department was defined and evaluated in the following way:

	Rating factor	Weight	Score	Assigned score
1	Effect of server failure (criticality) No immediate effect Inconvenience to users Loss of goodwill Loss of revenue Loss of business/revenue/goodwill	5	1 2 3 4 5	25
2.	Financial exposure None Small (<\$100,000) Moderate (\$100,000— \$1 m) High (\$1m—\$10 m) Very high (>\$10 m)	2	1 2 3 4 5	4
3.	Scope of the system Part of a department Complete department Multi department Organization wide Organization and external	2	1 2 3 4 5	4
4.	Prior audit findings Recent Audit—no weaknesses Recent Audit—minor weaknesses Audit—Some weaknesses	2	1 2 3 4	4

	Audit—Many weaknesses No previous audit		5	
	Total score			37

Although this method is rather subjective and limited to granularity of rating factors it presents a general overview of critical areas and can be used effectively to **compare risks** within an organization or department.

Another method uses the control objectives approach.

Based on ISACA recommendations³ I defined the following risks for the web server. The risks at the system level are the following:

- System confidentiality risks relating to violation of IT security policy, unauthorized access to resources, and weak protection barriers
- System integrity risks relating to the incomplete, inaccurate, untimely, or unauthorized processing of data
- System availability risks relating to the lack of system operational capability
- System maintainability risks relating to the inability to update the system when required in a manner that continues to provide for system availability, security, and integrity

Exposures to risks can be reduced by implementation of control objectives which are based upon probability of the occurrence of event.

Risk	Rank	Control Objectives	Probability	Consequences
<i>Confidentiality</i>				
Violation of system use policy and procedures	Critical	To detect violation of the security policy. Compliance of the system with IS policy and the best practices/standards	Medium. Depends on organization	Liability. Breach of confidentiality, integrity and availability of the server
Unauthorized access to resources	Critical	To determine that access to the server resources is restricted to authorized users. Determine whether the appropriate access rights are assigned to the directories and files.	Medium. Depends on organization culture and policy	Breach of confidentiality, integrity and availability of the server
Undetected	High	To determine	High	System and

attacks		whether protection filtering and IDS system are applied		services could be compromised
Weak protection barriers	Critical	To determine a level physical and network barriers (access to the server room, passwords)	Medium. Depends on organization culture and policy	Breach of confidentiality, integrity and availability of the server
Poor login and auditing controls	High	To determine whether audit logs are created for any specific files or resources, and who reviews the logs	Medium. Depends on organization culture and policy	Unauthorized access to files/resources
<i>Integrity</i>				
Presence of malicious programs	High	To determine whether antivirus programs are installed and configured properly	Medium. Depends on organization culture and policy	Presence of malicious programs can destroy data
<i>Availability</i>				
System failure	Medium	To detect efficiency of a Backup procedure (offside storage, schedule, test procedure)	Medium	Downtime of services might be considerable. Possible loss of data.
Power support failure	Low	To detect whether backup power is available. UPS configured properly.	Low	
<i>Maintainability</i>				
Exposure to vendor known vulnerabilities	Critical	To detect violation of patch/hotfixes management	High. Depends on organization culture and policy	System degradation. Breach of confidentiality, integrity and availability of data
Incorrect configuration	Critical	To detect violation in configuration relative to the best practices	Medium. Depends on the level of expertise of an administrator	Breach of confidentiality, integrity and availability of data

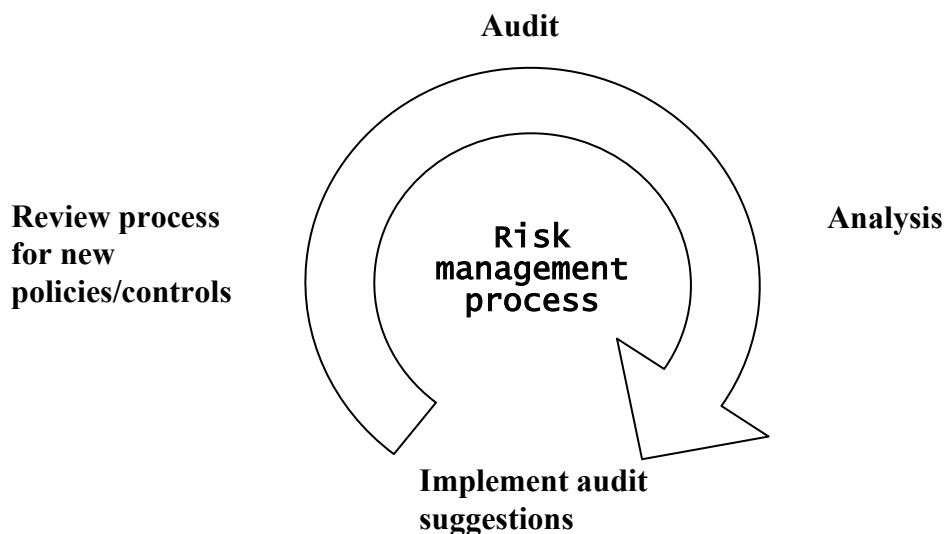
Exposure to IIS specific vulnerabilities	High	Ensure that the server is not vulnerable to known Web-based security attacks (CGI, HTTP, etc)	High	CGI-based attacks can destroy data and services
--	------	---	------	---

In the light of the control objectives framework the web server risk evaluation focused on two general and one application controls categories as they applied to web functions - Access controls, Service continuity controls, and System software controls. Where Access controls limit or detect access to computer resources to protect these resources against unauthorized modification, loss, and disclosure; Service continuity controls ensure that, when unexpected events occur, critical operations continue without interruption; and System software controls limit and monitor access to the “sensitive” programs and files that control the computer hardware and secure applications supported by the system.

1.2 System evaluation

Securing a system is not a single step process. Rather it is a never-ending cycle within a dynamic environment in which new vulnerabilities and threats appear often and have to be address. I consider audit as a vital component of this process. Results of an audit must comply with an established security policy. Adjustments in system settings, as well as change of the policy, should be considered, and the process must then begin anew.

Risk Management Process



The risk management process can comprise the following general audits:

- **Compliance Audits** (based on the organization information security framework)
 - Review of procedures, standards and guidelines to ensure they comply with organization approved policies and best practices
 - Assess the efficiency and effectiveness of security policies and procedures
 - Recommend that policies have been amended to reflect required changes
- **Platform specific Audits** to ensure that policies, procedures and standards for hardware and software have been implemented
- **Technical Audits** to examine of high risk business areas to provide management with assurance that the systems are properly configured according to the organization acceptable security risk level

The web server risk management fits into three types of general audits – compliance with the organization policy, implementation of vendor recommendations and standards, and examination of specific high-risk areas such as Internet business function.

All audits also “fit into one of the fundamental security principles, Defense in Depth”⁴. Taking this line of defense a web server security audit is best done with a structured approach based on the framework and concept of contemporary IT security auditing principles developed by the SANS.

1.2.1 Structured approach

Scope is a very important component of an audit. It gives a clear understanding what an auditor wants to assess or secure. I define scope as the following:

To ensure that the server has adequate control systems and that these comply with the organization and best practices regulations and procedures

The scope of the audit includes examination of IT policies and procedures limited to the web server, evaluating internal controls and testing compliance with best practices recommendations.

The scope defines the checklist – what should to be checked in order to comply with the company procedures and policies and what is the business goal an auditor is trying to reach.

Goal of a Web server security audit is usually a very clear - to assess security of the Web server.

The ultimate purpose of the audit is to check the integrity of the system, to assess its security level at the moment of audit and/or what should be done to make it more secure.

1.2.2 Audit standards

Qualifications, objectivity, independence and due care are essential to effectiveness of security auditing⁵.

- **Qualifications.** An auditor should possess adequate professional knowledge and skills necessary for the audit.
- **Objectivity.** The Auditor should be free from partial and bias judgment. It is important to maintain an objective mental attitude when performing auditing.
- **Independence.** Auditors should be independent of the activities they audit.
- **Professional due care.** Due care should be used in conducting the audit and in preparing related reports. Exercising due professional care means using sound judgment in establishing the scope, selecting the methodology, and choosing tests and procedures for the audit.

1.3 Compliance with written policies and procedures

The auditor should consider whether the written security policies of a company address best practices and governmental regulations relevant to the company's business practices. In a case of a web server the auditor defines compliance via interviewing process and testing.

1.3.1 Current state of practice.

1.3.1.1 Standards and regulations

In the last century arguably the most widely used standard was British Standard BS7799, which provided an overview of security issues to analyze in several areas⁶. It was originally published in the mid-nineties and then evolved in BS EN ISO 17799 in 2000. The ISO/IEC 17799⁷ international standard is based on security requirements established by the British Government form BS 7799 Part I. It is the only standard that has a global acceptance. In addition, it has essentially become the de facto standard in the Asia/Pacific region.

The standard not only covers IT related elements, but other elements such as physical and environmental security, personnel security, and business continuity management and relevant processes. In spite of popularity of ISO 17799 "it remains an incomplete and unevenly level-set document. In some areas of

control, ISO 17799 goes into substantial detail, while other areas are completely missing or addressed only at the macro level“⁸

The American standard **COBIT**⁹ is widely used in Australia, Canada, Philippines, and several other countries. COBIT has been developed as a standard for Information Technology security and control practices that provides a reference framework for management, users, and IS audit, control and security practitioners.

The COBIT¹⁰ Executive Summary states: "Organizations must satisfy the quality, fiduciary and security requirements for their information, as for all assets. Management must also optimize the use of available resources including data, application systems, technology, facilities and people. To discharge these responsibilities, as well as to achieve its objectives, management must establish an adequate system of internal control."

Audit Guidelines of this document outline and suggest specific activities to be performed corresponding to each of the 34 high-level IT control objectives, while substantiating the risk of control objectives not being met. This standard is relatively small in size and independent of the technical IT platforms adopted in an organization.

According to the COBIT the Control Objectives consist of:

- the development of a framework for control in IT as a foundation for the IT control objectives and as a driver for consistent research in IT audit and control;
- an alignment of the overall framework and individual control objectives, with existing de facto and de jure international standards and regulations;
- a critical review of the different activities and tasks underlying the control domains in IT and, where possible, the specification of relevant process performance benchmarks (norms, rules, etc.); and
- a critical review and update of the existing guidelines for performing information systems audits.

In summary COBIT is more business related whereas ISO 17799 is specifically Security related.

Federal Information System Controls Audit Manual (FISCAM) was developed to support financial statements audits. Now this standard is also used for non financial audits. The standard covers Entity wide Security Program, Access Controls, Application Software, System Software, Segregation of Duties, and Service Continuity.

The table below (from Symantec.com) lists widely acceptable standards and regulations that enterprise customers and government agencies are required to adhere to.

