



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

Interested in learning more?

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

Table of Contents	1
Robert_Shullich_GSNA.pdf	2

© SANS Institute 2005, Author retains full rights.

Auditing The Internet Information Services (IIS) 5.0 Feature Of Windows 2000 Server

SANS Track 7

Auditing Networks, Perimeters, and Systems

**GSNA Practical
Assignment**

Version 3.2 Option 1

Robert Shullich, CISSP, CISA, CISM

February 10, 2005

***Track 7
SANS Network Security (NS) 2004
Riviera Hotel, Las Vegas, NV
September 29th – October 4th, 2004***

Table of Contents

Abstract	11
Preface	12
Author Bio	13
Figure I-1: BloodLab Network Diagram	16
Figure I-2: Architecture of IIS 5.0 Isolation Mode	17
Figure I-3: Web Server Audit Scope is IIS Core	18
SECTION 1: RESEARCH - AUDIT, SCOPE, RISKS AND TOOLS	19
1.1 System to be Audited and its Role	19
1.1.1 Current Environment	19
1.1.2 Current Configuration	21
1.1.3 Scope of Audit	21
1.1.4 Tools used	22
1.2 Significant Risks to the System	23
1.2.1 Assets at Risk	24
• Brand, also known as Goodwill or Reputation (Brand)	24
• Clinical Laboratory License (LIC)	25
• Customer Service (CS)	26
• Accounts Receivable (AR)	27
• Payroll (PAY)	28
• Inventory (INV)	28
• Internally Developed Proprietary Software, Process and Procedures, Intellectual Property (IP)	29
• Patient Records (PR)	29
• Patient Lists (PL)	29
• Physician Records (PHY)	30
• Documents and briefs for current or pending litigation (PRIV)	30
• Ability to meet Service Level Agreements (SLA)	30
• Worker Productivity (WP)	31
1.2.1-A Assets at Risk / Risk Management	31
Figure 1-1: Mitigating Controls for Likelihood/Cost Quadrants	31
1.2.1-B Assets at Risk Likelihood/Cost	32
Figure 1-2 – Likelihood/Costs for Assets at Risk	32
1.2.2 Threats	33
1.2.3 Threats & Consequences	36
• Confidentiality	37
• Data Integrity	38
• Availability	40
1.2.4 Major Vulnerabilities	43
• Internal Staff	43
• Buffer Overflows	43
• Default installed Software and Features	43

• Limited or unrestricted Access Control	44
1.2.5 Impact of exploited Major Vulnerabilities	44
• Denial of Service	44
• Downstream liability	44
• Exposure of Compromise of sensitive files or data	45
• Execution of arbitrary commands on the server	46
• Complete compromise of the server	46
1.2.6 Microsoft Classifications	46
Microsoft Classifications of "impact of vulnerability"	46
Microsoft Severity Rating system	46
1.2.7 Magnitude of Impact	47
1.2.8 Risk Mitigation	47
1.3 Current State of Practice	48
SECTION 2: AUDIT CHECKLIST	53
Format used for checklist entries	53
IIS 2.1 Service Packs and Security Updates	55
IIS 2.2 File System Should be NTFS	60
IIS 2.3 IIS Should Not be Installed on Domain Controller	63
IIS 2.4 IIS Lockdown Tool	66
IIS 2.5 IIS Sample Applications Should be Removed	68
IIS 2.6 IISADMPWD Virtual Directory	71
IIS 2.7 IIS Parent Paths	74
IIS 2.8 MSADC and Scripts Virtual Directories on IIS	76
IIS 2.9 IIS Logging Should be Enabled	78
IIS 2.10 Remove or Disable Unnecessary Services	82
IIS 2.11 Directory Browsing	85
IIS 2.12 IUSR_computername Permissions and Rights	88
IIS 2.13 Service Account Permissions and Rights	92
IIS 2.14 IP Forwarding	94
IIS 2.15 Anonymous FTP Accounts	97
IIS 2.16 Install URLSCAN For Traffic Filtering	101
IIS 2.17 Unused Script Mappings Should be Removed	103
IIS 2.18 SMTP Open Relay Should be Restricted	106
SECTION 3: RESULTS - AUDIT, MEASUREMENTS, AND CONTROLS	109
Preparation for Performing the Audit	109
IIS 2.1 Service Packs and Security Updates Part 1	110
Artifact 1 Security Update Analysis - Missing Patches	110

IIS 2.1 Service Packs and Security Updates Part 2	111
Artifact 2 Security Update Analysis – Patch Exceptions	111
IIS 2.2 File System Should be NTFS	112
Artifact 3 MSBA Report Showing Windows Scan Results	112
IIS 2.3 IIS Should Not be Installed on Domain Controller	113
IIS 2.4 IIS Lockdown Tool	113
IIS 2.5 IIS Sample Applications Should be Removed	113
IIS 2.6 IISADMPWD Virtual Directory	113
IIS 2.7 IIS Parent Paths Part 1	113
IIS 2.8 MSADC and Scripts Virtual Directories on IIS	113
IIS 2.9 IIS Logging Should be Enabled Part 1	113
IIS 2.10 Remove or Disable Unnecessary Services Part 1	113
Artifact 4 MSBA Analysis IIS Scan Results	114
IIS 2.10 Remove or Disable Unnecessary Services Part 2	116
Artifact 5 MSBA Analysis – Unnecessary Services	116
IIS 2.7 IIS Parent Paths Part 2	117
Artifact 6 MSBA Analysis – Parent Paths	117
IIS 2.9 IIS Logging Should be Enabled Part 2	118
Artifact 7 BloodLab Web Site Property Page	118
IIS 2.10 Remove or Disable Unnecessary Services Part 3	119
Artifact 8 Telnet Analysis – Verify NNTP Service Running	119
IIS 2.10 Remove or Disable Unnecessary Services Part 4	120
Artifact 9 ISAPI DLL Found – Front Page Extensions	120
IIS 2.10 Remove or Disable Unnecessary Services Part 5	121
Artifact 10 Server Extensions 2002 – Share Point Installed	121
IIS 2.10 Remove or Disable Unnecessary Services Part 6	122
Artifact 11 Server Extensions	122
IIS 2.11 Directory Browsing Part 1	123
Artifact 12 BloodLab Web Site Home Directory Property Sheet	123
IIS 2.11 Directory Browsing Part 2	124
Artifact 13 Default Document Search Order	124
IIS 2.11 Directory Browsing Part 3	125
Artifact 14 Internet Information Services – MMC Plug-in	125
IIS 2.12 IUSR_computername Permissions and Rights Part 1	126
Artifact 15 Anonymous User Accounts – Setting Password	126
IIS 2.12 IUSR_computername Permissions and Rights Part 2	127
Artifact 16 Assignment and Password of IUSR Account	127
IIS 2.12 IUSR_computername Permissions and Rights Part 3	128
Artifact 17 Computer Management – Local Users And Groups	128
IIS 2.13 Service Account Permissions and Rights Part 1	129
Artifact 18 Services General Tab for WWW Service	129

IIS 2.13 Service Account Permissions and Rights Part 2	130
Artifact 19 Services Properties – Log On Tab – Local System Account	130
IIS 2.15 Anonymous FTP Accounts Part 1	131
Artifact 20 Internet Information Services – MMC Plug-in	131
IIS 2.15 Anonymous FTP Accounts Part 2	132
Artifact 21 IIS Lockdown Tool Services Template	132
IIS 2.16 Install URLSCAN For Traffic Filtering Part 1	133
Artifact 22 IIS Master WWW Property Sheet for ISAPI	133
IIS 2.16 Install URLSCAN For Traffic Filtering Part 2	134
Artifact 23 Web Site Local Property Sheet for ISAPI	134
IIS 2.17 Unused Script Mappings Should be Removed Part 1	135
Artifact 24 Download of Tool CGI Scanner V4	135
IIS 2.17 Unused Script Mappings Should be Removed Part 2	136
Artifact 25 CGI Scanner 4.0 – Using localhost	136
IIS 2.17 Unused Script Mappings Should be Removed Part 3	137
Artifact 26 CGI Scanner V4.0 Scanning the Website	137
IIS 2.17 Unused Script Mappings Should be Removed Part 4	138
Artifact 27 CGI Scanner – Scan of SIMBA	138
IIS 2.17 Unused Script Mappings Should be Removed Part 5	139
Artifact 28 Test of IDA scripting extension mapping.	139
IIS 2.17 Unused Script Mappings Should be Removed Part 6	140
Artifact 29 Test of HTW scripting extension mapping.	140
IIS 2.17 Unused Script Mappings Should be Removed Part 7	141
Artifact 30 Inspection of Script Mappings Part A	141
IIS 2.17 Unused Script Mappings Should be Removed Part 8	142
Artifact 31 Inspection of Script Mappings Part B	142
IIS 2.18 SMTP Open Relay Should be Restricted	143
Artifact 32 Display of Exchange 2000 Services	143
Summary Matrix	144
Table 3-1: Summary Table	144
SECTION 4: RISK ASSESSMENT	145
4.1 Executive Summary	145
4.1-A Assets at Risk / Risk Management	145
Figure 4-1: Mitigating Controls for Likelihood/Cost Quadrants	145
4.1-B Assets at Risk Likelihood/Cost	146
Figure 4-2 – Likelihood/Costs for Assets at Risk	146
Development of an Information Protection Program	147
Summary Annual Costs to Generate a Information Security Program	148
Table 4-1 Estimated Cost for Security Program Startup	148
4.2 Audit Findings	148
4.2.1 Audit Objectives	148
4.2.2 Audit Scope	148
4.2.3 Audit Checklist Result Summary	149
Checklist Items That Passed	149
Table 4-2 Passing Checklist Tests	149

Checklist Items That Did Not Pass	149
Table 4-3 Failing Checklist Tests	149
4.3 Recommendations and Costs Detail	150
IIS 2.17 Unused Script Mappings Should be Removed	150
Interview:	150
Findings:	150
Recommendation:	150
IIS 2.5 IIS Sample Applications Should be Removed	150
Interview:	150
Findings:	150
Recommendation:	151
IIS 2.7 IIS Parent Paths	151
Interview:	151
Findings:	151
Recommendation:	151
IIS 2.8 MSADC and Scripts Virtual Directories on IIS	151
Findings:	151
Recommendation:	151
IIS 2.10 Remove or Disable Unnecessary Services	152
Interview:	152
Findings:	152
Recommendation:	152
IIS 2.16 Install URLSCAN For Traffic Filtering	153
Findings:	153
Recommendation:	153
IIS 2.3 IIS Should Not be Installed on Domain Controller	153
Interview:	153
Findings:	153
Recommendation:	153
IIS 2.4 IIS Lockdown Tool	153
Findings:	153
Recommendation:	153
IIS 2.12 IUSR_computername Permissions and Rights	154
Findings:	154
Recommendation:	154
IIS 2.13 Service Account Permissions and Rights	154
Findings:	154
Recommendation:	154
4.4 Recommendations and Costs Summary	155
Cost to remediate failed checklist items	155
Table 4-4 Estimated Cost for Failing Checklist Items	155
4.5 Long Term Recommendation	155
4.6 Additional Controls	156
REFERENCES	157
APPENDIX A – MSBA 1.2.1 Help Messages	164
Messages from Microsoft Baseline Security Analyzer Version 1.2.1	164
[5311] Service Packs and Security Updates	165
Check Description	165
Additional Resources	166

[5311] Service Packs and Security Updates	168
Issue	168
Solution	168
Additional Resources	170
[5313] File System	171
Check Description	171
Additional Information	171
[5313] File System	172
Issue	172
Solution	172
Additional Information	172
[5321] IIS on Domain Controller	173
Check Description	173
[5321] IIS on Domain Controller	174
Issue	174
Solution	174
[5323] IIS Lockdown Tool	175
Check Description	175
Additional Resources	175
[5323] IIS Lockdown Tool	176
Issue	176
Solution	176
Additional Resources	176
[5324] IIS Sample Applications	177
Check Description	177
[5324] IIS Sample Applications	178
Issue	178
Solution	178
Instructions	178
[5325] IISADMPWD Virtual Directory	180
Check Description	180
Additional Information	180
[5325] IISADMPWD Virtual Directory	181
Issue	181

Solution _____	181
Instructions _____	181
Additional Information _____	182
[5326] IIS Parent Paths _____	183
Check Description _____	183
Additional Information _____	183
[5326] IIS Parent Paths _____	184
Issue _____	184
Solution _____	184
Instructions _____	184
Additional Information _____	186
[5327] MSADC and Scripts Virtual Directories on IIS _____	187
Check Description _____	187
Additional Resources _____	187
[5327] MSADC and Scripts Virtual Directories on IIS _____	188
Issue _____	188
Solution _____	188
Instructions _____	188
Additional Resources _____	189
[5328] IIS Logging _____	190
Check Description _____	190
Additional Information _____	190
[5328] IIS Logging _____	191
Issue _____	191
Solution _____	191
Instructions _____	191
Additional Information _____	192
[53116] Unnecessary Services _____	193
Check Description _____	193
[53116] Check for Unnecessary Services _____	194
Issue _____	194
Solution _____	194
Instructions _____	194
APPENDIX B – Inspecting Web Property Sheets _____	196

Figure B1: Local Disk Properties to determine file system in use	196
Figure B2: Web Site Properties Page	197
Figure B3: Default Document Properties Page	198
Figure B4: Installed ISAPI Filters	199
Figure B5: Home Directory Page	200
Figure B6: Home Directory Page – Execute Permissions	201
Figure B7: Application Configuration – Application Mapping	202
Figure B8: Application Configuration – Application Configuration	203
Figure B9: Application Configuration – Application Debugging	204
Figure B10: Web Site Operators	205
Figure B11: Simple Tree of Default Web Sites	206
Figure B12: Default FTP Site Properties	207
Figure B13: Security Accounts Tab for FTP Sites	208
Figure B14: Home Directory and Permissions Page	209
Figure B15: Default SMTP Virtual Server Properties	210
Figure B16: Relay Restrictions	211
Figure B17: Default NNTP Virtual Server Properties – General Tab	212
Figure B18: Default SMTP Virtual Server Properties – General Tab	213
Figure B19: Extended Logging Properties	214
Figure B20: Default Folder for IIS Log files	215
Figure B21: Expanded Default Web Site to Expose Virtual Directories	216
Figure B22: Sample of Browse Directory Screen	217
Figure B23: Sample Master Properties ISAPI Screen with URLSCAN	218
Figure B24: Sample Extension Mappings after IIS Lockdown	220
APPENDIX C – IIS Lockdown Tool V2.1 Sample	221
Figure C1: IIS Lockdown Welcome	221
Figure C2: IIS Lockdown EULA	222
Figure C3: IIS Lockdown Template Selection Screen	223
Figure C4: IIS Lockdown Services Selection	224
Figure C5: IIS Lockdown Remove Samples	225
Figure C6: IIS Lockdown Script Mapping Selection	226
Figure C7: IIS Lockdown URLSCAN Option	227
Figure C8: IIS Lockdown Ready To Apply Settings	228
Figure C9: IIS Lockdown Already Configured	229
Figure C10: Sample OBLT-LOG.LOG File	230
Figure C11: Sample IIS Lockdown LOG File	231
APPENDIX D – MSBA 1.2.1 Install & Run	232
Figure D1: MSBA Splash Screen	232
Figure D2: MSBA EULA	233
Figure D3: MSBA Destination Folder Selection	234
Figure D4: MSBA Setup – Start Installation	235
Figure D5: MSBA Installation In Progress, Please Wait	236
Figure D6: MSBA Install Complete!	236
Figure D7: MSBA Function Selection Screen	237
Figure D8: MSBA Scan One Computer	238
Figure D9: Downloading MSSecure.XML File	239
Figure D10: Security Reports Selection Screen	240
Figure D11: Sample MSBA Scan Report	241
Figure D12: Looking at RAW MSBA XML Files	242
Figure D13: Location where MSSecure.XML file is saved	243
Figure D14: Contents of MSSecure.XML file	244
APPENDIX E – Target System Characteristics	245
Figure E1: Computer Management	245

Figure E2: Computer Management – System Summary	246
APPENDIX F – URLScan	247
Figure F1: Sample URLSCAN.LOG Initialization	247
Figure F2: Sample URLSCAN.INI File	248
Figure F3: Sample URLSCAN.LOG File	249

© SANS Institute 2005, Author retains full rights.

Abstract

Microsoft Internet Information Services (IIS) 5.0 is 2nd in market share holding about 21% of the web page serving market (Apache is 1st with about 67% market share). Distributed as part of the Microsoft Windows 2000 Server Operating System as a free feature and installed by default, IIS becomes a web server ready and waiting to go. The risk of using a default installation of IIS is high for two reasons. First, IIS is not secure by default, and its initial install settings leaves the IIS component vulnerable even in the absence of an installed application. Second, IIS is installed and ready to go even if you don't need a web server, or any of the other IIS components such as NNTP, SMTP or FTP.

To help secure IIS there are published recommendations, templates and guidelines issued by security experts, the United States government agencies, and even Microsoft. Microsoft provides a configuration tool called IIS Lockdown. But once a server is secured, how do you know it was secured and remains secured? Even after lockdown, a configuration can be changed and IIS again becomes vulnerable.

This paper will present an audit framework to address key IIS configuration settings and some key Operating System settings that affect IIS. With proper auditing of IIS behavior we can determine that the IIS server is secure, and by performing these audits on a periodic basis we can ensure that the IIS component remains secure over time.

Preface

In this attempt to write my first GIAC paper, and keeping within the study area of Audit, I used information from a select few past GCNA papers that have a relation to my topic at hand. What I have included in my paper are copies of outline and/or format of the way the paper is organized, not copies of content. Another way to say this is that in some cases I have copied some of the look and feel of those papers. These are GSNA Version 3.2 Option 1 papers that were published recently.

I would like to point out that as far as content; these papers^{1 2 3 4} address audits of different classes of Windows servers. What you will find in these papers are common checklist items that involve antivirus, account management, audit logging, patch management, file permissions, and unneeded services and unneeded software.

Even Pfaff's² paper covers many of these areas in her IIS paper. I don't want to repeat the checklist content used in these papers, as it would be the same items all over again. This is the result of the commonalities of the servers, which are all based on a version of Windows Server.

However, in Pfaff's² paper, one of her checklist items, item "2.9 Check for IIS Vulnerabilities", appears to be the major focus on IIS while the remaining checks are more of the entire Windows Server. It is not that those checks are unimportant, but this provides an opportunity to take a deeper dive into the audit and analysis of the IIS base product and directing focus only on IIS configuration issues.

¹ SANS Institute Auditing a Microsoft Windows 2000 Terminal Server William Driskell, January 6, 2005

URL: <http://www.giac.org/practical/GSNA/William_Driskell_GSNA.pdf>

² SANS Institute Auditing a IIS Microsoft Windows 2000 Server Beverly Pfaff, November 11, 2004

URL: <http://www.giac.org/practical/GSNA/Beverly_Pfaff_GSNA.pdf>

³ SANS Institute Audit of a Corporate Security Systems Domain Controller Steve Graham, November 12, 2004 URL: <http://www.giac.org/practical/GSNA/Steven_Graham_GSNA.pdf>

⁴ SANS Institute Auditing a File Server - Microsoft® Windows Server™ 2003 Tamer Eltoni, May 2004 URL: <http://www.giac.org/practical/GSNA/Tamer_Eltoni_GSNA.pdf>

Author Bio

Robert Shullich is an information security officer for a major printing firm. With over 30 years of full time experience in Information Technology, his expertise has covered mainframes to personal workstations and servers, networking, and databases.