Standard/ Regulation	Industry	Type	Comments/URLs
ISO/IEC 17799	International - Baseline	Standard	"The International Organization for Standardization" www.iso-17799.com
BS 7799 Part 1	British Government	Standard	British Standard. Predecessor to ISO 17799 standard
AS4444/NZS4444	Australian Government	Standard	Australian Standard/New Zealand Standard. Replaced by ISO 17799 standard
HIPAA	Health Care	Regulation	Health Insurance Portability And Accountability Act of 1996.
CIS Benchmarks	Worldwide Consortium	Standard	The Center for Internet Security Solaris Benchmark
Gramm-Leach-Bliley Act (GLBA)	US Financial Services Law	Regulation	US Legislation passed Nov. 1999.
SANS/FBI Top 20 List	General Security	Standard	System Administration, Networking and Security/Federal Bureau of Investigation
CVE	General Security		MITRE's Common Vulnerabilities and Exposures
VISA	Banking	Standard	Visa International and Visa USA
ISO 15408 (Common Criteria)	International Security Program - Systems	Standard	May be replacing NSA's Red Book and Orange Book
CASPR	GNU Best Practices	Standard	Commonly Accepted Security Practices & Recommendations
OCC	Banking	Regulation	Office of the Comptroller of the Currency
FDIC	Banking	Regulation	Federal Deposit Insurance

			Corporation
SysTrust	AICPA	Standard	American Institute of Certified Public Accountants
FISCAM	GAO (Federal Govt.), Financial Systems	Regulation	Federal Information Systems Control Audit Manual
CobiT	ISACA	Standard	Control Objectives for Information and Related Technology
SEC	Brokerage	Regulation	U.S. Securities and Exchange Commission
Rainbow Series (Orange Book)	Military commands and contractors	Regulation	Being replaced by Common Criteria
FDA	Pharmaceutical	Regulation	Food and Drug Administration
NPG 2810 (NASA)	Facilities and Contractors	Regulation	NASA Policy Guideline
1974 Privacy Act and Amendments	US Companies	Regulation	www.usdoj.gov/04foia/privstat.htm
ISO 13335(Parts 1,2,3,4,5)	International - Educational	Technical Report	A five-part technical report giving guidance on security management.
SAS70	Auditing	Standard	Statement on Auditing Standards
GASSP	Older than CASPR	Standard	Generally Accepted Systems Security Principles
DITSCAP/NIACAP	Department of Defense (DOD)	Regulation	DoD Information Technology Security Certification and Accreditation Process
AS/NZS 4360:1999	Australian/New Zealand Government	Standard	Australian Standard / New Zealand Standard

FCC	US Government	Regulation	Federal Communications Commission
Other Standards	---	Standard and Regulation	http://www.auscert.org.au/Information/standards.html
RFC2196	Information Security	RFC	Site Security handbook

1.3.1.2 IIS benchmarks and guides

Last December in a joint initiative the national State Auditors Association and the US General Accounting Office (GAO) published a guide “Management Planning Guide for Information Systems Security Auditing”. Members of the National State Auditors Association (NSAA) and auditors from local government cooperated with the GAO to produce the guide. Security auditors can use the guide to develop a path for auditing that includes developing a strategy, implementing an audit, and assessing the results of an audit. The guide helps outline critical aspects of IT security audits, determine an audit environment, identify business and legal risks, and assess costs associated with IT security.

As of December 2002 the National Institute of Standards and Technology's security center has not released its guide to secure Microsoft IIS 5.0 server. However the "System Administration Guidance for Windows 2000 Professional," for system administrators has been released. It includes configuration guides, checklists and templates for applications such as Web browsers, antivirus software and e-mail clients. Another important document is Microsoft Prescriptive Guidance “Security Operations Guide for Windows 2000 server”¹¹.

Security benchmarks are available at www.cisecurity.org. The Consensus Baseline Security Settings provide detailed steps that administrators ought to implement. Some of the recommendations go without saying—or at least have been said many times before—but their breadth and depth provide a solid guideline for IT administrators.

SANS publishes annually a list of critical known security vulnerabilities www.sans.org/top20.htm known as “The SANS/FBI Top 20”. Some of them are independent of a system, but plenty of vulnerabilities are Microsoft specific and can be applied to the IIS server. Most of vulnerabilities are fixed by installation of the latest Service packs and security patches; others must be addressed using specifically tuned checklists and procedures.

1.3.2 Need for Improvement

The need to improve the current situation with regard the Server auditing comes down following points.

1. Free auditing Tools can increase efficiency and accuracy of the audit process.
2. Microsoft/ SANS checklists lack the audit format and categories

2 Audit Checklist

Checklists are important type of procedure to be used in an audit. In the context of the Time Based Security, checklists are related to the category of Protection when an auditor/administrator implements the standardized barriers to prevent penetration of the defense layers.

Microsoft provides extensive security configuration checklists that it recommends for sites that are exposed to the public Internet¹². Another great baseline is Top twenty SANS vulnerabilities¹³ which is smaller.

2.1 Internet Information Server Security Checklist

2.1.1 Policies and procedures

Reference	Company policy and procedures
Control Objective	Policies, procedures, and standards are available and en force.
Risk	Loss of server resources and company reputation
Compliance	Company policy and procedures
Test	<input type="checkbox"/> Physical security is implemented <input type="checkbox"/> Incident response procedure is developed <input type="checkbox"/> Security Best practices are implemented <input type="checkbox"/> Administration of web is secured <input type="checkbox"/> Hardware failure, backup and recovery procedures are implemented
Objective test	Are policies/procedures current? Are they enforceable?

2.1.2 Server Administration

Reference	Web Server - version 1.4 dated September 13, 2001
Control Objective	Adequate Administrator Support
Risk	Inadequate administrative support may lead to the server being compromised
Compliance	Best practices recommendations
Test	<input type="checkbox"/> System administrator has successfully completed vendor provided (or equivalent) training for the server administration. Name of System Administrator: _____ Date and location of training: _____ <input type="checkbox"/> System administrator or backup administrators are reachable by telephone (pagers) or email. <input type="checkbox"/> All administrators have access to the space in which the server is located.

	<input type="checkbox"/> Administration duties for the operating system and application have sufficient separation so as to preclude system mis-configuration.
Objective test	Subjective - administrator training and knowledge. Objective – certifications.

2.1.3 Physical security

Reference	Company policy and procedures
Control Objective	Physical security is a part of the departmental security policy Physical access to server is restricted to authorized users The Policy describes a physical access procedure Physical security controls are sufficient to protect the server resources from theft, fire, flood, malicious destruction, and power failure
Risk	Data theft and tampering, fire, flood, malicious destruction, and power failure
Compliance	Location must be secure, access restricted to operational personnel
Test	<input type="checkbox"/> Location is secure <input type="checkbox"/> Policy and access procedure exist <input type="checkbox"/> Web server is a stand-alone server <input type="checkbox"/> Surge protector is on <input type="checkbox"/> Backup power system is used
Objective test	Is location secure? Are physical security controls implemented?

2.1.4 Business continuity

Reference	Company policy and procedures
Control Objective	Web server operations are included into the disaster recovery plan
Risk	Loss of server resources. Substantial downtime.
Compliance	Disaster recovery plan
Test	<input type="checkbox"/> Web server operations included into the disaster recovery plan <input type="checkbox"/> System Administrator has a current Emergency Recovery Disk in a locked storage area <input type="checkbox"/> Universal Power Supply is implemented <input type="checkbox"/> Fixed IP (if DHCP fails)
Objective test	Are policies published? Are they current? Are they frequently tested?

2.1.5 Server configuration

Reference	Microsoft recommendations and updates.
------------------	--

	http://www.microsoft.com/technet/security
Control Objective	Win 2000 Server is configured in accordance to the best practices Periodic review of the server configuration is conducted
Risk	Server is vulnerable to networking attacks.
Compliance	Microsoft recommendations on security
Test	<input type="checkbox"/> Required Patches and hotfixes are installed <input type="checkbox"/> Win 2000 Server is configured in accordance to the best practices. MBSA Level 1 Score _____ <input type="checkbox"/> Configuration baseline exists <input type="checkbox"/> Multiple disks or partition volumes <input type="checkbox"/> Protocol stacks only TCP/IP <input type="checkbox"/> There are no modems connected to this server <input type="checkbox"/> No File and Printer Sharing for Microsoft Networks <input type="checkbox"/> Server can be shutdown only by Administrator <input type="checkbox"/> URL scan is installed
Objective test	Verifiable results

2.1.6 Unauthorized Access to resources.

Reference	Company policy and procedures
Control Objective	To determine that Authentication and Access controls are in place
Risk	Breach of confidentiality, integrity and availability of services
Compliance	Company policy and procedures. Best practices recommendations
Test	<input checked="" type="checkbox"/> Policies, procedures, and practices address access controls for web based systems and applications <input type="checkbox"/> Accounts are authenticated through the use of passwords <input type="checkbox"/> Account authentication is done in such a way to prevent eavesdropping (i.e. userid and password not sent in clear) <input type="checkbox"/> Guest / anonymous accounts/access are not allowed <input type="checkbox"/> No network access without explicit anonymous permissions <input type="checkbox"/> Automatic logon as Administrator is disabled. <input type="checkbox"/> There is a written enforced process for establishing, using, and terminating an account (or service) for this server. <input type="checkbox"/> A session is time out due to user inactivity <input type="checkbox"/> A standard defining warning banners usage is in place. The banners displayed to users addressing website <input type="checkbox"/> Logon banner contains an abbreviated version of the organizational acceptable use policy is displayed at logon for each user. <input type="checkbox"/> Logon banner advises users that use is subject to

	monitoring and that use constitutes consent to monitoring.
Objective test	Verifiable results

2.1.7 System Auditing

Reference	Microsoft recommendations and updates. http://www.microsoft.com/technet/security
Control Objective	System Configuration is monitored
Risk	Possible breach of system integrity
Compliance	Best practices recommendations
Test	<ul style="list-style-type: none"> <input type="checkbox"/> System auditing and logging functions enabled to capture audit trials <input type="checkbox"/> Auditing is configured to minimally audit - <ul style="list-style-type: none"> Account Logon Events (Success and Failure) Account Management (Success and Failure) Logon Events (Success and Failure) Object Access (Failure) Policy Change (Success and Failure) Privilege Use (Failure) System Events (Success and Failure) <input type="checkbox"/> System, security, and server logs are daily monitored for surveillance, DoS, and legitimate use patterns. <input type="checkbox"/> Alert notification is established <input type="checkbox"/> Audit logs are copied to a secure remote location
Objective test	Verifiable results

2.1.8 File System Configuration.

Reference	Microsoft Win2000 checklist. Windows 2000 Risk Assessment Helpfile
Control Objective	Proper file system configuration
Risk	Confidentiality, integrity, availability of services
Compliance	Best practices recommendations
Test	<ul style="list-style-type: none"> <input type="checkbox"/> System is configured as NTFS file system <input type="checkbox"/> Wiping of system page file occurs at system shutdown (sensitive information from process memory that may have made into the page file is not available to a snooping user. <input type="checkbox"/> Log file size is set high enough to prevent events from being overwritten. <input type="checkbox"/> NTFS permissions for website content volume (Full control for Administrators and System only). <input type="checkbox"/> Multiple disk or partition volumes. The content is separated from the rest of Web site. <input type="checkbox"/> IIS Read permission only for static content. Check for Script files and Other Executable and Include Files and

	Metabase permissions. <input type="checkbox"/> Disable File and Printer Sharing
Objective test	Verifiable results

2.1.9 Accounts

Reference	Company policy. Best practices recommendations for passwords http://www.nswc.navy.mil/ISSEC/Form/AccredForms/passwords
Control Objective	Password administration policy and procedures are in place
Risk	Breach of confidentiality, access to server resources
Compliance	Best practices recommendations, company policy and procedures
Test	<input type="checkbox"/> Best Practices for Passwords. Minimum Password Age -- 1 Day Maximum Password Age -- 90 Days Minimum Password Length -- 8 characters Password Complexity -- Required Password History -- 24 Remembered Store passwords using reversible encryption - disabled Account Lockout Duration -- 30 Minutes Account Lockout Threshold -- 5 Bad Login attempts Reset Account Lockout After -- 30 Minutes <input type="checkbox"/> User passwords are known only by the user <input type="checkbox"/> Users are required to maintain unique passwords <input type="checkbox"/> Administrator password is protected <input type="checkbox"/> Password is enabled for screen saver. <input type="checkbox"/> Secure IIS accounts. IUSR_computername (IUSR_computername moved from the Guest group to the Webusers group, used solely for web site access. Check account privileges). <input type="checkbox"/> Separate IIS admin group
Objective test	Verifiable results

2.1.10 Services required

Reference	Company policy and procedures
Control Objective	Ensure that unneeded services are disabled
Risk	Known vulnerabilities. Possible breach of confidentiality, integrity and availability
Compliance	Company policy and procedures
Test	Services are disabled: <input type="checkbox"/> Accessories and utilities (standard Windows Accessibility features (entertainment, games, communications, accessibility) <input type="checkbox"/> Certificate services. The web server rarely needs to be a certificate server

	<input type="checkbox"/> MS Indexing Service <input type="checkbox"/> Management and Monitoring Tools <input type="checkbox"/> Message Queuing Services <input type="checkbox"/> Networking Services <input type="checkbox"/> Other Networking File and Print Services <input type="checkbox"/> Remote Installation Services <input type="checkbox"/> Remote Storage <input type="checkbox"/> Script Debugger <input type="checkbox"/> Windows media Services <input type="checkbox"/> Uninstall any Resource kit or SDK IIS Recommended Services only: <input type="checkbox"/> Common files <input type="checkbox"/> IIS Snap-In <input type="checkbox"/> WWW Server Turn off the NetBIOS if possible <input type="checkbox"/> NetBIOS over TCP is disabled
Objective test	Verifiable results

2.1.11 Backup

Reference	Microsoft recommendations and updates http://www.microsoft.com/technet/security
Control Objective	Backup/restoration policy is well documented and in place. The policy addresses method, frequency, storage, rotation schedule, restoration and notification procedures
Risk	Possible loss of data. Increased server downtime
Compliance	Backup requirements
Test	<input type="checkbox"/> Backup/restoration policy exists and enforced <input type="checkbox"/> Backup/restoration are tested on a regular basis
Objective test	Verifiable results

2.1.12 Monitoring/Intrusion detection procedure

Reference	Windows 2000 Risk assessment form Version 1.5 dated October 1, 2002
Control Objective	Proactive and reactive Monitoring procedures are defined. IDS detects unauthorized and malicious activity
Risk	Misuse of computer resources
Compliance	Company policy and procedures
Test	<input type="checkbox"/> Monitoring procedures are clearly defined. <input type="checkbox"/> Monitoring tools have been installed as defined in the policy <input type="checkbox"/> Monitoring Reports are generated and regularly reviewed <input type="checkbox"/> If used, monitoring device(s) is approved in writing by the department manager (Including operating IS network interface in promiscuous mode)

	<input type="checkbox"/> Policies and procedures address intrusion detection <input type="checkbox"/> Automated notification process is in place <input type="checkbox"/> Unauthorized attempts to access the server are logged and included into security violations report <input type="checkbox"/> IDS logs are regularly reviewed and analyzed <input type="checkbox"/> Escalation process is defined <input type="checkbox"/> Vulnerability assessment procedure is defined
Objective test	Verifiable results

2.1.13 Malicious Code

Reference	Windows 2000 Risk assessment form Version 1.5 dated October 1, 2002
Control Objective	Malicious code controls are in place
Risk	Breach of confidentiality, integrity, and availability
Compliance	Company policy and procedures
Test	<input type="checkbox"/> Policies and procedures address malware detection and prevention <input type="checkbox"/> Notification procedure is established <input type="checkbox"/> Distribution of DAT files is secured <input type="checkbox"/> Antivirus tools are prevented from being disabled <input type="checkbox"/> All vendor recommended Security-related patches have been applied <input type="checkbox"/> Software that can detect modifications to files is run on regular basis. <input type="checkbox"/> Name of software package: _____ Frequency of virus scan: _____ <input type="checkbox"/> Automatic or manual (underline one) <input type="checkbox"/> Windows Scripting Host is disabled
Objective test	Verifiable results

2.1.14 Vulnerability testing

Reference	Web Server assessment form - version 1.4 dated September 13, 2001
Control Objective	Adequate functioning of the server under attack
Risk	Misuse, malicious activity
Compliance	Company policy and procedures
Test	<input type="checkbox"/> Vulnerability assessment test has been performed by an auditor <input type="checkbox"/> Vulnerability assessment tests are conducted regularly on a scheduled basis as well as after an incident <input type="checkbox"/> Vulnerability Testing was conducted against the operating system and server application. <input type="checkbox"/> Name of tool used (_____ <input type="checkbox"/> Version number of tool used (_____.

Objective test	Verifiable results
-----------------------	--------------------

2.1.15 System Modifications

Reference	Company policy and procedures
Control Objective	Detect system modifications. Compliance with the baseline. Web server security controls are implemented
Risk	System changes detection is not an inherited mechanism in IIS server therefore an absence of this mechanism creates a substantial risk of missing detection of malicious activity
Compliance	Baseline
Test	<input type="checkbox"/> No unexpected Files change <input type="checkbox"/> No unexpected services change <input type="checkbox"/> A procedure how HTML pages are secured to prevent unauthorized changes is implemented
Objective test	Verifiable results

2.1.16 Information posting and disclosure

Reference	Web Server risk assessment form - version 1.4 dated September 13, 2001
Control Objective	Information Posting Process is defined
Risk	Misuse of resources, breach of confidentiality
Compliance	Company policy and procedures
Test	<input type="checkbox"/> Process for the identification of information appropriate for posting to Web site is <i>attached to this form</i> <input type="checkbox"/> A copy of the written process used to review and approve web page content is attached. <input type="checkbox"/> Traffic is encrypted. If traffic is encrypted, list method and level of encryption _____ <input type="checkbox"/> Confidential documents are not stored on the server

2.1.17 Web specific

Reference	Web Server risk assessment form - version 1.4 dated September 13, 2001. Best practices.
Control Objective	Web content and scripting standards are implemented
Risk	The scripts can be run from the outside and harm confidentiality, integrity and availability of server
Compliance	Best practices recommendations
Test	<input type="checkbox"/> Access to CGI directories is limited <input type="checkbox"/> Users can not install CGI scripts <input type="checkbox"/> Programs and administrative scripts are not on the website content volume <input type="checkbox"/> Logical directory structure is implemented (separate

	<p>static content, asp, html, scripts, executables)</p> <ul style="list-style-type: none"> <input type="checkbox"/> No development tools or application software on the web server <input type="checkbox"/> Default website moved <input type="checkbox"/> Server Application does not use cookies. <ul style="list-style-type: none"> if FALSE <ul style="list-style-type: none"> (1) Cookie policy is displayed on server and attached on form. (2) Rationale is described in section entitled "ADDITIONAL COMMENTS AND EXPLANATIONS"
Objective test	Verifiable results

2.1.18 Web Audit trails

Reference	Web Server risk assessment form - version 1.4 dated September 13, 2001.
Control Objective	Inadequate audit trails
Risk	Misuse of resources
Compliance	Best practices recommendations
Test	<ul style="list-style-type: none"> <input type="checkbox"/> Logging settings: W3C Extended logging is enabled <input type="checkbox"/> Automated audit logs are maintained for at least 1 year <input type="checkbox"/> Web activity is logged in syslog or similar <input type="checkbox"/> Auditing is configured to record full web transactions <input type="checkbox"/> Logfile analysis is automated and accomplished daily <input type="checkbox"/> Reports of anomalous activity are sent automatically to the system administrator <input type="checkbox"/> Procedure defining who reviews logs and how often is implemented
Objective test	Verifiable results

Objective/Subjective

Most of the checklist tests are objective.

Objective elements:

- Documentation
- Documented hardware/software configuration
- Services and ports
- Network traffic
- Output of auditing tools

Subjective elements:

- Management's attitude toward security
- Administrator level of expertise
- User awareness

3 Audit of the server

3.1 Tools

Purpose of the auditing tools is to automate the tedious, time-consuming process of manually checking system logs, file integrity, network services, and checking vulnerabilities. Although the most common way to perform an audit still is a manual check list method which provides better opportunity to better understand security configuration of the system, the audit automation is positioning itself in a multi system implementation as well as under time constraint.

There are plenty of freeware tools available for all phases of securing a Web server. There are also some good commercial tools available such as Configuration Auditor2.0 from Ecora Software www.ecora.com, Web Application Security kit from SPI Dynamics www.spidynamics.com, [WhiteHat Arsenal](#), and others. Latest commercial tools are presented in Information Security magazine December 2002 issue¹⁴.

Independence

It is generally understood that the IS security audit capability should be independent of the area being audited so that the audit will be objective. However, to help ensure that this independence exists both in fact and perception, it is recommended that independence and outside sources be used. The neutral, independent tools and methods provide a **degree of separation** between audit capability and the audit area, thus increasing the level of objectiveness in the audit process.

One tool is good, but two are better

The auditor can find on the Internet and general market plenty of great commercial and freeware tools for the specific purposes of the audit, however she should keep in mind that there is no ideal universal tool to cover all tasks of the audit process. Thus, it is a safe approach to use multiple tools to verify and compare results.

Play the trust game

As often happens with the freeware tools the auditor must be careful enough to verify the integrity of the tool to use. It would be a terrible thing to conduct an extensive audit with a tool that was later called into question -- the results of the audit itself would be compromised.

Trust of the tool and integrity of its distribution became so important that commercial distributions of some tools offer a digital signature for all release binaries on companies' Web sites.

It might be appropriate to subject the tool itself, to its own security audit for integrity and quality of the overall audit.

3.2 Conduct an audit

10 most significant security concerns

3.2.1 Test 1 Policies and procedures

Control Objective: Policies, procedures, and standards are available and enforced.

Risk: Loss of server resources and company reputation

Compliance: Company policy and procedures

Test:

- Physical security is implemented
- Incident response procedure is developed
- Security Best practices are implemented
- Administration of web is secured
- Hardware failure, backup and recovery procedures are implemented

Objective test: Are policies/procedures current? Are they enforceable?

Results: Policies and procedures are current. However, not all the policies are enforceable.

3.2.2 Test 2 Server configuration

Control Objective: Win 2000 Server is configured in accordance to the best practices. Periodic review of the server configuration is conducted

Risk: Server is vulnerable to networking attacks.

Compliance: Microsoft recommendations on security

Test:

- Required Patches and hotfixes are installed
- Win 2000 Server is configured in accordance to the best practices.
MBSA Level 1 Score 7.3
- Configuration baseline exists
- Multiple disks or partition volumes
- Protocol stacks only TCP/IP
- There are no modems connected to this server
- No File and Printer Sharing for Microsoft Networks
- Server can be shutdown only by Administrator
- URL Scan is installed

Objective test: Verifiable results

Service pack information is available using winver command at the prompt of the server.



It is **critical** to know which patches have been applied to your system and, more importantly, which have not.

For checking hotfixes/patches on a server there are two tools available:

- Network Security Hotfix Checker¹⁵
- Windows Update from the IE Tools menu

With **Network Security Hotfix Checker** a baseline is the list of bulletins that are reported.

To monitor hotfix daily, I created a baseline report:

```
hfixchk > hotfix.log
```

Next, I created a command file with these two lines:

```
hfixchk > todayshotfix.log  
fc /L hotfix.log todayshotfix.Log
```

A shortcut to the file can be used to expedite the process.

Windows Update¹⁶ is another useful program. I always install everything in the Critical Update category and most things in the recommended category.