His Microsoft credentials include:

- MCSE (Windows NT 4.0, Windows 2000 and Server 2003)
- MCSA (Windows 2000 and Server 2003)
- MCSA+Security (Windows 2000 and Server 2003)
- MCSA+Messaging (Exchange 2000 and Exchange 2003)
- MCSE+Messaging (Exchange 2000)
- MCSE+Security (Windows 2000 and Server 2003)
- MCSE+Internet (Windows NT 4.0)
- MCDBA in SQL Server 2000
- MCDST in Windows XP

His security credentials include:

- ISC² (CISSP, SSCP, ISSMP, ISSAP)
- ISACA (CISA, CISM)
- EC COUNCIL (CEH)
- ACFE (CHS-III)
- Security Certified (SCNP)
- TrueSecure (TICSA)
- CompTIA (Security+)
- SANS (GHTQ)
- ProSoft (CIW Security Analyst)
- Symantec (SCSP)

Additional certification credentials:

- CompTIA (A+, Network+, Server+, iNet+)
- ProSoft (Master CIW Administrator)
- ICCP (ACP, CCP)
- Cisco (CCNA)

He also holds from accredited universities the following Masters Degrees:

- M.S. Computer Science (College of Staten Island)
- M.B.A. Management (Baruch College)
- M.S. Telecommunications Networking (Brooklyn Polytechnic)

Introduction

This audit is being performed for a clinical laboratory located and doing business in the United States. In this paper, the company will be called BloodLab, which is a fictitious name and will be used to protect the identity of the real corporation.

BloodLab has been in business for several years and specializes in clinical analysis of blood, serum and tissue. In a common scenario a walk-in patient visits one of Blood Lab's satellite blood draw stations with a physician issued prescription for tests to be run. At the draw station, if the prescription is for blood analysis, Phlebotomists will draw blood into a vacuum tube, and labels the tube for identification and tracking. Other serums and fluids are collected in specimen cups, which will also be labeled. Where required, the Phlebotomist will prepare the samples, which may include spinning down blood, or freezing the samples. Data entry of the patient information is performed remotely from the draw site to the central laboratory system. For each patient, a biohazard bag is prepared where all specimen collections and a lab order or original prescription is enclosed. A patient may have multiple tubes and/or specimen cups, so they are assigned the same lab control number and are kept together.

A courier will make periodic rounds on a predetermined route and pick up the specimen bags and deliver them to the main laboratory facility. BloodLab receives the specimen bags, and performs the prescribed tests, as ordered by the physician. Certain tests may be beyond the competency of BloodLab, and those tests are sent to a larger laboratory as a referral. When the tests are complete, the results are aggregated and prepared into reports and those reports are then sent to the prescribing physician. With these reports the physician can diagnose illness and determine necessary treatment. Depending on the criticality of the test results, some results must be reported to the prescribing physician immediately before the final reports are generated and sent to the physician.

A similar process occurs for collections that occur in the physician's office. In this case, the physician (or a nurse) will collect the samples, generate a lab order, and assemble these in a biohazard bag. The courier will make pickups during the day to collect the specimen bags and bring them to the main laboratory facility for processing. Most of the physicians have terminal and printer access to BloodLab's central computer from their office.

One final variation is that BloodLab makes house calls. A Phlebotomist will make a house call and collect tubes of blood and specimen samples, label them and package them into a biohazard bag. In this case the Phlebotomist will take the collection back to the main laboratory facility and data entry of patient information will be done onsite.

The web application provides the interface to the complete laboratory information system, which is a series of routines that make up one comprehensive system.

The web based, Internet facing, application written in Microsoft .NET technology makes these reports available to the physicians over the Internet. Reports may also be distributed in paper form and mailed or delivered via courier to the physician, or faxed to the physician's office. The software also supports transmission of critical results via pager or text messaging devices.

The web facing application is a front-end to all of the laboratory operations that include some of the following subsystems:

- Employee Time Records
- Userid/Password Management for the application
- Accounts Payable
- Accounts Receivable
- Billing
- Inventory
- Car Management system for the couriers
- Company Telephone Directory
- Patient Records
- Physician Records
- Worklists and Results

A major breach of this one single web application could provide unauthorized access and control over any operational function within BloodLab. All of these functions are accessible from both within BloodLab as well as externally from the Internet. This web application is mission critical.

The organization has not implemented any significant level of security on the Operating System end. A limited amount of application security has been incorporated into this application. There are no programming standards being followed, and the organization never developed or implemented a written security policy. Since this laboratory is a human clinical facility, it is subject to regulatory requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA)⁵.

The target for this audit will be the operating system specific part of the Web Server, which is a Windows 2000 IIS server running Service Pack 4. This server is also a domain controller and is also the Exchange 2000 Mailbox server.

In order to keep the scope of this practical to a manageable level, my task will be to measure some of the weaknesses of the IIS component. Since there are no written security policies or hardening templates in use, the standard metric that will be used will be based on best practices. Under normal circumstances, an

⁵ Centers for Medicare & Medicaid Services URL: <<http://www.cms.hhs.gov/hipaa/>>

audit would be performed to measure compliance of the audited objects to security policy.

BloodLab Inc. Network Diagram

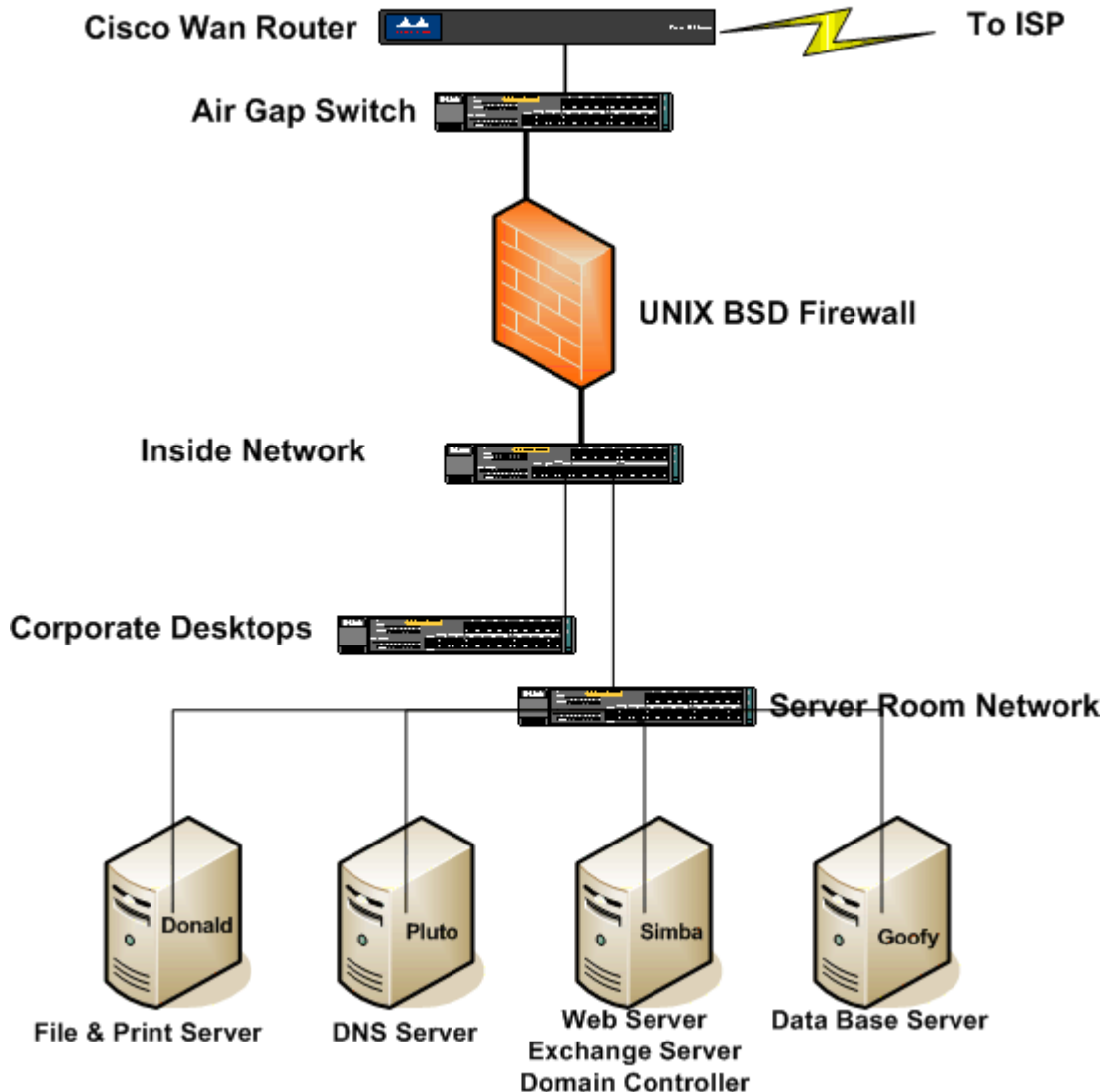


Figure I-1: BloodLab Network Diagram

BloodLab uses a single firewall to separate the entire corporate and server network from the Internet. A T1 line connects BloodLab to the ISP via a CISCO router.

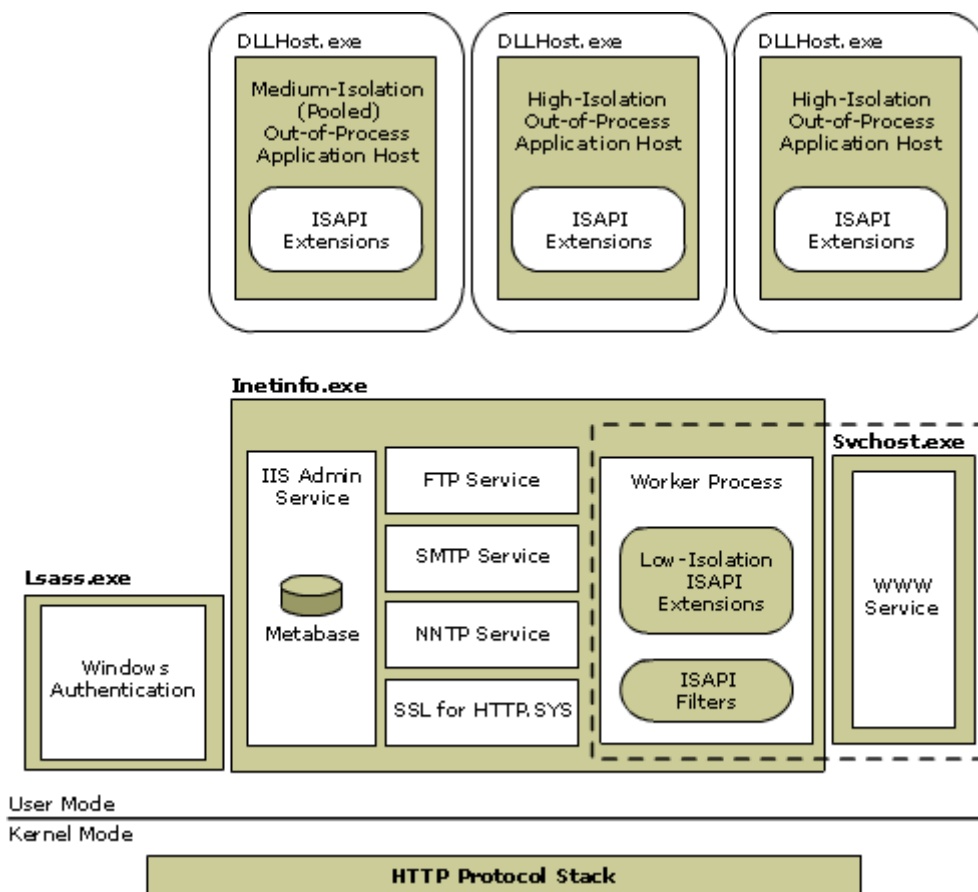
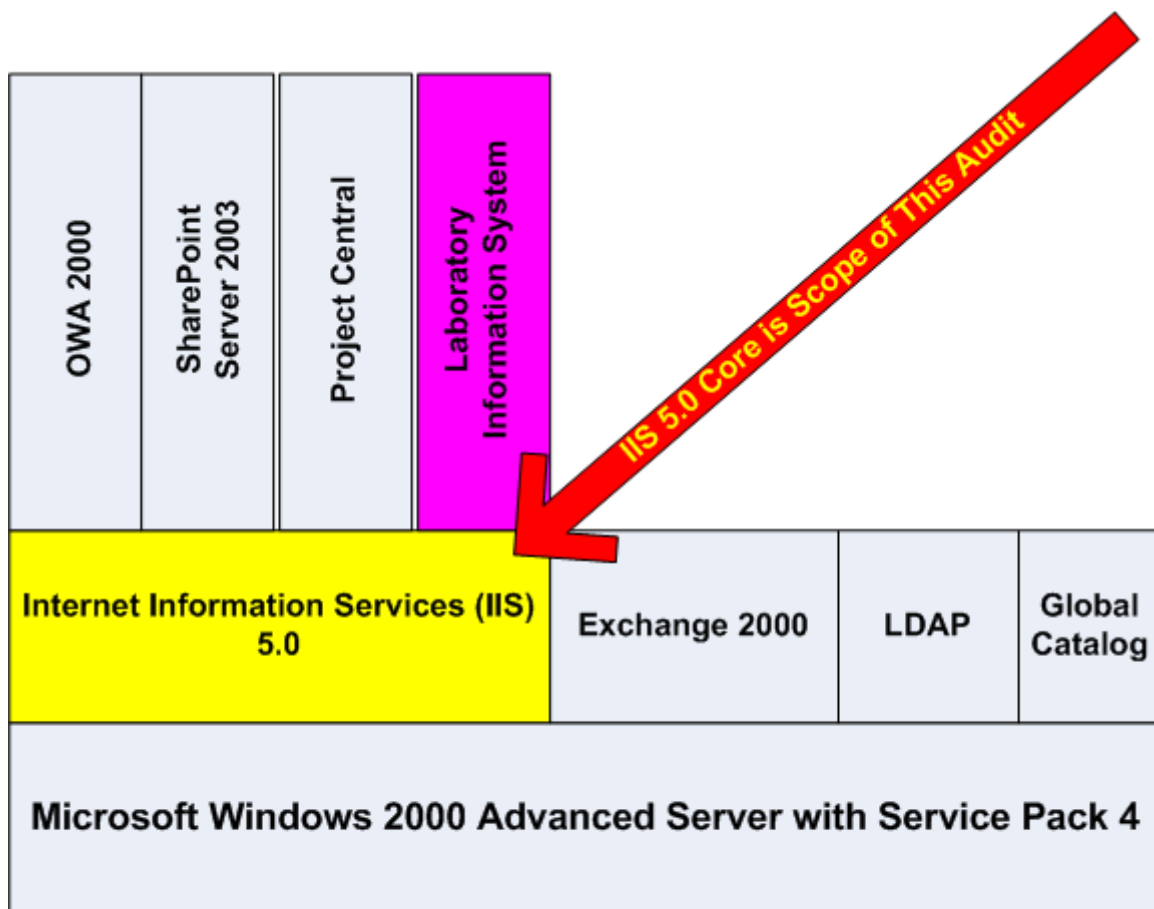


Figure I-2: Architecture of IIS 5.0 Isolation Mode⁶

The above picture shows the architecture of the IIS core services, in this case IIS 5.0 isolation mode.

⁶ Microsoft Resource Website. IIS 6.0 Technical Reference. Figure 2.2
 URL: <http://www.microsoft.com/resources/documentation/IIS/6/all/techref/en-us/iisRG_ARC_1.msp>



SIMBA Web Server

Figure I-3: Web Server Audit Scope is IIS Core

BloodLab's mission critical server is running multiple applications, the Laboratory Information System which is the mission critical application, along with Exchange 2000, SharePoint Portal Server 2003, Project Server 2003, OWA 2003, and the server is also functioning as a domain controller with Global Catalog services enabled.

SECTION 1: RESEARCH - AUDIT, SCOPE, RISKS AND TOOLS

1.1 System to be Audited and its Role

The target system is running Microsoft Windows Server 2000 with Service Pack 4. It is a server class hardware system built from raw components. It is not a name brand computer and was not bought off the shelf. We will use fictitious names for these servers modeled after Disney characters. We will call this server Simba⁷.

Simba is located behind a UNIX® firewall running a version of Berkeley Software Design, Inc (BSD). Since Simba has Internet exposure, it also serves as the e-mail gateway and OWA server. Simba is running Microsoft Exchange 2000, and is also configured as a Domain Controller.

The laboratory operates on a schedule of 24x7. When closed for holidays, technicians are on call. Since the operations of the laboratory are heavily dependent on the application running on the web server, the web application also requires 24x7 availability.

A physician can order a laboratory test at any time, and certain STAT⁸ reports have high priority and could mean life or death for a patient. Emergency reports will be called directly to the physician, and there are other backup methods of transmitting results if the web application should fail.

This web application was a big seller and attracted many physicians, especially since it allowed the physicians to have self-service in accessing patient records. When the system or application is down, running slow, or not operating well, it reflects poorly on the business and could lead to a loss of the physician. Availability, performance and proper operation of the system is of critical importance.

1.1.1 Current Environment

BloodLab has less than 12 servers, located in a locked server room. Most of these servers are Windows based, running Windows 2000 server. BloodLab has an external Internet presence and with its registered domain name houses its own external DNS servers in this room. Connection is via a leased T1 line.

⁷ From the Walt Disney Productions movie, *The Lion King*

⁸ STAT – Statim (Latin: immediately [medical]) using google acronym finder

URL: <<http://www.acronymfinder.com/af-query.asp?String=exact&Acronym=stat&Find=Find>>

Other servers located in this room include file and print servers, domain controllers, Exchange 2000, SQL 2000 and additional web servers. A MicroVAX computer runs some older legacy systems that are being converted to the Windows platform. This conversion is very recent since all the software had to be rewritten to comply with Health Insurance Portability and Accountability Act of 1996 (HIPAA)⁹ formats.

One server is a UNIX© BSD server running IPTABLES as a firewall. The corporate network is separated from the Internet using this firewall and overloaded NAT. Some of the other servers, including the target server are connected to the firewall. However, port filtering is very liberal, allowing many of the ports to be open – as if there was no firewall at all. This leaves many servers behind the firewall, but not fully protected since the firewall was not configured to perform port filtering. Port filtering is in effect for several of the dangerous protocols and ports, such as the NetBIOS and file sharing ports, where those ports are blocked.

Several of the servers are really workstations running in a server role. They don't perform well, and occasionally fail. With the migration of the MicroVAX applications to Windows using .NET programming, it was determined that BloodLab had to be realistic and use certified server class equipment with hardware redundancy. Within this project new servers were acquired for the Web server and database servers. The equipment is server class equipment, but from a cost decision, these servers were built from generic components and not purchased from a server vendor such as IBM, Dell, HP or Compaq. The decision to use OEM equipment represented significant cost savings.