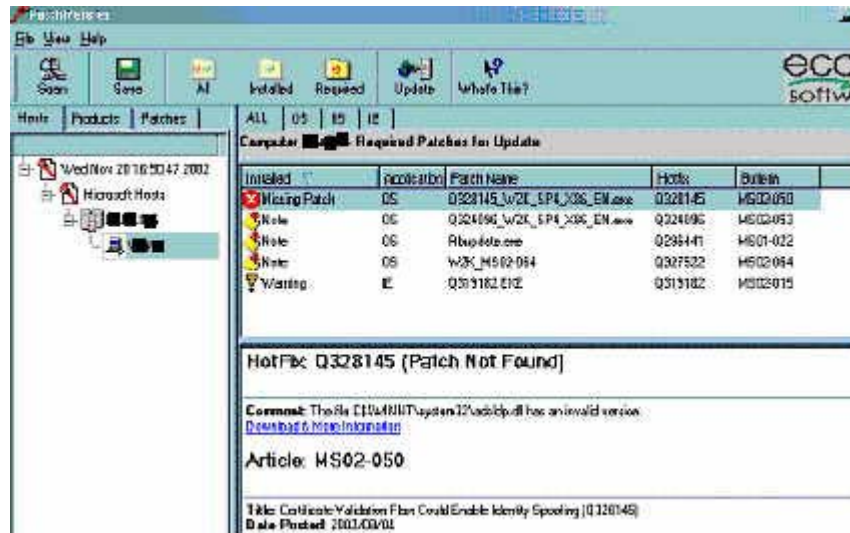
HFNetChk

Shavlik¹⁷ has released a command-line tool that enables an auditor to check the patch status of all the machines in a network from a central location.

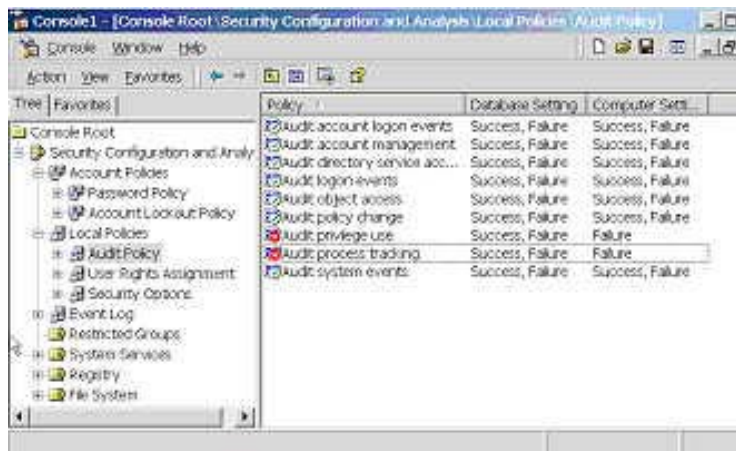
HFNetChkLT is the GUI based free version of HFNetChkPro – the industry standard patch management solution.

Ecora Patchmeister¹⁸

This utility is also very useful to check the latest updates.



Security analysis tool. This built in utility is very useful to apply templates and analyze account policies, groups, local policies, user rights, security options, services, and the registry of the server.



MBSA Microsoft Baseline Security Analyzer¹⁹

MBSA is a graphical utility, host based analysis I use superset of the functionality of HFNetChk. Whereas HFNetChk only deals with hotfixes and service packs while MBSA together with security policies and hot fixes checks provides an

easy-to-use interface and additional capabilities. These capabilities include examining servers for common security best practices such as strong passwords, common security mis-configurations, and checking for mis-configured security zone settings in Microsoft Office, Outlook, and Internet Explorer. It uses a continuously updated XML file from Microsoft Web site that contains a list of security patches and latest Microsoft security recommendations. MSBA checks user accounts in the local admin group, Guest account availability, simple or blank passwords, the type of file system, auditing availability, restrict anonymous settings, shares, autologon, and unnecessary services. The auditor can configure the list of unnecessary services listed in the Services.txt file that by default contains FTP, Telnet, WWW, SMTP, and RAS services. For IIS specifically the tool checks for all current IIS hotfixes, availability of IIS Lockdown tool, sample applications, and whether IIS is running on a domain controller.



This tool can also be efficiently used for continuous auditing of the server. Rather than using GUI interface I prefer to run the script at scheduled intervals.

Windows Benchmark Tool

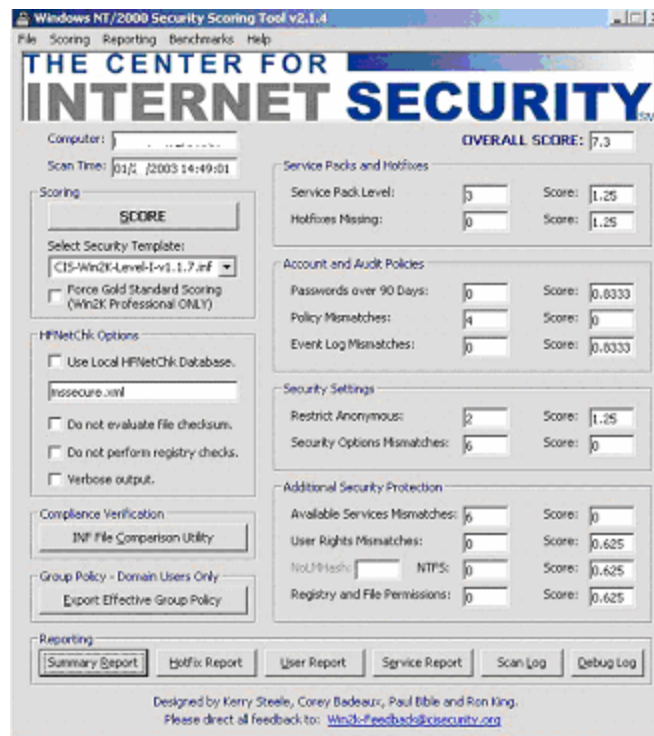
The Center for Internet security²⁰ is developing and implementing an excellent group of automated tools for scoring and monitoring the status of Benchmark settings. This approach for standardization of the benchmarking procedure across industries deserves high marks.

The Center has issued two benchmarks:

- **Level-1** Benchmark for Windows 2000 (v1.1.7) - is based on consensus minimum due care security configuration recommendations for Windows 2000 servers and workstations.

- Level-2 Windows 2000 Professional Operating System Benchmark - Consensus Baseline Security Settings (v1.0)** – is based on consensus beyond the minimum due care level for Windows 2000 workstations. This Benchmark reflects the content of the Consensus Baseline Security Settings document developed by the Members of The Center for Internet Security (CIS), The SANS Institute, and the following agencies of the United States federal government: The National Security Agency (NSA), The Defense Information Systems Agency (DISA), The National Institute of Standards and Technology (NIST), and The General Services Administration (GSA).

Each benchmark comes with an automated testing tool, *cis-scan*, which may be run on an individual system. The tool checks each of the configuration steps listed in the benchmark document and provides a 1-10 score to indicate what percentage of the benchmark items have been performed on the machine. The *cis-scan* tool also writes a report file, which indicates the status of each item from the benchmark and provides other diagnostic information. The *cis-scan* is a host based tool.

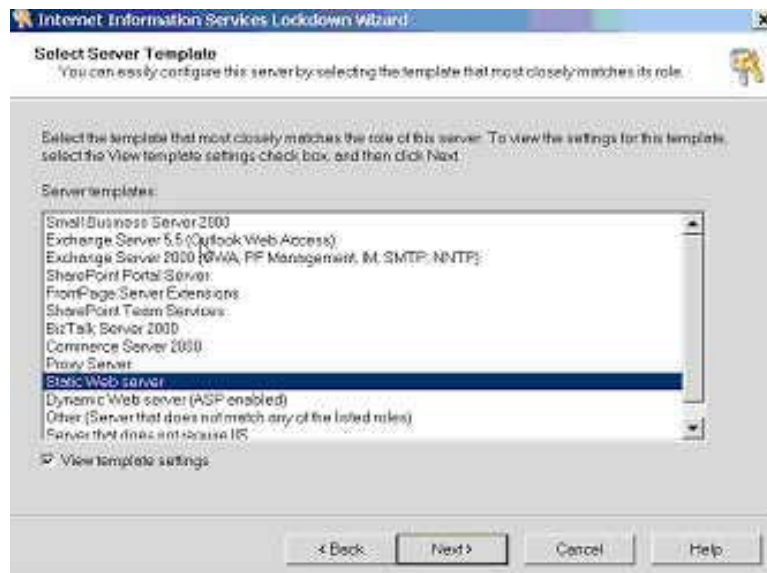


Although the benchmarks based on the best practices they do not contain all possible secure options respectfully, thus every organization is encouraged to customize benchmark according to its business needs. As indicated in the tool's documentation the current version of the tool only checks for exact compliance with the benchmark, meaning that even a more secure setting will be considered

a negative since it doesn't match the benchmark (for example my password age policy is maximum 42 days while major requirements are 90 days)

URLScan

URLScan²¹ scans the incoming requests to the IIS server and rejects those that don't match a set of rules that you define. For example, URLScan can filter based on URL length, character set, content, and other criteria. The version 2.1 has been integrated with the IIS Lockdown Wizard to provide automated configuration solution and saves time.



The wizard recommends the services for the security template, removes unselected services, disables script mappings and makes additional changes to strengthen security. For example IIS 5.0 installs with samples to demonstrate how to set up the server. These samples are known vulnerabilities to attack, because hackers know where they are and how to leverage them. The wizard removes selected virtual directories and disables remote Web content authoring. In a final step the wizard installs URL scan filter on the server.



Results: Missing hotfixes and patches. The benchmark score is 7.3 at the Level 1 benchmark.

3.2.3 Test 3 Monitoring/Intrusion detection procedure

Control Objective: Proactive and reactive Monitoring procedures are defined. IDS detects unauthorized and malicious activity

Risk: Misuse of computer resources

Compliance: Company policy and procedures

Test:

- Monitoring procedures are clearly defined.
- Monitoring tools have been installed as defined in the policy
- Monitoring reports are generated and regularly reviewed
 - If used, monitoring device(s) is approved in writing by the department manager (Including operating IS network interface in promiscuous mode)
- Policies and procedures address intrusion detection
- Automated notification process is in place
- Unauthorized attempts to access the server are logged and included into security violations report
- IDS logs are regularly reviewed and analyzed
 - Escalation process is defined
- Vulnerability assessment procedure is defined

Objective test: Verifiable results

Results: Monitoring devices use is not approved in writing by the manager. Escalation process is not clearly defined. However, the organization policy requires report all sever attacks to the ISO.

3.2.4 Test 4 System Auditing

Control Objective: System Configuration is monitored

Risk: Possible breach of system integrity

Compliance: Best practices recommendations

Test:

- System auditing and logging functions enabled to capture audit trials
- Auditing is configured to minimally audit -
 - Account Logon Events (Success and Failure)
 - Account Management (Success and Failure)
 - Logon Events (Success and Failure)
 - Object Access (Failure)
 - Policy Change (Success and Failure)
 - Privilege Use (Failure)
 - System Events (Success and Failure)
- System, security, and server logs are daily monitored for surveillance, DoS, and legitimate use patterns.
- Alert notification is established
- Audit logs are copied to a secure remote location

Objective test: Verifiable results

In an entry process an auditor with a manager should determine the level of auditing appropriate for the auditing environment. In the case of a production web server the more information we get the more appropriate will be the vulnerabilities assessment. However, the auditor should bear in mind that the more events log files generate the more difficult to spot critical events.

Audit events can be split in two categories: success events and failure events²². Success events are more difficult to interpret since the normal operations assume successful access to server resources. Failure events are useful in tracking attacks on the server, especially when they establish a pattern. Security auditors consider patterns almost as important as the events themselves. It is recommended to combine audit events with other information about users' activity, for example working hours, vacation, etc.

Audit event	Possible threat
Multiple Logon/logoff failures	Attack on passwords
Suspicious logon/logoff successes	Stolen credentials
User and Group management changes to users and groups	Misuse of user rights
Printer success and failures	Incorrect printer permissions

Successful and unsuccessful object/file access, such as attempts to write to program files (.exe and .dll)	Virus, incorrect permissions for sensitive files
Unexpected System restarts and shutdowns, and other dubious system events	Backdoor

There are three logs: system, security and application. From a security perspective the “do not overwrite” setting is best. However, the server halts when its logs become full. Considering inexpensive hard drive storage a maximum size of a log > 80 MB will be sufficient.

The first step in setting an audit policy is selecting the types of events that Windows 2000 audits. For each event to audit, the configuration settings indicate whether to track successful or failed attempts. I set audit policies by using the Group Policy snap-in.

By default, security logging is turned off²³. I use Group Policy to enable security logging. To turn on security logging

- Click Start, click Run, type *mmc /a*, and then click OK.
- On the Console menu, click Add/Remove Snap-in, and then click Add.
- Under Snap-in, click Group Policy, and then click Add.
- In Select Group Policy Object, click Local Computer, click Finish, click Close, and then click OK.
 - In Local Computer Policy, click Audit Policy.
 - Local Computer Policy
 - Computer Configuration
 - Windows Settings
 - Security Settings
 - Local Policies
 - Audit Policy

It is recommended to check the following events:

- Logon and logoff
- Use of User rights
- User and group Management
- Security policy changes
- System restarts and shutdowns

The standard **Security Analysis** tool of Win2000 server shows current setting of Audit policies.

For analysis Win2000 logs can be converted to text format in two ways “Save as” *.txt file or using Dumpel

Dumpel

Venerable Dumpel available in the Win NT resource kit is still a great help to analyze Win2000 log files. It dumps the system file by executing the following command:

```
Dumpel -f event.out -l system -t
```

The output file is dump into a tab-separated text file. I use to Excel spreadsheet for easy filtering and sorting.

ELDump²⁴

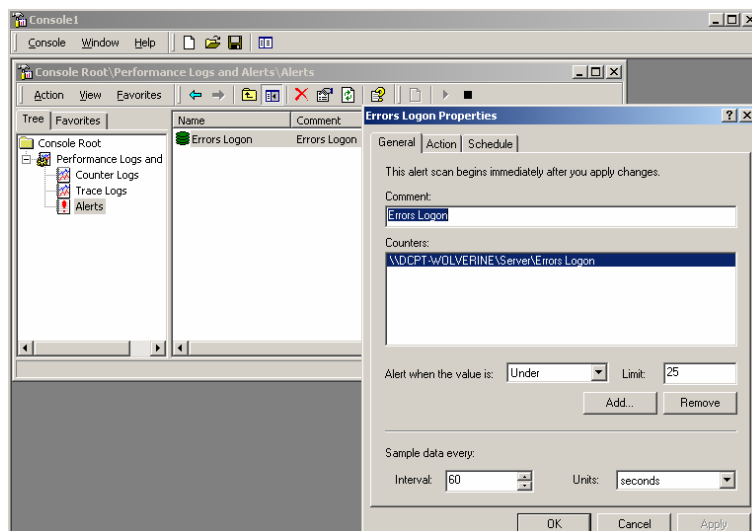
ELDump is a tool to dump the contents of a NT event log as text. It is very much like the Dumpel, but ELDump is more versatile and a lot faster.

Most importantly ELDump can:

- Dump from active event logs or from saved event logs with full message texts.
- Filter on all the same fields as the Event Viewer.
- Dump only the message strings instead of the full message texts.
- Dump several logs from several servers with one invocation of the ELDump command.
- Easily search and dump logs saved with the ELSavClr tool.

Alert notification

The basic Operating system alert notification can be established via MMC Performance monitor. It has capability to create alerts for Errors Access Permissions, Errors Granted Access, and Errors Logon.

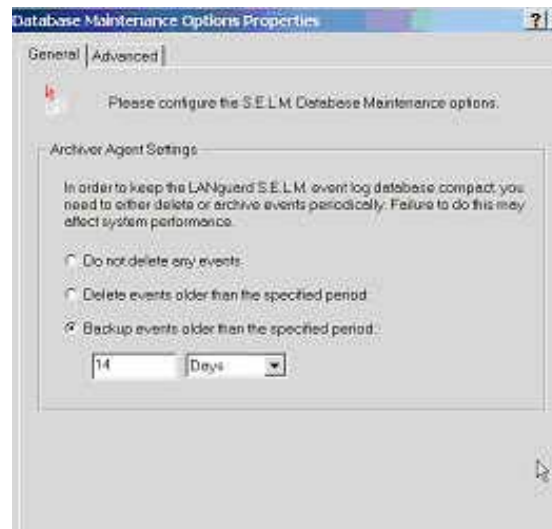


LANguard SELM

LANguard Security Event Log Monitor (S.E.L.M) offers intrusion detection through event log monitoring. It retrieves log events from all NT/2000 servers and workstations on a real time or schedule basis. It has a capability to alert the administrator of possible intrusions for immediate host based intrusion detection. The alerting method is based on the security level of the event.

The program can also create network security reports and identify target machines and local users trying to breach security policies. Because LANguard analyses the system event logs it is not impaired by switches, IP traffic encryption or speed of data transfer.

The reporter requires MDAC 2.5 to function properly. Also the message Queuing Services (MSMQ) must be installed. Back end database for storing the event can be either in Microsoft Access format (MS Access does not need to be installed) or located on the MS SQL server. Since the database needs plenty of space to avoid DOS it is recommended to allocate minimum 1 gigabyte of free space. Of course the disk space used for storing event depends on configuration of the program. Free licenses are currently available for 1 server/5 workstations.²⁵

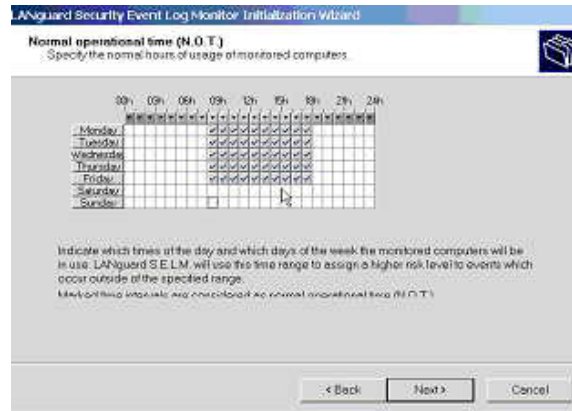


I use the following monitoring values:

- Automatically enable event monitoring
- Purge event logs after retrieving new events

The interval for retrieving security events is set for 14 days. It can be modified per computer basis, depending on business functions.

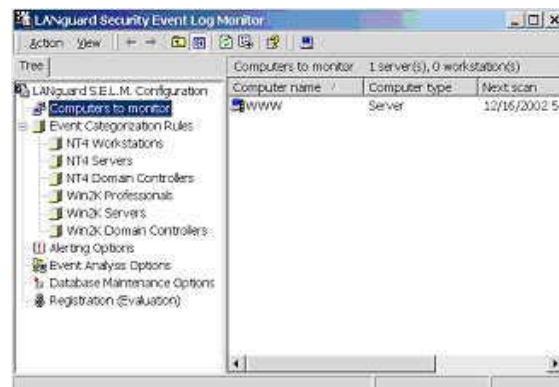
S.E.L.M. uses the operation time range to assign a higher security risk to events happening outside of working hours.



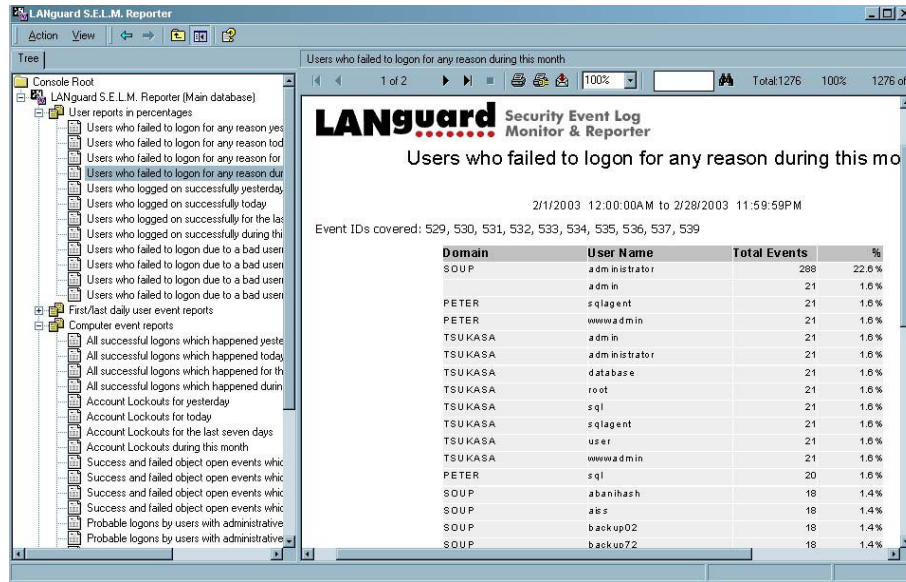
The program specifies the default security level for the analyzing computer. For a web server I use a high security level.



The free program can allow monitoring one server and up to five workstations.



The program generates a log report:



Results: There were multiple attempts to use password privileges to enter the system

3.2.5 Test 5 Services required

Reference: Company policy and procedures

Control Objective: Ensure that unneeded services are disabled

Risk: Known vulnerabilities. Possible breach of confidentiality, integrity and availability

Compliance: Company policy and procedures

Test: Services are disabled:

- Accessories and utilities (standard windows Accessibility features (entertainment, games, communications, accessibility))
- Certificate services. The web server rarely needs to be a certificate server
- MS Indexing Service
- Management and Monitoring Tools
 - Message Queuing Services
- Networking Services
- Other Networking File and Print Services
- Remote Installation Services
- Remote Storage
- Script Debugger
- Windows media Services
- Uninstall any Resource kit or SDK

IIS Recommended Services only:

- Common files
- IIS Snap-In
- WWW Server

- Turn off the NetBIOS if possible
- NetBIOS over TCP is disabled

Objective test: Verifiable results

An auditor must know what services and applications are running on the server which is audited and what ports are open. These details about the system will help uncover potential vulnerabilities.

Check Services configuration at Start >Administrative Tools > Services

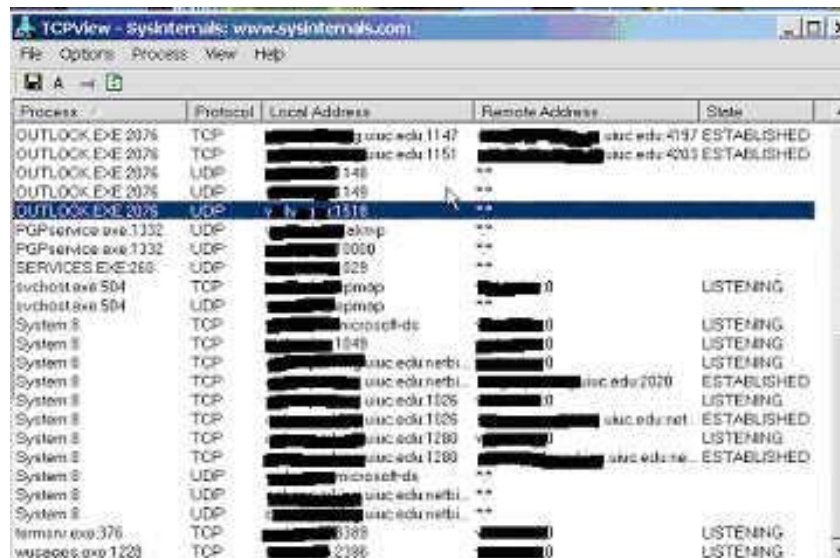
Baseline of services: The NT Resource Kit includes a utility called netsh.exe which allows you to manage services and drivers on remote NT systems. While this is primarily a management tool, one of the switches allows one to document all running services and drivers.

```
C: netsh \web_server /list
```

If the resource kit is not available using the net start command documents running services. However, the command does not work over the network.