⁹ Centers for Medicare & Medicaid Services URL: <<http://www.cms.hhs.gov/hipaa/>>

1.1.2 Current Configuration

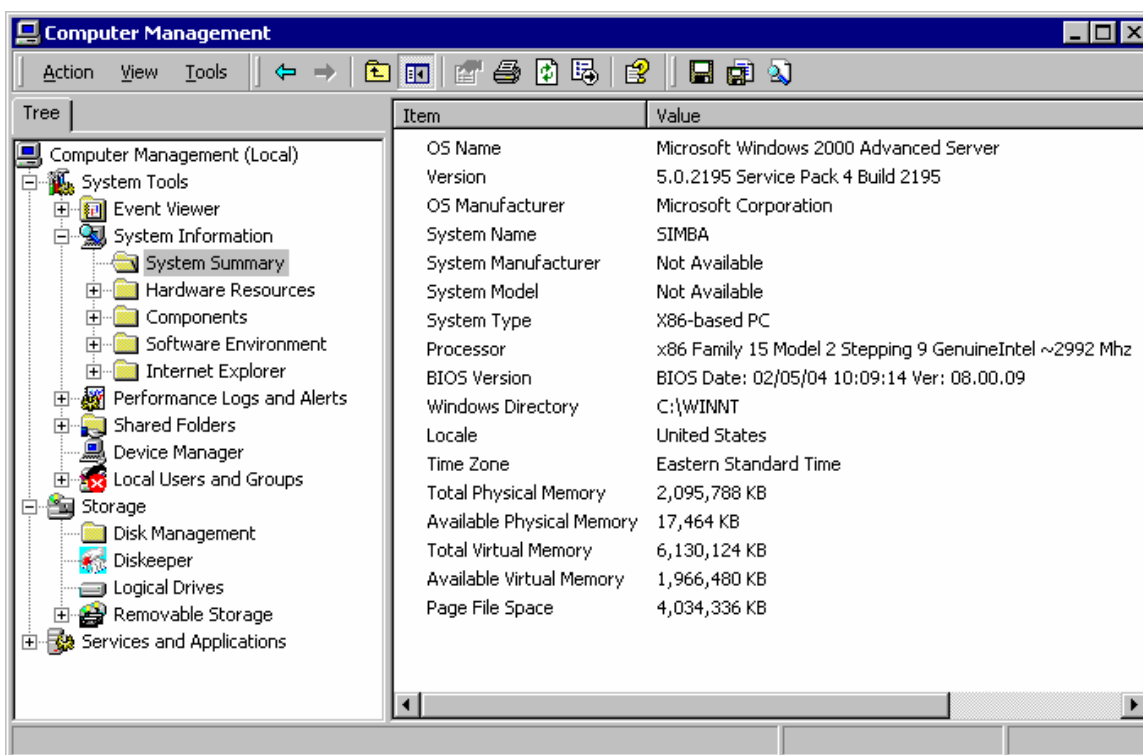


Figure E2: Computer Management – System Summary

We see from Figure E2 (Computer Management – System Summary) that the system is Windows 2000 Advanced Server with Service Pack 4 and Build 2195. Since this system is a custom build, Manufacturer and Model are unknown. The system is a 3GHZ processor, with 2GB of ram memory.

For disk, a RAID-5 Array which provides 300GB of disk space divided into two logical drives of 152GB each, one drive is C and the other is D. The CDROM is E.

Microsoft Security fixes are occasionally applied to the machine. There currently are no standards or guidelines for server hardening, and it is believed that the IIS Lockdown tool was never used to lock down any of the web servers.

1.1.3 Scope of Audit

The target for this assignment is to only assess the configuration of the IIS component and factors directly involving the IIS component of Microsoft Server.

IIS is an acronym for Internet Information Services, and is a feature of Windows 2000, and for Windows 2000 it is IIS Release 5.0.

The base Operating System and actual application processing are out of scope for this audit. This indicates that the audit will not be testing for application vulnerabilities, such as SQL insertion or Cross Site Scripting. Application testing of this nature, if needed in the future, could be performed using open source tools and available commercial scanners. The Open Web Application Security Project (OWASP)¹⁰ is a good resource on application vulnerabilities. Their website features a document from their Top 10 project: **Top Ten Most Critical Web Application Vulnerabilities**¹¹ that would complement SANS TOP 10 list¹².

Out of Scope

- Review of Firewall Configuration
- Review of Firewall Rule Base
- Review of Switch and Router ACL
- Review of Application Code
- Physical Security
- Operating System
- Database Server
- ODBC/JDBC Drivers
- Exchange Server
- Domain Controller
- Web server authentication
- Encryption (e.g. SSL)
- TCP/IP Stack
- Penetration Testing

1.1.4 Tools used

Most of the IIS configuration issues could be detected using The Microsoft Security Baseline Analyzer (MSBA)¹³. My checklist has some additional items that may require visual inspection using the IIS Admin console or Windows Explorer.

¹⁰ The Open Web Application Security Project URL: <www.owasp.net>

¹¹ OWASP Top Ten Project URL: <<http://www.owasp.net/documentation/topten.html>>

¹² SANS/FBI Top 20 List for Windows, Oct 8, 2004 URL: <<http://www.sans.org/top20/>>

¹³ Microsoft Download Site Microsoft Baseline Security Analyzer 1.2.1 August 16 2004 URL: <<http://www.microsoft.com/technet/security/tools/mbsahome.msp>>

1.2 Significant Risks to the System

Risk Management (RM) and Risk Analysis (RA) can be conducted using several methods. The basic two methods are Quantitative and Qualitative. There are additional methods that are based on the procedures that are used to assign values to the assets, probabilities or frequencies.

Some of these Risk Analysis methodologies are¹⁴:

- Facilitated Risk Analysis Process (FRAP)
- Failure Mode and Effects Analysis (FMEA)
- Hazard and Operability (HAZOP)
- Historical Analysis
- Human Error Analysis
- Probabilistic Risk Assessment (PRA)
- Tree Analysis

The above methodologies are provided for the reader in doing additional research. These methods are not described nor used in this paper. To keep the risk analysis manageable, a qualitative method will be used.

In order to do a good quantitative RA, asset valuation and threat probability need to be defined in very discrete and accurate numbers, and is not always possible or at least very difficult to estimate. However, qualitative is much easier and faster if the problem can be broken down into smaller discrete estimates. In a qualitative analysis we will divide the threats and probabilities into three values: High, Medium or Low.

The decision between using a Qualitative vs. Quantification analysis is compared in NIST¹⁵

“Quantitative versus Qualitative Assessment In conducting the impact analysis, consideration should be given to the advantages and disadvantages of quantitative versus qualitative assessments. The main advantage of the qualitative impact analysis is that it prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities. The disadvantage of the qualitative analysis is that it does not provide specific quantifiable measurements of the magnitude of the impacts, therefore making a cost-benefit analysis of any recommended controls difficult.”

¹⁴ Paul, Brooke. *Calculate Your Risk*. *Secure Enterprise* Jan 2005: pp: 16-22.

¹⁵ United States. National Institute of Standards and Technology. *NIST SP800-30 Risk Management Guide for Information Technology Systems* January 2002. P. 23

1.2.1 Assets at Risk

We must establish what assets are at risk, and why these assets are important to the organization. This section will establish which critical¹⁶ assets require protection and may be put at risk by the target system under this audit, i.e. failure of the IIS component could lead to a compromise or loss of these listed assets. The assets being chosen are based on specific assets required for the business to perform its function and deliver its services. These specific assets are critical to the business, such that their importance and value are all rated high if a major compromise of that asset occurs. These are some of the assets that keep the CEO awake at night.

- **Brand, also known as Goodwill or Reputation (Brand)**

The reputation of the company, and its Brand, is the most critical asset that requires protection. Since the reputation is difficult to assess financially, its value is subjective, it is considered an intangible asset. The key partner asset for the company being assessed and that drives the reputation is customer service. If another asset is compromised, and such compromise becomes public knowledge, there can be a ripple effect that can tarnish the reputation of the company. Depending on the compromise, there may be legal repercussions that can lead to lawsuits, loss of license, loss of revenue, and can be severe to a level that can put the lab out of business.

When services or a product become generic in nature, your name, your reputation, your brand may be all you have to separate yourself from the rest. If that becomes your main critical asset, any damage to the brand could be catastrophic.

Clinical laboratories are state licensed. However, since many laboratories process patients with Medicare insurance, those laboratories come under many federal rules and regulations. One set of regulations imposes a price list that controls the maximum amount of reimbursement for services. Even private insurance companies impose price lists that limit pricing to Reasonable and Customary (R&C). This limits any competition based on pricing, where competitive pricing would only impact a small amount of uninsured patients. The disbursement of free or discounted services to physicians is also forbidden by federal rules when Medicare is involved. For example, offering any type of incentive to a physician to influence the

¹⁶ The critical assets were defined by the business, and stated by the CEO. Criticality of assets will vary from organization to organization, and only the organization can determine what it considers valuable and important.

physician to recommend work to a particular laboratory may be considered a form of kickback, and may be illegal. A physician normally cannot demand that a patient use a specified laboratory (this could be done in the case of a HMO where HMO's are an exception).

Even on the state level, for example New York has Public Health Law 587 which has language: "Generally, Section 587 of the New York Public Health Law prohibits clinical laboratories from mak[ing], offer[ing], giv[ing], or agree[ing] to make, offer or give any payment or other consideration in any form to the extent such payment or other consideration is given for the referral of services. The law also prohibits any person or entity that provides health-related services (referred to as a health services purveyor) from solicit[ing], receiv[ing], accept[ing] or agree[ing] to accept any [such] payment or other consideration. Further, the law prohibits clinical laboratories and health services purveyors from participat[ing] in the division, transference, assignment, rebate or splitting of fees, with any [health services purveyor or clinical laboratory] in relation to clinical laboratory services."¹⁷

- **Clinical Laboratory License (LIC)**

Clinical laboratories that process human tissue and fluids are regulated on the state level, and require state licensing. (An example where this would not apply would be a laboratory that exclusively processes blood work for animals) Licensing may be based on the location of the laboratory or the location of the patient. For example, a clinical laboratory located in Maryland would be required to be licensed by an agency located in Maryland. (Under Maryland regulations, COMAR Title 10, Subtitle 10, a State license is required if a testing site performs clinical laboratory tests. A site must also meet certain federal operating requirements under 42 CFR Part 493, including having a CLIA certificate¹⁸). However, there are states that have requirements that any out of state laboratory performing processing of a resident must also be licensed by the state. In a situation such as this, a laboratory may need to be licensed for each state for which the laboratory processed resident patients. This situation would most likely occur when blood work is shipped over state lines to be processed in a laboratory operating in another state.

Licensing is based on several factors. A major part of the licensing includes the individual tests that the laboratory is proficient and certified for. Periodic proficiency exams test and confirm the accuracy of the lab. One method used is that the state will send samples to be processed, where the values of the samples are known, but only to the state testing agency. The final report issued by the lab should report test result values

¹⁷ Garfunkel, Wild & Travis, P.C. New York Health Law Update, Jan 2002

URL: <<http://www.gwtlaw.com/gwt/healthlawjan2002.html>>

¹⁸ URL: <<http://www.dhmd.state.md.us/ohcq/faq/labfaq.htm#2>>

that are within acceptable deviation. Since the state knew the proper values of the samples before shipping them, the state knows what to expect (i.e. that the report should say).

Since a laboratory may be licensed to run multiple tests, it is required that proficiency testing be performed individually in each area of competency. Failure of proficiencies in a particular testing procedure could decertify the laboratory from performing that clinical test until the proficiency can be reestablished at a passing grade.

These proficiency tests, if not recorded properly, could have an adverse affect on the license. The laboratory connects the laboratory equipment (such as a chemistry analyzer) by a computer network to the servers where test results are downloaded into the database directly from the equipment. A breach of the network integrity could allow the results of any test to be discovered, lost or modified – which violates confidentiality and integrity requirements.

If any data is changed or corrupted during transmission or while stored in the database to a different value than the one reported by the testing device, then the recorded accuracy will be wrong as the result of an integrity failure. This could lead to proficiency testing failures, and loss of the ability to perform tests, or even revocation or suspension of the laboratory license. If the license is suspended or revoked, the laboratory is either temporarily or permanently out of business.

Other requirements for licensing include documented procedure manuals and record keeping. These are produced from documents and files that are stored on the computer system. A breach of the computer system that may cause these files to be corrupted or lost may contribute to a failure in the audit and review that occurs periodically and as part of license renewal.

No License = No Laboratory.

- **Customer Service (CS)**

The only revenue stream for the laboratory is fees for laboratory testing. Price competition is not an option, nor is incentives to attract clients. When evaluating a change in clients – either the loss of clients or attracting clients from competitive laboratories the reason most given for the change is customer service and how the client was treated. The laboratory will address two classes of clients: The patient and the physician. Both must be kept happy to insure that the patient will use the laboratory as well as return for future testing.

In the case of the physician, blood or serum may be drawn by the physician and directly sent to the laboratory for processing. In this

scenario, the specimens are picked up by a laboratory courier and brought to the laboratory for testing. In the case of the patient, the physician gives the patient a prescription indicating which tests are to be performed, and the patient goes to a draw station run by the laboratory.

So, keeping either or both happy will be important. If the physician is not happy with the service provided by the laboratory, then he will send the work to someone else. For all intents and purposes, when the physician does the draw and sends the work order, this is really a referral. In the case of a walk-in patient, how that patient is treated may determine if they come back next time.

Since the entire laboratory is run off the laboratory computer system, that system is a key factor to all operations. If the computer is slow, due to performance issues, then wait lines can be longer, phone requests for results may be slow, and reports may not be issued on time. An attack on the integrity of the data may also impact the ability to service patients and physicians. A very large part of customer service is billing. If the information in the database is not accurate, this may cause billing errors or loss of billing. Clients do not want problems and they don't want to wait when trying to get information or resolve a problem.

- **Accounts Receivable (AR)**

Revenue received by the lab is all test related. The majority of the revenue comes directly from insurance companies, with the largest being Medicare. Some billing will be paid by patients, to either cover deductibles or for uninsured patients. Payments may cover the process of actual drawing of blood (a stick fee, e.g. Medicare reimburses each stick at \$3 each), mileage reimbursement if a patient has to be visited (a home draw), and the charges for the actual test (limited by a fee schedule).

Billing has time limits, a statute of limitations. If not billed within a reasonable time, then the bill may be uncollectible. Timely billing is required, as the more timely the billing the better the chances of getting paid.

The threats against billing and accounts receivable are integrity based. A change in the billing values could lead to inadequate billing, over billing, or no billing at all. Loss of billing is a direct dollar loss in revenue. Over billing will not lead to excess income since most amounts are capped by the reimbursement fee schedules and in worst case will cause customer service headaches handling billing inquiries. An attack on the availability may include delaying the billing making it too late to bill.

Account Receivable is a tangible asset and can be sold off. After a predetermined time, which the receivables are still collectable, the accounts receivable can be sold off to a collection agency.

- **Payroll (PAY)**

Payroll has a direct effect on the bottom line and the profitability of the laboratory. Availability issues may cause employees not to be paid or paid late. Integrity issues may underpay or overpay an employee. Overpaying could be a method that would allow an employee to extract extra money that they would not be entitled to.

Payroll is handled by a different external system, so an integrity attack to increase salary or hourly rates is unlikely. The laboratory system does handle and process time cards, so payment can be manipulated through the number of hours. Employees can double their hourly paycheck by doubling the hours.

- **Inventory (INV)**

Inventory is an asset, and it takes assets such as hard cash to keep the inventory up to the proper level. Inventory includes office supplies such as paper, toner, and even toilet paper. Laboratory processing supplies include reagents (chemicals used in testing and analyzer machines) which make up a major percentage of supplies. Then there are drawing supplies, such as lances, needles and vacuum specimen tubes.

Supplies may be used onsite at the main facility, at a satellite facility (draw station), and certain supplies are sent directly to physicians. All the supplies that are used in testing, including reagents, have an expiration date. If not used within that date, the expired item has to be discarded.

Manipulation of the inventory can cause an under or over inventory condition. In the case of an under inventory condition, there may not be enough supplies to do a days work. In one case several patients had to be turned away because one of the satellite sites ran out of vacuum tubes. Over inventory may occur when too much is ordered. The issue with over inventory is that unused supplies have to be discarded if they expire.

An integrity attack on the inventory can cause these under and overage situations. It can also be used to directly remove and acquire inventory. Most inventory for use outside the laboratory is delivered to the laboratory via UPS or FedEx but then delivered to satellite sites and physicians via courier. A change to the inventory order system could be introduced by a hacker to reroute an order to a bogus location for pickup.

Now in most of these situations, many items are not usable. There is no profit in stealing reagents or other medical supplies (unless you own your own laboratory), so manipulation of those orders is more of a nuisance and may cost the laboratory a lot of money. The order system and inventory also hold items of interest that can be used, such as computers, software, and house cleaning supplies.

An attack on the integrity of the inventory can lead to losses as the asset become unusable or loss of business revenue if you don't have supplies to process the patient or do the tests.

- **Internally Developed Proprietary Software, Process and Procedures, Intellectual Property (IP)**

The laboratory system is internally developed. It also includes internally developed drivers that read analyzer machines and automatically inputs the test results. Without the drivers, test results would be read from the device and manually inputted into the data entry application.

Process and Procedures are critical business confidential information, and are produced from Word documents stored on the servers.

This software and system is integral to the operations of the laboratory and is critical to its competitive advantage.

- **Patient Records (PR)**

The information stored in patient records are subject to privacy regulations, in this case Health Insurance Portability and Accountability Act of 1996 (Health Insurance Portability and Accountability Act of 1996 (HIPAA)¹⁹). Storage of other personal information, such as credit card information, must also be protected.

Unauthorized disclosure of this information could lead to lawsuits and negative publicity. Integrity attacks can cause headaches of increased customer service or even death. Manipulation of actual test results in the patient record – and subsequently reported to the physician could cause a patient to not receive necessary medical care, or cause overmedication of the patient.

- **Patient Lists (PL)**

A patient list is similar to patient records, but is more demographic and does not contain medical information. Patient lists are used to solicit via mail promotional offers, such as annual health fairs. Many entities hold health fairs during the year, and these health fairs are not subject to insurance because these health fairs provide screening, not full services.

¹⁹ Centers for Medicare & Medicaid Services URL: <<http://www.cms.hhs.gov/hipaa/>>

Patient lists can provide some competitive advantage when running a service like this.

Unauthorized disclosure of this information may lead to a loss of business for these specialized health fairs, or lead to lawsuits for violation of privacy.

- **Physician Records (PHY)**

The patient demographic also includes the information on the physician ordering the tests. Disclosure of the information may not be of issue, however – changing the information can be catastrophic.

Critical result information, especially in a STAT²⁰ situation, may need to be reported to the ordering physician immediately. These situations include circumstances where the results indicate severe readings that are at life and death levels. Informing the physician within an hour might allow the physician to adjust medication to save the patient. Waiting four hours may be too late and the patient might expire. Critical thresholds that dictate when a physician must be immediately contacted are recorded in the laboratory system.

Failure to promptly notify the physician can make the laboratory liable for when these severe result readings are not transmitted and could have saved the patient life.

An integrity attack could remove or corrupt the physician's contact information. Phone numbers and fax numbers could be removed or deleted, making contact difficult or impossible, especially if automated alerts are transmitted via pager, cell phone or fax.

- **Documents and briefs for current or pending litigation (PRIV)**

Disputes happen. The laboratory sues and gets sued. Corporate counsel is employed by the laboratory and is resident in the main office. The computer systems, in this case servers, are used to hold copies of all litigation documents, including many that would fall under client/attorney privilege or work product rules.

These documents include extremely confidential documents that could expose litigation strategy and derail the laboratory's position in a case.

- **Ability to meet Service Level Agreements (SLA)**

Part of the service objective is quick turnaround on laboratory testing. Sometimes the timely delivery of the results of a test could mean the difference between life and death. In most cases, the physician would be

²⁰ STAT – Statim (Latin: immediately [medical]) using google acronym finder

URL: <<http://www.acronymfinder.com/af-query.asp?String=exact&Acronym=stat&Find=Find>>

aware of critical issues and order the test with a mandated quick turnaround by ordering the test on a “STAT²¹” basis. This type of turnaround is usually within hours, or less.

Not all test turnarounds can be (or should be) indicated as a STAT²² test. If it is not an emergency, then test results could be turned over with 24-72 hours. BloodLab provides a 24 turnaround on 95% of non-stat orders. Although not always needed, the physicians consider the quick turnaround as great customer service compared to the larger major competitors that take 3-5 days to return results.

- **Worker Productivity (WP)**

The entire laboratory system is one complete application system. It is also a single point of failure. If the system goes down, then most of the operations can come to a halt. Analyzer machines that run the tests can run offline and will cache the result values. But without the application running reports cannot be generated, results cannot be sent out, billing cannot be done, and customer calls cannot be processed. Maximizing the availability and performance of the system will affect the productivity of the back office operations.

1.2.1-A Assets at Risk / Risk Management

Quadrant	Type Of Control
Unlikely / Low	Acceptance
Unlikely / High	Financial/Insurance
Likely / Low	Technical
Likely / High	Procedural/Training

Figure 1-1: Mitigating Controls for Likelihood/Cost Quadrants

²¹ STAT – Statim (Latin: immediately [medical]) using google acronym finder

URL: <<http://www.acronymfinder.com/af-query.asp?String=exact&Acronym=stat&Find=Find>>

²² STAT – Statim (Latin: immediately [medical]) using google acronym finder

URL: <<http://www.acronymfinder.com/af-query.asp?String=exact&Acronym=stat&Find=Find>>

1.2.1-B Assets at Risk Likelihood/Cost

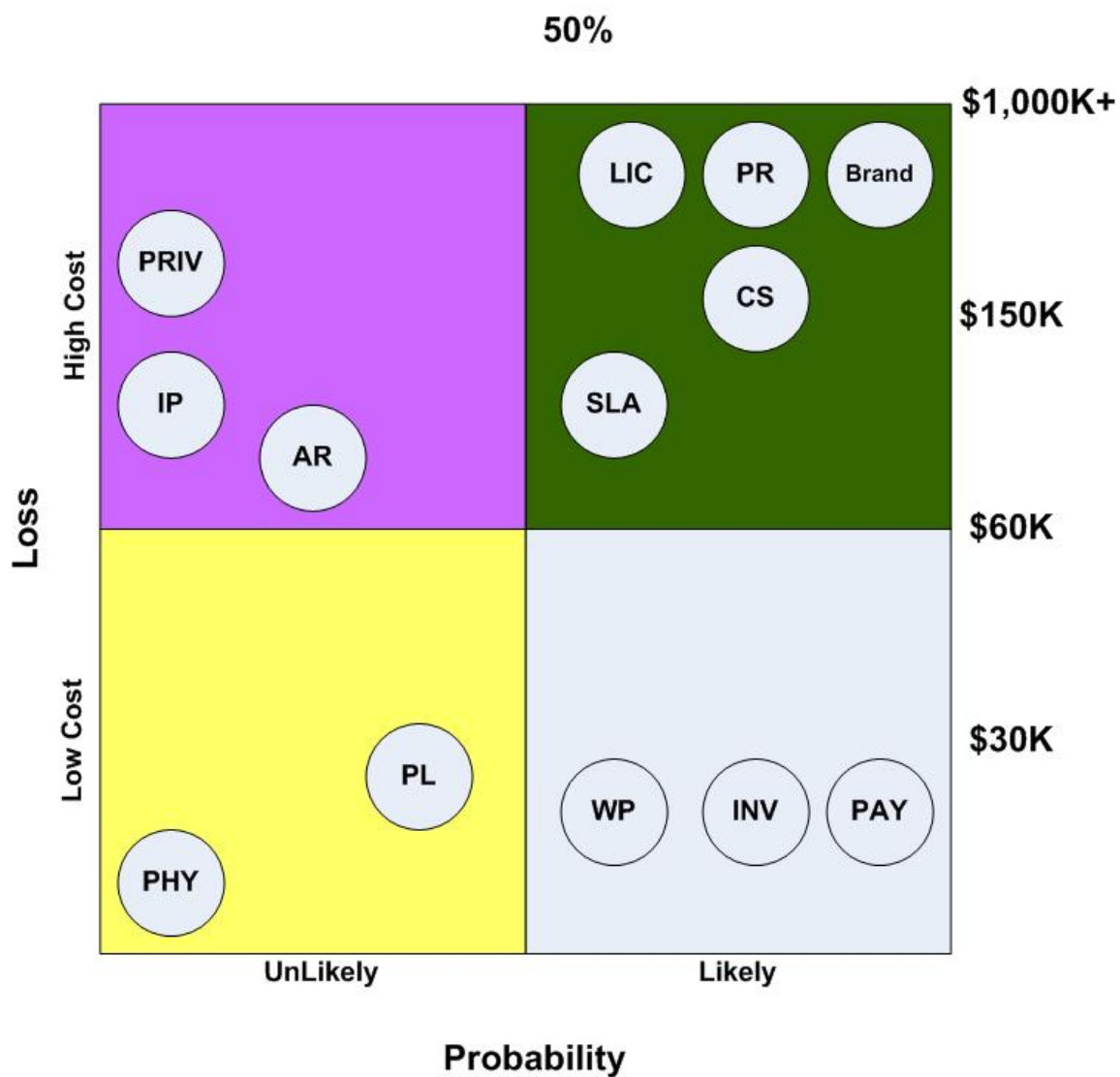


Figure 1-2 – Likelihood/Costs for Assets at Risk

1.2.2 Threats

In order to have a threat, you must first have vulnerability. Then, to carry out that threat, you must have an exploit that will take advantage of that vulnerability. You can still have a threat without an exploit, in that case there is a threat that an exploit may be developed that can take advantage of the vulnerability.

The creation or discovery of the exploit changes the level or severity of the threat. For example, when a vulnerability is discovered and a patch is released, there is a window that allows you to take some time to test the patch before actually applying it. Once the exploit is out in the wild, then time has run out and patching, or some other control, needs to be put in place.

It is assumed that either the exploit or vulnerability is actually known. If there is no vulnerability, there is no threat. But there can be vulnerability and no one has discovered it yet, and that itself is actually a threat in its own right. (In other words, vulnerability is a threat regardless of whether anyone has discovered it yet) In the case of a Microsoft Operating System, just based on experience, there is a high probability that there are vulnerabilities not yet discovered. There are actually vulnerabilities that Microsoft has been aware of and have not been announced to the user community while the patches are being developed.

For example, if we look at MS04-028²³ that was initially released on September 14th 2004, it has a Common Vulnerabilities and Exposures (CVE) number of CAN-2004-0200²⁴. The CVE entry was assigned 20040311 (March 11, 2004) which is 6 months between the creation of the CVE (When someone first reported the discovery of the vulnerability) and the release of a patch by Microsoft. Someone out there knew of this vulnerability for 6 months. When Microsoft finds out, a fix is not generated and released immediately. Luckily, the discoverer of the vulnerability performed responsible disclosure – where the vulnerability was not disclosed until a fix was available and released.

But without knowing the specific vulnerability or an exploit, the threat is low because no one is able to take advantage of the unknown vulnerability yet. Then it becomes a race against the clock where you hope that the vulnerability is discovered and a patch is made available before anyone figures out how to exploit it.

²³ Microsoft Support Website [Buffer Overrun in JPEG Processing \(GDI+\) Could Allow Code Execution \(833987\)](http://www.microsoft.com/technet/security/bulletin/ms04-028.mspx) URL: <<http://www.microsoft.com/technet/security/bulletin/ms04-028.mspx>>

²⁴ Mitre CVE Website [CAN-2004-0200](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0200) URL: <<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0200>>

If we wanted to produce precise risk values, we would need to not only look at the threat, but the threat source²⁵. The probability that a threat may be carried out or the level of success that vulnerability is exploited may depend on the source of the threat and the motivation of that source.

© SANS Institute 2005, Author retains full rights.

²⁵United States. National Institute of Standards and Technology. NIST SP800-30 Risk Management Guide for Information Technology Systems January 2002. p. 12

Table 3-1. Human Threats: Threat-Source, Motivation, and Threat Actions²⁶

Threat-Source	Motivation	Threat Actions
Hacker, cracker	Challenge Ego Rebellion	<ul style="list-style-type: none">• Hacking• Social engineering• System intrusion, break-ins• Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	<ul style="list-style-type: none">• Computer crime (e.g., cyber stalking)• Fraudulent act (e.g., replay, impersonation, interception)• Information bribery• Spoofing• System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	<ul style="list-style-type: none">• Bomb/Terrorism• Information warfare• System attack (e.g., distributed denial of service)• System penetration• System tampering
Industrial espionage (companies, foreign governments, other government interests)	Competitive advantage Economic espionage	<ul style="list-style-type: none">• Economic exploitation• Information theft• Intrusion on personal privacy• Social engineering• System penetration• Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	<ul style="list-style-type: none">• Assault on an employee• Blackmail• Browsing of proprietary information• Computer abuse• Fraud and theft• Information bribery• Input of falsified, corrupted data• Interception• Malicious code (e.g., virus, logic bomb, Trojan horse)• Sale of personal information• System bugs• System intrusion• System sabotage• Unauthorized system access

An estimate of the motivation, resources, and capabilities that may be required to carry out a successful attack should be developed after the potential threat-sources have been identified, in order to determine the likelihood of a threat exercising a system vulnerability.

²⁶ United States. National Institute of Standards and Technology. NIST SP800-30 Risk Management Guide for Information Technology Systems January 2002. P. 14 Table 3.1

1.2.3 Threats & Consequences

Threats relate to assets of the organization. Previously the critical assets of BloodLab have been listed. In this section we will look at how a threat relates to security goals²⁷ of those assets.

The threats that will be presented here are grouped according to the Security CIA triad, which may be found referenced in many books on security, especially if you were studying for the ISC² CISSP²⁸ exam. One such study guide²⁹ discusses the triad.

The CIA triad stands for: Confidentiality, Integrity, and Availability. A threat is a potential event that can compromise the Confidentiality, Integrity, or Availability of an asset in an undesirable manner. Threats may have impacts that ripple through other assets and eventually may impact the business as a whole.

The following tables show the potential threat and the possible impact if the threat is partially or completely carried out.

²⁷United States. National Institute of Standards and Technology. NIST SP800-30 Risk Management Guide for Information Technology Systems January 2002. P. 28

²⁸URL: <<http://www.isc2.org>>

²⁹Krutz, Ronald L. and Vines, Russell Dean. The CISSP Prep Guide – Mastering the Ten Domains of Computer Security, New York: Wiley Computer Publishing 2001 (ISBN: 0-471-41356-9) p. 8

- **Confidentiality**

Threat	Consequences if Threat is successfully carried out
Unauthorized disclosure of patient information and records which may include medical information. Information may include lab results, diagnosis, and protected health information (PHI) under HIPAA.	<ul style="list-style-type: none"> • HIPAA violation that could lead to fines, penalties, and imprisonment³⁰. • Individual lawsuits from patients that were harmed. • Loss of confidence of physicians. • Loss of referrals from physicians. • Loss of patients. • Degrading of reputation. • Loss or suspension of license. • Violation of other privacy laws.
Unauthorized disclosure of work product, attorney/client communications, or any other privileged communications used for active or pending litigation.	<ul style="list-style-type: none"> • Reduction in possible settlement amounts. • Possible loss of case. • Increased legal fees due to a more complicated litigation.
Unauthorized disclosure of patient demographic information NOT including any medical information, so that HIPAA would not apply but local privacy laws, such as Ca. Senate Bill (SB) 1386 ³¹ might apply.	<ul style="list-style-type: none"> • Individual lawsuits from patients that were harmed. • Loss of confidence of physicians. • Loss of referrals from physicians. • Loss of patients. • Degrading of reputation. • Violation of other privacy laws. • Exposing the patient to Identity Theft if private information is breached. • Exposing the patient to credit card losses if disclosure results in unauthorized use of the credit card information stored in the laboratory database.
Unauthorized disclosure of application source code for the laboratory system.	<ul style="list-style-type: none"> • Loss in competitive advantage • Loss of value in internally generated and developed propriety software.

³⁰ HIPAA Complete Avoid HIPAA non-compliance penalties

URL: <<http://www.hipaacomplete.com/penalties.asp>>

³¹ California State Senate Official California Legislative Information Bill Information

URL: <http://info.sen.ca.gov/cgi-bin/postquery?bill_number=sb_1386&sess=PREV&house=B&site=sen>

- **Data Integrity**

Threat	Consequences if Threat is successfully carried out
Unauthorized alteration of patient records, specifically lab result data, where lab test results get changed causing physician to improperly treat the patient.	<ul style="list-style-type: none"> • HIPAA violations that can result in fines, penalties and possible imprisonment. • Serious Injury to patient. • Death of patient. • Patient suffers a serious health event requiring hospital admission³² • Delayed diagnosis and treatment • Patient or others at increased risk or harm • Patient loses trust in physician or lab • Patient Financial, Time and other costs • Physician Financial, Time and other costs • Health System misuse • Lawsuits for malpractice. • Insurance violations. • Insurance fraud. • Suspension or loss of license. • Degradation of reputation usually from bad publicity. • Increases in insurance premiums for liability and malpractice.
Unauthorized alteration of physician records, which could lead to delays in treating the patient in an emergency due to inability of laboratory to contact physician.	<ul style="list-style-type: none"> • Serious injury to patient. • Death of patient. • Lawsuits for malpractice. • Degradation of reputation usually from bad publicity. • Violation of service level agreements for prompt notification. • Increases in insurance premiums for liability and malpractice.
Unauthorized alteration of account receivable A/R records.	<ul style="list-style-type: none"> • Loss of revenue, billing records lost. • Revenue uncollectible due to lapse time period. (Took too long to collect) • Wrong party paid. • Embezzlement of money or services.

³² Philips, Robert MD. Laboratory Safety and Quality in Primary Care: Evidence and Revolution
URL: <http://www.phppo.cdc.gov/mlp/QIConference/Presentations/Phillips-Quality%20Institute.pdf>> P25

	<ul style="list-style-type: none"> • Increased billing errors. • Increased billing complaints • Perception of bad customer service. • Increases in insurance premiums for liability and malpractice.
Unauthorized alteration of inventory records.	<ul style="list-style-type: none"> • Loss of inventory stock, changes could be used to cover for embezzled items. • Overstocking, resulting in time sensitive items expiring (going bad) and having to be thrown out. The asset is wasted. • Under stocking, resulting in loss opportunity to service patients. Could cause increased overhead costs if tests must be referred to another laboratory in order to get the work done.
Unauthorized seizure of the IIS server by a hacker, or unauthorized remote code execution on the server, used as a zombie to either issue SPAM to other targets or even outright attack other targets.	<ul style="list-style-type: none"> • In the case of a zombie that is used to attack other companies, including a distributed denial of service attack, the owner of the compromised machine could be subject to downstream liability for the attack. • In the case of becoming an open relay for SPAM, state an federal laws may be violated, including the CAN SPAM act of 2003³³. • Lawsuits, fines or penalties in this situation will affect the money in the bank, but will also degrade the reputation and trust of the laboratory (assuming public exposure).

³³ URL: <<http://www.spamlaws.com/federal/108s877.html>>

- **Availability**

Threat	Consequences if Threat is successfully carried out
Unauthorized destruction of patient records prior to legal requirement for retention (record is deleted too soon).	<ul style="list-style-type: none"> • Insurance fraud. • Inability to service the patient. • Inability to justify work performed. • Cannot associate tests to account receivables (A/R) result in loss of revenue. • Cost of having patient retested if this is a recent draw. • Suspension or loss of license for improper record keeping. • Fines and penalties associates with erroneous record keeping.
Unauthorized destruction of patient records before reporting results to physician (physician is never notified of laboratory results)	<ul style="list-style-type: none"> • Serious Injury to patient. • Death of patient. • Patient suffers a serious health event requiring hospital admission³⁴ • Delayed diagnosis and treatment • Patient or others at increased risk or harm • Patient loses trust in physician or lab • Patient Financial, Time and other costs • Physician Financial, Time and other costs • Health System misuse • Increases in insurance premiums for liability and malpractice.
Unauthorized destruction of physician records prior to legal requirement for retention (record is deleted too soon).	<ul style="list-style-type: none"> • Inability to associate a patient to a physician. Since a prescription is required for tests, the physician ordering the test must be identified, otherwise additional issues may occur. • Insurance fraud • Inability to contact physician in emergency, leading to patient injury or even death because proper treatment is

³⁴ Philips, Robert MD. Laboratory Safety and Quality in Primary Care: Evidence and Revolution
URL: <<http://www.phppo.cdc.gov/mlp/QIConference/Presentations/Phillips-Quality%20Institute.pdf>> P25

	<p>delayed.</p> <ul style="list-style-type: none"> • Lawsuits, malpractice, and other actions taken should injury or death result. • Increases in insurance premiums for liability and malpractice.
Unauthorized destruction of account receivable records prior to legal requirement for retention (record is deleted too soon)	<ul style="list-style-type: none"> • Account receivables, like inventory, are needed to determine profit/loss and complete income taxes. • Inaccurate tax filings • Inaccurate sales tax filings • Loss of collectable income
Unauthorized destruction of payroll or employee records prior to legal requirements for retention (record is deleted too soon)	<ul style="list-style-type: none"> • Income tax violations because employee tax records not retained. • Inability to report withholding tax if records deleted before W2/1099 are generated. • Employees might not get paid. • Employee insurance may disappear and the employee would not show benefits. • Underpaid withholding taxes
Unauthorized destruction of inventory records prior to legal requirement for retention (record is deleted too soon)	<ul style="list-style-type: none"> • Loss of ability to track inventory. • Promotes embezzlement because someone stealing inventory can cover their tracks. • May affect profit and loss statements used for income tax filing and may be required for a future income tax audit.
Unauthorized destruction of work product and attorney/privilege documents required for litigation.	<ul style="list-style-type: none"> • Loss of critical information may be expensive to reproduce.
Unauthorized destruction of source documents for application software.	<ul style="list-style-type: none"> • Cost to reproduce the application source code, if the original files cannot be retrieved from backup or CDROM. • The cost is in inconvenience to recover or rebuild the original source code.
Unauthorized destruction of source documents for laboratory procedure manuals.	<ul style="list-style-type: none"> • Cost to reproduce the source of the manuals in word format, if the original files cannot be retrieved from backup or CDROM. • The cost is in inconvenience to recover or rebuild the original source file.
Unauthorized destruction of operational code on the IIS server, including the	<ul style="list-style-type: none"> • This is a denial of service if the server becomes disabled. • Inability to meet service level

Operating System and IIS. This may be destruction or degraded performance caused by malware (viruses, worms and spyware).	<p>agreements.</p> <ul style="list-style-type: none"> • Inability to service the physician. • Inability to service the patient. • Inability to produce and distribute patient reports. • Physician and Patient dissatisfaction leading to loss of business and revenue. • Loss of worker productivity.
Storage and transmission of unauthorized data files, including warez, copyrighted media materials (e.g. Movies, MP3)	<ul style="list-style-type: none"> • This is a denial of service if the communications links (the T1) becomes saturated. (Bandwidth stealing). • Application can lock up with the inability to create new records or expand files if all disk space is consumed and no free space is left. • Inability to meet service level agreements. • Inability to service the physician. • Inability to service the patient. • Inability to produce and distribute patient reports. • Physician and Patient dissatisfaction leading to loss of business and revenue. • Loss of worker productivity.