TCPView

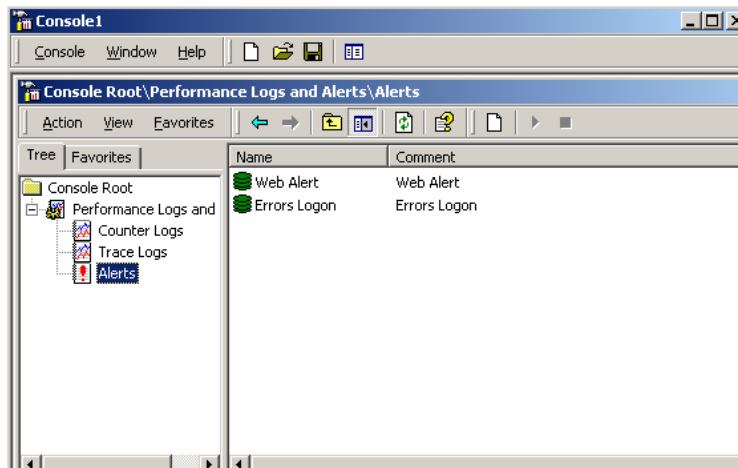
I use TCPView by Mark Russinovich from Sysinternals²⁶
 This nice program shows detailed listings of all TCP and UDP endpoints on the system, including the local and remote addresses and state of TCP connections. On Windows NT, 2000 and XP TCPView also reports the name of the process that owns the endpoint.



IIS logs to WINNT\system32\LogFiles the **IIS Web server log**. This log is already in comma delimited format, and can be easily imported into spreadsheet or database. By default this log is located in %winnnt%\system32\logfiles\w3svcx where x is the web instance. To obtain more information about an event I enable the following fields:

- Client IP address
- User name
- Method
- URI stem
- URI query (filled up by the server when error occurs)
- Protocol status
- Win32 status
- Bytes received
- User Agent

Web alerts system is established in a manner similar to the one for OS alerts via MMC Performance Monitor.



Results:

Normal file retrieval:

*192.168.1.50, -, 12/12/02, 12:23:45, W3SVC, WWW,
XXX..XXX.123.11, 46277, 171, 145, 401, 5, GET,/default.asp, -,*

In the first log entry, the remote system accessed the Web server using a standard anonymous logon. While this is not stated the “-“ the entry following the remote system’s IP address means anonymous logon.

Trying to access as Administrator:

192.168.1.50, Administrator, 12/12/02, 0:20:12, W3SVC, WWW, XXX.XXX.123.11, 20, 214, 317, 302, 0, GET, /password_dir/, -,

In the second entry the word “Administrator” appears because the user at 192.168.1.50 attempted to authenticate through IIS in order to access the password_dir directory.

Log system analysis is not automated. Reports of anomalous activity are not sent automatically to the system administrator. The administrator manually checks the logs.

3.2.7 Test 7 System Modifications

Control Objective: Detect system modifications. Compliance with the baseline. Web server security controls are implemented

Risk: System changes detection is not an inherited mechanism in IIS server therefore an absence of this mechanism creates a substantial risk of missing detection of malicious activity

Compliance: Baseline

Test:

- No unexpected Files change
- No unexpected services change
- A procedure how HTML pages are secured to prevent unauthorized changes is implemented

Objective test: verifiable results

Regdmp. Even though **sysdiff** will report any registry key changes, it’s still a good idea to have a dump of the registry in raw text format in case you need to identify the original value of any key settings.

This can be performed using the regdmp.exe utility. Regdmp is a popular network tool to query remote systems.

I usually run a couple of baselines to determine what is “normal”

```
regdmp -m \\web-server > regfile.txt
```

Win2000 includes a utility called **fc.exe** which can be used for comparing the contents of two files. It is comparing the contents of file1.txt and file2.txt and then generating a third file called diff.txt. The auditor checks diff.txt to see if there have been any changes since our baseline was created. There are a couple of useful switches: the /C switch tells fc to ignore alphabetic case when performing a

comparison. The /N switch is of note because it adds reference line numbers to the diff file. If you are comparing two large files, /N can be valuable when manually checking the files in order to verify the difference that fc has flagged.

Useful switches

-/C - Disregard case

-/N - Display line numbers

fc -N c:\path\file1.txt

c:\path\file.txt > diff.txt

System File Checker (sfc.exe) is another tool included in Windows File Protection Service. It can be used to scan files, detect changes to baseline operation system and replace modified files with the last known good version. This tool is recommended to run whenever file change is suspected.

```
Microsoft(R) Windows 2000 Windows File Checker Version 5.00
(C) 1999 Microsoft Corp. All rights reserved

Scans all protected system files and replaces incorrect versions with correct Microsoft versions.

SFC [/SCANNOW] [/SCANONCE] [/SCANBOOT] [/CANCEL] [/ENABLE] [/PURGECACHE] [/CACHESIZE=x] [/QUIET]

/SCANNOW      Scans all protected system files immediately.
/SCANONCE    Scans all protected system files once at the next boot.
/SCANBOOT    Scans all protected system files at every boot.
/CANCEL      Cancels all pending scans of protected system files.
/QUIET      Replaces all incorrect file versions without prompting the user.

/ENABLE      Enables Windows File Protection for normal operation
/PURGECACHE  Purges the file cache and scans all protected system files immediately.
/CACHESIZE=x Sets the file cache size

H:\Documents and Settings\skrasavi>sfc.exe /scannow
```

Foundstone's fport

Fport shows current processes. To create a baseline ports output should be sent to a .txt file

Fport> baseport.txt

To baseline the running services execute netsh command:

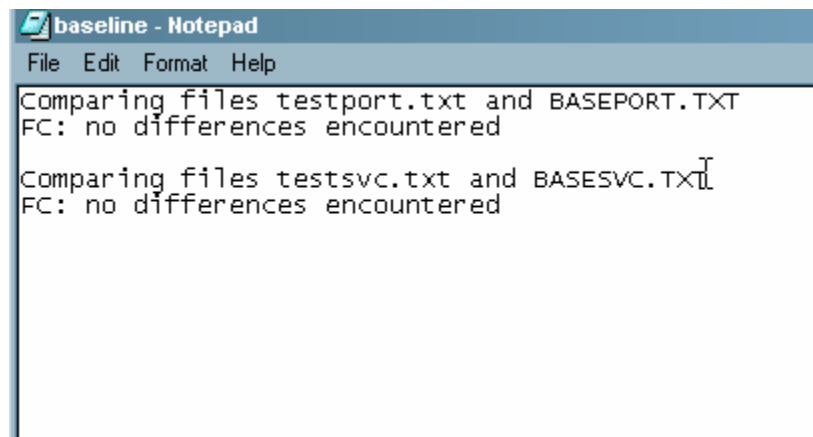
>netsh \wwwserver /list > basesvc.txt

Most checks can be run via batch file through "AT" or Windows scheduler. The audits should be scheduled with a simple .bat file

*@echo off
cd \daily\audit*

```
fport > testport.txt
netsvc \\dcpt-kora /list >testsvc.txt
fc /N testport.txt baseport.txt > baseline.txt
fc /N testsvc.txt basesvc.txt >> baseline.txt
```

To use the windows Scheduler I select baseline.bat to schedule, than enter the task name and task time to perform. I use daily audits. The typical results are shown below:

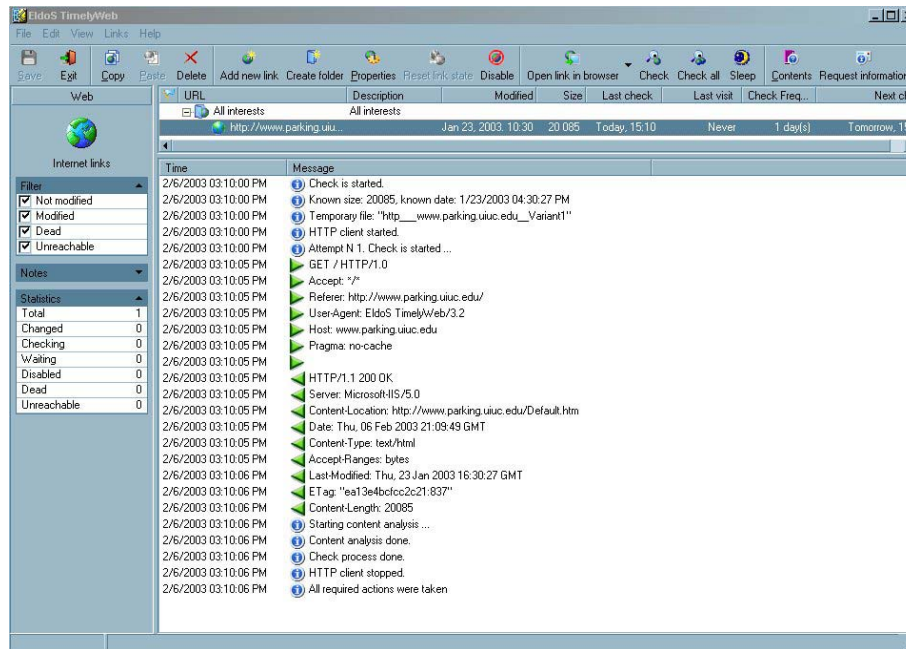


```
baseline - Notepad
File Edit Format Help
Comparing files testport.txt and BASEPORT.TXT
FC: no differences encountered
Comparing files testsvc.txt and BASESVC.TXT
FC: no differences encountered
```

I usually pay extreme attention to suspicious processes with innocuous-sounding names like WIN, SCSI, UPS.

EldoS TimelyWeb²⁷

The primary goal of web site monitoring tool is to monitor the resource and its availability and notify administrator whenever the change takes place. Dynamically generated web pages can be checked for changes using smart content analysis. It supports HTTPS, FTP, and SOKS proxies. When the change is detected, TimelyWeb uses different notification methods, such as e-mail, display, opens web page, network message.



3.2.8 Test 8 Vulnerability testing

Control Objective: Adequate functioning of the server under attack

Risk: Misuse, malicious activity

Compliance: Company policy and procedures

Test:

- Vulnerability assessment test has been performed by an auditor
- Vulnerability assessment tests are conducted regularly on a scheduled basis as well as after an incident
- Vulnerability Testing was conducted against the operating system and server application.
- Name of tool used (NMap, Languard Network Scanner, Typhon, X-scan)
- Version number of tool used (_available_)

Objective test: Verifiable results

Approach

The methodology for a test duplicates methods an attacker might take when attempting to breach a server. The goal is to produce an accurate map of the server and find vulnerabilities. This approach reflects that of a random attacker penetrating the server.

Risk level

To evaluate the potential impact on the server security different risk level is assigned to vulnerability that is found.

- Level 1 information can be obtained
- Level 2 (low) - sensitive information can be collected (version of OS and software)
- Level 3 (medium) - incidents (directory browsing, denial of service, read of limited files)
- Level 4 (high) - file theft, potential backdoors, read and write access on files, remote execution, or other activities

In using an attacker approach the first step in the process is to gain a clear picture of the technological characteristics and configuration of the server. To do this I use different tools to verify and compare results.

NMAP

Nmap <http://www.insecure.org/nmap/> uses raw IP packets to determine:

- hosts available on network
- open ports (services)
- operating system (and version of that operating system)
- packet filters/firewalls
- other characteristics.

This information gives the auditor a clear picture of how the web server is put together and protected. I use NmapFE v0.2.54 Beta3.1

Operating System Identification

Nmap is a great tool for operating system identification.

```
nmap -sS -O XXX.XXX.XX.XXX
```

```
Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )  
TCP Sequence Prediction: Class=truly random  
Remote OS guesses: Windows ME or Windows 2000 RC1 through final  
release, Windows Millennium Edition v4.90.3000
```

This output says that the target Web server is a Windows based machine. Nmap determined the operating system by the responses it received from packets sent.