© SANS Institute 2005

1.2.4 Major Vulnerabilities

- **Internal Staff**

Internal staff represents a major vulnerability in that their actions can either directly or indirectly cause harm to the systems. Just through social engineering critical information that can be used to breach and compromise a system could be leaked. Without formal written security procedures reinforced by security and awareness training makes the insider the weakest link in the security chain.

- **Buffer Overflows**

A successfully exploited buffer overflow can lead to exploits of either execution of code (choice of user) or escalation of privilege, or both. Buffer overflows are the most common vulnerability of Windows systems for worm generation and propagation. Buffer overflows were the mechanism for the Slammer (MS02-039)^{35 36}, Blaster (MS03-026)^{37 38}, and Sasser (MS04-011)^{39 40} worms. The common techniques to protect from buffer overflows are to either remove the software if not used, or keep up to date with security fixes.

- Lack of service pack application for known security fixes
- Running unnecessary services
- Zero-Day Exploits – Exploits that are released to the wild before a fix or patch is available

- **Default installed Software and Features**

Misuse of current installed features can lead to exploits of either execution of code (choice of user) or escalation of privilege, or both. This may also provide unintentional disclosure of data without actual compromise of the IIS server. Some of the common techniques for protection is removal of the feature or setting effective permission to prevent misuse of the feature. Defaults also apply to default accounts, passwords, and configurations that represent the state of software or an operating system when freshly

³⁵ URL: <<http://securityresponse.symantec.com/avcenter/venc/data/w32.sqlexp.worm.html>>

³⁶ Microsoft Support Site.

URL: <<http://www.microsoft.com/technet/security/bulletin/MS02-039.msp>>

³⁷ URL: <<http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.html>>

³⁸ Microsoft Support Site.

URL: <<http://www.microsoft.com/technet/security/bulletin/MS03-026.msp>>

³⁹ URL: <<http://securityresponse.symantec.com/avcenter/venc/data/w32.sasser.worm.html>>

⁴⁰ Microsoft Support Site.

URL: <<http://www.microsoft.com/technet/security/bulletin/MS04-011.msp>>

installed. A default configuration is wide-open permissions where the “everyone” group gets full permission access by default.

- Sample Applications
- Parent Paths
- MSADC and Scripts Virtual Directories on IIS
- IIS on Domain Controller
- Unused extension mappings

- **Limited or unrestricted Access Control**

One of the security best practices and a fundamental security principle is “Least Privilege”. In least privilege, you provide enough access permissions and user rights as needed by the user to carry out their purpose. Everyone should not be running super user (Administrator-Windows, Root – Unix) and even an administrator who needs such privileges don’t normally require such power for the entire duration of their session. This also includes access to data. Not everyone needs write access to all data, as a matter of fact not everyone needs to have read access either. Data access can be defined in data classification and categories such as “Need to Know” and “Right to Know”. If you don’t have the “need” or “right”, then you probably should not have any access at all.

- Directory Browsing
- Lack of permission support (non-NTFS File System)
- Permission and rights of accounts used by IIS
- Default file permissions (“everyone group”)

1.2.5 Impact of exploited Major Vulnerabilities⁴¹

- **Denial of Service**

A denial of service may be in effect when the IIS server is disabled or severely degraded. A denial of service can occur when the server is compromised by either a buffer overflow exploit or a misuse of current features.

- Anonymous FTP account (consume all disk space)
- Running or zombie code (consume all CPU cycles)

- **Downstream liability**

Downstream liability can occur when your resources are compromised and then used to relay and attack someone else. The hacker forces you

⁴¹ SANS/FBI Top 20 List for Windows, Oct 8, 2004 URL: <<http://www.sans.org/top20/>>

as a middleman and usually disguises their identity. This makes you a pawn or puppet where the hacker is pulling the strings. This concept is called downstream because the node being attacked will attempt to trace the attack upstream, and will trace to your compromised systems that are “owned” by the hacker. This leaves you with a liability to the victim downstream who suffered from your system attacking it. The amount of liability may be determined by whether the initial compromise could have been prevented. If it was preventable, then you may be liable for not taking the appropriate steps to safeguard the system from compromise.

Determining whether a downstream liability can be established, and the amount of liability, are assignments for the lawyers. It is probably impossible to prevent such an attack, but at least for the minimum, certain best practices should be performed to reach levels of “due diligence” and “due care”.

- SMTP Open Relay
- Running of zombie code

Some newer concepts of downstream liability are being formulated. Joann Kennedy⁴² mentions about the use of Steganography⁴³ to hide and trade images on a compromised machine. Imagine the damage and negative publicity is the material was child porn. The most common exposure in this area has always been anonymous FTP servers which allow uploads of these types of files. To date, the exposure of the anonymous FTP servers have been changing innocent bystander web and FTP sites into Warez⁴⁴ sites that illegally trade copyrighted computer programs, music and even movies in DVD quality. Where downstream liability in the past had to do with pass-thru attacks, it may now be expanded to cover being conned to trade illegal software or media files. The measure of how much trouble you may expect will be related to the amount of negligence in providing protection to that server.

- **Exposure of Compromise of sensitive files or data**

Considering regulatory requirements, in this case HIPAA, the extent of exposure could lead to loss of reputation, loss of license, fines, penalties, and even imprisonment.

⁴² SANS Institute Steganography In the Corporate Environment Joann Kennedy April 9, 2004
URL: <http://www.giac.org/practical/GSEC/Joann_Kennedy_GSEC.pdf> P 4.

⁴³ Webopedia Definition Steganography
URL: <<http://www.webopedia.com/TERM/S/steganography.html>>

⁴⁴ Webopedia Definition Warez URL: <<http://www.webopedia.com/TERM/w/warez.html>>

- **Execution of arbitrary commands on the server**

Execution of arbitrary commands not only can expose data, but change and corrupt it as well. In the case of patient laboratory results, this is a true life and death impact.

- **Complete compromise of the server**

A full compromise and you have lost ownership of the server, the hacker now owns it. Data can be exposed and changed. This goes beyond the application as the operating system itself and other applications have now been compromised and taken control.

1.2.6 Microsoft Classifications

Microsoft Classifications of “impact of vulnerability”

- Remote Code Execution
- Information Disclosure
- Denial Of Service
- Local Elevation of Privilege
- Spoofing

Microsoft Severity Rating system⁴⁵

Rating	Definition
Critical	A vulnerability whose exploitation could allow the propagation of an Internet worm without user action.
Important	A vulnerability whose exploitation could result in compromise of the confidentiality, integrity, or availability of users data, or of the integrity or availability of processing resources.
Moderate	Exploitability is mitigated to a significant degree by factors such as default configuration, auditing, or difficulty of exploitation.
Low	A vulnerability whose exploitation is extremely difficult, or whose impact is minimal.

⁴⁵ Microsoft TechNet Website. Microsoft Security Response Center Security Bulletin Severity Rating System (Revised, November 2002). Unnumbered Table from Website
URL: <<http://www.microsoft.com/technet/security/bulletin/rating.msp>>

1.2.7 Magnitude of Impact

NIST⁴⁶ provides a magnitude of impact table defining high, medium and low, with the definition of **HIGH** as:

“Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization’s mission, reputation, or interest; or (3) **may result in human death or serious injury.**”

When we look at BloodLab’s asset definitions, and the importance of the IIS server to BloodLab’s mission, we are definitely looking at high impact issues, especially impeding reputation and human death or serious injury. Any viable threat to these assets would result in high losses.

All the major vulnerabilities can lead to a high impact incident. Estimates are needed to estimate the likelihood of an attack.

1.2.8 Risk Mitigation

Once we determine the exposures and know the risk, we now have to manage risk. Different ways to achieve this are provided by NIST⁴⁷

- **Risk Avoidance.** To avoid the risk by eliminating the risk cause and/or consequence (e.g., forgo certain functions of the system or shut down the system when risks are identified)
- **Risk Limitation.** To limit the risk by implementing controls that minimize the adverse impact of a threats exercising a vulnerability (e.g., use of supporting, preventive, detective controls)
- **Risk Planning.** To manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls
- **Research and Acknowledgment.** To lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability
- **Risk Transference.** To transfer the risk by using other options to compensate for the loss, such as purchasing insurance.

⁴⁶ United States. National Institute of Standards and Technology. NIST SP800-30 Risk Management Guide for Information Technology Systems January 2002. P. 23

⁴⁷ United States. National Institute of Standards and Technology. NIST SP800-30 Risk Management Guide for Information Technology Systems January 2002. P. 27

Once the audit is complete, and the exposures are determined, a remediation plan can be developed and presented based on the risk posture of the company being audited.

1.3 Current State of Practice

Security auditing of a system or system component is to measure compliance of that system to security policy. In simplistic term, this takes at least four tasks:

- *Define the Policy* – Define the acceptable configuration of the target through security policy, security standards, security guidelines and security standard operating procedures (SOP).
- *Apply the Policy* – Using security standard operating procedures, which may include templates, securely configure the system or system component in compliance to security policy. This process should consist of a hardening phase.
- *Audit Compliance to the Policy* – Using checklists, establishes whether a security policy criterion has been met. The challenge is that a system or system component may have been properly hardened according to the security standard operating procedures, but overall policy has not been met. This is a driver for performing stimulus/response tests where possible and not just checking a setting.
- *Adjust Risk* – This step requires mitigating risk back to the acceptable level, as determined by the organization's risk posture. Any items discovered in the audit that poses an unacceptable risk value or exposure should undergo changes that either directly removes the risk (fix the problem) or indirectly compensates by implementing some other control.

The lockdown and securing of a Microsoft Windows Server has been documented in several books on securing and hardening Windows. Some of the books already referenced in this paper are:

- Staneck, William R. Microsoft Windows 2000 and IIS 5.0 Pocket Reference. Redmond: Microsoft Press, 2001 (ISBN: 0-7356-1024-X)
- SANS Institute Windows 2000 Security Step By Step Version 1.5, July 1 2001
- Internet Security Systems. Microsoft Windows 2000 Security Technical Reference. Redmond: Microsoft Press, 2000 (ISBN: 0-7356-0858-X)

- Todd, Chad. Hack Proofing Windows 2000 Server. Rockland: Syngress, 2001, (ISBN: 1-931836-49-3)
- Philip Cox and Tom Sheldon. Windows 2000 Security Handbook. Berkeley: McGraw Hill/Osborne, 2001, (ISBN: 0-07-212433-4)
- Bragg, Roberta. Windows 2000 Security. Indianapolis: New Riders Publishing, 2001 (ISBN: 0-7357-0991-2)
- Smith, Ben and Komar, Brian. Microsoft Windows Security Resource Kit. Redmond: Microsoft Press, 2003 (ISBN: 0-7356-1868-2)
- Internet Security Systems. Microsoft Windows 2000 Security Technical Reference. Redmond: Microsoft Press, 2000 (ISBN: 0-7356-0858-X)
- Bragg, Roberta. Hardening Windows Systems. Emeryville: McGraw Hill/Osborne, 2004, (ISBN: 0-07-225354-1)

The primary reason for selection of these books was that these were already available in my personal library. I have acquired these books over the past few years as they provide guidance for the actual hardening of Windows 2000. What I have found just in this sample of titles is that although there is a common body of items that almost all the books cover, the amount of detail in each book or the approach taken by each book differs. Some books may cover or discuss an area for lockdown that the other books never even mention.

It is my personal conclusion that there is no one single source for accomplishing the hardening or the auditing. Not that this is bad, but I have not seen one “complete” and comprehensive book on IIS hardening.

The government publishes its recommendations for government systems. Although in some cases those recommendations for lockdown may be overkill for running a regular business, the configurations are realistic and reasonable and provide value.

One United States government resource is the Computer Security Resource Center (CSRC)⁴⁸ of the National Institute of Standards and Technology (NIST)⁴⁹. Some of the guides available and references in this paper are:

- Web Server SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) V5.0, NIST/Computer Security Resource Center (CSRC), Jul 26, 2004

⁴⁸ Website Homepage. URL: <<http://csrc.nist.gov>>

⁴⁹ Website Homepage. URL: <<http://www.nist.gov>>

- WEB SERVER CHECKLIST Version 4, Release 1.3 Microsoft IIS Server, NIST/Computer Security Resource Center (CSRC), May 26, 2004
- Guidelines on Securing Public Web Servers (Special Publication 800-44), NIST, September 2002

Another United States government source is The National Security Agency (NSA) provides security configuration guides at its System and Network Attack Center (SNAC)⁵⁰.

- Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0, NSA/System and Network Attack Center (SNAC), Oct 29, 2003

Then there is the vendor, in this case it is Microsoft. Microsoft publishes several books, some already mentioned above, through its publishing division (i.e. Microsoft Press). In addition to publications in that class, Microsoft also provides information, guidance, and tools through the Microsoft Website and offerings of TechNet⁵¹ and MSDN⁵². TechNet and Microsoft Developer Network (MSDN) are subscription based and provide a collection distributed periodically on CDROM, and some of the content is free and online.

The easy access point for Microsoft Security is to start at:

<http://www.microsoft.com/security>

For this paper, I have drilled down to Security Guidance Center for Developers and IT Pros⁵³. This page has links pointing to How-To articles and checklists.

- Checklist: Securing Your Web Server. Microsoft Corporation, January 2004⁵⁴.
- Securing Your Web Server. Microsoft Corporation, January 2004⁵⁵.

⁵⁰ Website Homepage. URL: <<http://www.nsa.gov/snac/>>

⁵¹ Website Homepage. URL: <<http://www.microsoft.com/technet/default.mspx>>

⁵² Website Homepage. URL: <<http://msdn.microsoft.com/>>

⁵³ Website Homepage. URL: <<http://www.microsoft.com/security/guidance/default.mspx>>

⁵⁴ Microsoft Security Website. Checklist: Securing Your Web Server. Microsoft Corporation, January 2004 URL: <<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/secmod/html/secmod104.asp>>

⁵⁵ Microsoft Security Website. Securing Your Web Server. Microsoft Corporation, January 2004 URL: <<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/secmod/html/secmod89.asp>>

Additional resources, not referenced or used in this paper are articles from the following two periodicals:

- Redmond Magazine (formerly MCP Magazine)⁵⁶
- Windows IT Pro (formerly Windows NT Magazine)⁵⁷

Both of these magazines provide online access to recent articles, and Windows IT pro has a CDROM based subscription that holds all past articles. These magazines focus on the Microsoft Windows platforms.

In order to build any foundation in information security, you need a basic set of fundamental principles to follow. Since you can't have perfect security and security has not been one size fits all, one must always make choices in security and is forced to balance "best practices" with "risk". In the Software Development Life Cycle (SDLC), NIST provides a document that I believe is a good starting point for security principles and best practices⁵⁸. Section 3.3 lists 33 principles. This combined with its predecessor document⁵⁹ at least provides a starting point to help in making judgments on which security configurations may be best.

To this point, I have discussed books and references that detail the techniques for a lockdown. Microsoft provided the IIS Lockdown Tool to help lockdown the IIS server, but it is only a starting point. To match this, Microsoft also provided The Microsoft Security Baseline Analyzer (MSBA)⁶⁰ tool to verify the actions taken during hardening.

But what is done in real life, in the job of doing an audit? To audit an entire Windows IIS server from the base OS up to the IIS server itself, there could be 1000's of tests. The only way to realistically cover all the possibilities is to use a scanning tool. Each scanning tool has its strengths, weaknesses, and value. Some of the common commercial tools that are used to do a vulnerability assessment against a device are:

- Microsoft Security Baseline Analyzer (MSBA) – Microsoft

⁵⁶ Website Homepage. URL: <<http://www.mcpmag.com>>

⁵⁷ Website Homepage. URL: <<http://www.winntmag.com>>

⁵⁸ United States. National Institute of Standards and Technology. Engineering Principles for Information Technology Security (A Baseline for Achieving Security) NIST Special Publication SP800-27 June 2001 Section 3.3

⁵⁹ United States. National Institute of Standards and Technology. Generally Accepted Principles and Practices for Securing Information Technology Systems NIST Special Publication SP800-14 September 1996

⁶⁰ Microsoft Download Site Microsoft Baseline Security Analyzer 1.2.1 August 16 2004
URL: <<http://www.microsoft.com/technet/security/tools/mbsahome.msp>>

- Retina Network Security Scanner⁶¹ – eEye
- Internet Scanner⁶² – ISS Systems
- GFI LAN Guard Network Security Scanner (N.S.S)⁶³ - GFI
- STAT Network Scanner⁶⁴ – Harris Co.

Nessus is an open source network and vulnerability scanner⁶⁵.

Some websites have downloadable free Security Tools for scanning or performing other vulnerability testing. Just to name a few:

- Security Focus - <http://www.securityfocus.com/tools/category/77>
- Foundstone - <http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/overview.htm>
- Sysinternals - <http://www.sysinternals.com/ntw2k/utilities.shtml>
- Insecure.org (Home of NMAP) - <http://www.insecure.org/>

⁶¹ Website Homepage. URL: <<http://www.eeye.com/html/products/retina/index.html>>

⁶² Website Homepage. URL: <http://www.iss.net/products_services/enterprise_protection/vulnerability_assessment/scanner_in_ternet.php>

⁶³ Website Homepage. URL: <<http://www.gfi.com/lannetscan/>>

⁶⁴ Website Homepage. URL: <http://www.stat.harris.com/solutions/vuln_assess/scanner_index.asp>

⁶⁵ Webpage Homepage. URL: <<http://www.nessus.com/>>

SECTION 2: AUDIT CHECKLIST

Format used for checklist entries

- Checklist Item Number
This will be used for cross-referencing in various parts of the paper.
- Checklist Item Title
This is a brief description of the checklist item.
- Reference
References related to the checklist item to support or validate its value and risk. These references will originate from several sources. Microsoft publications will provide vendor recommendations. Government sources and documents will detail practices used by the government. Now we are auditing a business and not the military, and the government may be applying safeguards that are overkill for a business. However, if these are in line with both the vendor and outside opinion, these recommendations just provide more evidence and support. And then there is the outside opinion – the non-vendor opinions indicating best practices for protection of the server as well as what should be checked.
- Component Tested
This may focus on IIS, the Operating system, or a specific component, but for the scope of this paper we want to specifically target IIS parameters.
- Risk
 - Vulnerabilities being tested
This describes the details of the vulnerability being tested.
 - Assets at risk
These would be the assets that can be compromised if the vulnerability is successfully exploited.
 - Likelihood of threat
This will be the probability that an exploit will be developed and assets exploited.
 - Explanation
More detail and discussion about the risk and the importance of the of the test in this checklist entry.
- Test Procedure
 - Settings

Testing the vulnerability is determined by the value of a setting or configuration.