Port Scanning

Port scanning looks for open ports that can allow potential connection to the system. If a connection can be made to the system, vulnerability may exist if the service is running on that open port.

```
nmap -sS XXX.XXX.XX.XXX
```

```
Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )  
Interesting ports on 192.168.1.1:
```

```
(The 1541 ports scanned but not shown below are in state: closed)  
Port State Service
```

```
21/tcp      open  ftp  
23/tcp      open  telnet  
25/tcp      open  smtp  
80/tcp      open  http  
135/tcp     open  loc-srv  
139/tcp     open  netbios-ssn  
443/tcp     open  https  
445/tcp     open  microsoft-ds
```

```
Nmap run completed -- 1 IP address (1 host up) scanned in 12 seconds
```

In addition to TCP port scanning, we need to know what UDP ports are open. UDP ports can pose a threat in the same manner as TCP ports.

```
nmap -sU XXX.XXX.XX.XXX
```

```
135/udp     open  loc-srv  
137/udp     open  netbios-ns  
138/udp     open  netbios-dgm  
445/udp     open  microsoft-ds
```

GFI Languard Network scanner

Another good tool is **GFI Languard Network scanner** (version 3.1 is a latest version at the moment of writing). Scanning and security alerts are freeware. Reporting, comparison and automatic service pack and patch deployment features are limited to a 30-day trial for up to 25 machines. GFI LANguard Network Security Scanner 3.1 adds the possibility to push service packs and custom patches to remote computers.












Remote TOD (time of day)






- Time of day : 22 Jan 2003 , 21:21.10 , GMT - 6
- UpTime : 1 days, 20 hours, 15 minutes, 50 seconds



Open Ports (10)

- 21 [Ftp => File Transfer Protocol]
- 503 Service Unavailable

- 23 [Telnet => Remote Login Protocol]
 -  login:
-  25 [Smtplib => Simple Mail Transfer Protocol]
 -  503 Service Unavailable
-  80 [Http => World Wide Web, HTTP]
 -  HTTP/1.1 400 Bad Request
 -  Server: Microsoft-IIS/5.0
 -  Date: Wed, 22 Jan 2003 21:21:16 GMT
 -  Content-Type: text/html
 -  Content-Length: 87
- 135 [epmap => DCE endpoint resolution]
- 139 [Netbios-ssn => NETBIOS Session Service]
- 443 [Https => Secure HTTP]
- 445 [Microsoft-Ds]


 Alerts (3) (Legend :  - High  - Medium  - Low  - Information)

 CGI Abuses (2)

 [Frontpage check \(1\)](#)

 Impact : Frontpage extensions are installed on this computer

 [Frontpage check \(3\)](#)

 Impact : Some versions of Frontpage are vulnerable to denial of service attacks

 [Bugtraq ID/URL : 1608](#)

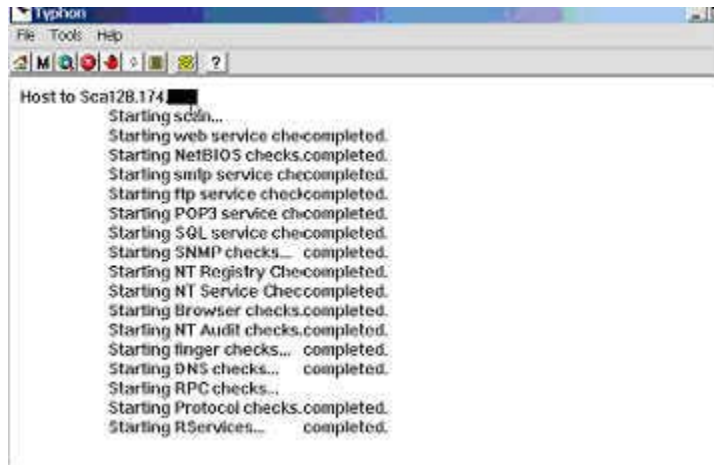
 Info_Alerts (1)

 Terminal Services

 Description : Terminal Services are installed on this computer

Typhon

Typhon is another multipurpose scanner based on an old time favorite former Cerberus Internet Scanner (CIS) written by David Litchfield. Next Generation Security Software²⁸ (NGSS) has rewritten the code for its renaming the revised version Typhon Security Scanner. Typhon performs checks against servers and systems such as the Web, FTP, SMTP, POP3, DNS, SNMP, NetBIOS, remote procedure call (RPC), and Microsoft SQL Server. In addition, Typhon analyzes settings on the system registry and services and inspects audit settings for user account passwords. Typhon also checks security configuration settings for Internet Explorer (IE). [Typhon](#) is available (432KB) on the NGSS Web site.

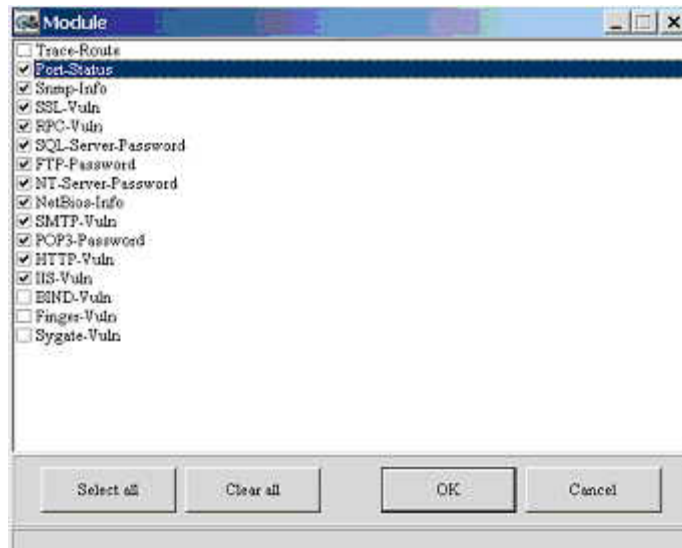


Once a scan is complete, Typhon produces an HTML-based report that offers detailed information regarding any problems it found, including information about how to fix those problems.

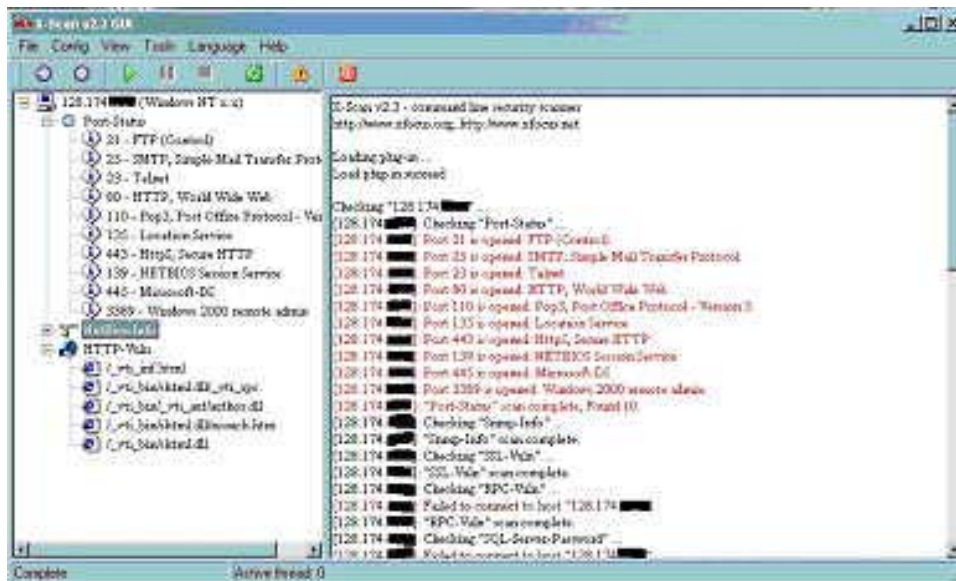


X-scan

X-scan <http://www.xfocus.org/> is another port/CGI scanner that gained popularity among attackers. It is a general network vulnerabilities scanner with multiple functions.



The latest version v2.3 has been released in September 2002. The scanner also produces report in an HTML format.



Results of the vulnerability test are in the Audit Findings Table

3.2.9 Test 9 Malicious Code

Control Objective: Malicious code controls are in place

Risk: Breach of confidentiality, integrity, and availability

Compliance: Company policy and procedures

Test:

- Policies and procedures address malware detection and prevention
- Notification procedure is established
 - Distribution of DAT files is secured
- Antivirus tools are prevented from being disabled
- All vendors recommended Security-related patches have been applied
- Software that can detect modifications to files is run on regular basis.
- Name of software package: NetShield 4.5
- Frequency of virus scan: Daily
- Automatic or manual (underline one)
- Windows Scripting Host is disabled

Objective test: Verifiable results

Results: Distribution of DAT files is from the intranet ftp server.

3.2.10 Test 10 Web specific

Control Objective: Web content and scripting standards are implemented

Risk: The scripts can be run from the outside and harm confidentiality, integrity and availability of server

Compliance: Company policy and procedures. Best practices recommendations

Test:

- Access to CGI directories is limited
- Users can not install CGI scripts
- Programs and administrative scripts are not on the website content volume
- Logical directory structure is implemented (separate static content, asp, html, scripts, executables)
- No development tools or application software on the web server
- Default website moved
- Server Application does not use cookies.
 - if FALSE
 - (1) Cookie policy is displayed on server and attached on form.
 - (2) Rationale is described in section entitled "ADDITIONAL COMMENTS AND EXPLANATIONS"

Objective test: Verifiable results

Results: Server does not use cookies

3.3 *Is the system auditable?*

Yes, the system is auditable. The following audit techniques were used to accomplish the objective to check the integrity of the system whether it is secure at the moment of audit or what should be done to make it secure:

- Test of departmental security policies for compliance with the best practices recommendations
- Test to determine the level of security of the web server

4 Follow up Report

The follow up report contains confidential information about the state of the server. Access to this information by unauthorized personnel may allow it to compromise the server.

The report contains all observations, recommendations, and findings.

4.1.1 Executive summary

Audit review found that the department had an effective program for managing the IT security. The department has implemented numerous computer security controls designed to protect and preserve its web-based assets.

The server is in compliance with the department security policy and regulations. Internet acceptable use policy is available and defines specific services that are available to users, users' responsibility, authorized protocols, ownership of resources, and contingency measures. The server is configured with agreement to this.

4.1.2 Audit Results

The web Server is setup in closed room with limited access of the personnel. Backup procedure is in compliance with the best practices – backup is scheduled, rotated, tapes are stored in a different location.

Audit findings table

This output indicates that the Web server has missing latest patches a number of open ports. Our concern is mainly for the Web server ports 80 and 443. However, all open ports can pose a risk to the Web server.

There were 30 vulnerabilities found during the risk assessment test. Of these, 3 were critical vulnerabilities. Critical vulnerabilities require immediate attention. Moderate vulnerabilities have been discovered. These often provide information to attackers that may assist them in mounting subsequent attacks on the server. These should also be fixed in a timely manner, but are not as urgent as the other vulnerabilities.

Audit Findings

Prepared By _____ Date _____
 Reviewed By _____ Date _____

Purpose of server	Departmental server	
Target audience	Public at large and employees	
Sensitivity of the data	Publicly available and departmental data	

Audit Test Results	Possible Risk Exposure	Recommended Action		Management Comments
		<i>Immediate</i>	<i>Procedural</i>	
Hotfixes are missing	Attacker can exploit known vulnerability	Install hotfixes	Enforce implementation of update procedure (SUS, Ecora, MS update agent, etc)	
Administrator account exists	Easier to crack the admin account password		Recommend administrator to consider best practices Rename the account	
Alert services enabled	This service could be use in social engineering attacks.		Disable this service.	
The server responds to ICMP echo requests The server responds to ICMP timestamp requests	There are several issues relating to ICMP echo requests, notably the "ping of death" exploit. Also ICMP scanning can be used to determine filtering rules in		Consider blocking ICMP access at firewall Filter out the icmp	

<p>Receive timestamp:81493218 (22:38:13 GMT) Transmit timestamp:81493218 (22:38:13 GMT)</p>	<p>firewall. Answers to an ICMP timestamp request allows an attacker to know the date which is set on the machine. This may present risk for time based authentications protocols.</p>		<p>timestamp requests and the outgoing icmp timestamp replies on the server</p>	
<p>Open ports: 21/tcp ftp File Transfer Protocol 23/tcp telnet 25/tcp smtp 80/tcp http 135/tcp loc-srv 139/tcp netbios-ssn 443/tcp https 445/tcp microsoft-ds 3389/tcp Windows 2000 remote admin</p>	<p>Although the services were unavailable on these ports an attacker can detect the status of the port. Also certain Trojans are registered for the ports 21,23, 25, 135 Port 139 Internet users should never be allowed to access any internal computer not specifically built for external access. Port 445 tcp/udp. 2k+ Server Message Block. Win LANMAN service on Microsoft Windows 2000 allows remote attackers to cause a denial of service via a stream of malformed data. CAN-2002-0597. http://support.microsoft.com/default.aspx?scid=kb;en-us;Q320751</p>	<p>Check whether ports 135, 137, 138, 139 and 445 are blocked at the external router or firewall Restrict usage of the port 445.</p>	<p>Enable port filtering at Win2000 settings to commonly attacked ports or install a host-based firewall. Recommend to conduct periodical scan of the server and employ port/process watchers</p>	
<p>FrontPage extensions are installed on this computer http://128.174.X.X/_vti_bin/shtml.dll/</p>	<p>Known security problems such as buffer overflow, resulting in the service crashing, and possibly allowing the execution of arbitrary code.</p>		<p>Consider disable FP extensions, ensure that the latest version of FrontPage is being used and authors</p>	

<p>/_vti_inf.html /_vti_bin/shtml.dll/_vti_rpc /_vti_bin/_vti_aut/author.dll /_vti_bin/shtml.dll/nosuch.htm</p>	<p>Shtml.dll can be abused to gain the source of server side scripts such as ASP pages. FrontPage Server Extensions allows remote attackers to determine the name of the anonymous account via an RPC POST request to shtml.dll in the /_vti_bin/ virtual directory. FrontPage Extensions configuration file is visible. Wrong Permission settings on FrontPage Extensions may allow defacements of web pages. The extension author.dll allows remote authoring of web pages on the site and access must be restricted to administrators and only those authors who are allowed to change the web pages. Bugtraq ID/URL : 1608 http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=shtml.dll</p>		<p>proper maintain passwords</p>	
<p>Web Server Directories / /_private/ /_vti_bin/ /_vti_bin/_vti_adm/ /_vti_bin/_vti_aut/ /_vti_log/ /_vti_txt/ /cgi-bin/</p>	<p>This set of checks uses the distinction between 404 - file not found, and 403 - access denied error codes to determine whether certain well - known directories exist.</p>		<p>Consider standardize error codes.</p>	

/dom/ /images/ /new/				
Terminal Services are installed on this computer			Consider to uninstall Win 2000 terminal services	
Registry Keys:				
HKLM\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg Value:	The winreg key does not exist. The ACLs set on this key control who has network access to the registry. Article 153183 .		Create this key and give administrators full control. This will ensure that only administrators have network access to the registry	

4.1.3 Additional control objectives

It is recommended to employ the following preventative controls:

- Separation of duties.
- Security awareness and technical training

Other controls, such as disaster recovery plans, user registration for computer access, security policy and procedures have been put in place.

Possible additional protection controls are:

- Security events monitoring through CERT, CIAC, SANS, Symantec, Bugtraq or other reputable IT security information source.
- Documentation of corrective actions
- Strong control over patches/hotfixes implementation so the new code is applied after testing on a test server

Costs .

As defined by the topic of this paper no software costs are associated with the auditing process. Initial costs will be attributed to time required for implementing recommendations.

Approximate estimation:

Installation of TCP/IP filters or free host firewall (0.5 hr- 1 hr @ \$50/hour=\$25-\$50)

Removing unneeded services, reconfiguration of the server, error code standardization (1.5 hr @\$50/hr= \$75)

All low cost measures that can be performed by the system administrator.

Compensating Controls

No separation of duties: the same employee performs both the network and security administration thus the employee maintains control of an entire process. The discrepancy in business functions can be alleviated by implementing the internal automated auditing procedure with free tools described in this study. However external audit should be conducted periodically to review the internal auditing process.

4.1.4 Report Distribution

It is also important to determine who will receive copies of the audit report (network administrator or manager) and to make them sign for their copy for which they will be responsible. Distribution should be extremely limited and the

original report is recommended to be stored in a secure place for comparison with the next server audit.

5 Conclusion

We discussed the methodology and a collection of free tools for auditing Windows IIS 5.0 server. My server auditing toolkit includes the following free tools:

Internal Control Phase

- Compliance audit
 - Industry standards, company policy and procedures, best practices and the checklist

Testing Phase

- Technical Audit
 - Web server baseline (HFNetChck, Ecora Patchmeister, URLScan, Windows Benchmark tool, TCPView or Active Ports)
 - Vulnerability assessment (MBSA, Nmap, GFI Languard network Scanner, Typhon, X-scan)
 - Maintenance of a secure configuration (Update checkers, MBSA, Regdmp, Auditpol, Fport, Dumpel, Languard SELM, TimelyWeb)

Having used the latest audit tools, even those that are fully automated, is not an excuse to miss the planning and analytical work. What is important; however, is the audit process itself, and a prudent caution of what might be coming out from the failure events.

One should not consider audit as a silver bullet to all security problems. It is a part of a comprehensive security management “Defense in Depth” that plays a vital role in protecting the web server.

An Audit process never stops. It is always time to reassess the original risk analysis and security policy, followed by the next audit and interpretation of the reports it generates. Again we are back to the cycle of a risk management process. This cycle should continue until the server is disconnected from network.

6 Appendix

RELATED INFORMATION

CAATs - any automated audit techniques, such as generalized audit software, utility software, test data, application software tracing and mapping, and audit expert systems. <http://www.isaca.org/standard/appendix.htm#c> (12.20.02)

Monitoring tools

A group of excellent utilities from Sysinternals
<http://www.sysinternals.com/ntw2k/utilities.shtml> (12.20.02)

Recent Regulations and Proposals

Gramm-Leach-Bliley Financial Services Modernization Act:
<http://www.senate.gov/~banking/conf/> (12.20.02)

HIPAA: Health Insurance Portability and Accountability Act
<https://www.ecora.com/ecora/medium/>

Computer Security Act of 1987. Public Law 100-235 (H.R. 145)
<http://www.cio.gov/docs/csa.htm> (12.20.02)

Security of Federal Automated Information Resources
http://www.cio.gov/docs/Appendix_III.htm (12.20.02)

Guidance on Implementing the Government Information Security Reform Act
http://www.cio.gov/docs/Security_Act_Memo_and_Guidance.htm
(12.20.02)

Policy, guides, and tools

Audit Policy http://www.sans.org/newlook/resources/policies/Audit_Policy.pdf
(12.20.02)

Web Security Basics and IIS Tools Talk to IUPUI and IUB User Groups
http://www.itso.iu.edu/staff/fnevers/talks/Web_Security_Basics_and_IIS_Tools.ppt
(12.20.02)

Microsoft Resource page for securing IIS [Article ID: Q282060](#) (12.20.02)

Microsoft Security Tools and Checklists
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools.asp> (12.20.02)

From Blueprint to Fortress: A Guide to Securing IIS 5.0

<http://www.microsoft.com/technet/prodtechnol/iis/deploy/depovg/securiis.asp>
(12.20.02)

Manage Security of Your Windows IIS Web Services
<http://www.microsoft.com/technet/security/bestprac/mcswebbp.asp> (12.20.02)

ITSO IIS Alert list:
<https://www.itso.iu.edu/services/alerts/index.pl?action=editsubs> (12.20.02)

Windows 2000 Magazine
<http://www.win2000mag.com/Articles/Index.cfm?ArticleID=21323> (12.01.03)

Microsoft IIS Newsgroups
<news://msnews.microsoft.com/microsoft.public.inetserver.iis.security> (12.01.03)

HOW TO: Enable and Apply Security Auditing in Windows 2000
<http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q300549&> (12.01.03)

National Security Agency (NSA) "Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0"
<http://nsa1.www.conxion.com/win2k/guides/w2k-14.pdf> (12.01.03)

SystemExperts "Hardening Windows 2000 Guide"
<http://www.systemexperts.com/win2k/HardenWin2K.html> (12.01.03)

SANS sources

SANS Reading Room "Securing IIS on Windows 2000"
http://www.sans.org/infosecFAQ/win2000/sec_IIS.htm (12.01.03)

Top 20 vulnerabilities <http://www.sans.org/top20/> (12.01.03)

Securing IIS on Windows 2000 By Carl Denowh
http://rr.sans.org/win2000/sec_IIS.php (12.01.03)

Step-by-Step guide to securing windows 2000 server using the Security Configuration & Analysis tool By Jason Morris
<http://rr.sans.org/win2000/hardening.php> (12.01.03)

¹ IS Risk Assessment measurement <http://www.isaca.org/standard/procedure1.pdf> (01.12.03)

² IS Auditing Guidelines <http://www.isaca.org/standard/procedure.htm> (12.01.03)

-
- ³ Application Systems review <http://www.isaca.org/standard/guide20.htm>
- ⁴ David Hoelzer. SANS Audit track. Auditing Principles and Concepts. 2002
- ⁵ Audit ANSI standards <http://www.ansi.org> (12.01.03)
- ⁶ BS 7799-1. 1999
- ⁷ ISO -17799 <http://www.iso-17799.com/> (12.01.03)
- ⁸ **[Will Ozier Introduction to Information Security and Risk Management](#) (03.01.03)**
- ⁹ COBIT Control Objectives for Information and Related Technology standard.
- ¹⁰ <http://www.isaca.org/cobit.htm> (12.01.03)
- ¹¹ Security Operations Guide for Windows 2000 server <http://www.microsoft.com/technet/security/prodtech/> (12.01.03)
- ¹² Windows 2000 Security configuration checklist
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/issues/W2kCCSCG/W2kSCGca.asp> (12.01.03)
- ¹³ SANS Top 20 vulnerabilities. <http://www.sans.org/top20.htm#W> (12.01.03)
- ¹⁴ <http://www.infosecuritymag.com/2002/dec/Sect3.pdf> (12.01.03)
- ¹⁵ <http://support.microsoft.com/?kbid=303215> (02.03.03)
- ¹⁶ <http://v4.windowsupdate.microsoft.com/en/default.asp> (02.03.03)
- ¹⁷ <http://www.shavlik.com/pHFNetChkLT.aspx> (12.01.03)
- ¹⁸ <http://www.ecora.com/ecora> (12.01.03)
- ¹⁹ MBSA
<http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/Security/tools/tools/MBSAHome.ASP>
- ²⁰ Center for Internet Security. <http://www.cisecurity.org>(12.01.03)
- ²¹ URLscan
<http://www.microsoft.com/windows2000/downloads/recommended/urlscan/default.asp>(12.01.03)
- ²² Windows 2000 Audit category and events
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/issues/W2kCCSCG/W2kSCGca.asp>(12.01.03)
- ²³ Windows 2000 Default security settings
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/issues/W2kCCSCG/W2kSCGca.asp> (12.01.03)
- ²⁴ <http://www.ibt.ku.dk/jesper/ELDump/default.htm> (12.01.03)

²⁵ <http://www.gfi.com/press/lanselmoofferpr.htm>(12.01.03)

²⁶ <http://www.sysinternals.com/ntw2k/source/tcpview.shtml> (01.12.03)

²⁷ EldoS Group. <http://www.eldos.org> (02.10.03)

²⁸ <http://www.winnetmag.com/FindIT/Index.cfm?ID=36> (12.01.03)