- Inspection by hand (Stimulus/Response)
Testing the vulnerability is done via a stimulus/response test. This form of test may be done to validate the settings.

- Remediation Procedure

- Immediate
This is a procedure that can be implemented quickly. It may be a complete solution, or a temporary solution (mitigation). It provides for situations that may require a longer period of time to fix the exception.
- Long Term
This is a long term solution. In some cases immediate may fix the problem and long-term may put in controls to insure the problem does not reoccur in the future.
- Inhibitors
This lists/describes any stumbling blocks or caveats in the recommended solution. These may be things to watch out for.

- Test Nature

This may be specified as either subjective or objective.

- Evidence

This is a place in the checklist for artifacts or proof showing the results of the testing procedure. For example, screenshots of results can be stored or linked from here.

- Findings

This is where conclusions about evidence and compliance criteria can be recorded.

- Recommendations

Recommendations specifically based on the checklist item can be recorded here and then used in the overall Audit report.

IIS 2.1 Service Packs and Security Updates

Reference	<ul style="list-style-type: none"> • MSBA: 5311 (see Appendix A) • Managing Web Server Security: Applying Service Packs, Hot Fixes, and Templates⁶⁶ • Install all patches for the Operating System and IIS⁶⁷ • Keep up with the latest updates, Section 9.1 Internet Information Services 5⁶⁸ • Procedure in place to ensure that vendor security patches/updates are regularly applied⁶⁹ • Apply latest Service Packs and hotfixes available from Microsoft⁷⁰
Component Tested	IIS, Core O/S, XML, and Miscellaneous Products
Risk	<p>Vulnerabilities being tested: Server being left vulnerable because available security patches have not been applied. Check to see if server is being patched. Vulnerabilities are specific to missing security patches, so actual vulnerabilities cannot be enumerated in this checklist.</p> <p>Assets at risk: Actual assets at risk will depend on the individual vulnerabilities left on the server due to missing patches. For example, critical security patches that allow any type of code execution of attackers' choice could put all assets located on the server at risk. If an attacker can expand an attack to a network attack, then any asset reachable on the network is at risk.</p> <p>A major or complete compromise of the IIS component could lead to a major or complete compromise of the application code, or a direct compromise of the application data. In this case all assets listed in section 1.2.1 Assets at risk are controlled by a single application on this IIS web</p>

⁶⁶ Staneck, William R. Microsoft Windows 2000 and IIS 5.0 Pocket Reference. Redmond: Microsoft Press, 2001 (ISBN: 0-7356-1024-X) p. 144

⁶⁷ Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0, NSA/System and Network Attack Center (SNAC), Oct 29, 2003 p. 23

URL: <http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/os/win2k/iis_5_v1_4.pdf>

⁶⁸ SANS Institute Windows 2000 Security Step By Step Version 1.5, July 1 2001 p. 55

⁶⁹ Commonwealth Agency of the Australian Government Website and Internet System Security Checklist V1.1 Dec 2003

URL: <http://www.agimo.gov.au/data/assets/file/9043/security_checklist.pdf> Item 38

⁷⁰ Internet Security Systems. Microsoft Windows 2000 Security Technical Reference. Redmond: Microsoft Press, 2000 (ISBN: 0-7356-0858-X) p. 479

server, all which may be exposed either directly or indirectly. The potential damage of a successful compromise can be rated as high. The types of damage to the assets may be the unauthorized disclosure, modification, or destruction of protected data.

Likelihood of threat:

The likelihood of a server with missing critical security patches from being compromised is usually very high. The reason for assigning a high probability is due to automated attack tools that make delivery of exploits easy and in some severe cases – self propagating (worms).

Explanation:

No one has been able to produce error-free software code for a very large and complex system. As software ages through its lifecycle, errors (called bugs) are discovered. When encountered, errors may be ignored or reported to the software support center for that software and a fix may be issued. Many of these fixes, since they are software code, may change the characteristics of the original software, or may introduce new bugs. And then the cycle repeats over again.

Probably the most common and severe software error that relates to security is the buffer overflow. With a buffer overflow, a specially crafted software data packet can take advantage (exploit) of a software error (vulnerability) and reprogram the vulnerable program. When this can be successfully accomplished, the attacker can take over the system, or change function in the system, such as increasing the authority of the running task (escalation of privilege).

Part of security by obscurity is the period when the vulnerabilities are unknown and still remain a secret. No one can take advantage of the software bug, and in this state the software bug may not have even been discovered yet. At this point there would be no exploit developed because the vulnerability is not known. There is no risk at this point, as there is no threat.

Now someone discovers a vulnerability that could lead to a security compromise. Now a threat may develop, and that

⁷¹ Symantec Internet Security Threat Report, Volume IV. September 2004.
URL: <<http://enterprisesecurity.symantec.com/content.cfm?articleid=1539>>

	<p>risk will be partly based on how easy an exploit can be developed and the impact of that exploit. If the vulnerability is easy to take advantage of, exploit writers may develop an exploit and distribute it. In many cases the first distribution is proof of concept code which may only crash the application, then followed by a full fledged exploit that has stable functionality.</p> <p>In the Symantec Internet Security Report⁷¹ it is reported that the lead-time from vulnerability announcement or discovery to development and release of an exploit is averaging to less than 6 days. From this you can derive that when Microsoft announces a security flaw you have less than a week to put the patch on – if you want to be patched before you would most likely be attacked.</p> <p>When you look at the risk factors, the threat becomes real when the exploit is released and in the wild. Another component of risk factors is the probability of the threat. With automated tools, including worms to automate the delivery of payloads, the probability of an attack becomes large not only because of ease of delivery but also due to the indiscriminate nature of the propagation mechanisms. A company may be in denial stating that no one would be interested in launching an attack against them, but automated tools, such as a worm delivery, will attack what it can find.</p> <p>So the bottom line is that systems must be patched for security vulnerabilities. And they must be patched within a reasonable timeframe or they may be exposed to an attack. Once a vendor, such as Microsoft, announces a security flaw, it is a race against the clock to see if you can get the patch on before the attack.</p> <p>The level of risk will vary based on the risk of individual unapplied security patches. This requires risk analysis on each bulletin released.</p>
Test Procedure	<p>Settings:</p> <p>For this checklist item, what will be tested is whether the security fixes are actually installed. What will NOT be tested, i.e. out of scope for this checklist item, is whether the vulnerability targeted by the security patch was actually fixed. In order to assess whether a particular security patch actually fixed a problem, a separate stimulus/response test would be required to be developed and executed. So to say</p>

it again, there are two possible tests, 1) The patch is applied and 2) the patch fixes the problem. This checklist does not do option 2.

In the case of IIS and Microsoft products, the application of a security or otherwise critical patch is associated by a XML database called mssecure. This file is produced by Microsoft and used by The Microsoft Security Baseline Analyzer (MSBA)⁷². Vendors of vulnerability scanners are also using this database file in their scanners. GFI Network Scanner⁷³ will perform patch checking in their Languard Network Security Scanner, version 5 and above. eEYE digital security⁷⁴ will use the database in its version 5 and above Retina scanner software.

Verification of patch compliance is based on several checks. When a program is compiled, it may have a build number and used as a version number can be used to determine the level of the module. The mssecure.xml file also contains checksums which can be used to verify the version of the module. Another test is checking the registry for keys that are added as part of the update process.

To test if the system is patched The Microsoft Security Baseline Analyzer (MSBA)⁷⁵ tool will indicate which patches are installed, missing, or in a state that cannot be determined.

Another test that can be performed is to run Windows Update on the target server. This scan will indicate missing service packs and patches, and provide an opportunity to actually install the missing updates.

Inspection by hand (Stimulus/Response):

This checklist item is an inventory of security patch installation, and measures compliance in keeping a system patched. It does not check for a specific vulnerability that can be tested.

⁷² Microsoft Download Site Microsoft Baseline Security Analyzer 1.2.1 August 16 2004

URL: <<http://www.microsoft.com/technet/security/tools/mbsahome.msp>>

⁷³ Website Homepage. GFI Languard Network Security Scanner.

URL: <<http://www.gfi.com/languard/>>

⁷⁴ Website Homepage. eEye Digital Security. Retina Network Security Scanner.

URL: <<http://www.eeye.com/html/products/retina/index.html>>

⁷⁵ Microsoft Download Site Microsoft Baseline Security Analyzer 1.2.1 August 16 2004

URL: <<http://www.microsoft.com/technet/security/tools/mbsahome.msp>>

Remediation Procedure	<p>Immediate: The system will need to be patched. Windows update⁷⁶, System Management Server (SMS)⁷⁷, Software Update Services (SUS)[to be replaced by Windows Update Services (WUS)]⁷⁸, vendor patch management tools, or some repository should be used to apply the patches.</p> <p>Long term: Once the system is brought to compliance, some form of schedule, which may include automation, should be implemented.</p> <p>Inhibitors: Patching sometimes breaks applications, therefore adequate testing is required, otherwise the risk of disabling the application leading to loss of service. Windows update requires access to the Internet, which may be restricted. Other tools, depending on where they execute, may require opening ports and protocols on firewalls (when the server is located in a DMZ), increasing the risks to applications in the DMZ as well as where the tools are running.</p>
Test Nature	Subjective. Determination of whether a security patch has been applied is not always detectable. The tool will error on the conservative side flagging certain security patches in a manner that requires further examination by hand.
Evidence	Placeholder for artifacts, such as screenshots, logs, etc
Findings	Placeholder
Recommendation	Placeholder

⁷⁶ Windows Update may be invoked by using URL: <<http://windowsupdate.microsoft.com>>

⁷⁷ Microsoft Website. System Management Server (SMS).

URL: <http://www.microsoft.com/smsserver/default.asp>

⁷⁸ Microsoft Website. Windows Update Services (SUS).

URL: <<http://www.microsoft.com/windowsserversystem/sus/default.msp>>

IIS 2.2 File System Should be NTFS

Reference	<ul style="list-style-type: none"> • MSBA: 5313 (see Appendix A) • Securing Internet Information Services 5.0⁷⁹ • Securing the Microsoft Internet Information Server Chapter 19⁸⁰. • Securing the Web Site – Web Site Security⁸¹ Best Practices. • All volumes that host Web content should be formatted by using the NTFS file system⁸² • Use NTFS⁸³
Component Tested	IIS, Core O/S
Risk	<p>Vulnerabilities being tested: Use of file systems that cannot be secured or protected. Without the ability to set permissions, i.e. set access control lists (ACL), files and folders cannot be individually protected from accidental or intentional damage or misuse.</p> <p>Assets at risk: All assets located on file systems that do not support permissions. A breach of those assets could cascade to additional breach of assets on other protected and non-protected disks, e.g. obtaining valid credentials from a file system where the credentials were stored but could not be protected.</p> <p>A major or complete compromise of the IIS component could lead to a major or complete compromise of the application code, or a direct compromise of the application data. In this case all assets listed in section 1.2.1 Assets at risk are controlled by a single application on this IIS web server, all which may be exposed either directly or indirectly. The potential damage of a successful compromise can be rated as high. The types of damage to</p>

⁷⁹ Todd, Chad. Hack Proofing Windows 2000 Server. Rockland: Syngress, 2001, (ISBN: 1-931836-49-3) Chapter 11

⁸⁰ Philip Cox and Tom Sheldon. Windows 2000 Security Handbook. Berkeley: McGraw Hill/Osborne, 2001, (ISBN: 0-07-212433-4) p. 577

⁸¹ Bragg, Roberta. Windows 2000 Security. Indianapolis: New Riders Publishing, 2001 (ISBN: 0-7357-0991-2) p. 511

⁸² Smith, Ben, and Komar, Brian. Microsoft Windows Security Resource Kit. Redmond: Microsoft Press, 2003 (ISBN: 0-7356-1868-2) p. 444

⁸³ Internet Security Systems. Microsoft Windows 2000 Security Technical Reference. Redmond: Microsoft Press, 2000 (ISBN: 0-7356-0858-X) p. 478

	<p>the assets may be the unauthorized disclosure, modification, or destruction of protected data.</p> <p>Likelihood of threat: If file systems that do not support permissions is used, then the likelihood of compromise is high. This threat also includes accidental damage and corruption of files on those file systems.</p> <p>Explanation: The base operating system supports several different file systems. The native file systems are FAT, FAT32 and NTFS. There are also other file systems in use, such as Common Internet File System (CIFS) that is remote file sharing and CD-ROM File Sharing (CDFS).</p> <p>FAT and FAT32 do not provide any form of local permissions. Without the capability to specify and enforce permissions on the file system level, data and programs can be modified, deleted, or otherwise corrupted. This could occur either intentionally or accidentally. Without permissions, there is an inability to implement authorization into the file system. The only available option that will provide this facility is NTFS.</p> <p>The risk in question is the risk of not implementing and enforcing file and folder permissions. Failure to correctly use permissions may cause:</p> <ul style="list-style-type: none"> • Damage of the executable code (loss of code integrity, exposure to viruses) • Damage of the data (loss of data integrity) • Disclosure of executable code (piracy) • Disclosure of data (loss of confidentiality) <p>A separate checklist item should be developed to actually check the access control lists (ACL). However, NTFS is the only Windows file system that will support ACL.</p>
Test Procedure	<p>Settings: The tool Microsoft Security Baseline Analyzer (MSBA) will indicate if NTFS is in use.</p> <p>There are different manual procedures. In one procedure, open MY Computer, and select the Details view. The file system should be displayed. On some systems, you need to enable the "File System" column. This works for Windows XP and Server 2003. Another method is to open</p>

	<p>each drive and view the properties of the drive. See figure B1 for a screenshot of the drive properties.</p> <p>The following drives should be NTFS:</p> <ul style="list-style-type: none"> • The Windows 2000 Boot Drive • The drive with the inetpub folder • All drives holding directories used by the IIS server <p>If NTFS is not reported as the file system in use, this will be a finding.</p> <p>Inspection by hand (Stimulus/Response): N/A</p>
Remediation Procedure	<p>Immediate: The drives in question may be converted. The following command line may be used:</p> <p style="text-align: center;">Convert x: /fs:ntfs</p> <p>Where x: is the FAT/FAT32 drive to be converted to NTFS</p> <p>Long term: Use NTFS for all file system specifications.</p> <p>Inhibitors: Conversion does not retrofit any permission, especially at the operating system level. NTFS is not supported by all Operating Systems, and may cause issues when a dual boot system is used.</p>
Test Nature	Objective
Evidence	Placeholder for artifacts, such as screenshots, logs, etc
Findings	Placeholder
Recommendation	Placeholder

IIS 2.3 IIS Should Not be Installed on Domain Controller

Reference	<ul style="list-style-type: none"> • MSBA: 5321 (see Appendix A) • Install IIS on a standalone server when possible⁸⁴ • A web server will not be installed on the same computer as a Microsoft Domain Controller⁸⁵ • When the IUSR account is installed on a domain controller, it is assigned excess privileges because the account is added to the domain users global group⁸⁶ • Use isolated domain controllers if you need to run IIS on a domain controller⁸⁷
Component Tested	IIS
Risk	<p>Vulnerabilities being tested: The installation of IIS on a Domain Controller. If the IIS component is compromised, then the Domain Controller can be seized as part of the same attack.</p> <p>Assets at risk: The Domain Partition, the LDAP directory, user credentials and passwords. Domain controllers contain sensitive information that may be exposed if the IIS component is compromised.</p> <p>A major or complete compromise of the IIS component could lead to a major or complete compromise of the application code, or a direct compromise of the application data. In this case all assets listed in section 1.2.1 Assets at risk are controlled by a single application on this IIS web server, all which may be exposed either directly or indirectly. The potential damage of a successful compromise can be rated as high. The types of damage to the assets may be the unauthorized disclosure, modification, or destruction of protected data.</p>

⁸⁴ Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0, NSA/System and Network Attack Center (SNAC), Oct 29, 2003 p. 19
URL: <http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/os/win2k/iis_5_v1_4.pdf>

⁸⁵ WEB SERVER CHECKLIST Version 4, Release 1.3 Microsoft IIS Server,

NIST/ Computer Security Resource Center (CSRC), May 26, 2004
URL <http://csrc.nist.gov/pcig/CHECKLISTS/web_checklist_052604.zip> Item: WG090

⁸⁶ Smith, Ben, and Komar, Brian. Microsoft Windows Security Resource Kit. Redmond: Microsoft Press, 2003 (ISBN: 0-7356-1868-2) p. 443

⁸⁷ Internet Security Systems. Microsoft Windows 2000 Security Technical Reference. Redmond: Microsoft Press, 2000 (ISBN: 0-7356-0858-X) p.478

	<p>Likelihood of threat: Either from an IIS compromise or IIS bad configuration, this could be a high risk.</p> <p>Explanation: If IIS is installed on a Domain Controller, and IIS is compromised, then the databases on the domain controller may also be compromised, exposing the entire user base recorded in the domain. For an internal corporate IIS server on the Intranet, this could be less risk. However, install an IIS/DC configuration in a DMZ, then this is high risk and more dangerous. It will depend on the contents of the domain partition. This will require a case by case examination, but finding IIS on a domain controller should raise a lot of questions. It is not a recommended configuration due to the security exposure and risk that IIS will impose on the domain controller.</p>
Test Procedure	<p>Settings: Microsoft Security Baseline Analyzer (MSBA) will flag this situation.</p> <p>Another way to determine without using MSBA:</p> <p>To inspect a machine, enter in a command window:</p> <p style="text-align: center;"><i>Net accounts</i></p> <p>This command will return the server role. If the role is <i>primary</i> or <i>backup</i>, it is a domain controller. If the role is <i>server</i>, then this is a member server.</p> <p>Inspection by hand (Stimulus/Response): N/A</p>
Remediation Procedure	<p>Immediate: The only quick action to be taken is to limit the impact that the IIS server can impose onto the Domain Controller. Separation of disks and tightening of ACL permissions are some actions that can be taken to reduce the risk.</p> <p>Long term: Migrate the IIS server to a different server that does not also function as a Domain Controller. If there are sufficient Domain Controllers in the organization, removal of the Domain Controller function (run dcpromo) may be sufficient action.</p>

	Inhibitors: The application may depend on sharing IIS with the Domain Controller, or costs for a separate Domain Controller may be prohibitive.
Test Nature	Objective
Evidence	Placeholder for artifacts, such as screenshots, logs, etc
Findings	Placeholder
Recommendation	Placeholder

© SANS Institute 2005, Author retains full rights.

IIS 2.4 IIS Lockdown Tool

Reference	<ul style="list-style-type: none">• MSBA: 5323 (see Appendix A)• Securing the Web Site – Web Site Security⁸⁸• Two tools are available to secure an IIS server, IIS Lockdown and URLSCAN⁸⁹
Component Tested	IIS
Risk	<p>Vulnerabilities being tested: Checking to see if the Microsoft IIS Lockdown hardening tool was ever used. If the tool was never used, it is possible that hardening of the IIS component was never performed. This setting could be inconclusive, since adequate and proper hardening can be accomplished without the tool.</p> <p>Assets at risk: A major or complete compromise of the IIS component could lead to a major or complete compromise of the application code, or a direct compromise of the application data. In this case all assets listed in section 1.2.1 Assets at risk are controlled by a single application on this IIS web server, all which may be exposed either directly or indirectly. The potential damage of a successful compromise can be rated as high. The types of damage to the assets may be the unauthorized disclosure, modification, or destruction of protected data.</p> <p>Likelihood of threat: High if no hardening was ever performed, low if hardening was performed.</p> <p>Explanation: Many of the settings that can make the IIS server vulnerable can be securely set as part of the IIS lockdown wizard. Many of these settings can be done by hand, so use of the lockdown tool – or lack of it – does not indicate how secure the IIS server may be. Each individual setting should be examined and validated. However, knowing that the tool was run provides some hardening information which can be examined from the log files.</p>

⁸⁸ Bragg, Roberta. Windows 2000 Security. Indianapolis: New Riders Publishing, 2001 (ISBN: 0-7357-0991-2) p. 502

⁸⁹ Smith, Ben, and Komar, Brian. Microsoft Windows Security Resource Kit. Redmond: Microsoft Press, 2003 (ISBN: 0-7356-1868-2) p. 456

Test Procedure	<p>Settings: Microsoft Baseline Security Analyzer (MSBA) will report if the tool was run.</p> <p>Inspection by hand (Stimulus/Response): N/A</p>
Remediation Procedure	<p>Immediate: If the tool was not used, make sure that appropriate hardening was done by other means.</p> <p>Long term: Develop a procedure for hardening new IIS servers as part of the server build process. Development and application of standard templates to assign general security settings will provide a uniform and consistent security profile.</p> <p>Inhibitors: IIS Lockdown, as well as any hardening attempts, can disable IIS and break applications. Must be used with care and sufficient testing of applications.</p>
Test Nature	Objective
Evidence	Placeholder for artifacts, such as screenshots, logs, etc
Findings	Placeholder
Recommendation	Placeholder

© SANS Institute 2005

IIS 2.5 IIS Sample Applications Should be Removed

Reference	<ul style="list-style-type: none"> • MSBA: 5324 (see Appendix A) • Securing the Web Site – Web Site Security⁹⁰ • Managing Web Server Security: Disabling Remote Administration from the Web⁹¹ • Delete or move all directories that contain “samples” and scripts used to execute the “samples”.⁹² • Never install IIS Samples folders on machines connected to the Internet, Section 9.1 Internet Information Services 5⁹³ • These files should be removed, Appendix D p.85⁹⁴ • Vulnerable programs have not been removed from the web server⁹⁵ • Procedure in place to ensure that vendor security patches/updates are regularly applied⁹⁶
Component Tested	IIS
Risk	<p>Vulnerabilities being tested:</p> <p>Sample applications may provide capabilities that are useful during testing and debugging but were not intended for production use. Sample applications could be misused to gain access and control of the IIS server. Folders holding sample code and scripts may have execution permissions and write permissions. This would allow attackers to place their own code into these directories that provide execution ability.</p>

⁹⁰ Bragg, Roberta. Windows 2000 Security. Indianapolis: New Riders Publishing, 2001 (ISBN: 0-7357-0991-2) p. 494

⁹¹ Staneck, William R. Microsoft Windows 2000 and IIS 5.0 Pocket Reference. Redmond: Microsoft Press, 2001 (ISBN: 0-7356-1024-X)

⁹² Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0, NSA/System and Network Attack Center (SNAC), Oct 29, 2003

URL: <http://www.nsa.gov/notices/notice00004.cfm?Address=/snac/os/win2k/iis_5_v1_4.pdf> p. 25

⁹³ SANS Institute Windows 2000 Security Step By Step Version 1.5, July 1 2001 p. 55

⁹⁴ Web Server SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) V5.0, NIST/Computer Security Resource Center (CSRC), Jul 26, 2004

URL: <<http://csrc.nist.gov/pcig/STIGs/WebV5R0.zip>> p. 85

⁹⁵ WEB SERVER CHECKLIST Version 4, Release 1.3 Microsoft IIS Server, NIST/ Computer Security Resource Center (CSRC), May 26, 2004

URL: <http://csrc.nist.gov/pcig/CHECKLISTS/web_checklist_052604.zip> Item: WG380

⁹⁶ Commonwealth Agency of the Australian Government Website and Internet System Security Checklist V1.1 Dec 2003

URL: <http://www.agimo.gov.au/_data/assets/file/9043/security_checklist.pdf> Item 35.

	<p>Assets at risk: All assets located on the IIS server. If network access can be achieved, then all assets reachable from the IIS server may also be at risk.</p> <p>A major or complete compromise of the IIS component could lead to a major or complete compromise of the application code, or a direct compromise of the application data. In this case all assets listed in section 1.2.1 Assets at risk are controlled by a single application on this IIS web server, all which may be exposed either directly or indirectly. The potential damage of a successful compromise can be rated as high. The types of damage to the assets may be the unauthorized disclosure, modification, or destruction of protected data.</p> <p>Likelihood of threat: High since this is well known code and code install paths.</p> <p>Explanation: Sample applications may not be well written and could contain code that has errors in it. Depending on the state of the program, exploiting the program could compromise the system. Sample scripts and programs may provide functions that may be used to run code that is the choice of the user. Even good well-behaved code presents a problem. Microsoft has provided these tools that are installed, by default, on all IIS servers. Attackers know the code, what the code does, and where the code resides, and with that information can use the sample library against you.</p>
Test Procedure	<p>Settings: The Microsoft Security Baseline Analyzer (MSBA)⁹⁷ will report this. It may not be obvious whether the sample library folder was removed, since the lockdown tool does not actually delete the folder and its contents, only the Virtual Directory is deleted.</p> <p>An additional inspection should be done to see if the folder was removed, just in case different path navigation provides access to the code. The folder in question will be located at:</p> <p style="text-align: center;">x:\inetpub\issamples</p> <p>Where x: is the drive containing the IIS root directories.</p>

⁹⁷ Microsoft Website. Microsoft Security Baseline Analyzer (MSBA).
URL: <<http://www.microsoft.com/technet/security/tools/mbsahome.mspx>>

	<p>Inspection by hand (Stimulus/Response):</p> <p>You can type in the following URL:</p> <p>http://targetip/iisamples</p> <p>By default, the directory browsing is enabled and you should get a directory listing if the IIS samples are still installed.</p> <p>If you don't get a response, IIS Samples may still be active but with browsing turned off. The following URL will attempt to access and display a gif file from the samples:</p> <p>http://targetip/iisamples/sdk/asp/components/ie.gif</p> <p>If this works, you will get a box image that says Microsoft Internet Explorer with a rotating world icon.</p> <p>If you still get no response, then to be absolutely sure, go to the property sheet of the web site and view the defined virtual directories. Make sure IISSAMPLES is not a defined virtual directory.</p> <ul style="list-style-type: none"> • From Administrator Tools • Select Internet Services Manager • Click on each web site, including the Default Web Site • In the tree for the web site, the virtual directories will be listed • Make sure IISSAMPLES is not in the list
Remediation Procedure	<p>Immediate: Remove IISSAMPLES Virtual Directory Definition</p> <p>Long term: Remove IISSAMPLES folder</p> <p>Inhibitors: This should not be an issue unless the IISSAMPLES directory was used for real production code. In that case, the code will need to be migrated to a proper directory.</p>
Test Nature	Objective
Evidence	Placeholder for artifacts, such as screenshots, logs, etc
Findings	Placeholder
Recommendation	Placeholder

IIS 2.6 IISADMPWD Virtual Directory

Reference	<ul style="list-style-type: none"> • MSBA: 5325 (see Appendix A) • Managing Web Server Security: Removing the IISADMPWD Virtual Directory⁹⁸ • If not using functionality, directory needs to be removed, Appendix D⁹⁹ • Changing the password over the Internet is a security risk, Q184619¹⁰⁰
Component Tested	IIS
Risk	<p>Vulnerabilities being tested:</p> <p>The changing of passwords using this feature could expose userid/password credentials. This can be accomplished by capturing traffic between the user making the change and the web server, in most cases using a network packet-capturing device, such as a sniffer.</p> <p>IISADMPWD may also be classified as an unnecessary service. It has been compromised where an attack can cause a denial of service¹⁰¹. Removal of the function will help avert any future attacks or compromise of the feature.</p> <p>IISADMPWD may also be used in a brute force attack to guess credentials to gain server access.</p> <p>Assets at risk:</p> <p>A major or complete compromise of the IIS component could lead to a major or complete compromise of the application code, or a direct compromise of the application data. In this case all assets listed in section 1.2.1 Assets at risk are controlled by a single application on this IIS web server, all which may be exposed either directly or indirectly. The potential damage of a successful compromise can be rated as high. The types of damage to</p>

⁹⁸ Staneck, William R. Microsoft Windows 2000 and IIS 5.0 Pocket Reference. Redmond: Microsoft Press, 2001 (ISBN: 0-7356-1024-X) p. 146

⁹⁹ Web Server SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) V5.0, NIST/Computer Security Resource Center (CSRC), Jul 26, 2004
URL: <<http://csrc.nist.gov/pcig/STIGs/WebV5R0.zip>> p. 85

¹⁰⁰ Microsoft Support Website. How to Change Windows NT Account Passwords Using Internet Information Server (IIS) 4.0 URL: <<http://support.microsoft.com/default.aspx?scid=kb;en-us;184619>>

¹⁰¹ Microsoft IIS Remote Denial of Service Attack
URL: <<http://www.securiteam.com/windowsntfocus/5BP0C151FU.html>>

	<p>the assets may be the unauthorized disclosure, modification, or destruction of protected data.</p> <p>Likelihood of threat: Low. Getting a vantage point on the Internet to do the sniffing may be difficult. It is not impossible when using Cable Modems or DSL where common hubs and switches may be used for network segments. This feature is not available for IIS 5.0 or above unless it was previously installed from an IIS 4.0 system, so its existence on an IIS 5.0 system should be extremely rare.</p> <p>Explanation: The IISADMPWD is the IIS Administer Password function and allows passwords to be changed. It was intended for Intranet (internal) and not Internet (external) scenarios. It is a feature of IIS 4.0 and not installed by IIS 5.0, however if an upgrade from IIS 4.0 to IIS 5.0 is performed, the functionality remains.</p>
Test Procedure	<p>Settings: The Microsoft Security Baseline Analyzer (MSBA)¹⁰² will report detection or non-detection of the IISADMPWD directory.</p> <p>Inspection by hand (Stimulus/Response): IISADMPWD is a virtual directory, and each web site should be checked using Internet Services Manager to see if the virtual directory is defined. If detected, both the virtual directory and the folder should be removed.</p> <p>The script is in the form of aexp*.httr. (e.g. aexp2b, aexp3b). Look for these files in the IISADMPWD folder, but make sure that they also do not exist in any other accessible virtual directory or path.</p>
Remediation Procedure	<p>Immediate: Remove the virtual directory. Remove mappings to the htr extension.</p> <p>Long term: Remove the folder.</p> <p>Inhibitors: If this function is in use, then alternate arrangements must be made. At a minimum, if this function is absolutely</p>

¹⁰² Microsoft Download Site [Microsoft Baseline Security Analyzer 1.2.1](http://www.microsoft.com/technet/security/tools/mbsahome.mspx) August 16 2004
URL: <<http://www.microsoft.com/technet/security/tools/mbsahome.mspx>>

	<p>required, then the channel should be encrypted (i.e. use SSL) to prevent eavesdropping.</p> <p>In the case of a brute force attack, some form of host based Intrusion Detection System (HIDS) is required to look for an attack signature of excessive logon attempts and failures.</p>
Test Nature	Objective
Evidence	Placeholder for artifacts, such as screenshots, logs, etc
Findings	Placeholder
Recommendation	Placeholder

© SANS Institute 2005, Author retains full rights.

IIS 2.7 IIS Parent Paths

Reference	<ul style="list-style-type: none"> • MSBA: 5326 (see Appendix A) • Disable “Parent Paths” in scripts, Section 9.1 Internet Information Services 5¹⁰³ • CGI scripts do not have proper access controls¹⁰⁴
Component Tested	IIS
Risk	<p>Vulnerabilities being tested: When parent paths are enabled, folders not intended for access could be accessed by accident or maliciously. If the accessed folder has the proper permissions, programs and scripts in that folder can be executed. This could produce results that allow compromise of the server.</p> <p>Assets at risk: A major or complete compromise of the IIS component could lead to a major or complete compromise of the application code, or a direct compromise of the application data. In this case all assets listed in section 1.2.1 Assets at risk are controlled by a single application on this IIS web server, all which may be exposed either directly or indirectly. The potential damage of a successful compromise can be rated as high. The types of damage to the assets may be the unauthorized disclosure, modification, or destruction of protected data.</p> <p>Likelihood of threat: High. Parent paths are the default in IIS 5.0, so they are set by default.</p> <p>Explanation: If dangerous executable code is within the parent path, then we may have vulnerability. Directory traversal was used by the Nimda¹⁰⁵ worm that navigated to the cmd.exe program and executed Windows commands. In Nimda the vulnerability that was exploited was a “web server folder</p>

¹⁰³ SANS Institute Windows 2000 Security Step By Step Version 1.5, July 1 2001 p. 55

¹⁰⁴ WEB SERVER CHECKLIST Version 4, Release 1.3 Microsoft IIS Server, NIST/ Computer Security Resource Center (CSRC), May 26, 2004

URL: <http://csrc.nist.gov/pcig/CHECKLISTS/web_checklist_052604.zip> Item: WG410

¹⁰⁵ CERT/CC Website. CERT[®] Advisory CA-2001-26 Nimda Worm. Revised September 2001.

URL: <<http://www.cert.org/advisories/CA-2001-26.html>>

¹⁰⁶ CERT/CC Website. CERT[®] Advisory CA-2001-12 Superfluous Decoding Vulnerability in IIS. May 15, 2001. URL: <<http://www.cert.org/advisories/CA-2001-12.html>>

	traversal” ¹⁰⁶ vulnerability, but the concept of navigating outside the scope of the application folder tree and executing code from a different folder tree on the web server is similar to the manipulation of folder paths that can be caused when using parent paths.
Test Procedure	<p>Settings: The Microsoft Security Baseline Analyzer (MSBA)¹⁰⁷ will report if any website has this option activated.</p> <p>Inspection by hand (Stimulus/Response): The parent paths option is activated by website. The individual settings for each website would have to be inspected. Figure B8 shows the application configuration page of a website. This option should control the AspEnableParentPaths setting used by asp.</p>
Remediation Procedure	<p>Immediate: Go to each website application configuration property sheet and uncheck the “Enable parent paths” box.</p> <p>Long term: Search the parent path and remove any harmful script or program in the path. Remove any script and executable permission from the website property pages where the folder does not require such privileges. Isolate each website to its own drive letter to isolate each website from each other. Do not install the website folder root on the same drive as the operating system so that the operating system does not fall within the parent path.</p> <p>Inhibitors: Easier said than done. Applications may heavily depend on the use of parent paths to a point that the application may require a complete rewrite and redesign. Even Microsoft applications will break, such as Application Center 2000¹⁰⁸, Project Central and Project Server 2003.</p>
Test Nature	Objective
Evidence	Placeholder for artifacts, such as screenshots, logs, etc
Findings	Placeholder
Recommendation	Placeholder

¹⁰⁷ Microsoft Download Site Microsoft Baseline Security Analyzer 1.2.1 August 16 2004

URL: <<http://www.microsoft.com/technet/security/tools/mbsahome.msp>>

¹⁰⁸ Microsoft Support Site. Disabling Parent Paths Breaks User Interface.

URL: <<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q288309>>

IIS 2.8 MSADC and Scripts Virtual Directories on IIS

Reference	<ul style="list-style-type: none">• MSBA: 5327 (see Appendix A)
Component Tested	IIS
Risk	<p>Vulnerabilities being tested: Sample scripts and programs distributed with IIS may provide an attack surface since these are common libraries and their contents are well known. Certain abuse scenarios may lead to server compromise.</p> <p>Assets at risk: A major or complete compromise of the IIS component could lead to a major or complete compromise of the application code, or a direct compromise of the application data. In this case all assets listed in section 1.2.1 Assets at risk are controlled by a single application on this IIS web server, all which may be exposed either directly or indirectly. The potential damage of a successful compromise can be rated as high. The types of damage to the assets may be the unauthorized disclosure, modification, or destruction of protected data.</p> <p>Likelihood of threat: High. Sample code is well known and accessible to anyone.</p> <p>Explanation: MSADC and Scripts are actual virtual directory names. MSADC is usually found in the Program Files directory and may actually be on the root drive with the Windows boot directory (%windir%, usually c:\winnt or c:\windows). Scripts can be found in the web site root folder, which is usually in the inetpub tree – unless otherwise overridden. Access to these directories may give access to dangerous scripts and programs in these directories. They may also provide anchor points when using parent paths to gain access to other logical drives in the disk system.</p>
Test Procedure	<p>Settings: The Microsoft Security Baseline Analyzer (MSBA)¹⁰⁹ will flag if these virtual directories are found.</p> <p>Inspection by hand (Stimulus/Response):</p>

¹⁰⁹ Microsoft Download Site [Microsoft Baseline Security Analyzer 1.2.1](http://www.microsoft.com/technet/security/tools/mbsahome.mspx) August 16 2004
URL: <<http://www.microsoft.com/technet/security/tools/mbsahome.mspx>>

	To detect these virtual directories, check each web site using Internet Services Manager. As an example, look at figure 21. Both the Scripts and MSADC virtual directories are listed.
Remediation Procedure	<p>Immediate: Remove Virtual Directories.</p> <p>Long term: Remove or relocate Scripts folder.</p> <p>Inhibitors: Not that easy. Some applications may require these directories, and may need to be redesigned. Some Microsoft applications (Project Central, Project Server) are dependent on the MSADC, and will create one during install if one does not already exist. It may be possible to just remove the Scripts directory and leave the MSADC. If either directory must remain, the contents should be evaluated and unneeded dangerous scripts and programs removed. Permissions on these folders should be made as tight as possible.</p>
Test Nature	Objective
Evidence	Placeholder for artifacts, such as screenshots, logs, etc
Findings	Placeholder
Recommendation	Placeholder

IIS 2.9 IIS Logging Should be Enabled

Reference	<ul style="list-style-type: none"> • MSBA: 5328 (see Appendix A) • Securing the Microsoft Internet Information Server Chapter 19¹¹⁰ • Securing the Web Site – Web Site Security¹¹¹ • Web server logs are not maintained¹¹²
Component Tested	IIS
Risk	<p>Vulnerabilities being tested: Lack of an auditing control. Without logging, there is no recording mechanism in place to record site activity. Whatever is occurring on the server, including attacks, you are running blind and have no way of knowing what is occurring. An attack can take down the entire site, i.e. Denial of Service (DoS), or unauthorized modification or misuse of data. Without a record – you can't identify the attacker and you lack non-repudiation evidence.</p> <p>Assets at risk: The IIS sites and data in those sites. Any data accessible by the application code running on the website, including the code itself can be disclosed, or modified without detection. Any of the IIS sites could be taken down and disabled by an attack without detection.</p> <p>A major or complete compromise of the IIS component could lead to a major or complete compromise of the application code, or a direct compromise of the application data. In this case all assets listed in section 1.2.1 Assets at risk are controlled by a single application on this IIS web server, all which may be exposed either directly or indirectly. The potential damage of a successful compromise can be rated as high. The types of damage to the assets may be the unauthorized disclosure, modification, or destruction of protected data.</p> <p>Likelihood of threat:</p>

¹¹⁰ Philip Cox and Tom Sheldon. Windows 2000 Security Handbook. Berkeley: McGraw Hill/Osborne, 2001, (ISBN: 0-07-212433-4) p. 580

¹¹¹ Bragg, Roberta. Windows 2000 Security. Indianapolis: New Riders Publishing, 2001 (ISBN: 0-7357-0991-2) p. 493

¹¹² WEB SERVER CHECKLIST Version 4, Release 1.3 Microsoft IIS Server, NIST/ Computer Security Resource Center (CSRC), May 26, 2004
URL: <http://csrc.nist.gov/pcig/CHECKLISTS/web_checklist_052604.zip> Item: WG240

	<p>If there are no other monitors in place, there is a medium to high probability that attacks against the IIS sites will not be detected. The use of automated and self-propagating attacks (e.g. worms) may attack the server, and without logging may go unnoticed. If alternate monitoring is in place, such as a network Intrusion detection system (NIDS), the likelihood may drop down to low because other detection controls will be in place.</p> <p>Explanation: The use of logging coupled with proactive monitoring can be an effective detective control that can be used to detect misuse and attacks. With the growth of regulatory compliance and privacy laws, detailed logging of transactions is becoming more critical. If the logs are accumulated, but not checked periodically, they still have value in conducting forensics to backtrack and determine what happened. In this mode, the damage has been done and it is probably too late as the assets may have already been compromised.</p> <p>Another triad in security is AAA, Authentication, Authorization, and Accounting. This concept is widespread in the Cisco community for its security implementation. The 3rd A – Accounting, is where log files come to play.</p>
Test Procedure	<p>Settings: The settings for the log appear on the property pages. In Figure B2, we observe the web page properties, Figure B12 the FTP site properties, Figure B17 the NNTP and Figure B18 for SMTP site properties. In each of these properties pages, there is a check box to enable logging, a pull down window to select the active log file format, and a properties button to provide information as to where the log file should be stored, the naming format, and in some cases the fields to be recorded into the log. A sample of the property page can be found in Figure B19. The default location for the log files are in the folder:</p> <p style="text-align: center;">%windir%\system32\logfiles</p> <p>Figure B20 shows the folder on a sample system, and there are two log file folders, one for the default FTP site and the other for the default web site. The actual log files are txt files stored in the appropriate folder.</p> <p>When checking settings, both the enable logging box and the log visits box need to be checked to approach the</p>

	<p>maximum level of logging.</p> <p>Inspection by hand (Stimulus/Response): The settings may indicate logging, but logging might not actually be active and working. A physical inspection of the log files is required. The following procedure will work when logging is to folders. There is a logging option to log to SQL databases. Inspection of the log data from a SQL database is more advanced and not covered in this scenario.</p> <p>First, the folder holding the log file for the site being tested should be located.</p> <ul style="list-style-type: none"> • Using Administrator Tools open the internet Services Manager • Right click on the web site to be tested, select properties • Go to the general tab • Next to the active log format, click the properties button • You will now have a page similar to Figure B19 • Below the Log File Directory is the Log File name • These two tell you where the log files are stored and the naming convention of the file name <p>Next find the latest file and examine its contents</p> <ul style="list-style-type: none"> • Look for the file with the most current modify name/date • One way to do this is navigate with windows explorer • Use the view pull down window • Select sort by modified date • Use notepad to open the log file <p>Now, create data for the log file</p> <ul style="list-style-type: none"> • If SMTP, you can generate a sample e-mail. • If FTP, try to log on as anonymous • If Web, just type in a URL for that website <p>Finally, you should have created at least one log entry. Open the log file again and see if your entry was added to the log file. If the log file did not change, logging is not working.</p>
Remediation Procedure	<p>Immediate: Turn on logging, Turn on Log Visits, make sure for extended logging the required fields are selected.</p> <p>Long term: Incorporate procedures to examine, analyze, and archive log files, as needed and according to the retention</p>

	<p>requirements of the organization.</p> <p>Inhibitors: Log files take up space. Turning on logging will consume disk space resources, as well as CPU cycles. Resource and Performance issues need to be addressed so that logging does not seriously impact IIS, the applications, or the server as a whole. Logs of are little use if no one ever looks at them, but even in that case they may provide an evidence trail for forensics.</p>
Test Nature	Objective
Evidence	Placeholder for artifacts, such as screenshots, logs, etc
Findings	Placeholder
Recommendation	Placeholder

© SANS Institute 2005, Author retains full rights

IIS 2.10 Remove or Disable Unnecessary Services

Reference	<ul style="list-style-type: none">• MSBA: 53116 (see Appendix A)• Securing the Microsoft Internet Information Server Chapter 19¹¹³ securing WebDav.• Securing the Web Site – Web Site Security¹¹⁴ do not install FTP unless required, and removal of FrontPage server extensions.• Harden Network Infrastructure Roles Chapter 5¹¹⁵• Remove FrontPage extensions if they are not going to be used, Section 9.1 Internet Information Services 5¹¹⁶• Run minimal services¹¹⁷
Component Tested	IIS
Risk	<p>Vulnerabilities being tested: Unneeded services that are installed and running provide an attack surface. Since any executable program may have vulnerabilities, running that program presents an exposure.</p> <p>Assets at risk: A major or complete compromise of the IIS component could lead to a major or complete compromise of the application code, or a direct compromise of the application data. In this case all assets listed in section 1.2.1 Assets at risk are controlled by a single application on this IIS web server, all which may be exposed either directly or indirectly. The potential damage of a successful compromise can be rated as high. The types of damage to the assets may be the unauthorized disclosure, modification, or destruction of protected data.</p> <p>Likelihood of threat: Medium. Anyone can try to attack code. However, if you are not using the function, and don't install it, you can't be vulnerable because the function is not running or installed.</p>

¹¹³ Philip Cox and Tom Sheldon. Windows 2000 Security Handbook. Berkeley: McGraw Hill/Osborne, 2001, (ISBN: 0-07-212433-4) p.596

¹¹⁴ Bragg, Roberta. Windows 2000 Security. Indianapolis: New Riders Publishing, 2001 (ISBN: 0-7357-0991-2) p. 494

¹¹⁵ Bragg, Roberta. Hardening Windows Systems. Emeryville: McGraw Hill/Osborne, 2004, (ISBN: 0-07-225354-1)

¹¹⁶ SANS Institute Windows 2000 Security Step By Step Version 1.5, July 1 2001 p. 55

¹¹⁷ Internet Security Systems. Microsoft Windows 2000 Security Technical Reference. Redmond: Microsoft Press, 2000 (ISBN: 0-7356-0858-X) p. 478

	<p>This is probably the best defense against a zero day attack¹¹⁸.</p> <p>Explanation: All software has bugs, regardless of whether anyone discovered them yet. You can't take advantage of code that is not installed and running. Most exploits are based off some vulnerability such as a buffer overflow. If the code isn't executing, it can't overflow.</p> <p>Features such as WebDav and FrontPage Server extensions should be included here, or put into their own checklist item. They might not be a service in the true sense of a Windows Server service, but do represent component parts of IIS that may be installed but not required.</p>
Test Procedure	<p>Settings: The Microsoft Security Baseline Analyzer (MSBA), using the services.txt file distributed with MSBA, will check to see if those services are running. A default install of MSBA 1.2.1 looks for 4 services:</p> <ul style="list-style-type: none"> • MSFTPSVC (FTP) • TlntSvr (Telnet) • W3SVC (WWW) • SMTPSVC (SMTP) <p>Actually, if you follow the format of the services.txt file, you can add additional services to be checked. For example, if you were running McAfee McShield virus scan, just add McShield to the services.txt file.</p> <p>Inspection by hand (Stimulus/Response): Security policy should establish which services should and should not be installed on the IIS server. This should also specify which features are allowed and which are not.</p> <p>The Network News Transmission Protocol (NNTP) service should be checked, and if running probably is not required. This can be checked by looking for the <u>Network News Transport Protocol (NNTP)</u> service in the services list. To automate this in MSBA, add the following service to the services.txt file: NntpSvc.</p>

¹¹⁸ A zero-day attack or zero-day exploit is when an exploit against a vulnerability comes out BEFORE the vulnerability is announced and a vendor supplied fix is available.

	<p>Looking for the execution of the service may be missed. Sometimes you don't have direct access to the server to do a local check, or the service may be hidden. NNTP runs on a default TCP port of 119, and we can check this via a Telnet client.</p> <ul style="list-style-type: none"> • Open a CMD prompt (run cmd.exe) • Telnet "target machine ip address" 119 • (ex: if on local machine type: telnet 127.0.0.1 119) • If nothing is running, will time out. • If NNTP is running, should get a 200 command such as: • 200 NNTP Service 5.00.0984 Version 5.0.2195.6972 Posting Allowed
Remediation Procedure	<p>Immediate: Stop the service and disable it. Use services from either Administrator Tools or Computer Management.</p> <p>Long term: Use Control Panel Add/Remove Programs Windows Components and uninstall the component if it can be removed¹¹⁹.</p> <p>Inhibitors: Component might be in use – but then keep in mind that if it is being used – it would be necessary, not unnecessary. Dangerous services such as WebDav and FrontPage Server extensions may be required, but if not then they should be removed if not needed. WebDav is required for Exchange Server, and could conflict if IIS is installed on an Exchange Server, which is a given for an Exchange 2000/2003 Front-End Outlook Web Access (OWA) node.</p>
Test Nature	Objective
Evidence	Placeholder for artifacts, such as screenshots, logs, etc
Findings	Placeholder
Recommendation	Placeholder

¹¹⁹ Microsoft Support Website. How to Disable or Remove Unnecessary IIS Services.
URL: <<http://support.microsoft.com/default.aspx?scid=kb;en-us;321141>>

IIS 2.11 Directory Browsing

Reference	<ul style="list-style-type: none"> • Securing the Microsoft Internet Information Server Chapter 19¹²⁰ • Securing the Web Site – Web Site Security¹²¹ • Managing Web Server Security: Disabling Directory Browsing¹²² • Directory Browsing Not Recommended¹²³ • Disable directory browsing in the Site Property sheet, Section 9.1 Internet Information Services 5¹²⁴ • Non-administrators should not have access to the directory tree, the shell, or operating system functions and utilities¹²⁵
Component Tested	IIS
Risk	<p>Vulnerabilities being tested: Reduction or prevention of server directory structure reconnaissance. In some cases, various web pages might be protected using security by obscurity (in other words, if you don't know about it you can't find it). Directory browsing allows the contents of directories to be listed, and with the right permissions web pages and files can be executed or downloaded. This can be an exposure if files are also stored in that directory that was never intended to be viewed or executed.</p> <p>Assets at risk: A major or complete compromise of the IIS component could lead to a major or complete compromise of the application code, or a direct compromise of the application data. In this case all assets listed in section 1.2.1 Assets at risk are controlled by a single application on this IIS web</p>

¹²⁰ Philip Cox and Tom Sheldon. Windows 2000 Security Handbook. Berkeley: McGraw Hill/Osborne, 2001, (ISBN: 0-07-212433-4) p. 577

¹²¹ Bragg, Roberta. Windows 2000 Security. Indianapolis: New Riders Publishing, 2001 (ISBN: 0-7357-0991-2) p. 494

¹²² Staneck, William R. Microsoft Windows 2000 and IIS 5.0 Pocket Reference. Redmond: Microsoft Press, 2001 (ISBN: 0-7356-1024-X) p. 143

¹²³ Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0, NSA/System and Network Attack Center (SNAC), Oct 29, 2003

URL: <http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/os/win2k/iis_5_v1_4.pdf> p. 42

¹²⁴ SANS Institute Windows 2000 Security Step By Step Version 1.5, July 1 2001 p. 55

¹²⁵ WEB SERVER CHECKLIST Version 4, Release 1.3 Microsoft IIS Server,

NIST/ Computer Security Resource Center (CSRC), May 26, 2004

URL: <http://csrc.nist.gov/pcig/CHECKLISTS/web_checklist_052604.zip> Item: WG200

	<p>server, all which may be exposed either directly or indirectly. The potential damage of a successful compromise can be rated as high. The types of damage to the assets may be the unauthorized disclosure, modification, or destruction of protected data.</p> <p>Likelihood of threat: Medium. Automated attack tools can detect if browsing is available based on the server response.</p> <p>Explanation: No one should be looking inside your directory structure and trying to figure out the application's construction and design.</p>
Test Procedure	<p>Settings: The Microsoft Security Baseline Analyzer (MSBA) ¹²⁶ doesn't help here you will need to do this by hand. Directory browsing is a security checkbox in the Home Directory tab of the Web Site Properties page; see Figure B5 of an example. The filed is labeled "Directory browsing".</p> <p>Each property page for web sites and virtual directories should be checked.</p> <p>Inspection by hand (Stimulus/Response): The web site will go into browsing mode if the URL does not specify a start document page (ex: index.html, default.asp, etc) and the Documents settings (see page B3) either does not have a default document enabled or the default document cannot be found. By typing in a URL for each defined website and virtual directory, you should either get one of the following:</p> <ul style="list-style-type: none"> • Default Document • 404 Not Found Error Page • A directory listing of the files in the folder <p>If you get the listing, then browsing is in effect. But keep in mind that browsing may be specified and might not be apparent if there is a default document match. It may take deletion of the default document to cause browsing to then take effect.</p>

¹²⁶ Microsoft Download Site [Microsoft Baseline Security Analyzer 1.2.1](http://www.microsoft.com/technet/security/tools/mbsahome.msp) August 16 2004
URL: <<http://www.microsoft.com/technet/security/tools/mbsahome.msp>>

	See Figure B22 for a sample of what a directory browse listing would look like.
Remediation Procedure	<p>Immediate: Turn off browsing. Make sure a default document is specified, and that there is a default document in the directory.</p> <p>Long term: Same as immediate</p> <p>Inhibitors: Directory browsing may be a requirement. One case where it may be valid is a download page where HTTP is used instead of FTP. Files are the downloaded by using the directory listing to find the file.</p>
Test Nature	Objective
Evidence	Placeholder for artifacts, such as screenshots, logs, etc
Findings	Placeholder
Recommendation	Placeholder

© SANS Institute 2005, Author

IIS 2.12 IUSR_computername Permissions and Rights

Reference	<ul style="list-style-type: none"> • Securing the Microsoft Internet Information Server Chapter 19¹²⁷ on sharing the anonymous account between WEB and FTP sites. • Securing the Web Site – Web Site Security¹²⁸ • Recommended checklist for chapter 1¹²⁹ • Verify user IUSR_machinename is not part of any privileged group, Section 9.1 Internet Information Services 5¹³⁰ • Non-administrators should not have access to the directory tree, the shell, or operating system functions and utilities¹³¹ • CGI scripts do not have proper access controls¹³² • When the IUSR account is installed on a domain controller, it is assigned excess privileges because the account is added to the domain users global group¹³³
Component Tested	IIS
Risk	<p>Vulnerabilities being tested:</p> <p>Verifying the application of least privilege and insuring that the default anonymous IIS account does not have too much privilege. If it does, then access and modification of system files may occur.</p> <p>Assets at risk:</p> <p>A major or complete compromise of the IIS component could lead to a major or complete compromise of the application code, or a direct compromise of the application</p>

¹²⁷ Philip Cox and Tom Sheldon. Windows 2000 Security Handbook. Berkeley: McGraw Hill/Osborne, 2001, (ISBN: 0-07-212433-4) p. 600

¹²⁸ Bragg, Roberta. Windows 2000 Security. Indianapolis: New Riders Publishing, 2001 (ISBN: 0-7357-0991-2) p. 495

¹²⁹ Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0, NSA/System and Network Attack Center (SNAC), Oct 29, 2003

URL: <http://www.nsa.gov/notices/notice00004.cfm?Address=/snac/os/win2k/iis_5_v1_4.pdf> p.

30

¹³⁰ SANS Institute Windows 2000 Security Step By Step Version 1.5, July 1 2001 p. 55

¹³¹ WEB SERVER CHECKLIST Version 4, Release 1.3 Microsoft IIS Server,

NIST/ Computer Security Resource Center (CSRC), May 26, 2004

URL: <http://csrc.nist.gov/pcig/CHECKLISTS/web_checklist_052604.zip> Item: WG200

¹³² WEB SERVER CHECKLIST Version 4, Release 1.3 Microsoft IIS Server,

NIST/ Computer Security Resource Center (CSRC), May 26, 2004

URL: <http://csrc.nist.gov/pcig/CHECKLISTS/web_checklist_052604.zip> Item: WG410

¹³³ Smith, Ben, and Komar, Brian. Microsoft Windows Security Resource Kit. Redmond: Microsoft Press, 2003 (ISBN: 0-7356-1868-2) p. 443

	<p>data. In this case all assets listed in section 1.2.1 Assets at risk are controlled by a single application on this IIS web server, all which may be exposed either directly or indirectly. The potential damage of a successful compromise can be rated as high. The types of damage to the assets may be the unauthorized disclosure, modification, or destruction of protected data.</p> <p>Likelihood of threat: Medium. Some other attack has to occur to get control. However, if the IUSR account has too much access privilege then there would be less of a need to escalate privilege. The threat is much higher on a domain controller.</p> <p>Explanation: As part of the IIS installation, two special guest accounts are created for IIS to run anonymous. These are the IUSR and IWAM accounts. The accounts being used will depend on the application isolation being used. Since they both have similar purposes, I will discuss IUSR, but everything here applies to BOTH user accounts.</p> <p>The IUSR account has a limited set of privileges. It is a guest account and doesn't have much more power and authority than a guest. But if compromised, coupled with a successful escalation of privilege, then the attacker can own the machine. The more privileged the IUSR account, the less privilege escalation required. For example, if the IUSR account was an administrator, then a compromise using that account is almost endgame.</p> <p>The most interesting in the research is when IIS is installed on a Domain Controller, where both the IUSR and IWAM accounts are added to Domain Users. This is already highly excessive and dangerous.</p>
Test Procedure	<p>Settings: If on a member of a domain: Use Administrator Tools, Active Directory User and Computers If on a stand-a-lone system: Use computer management</p> <p>Examine the membership of the IUSR and IWAM accounts and determine if they are located in any non-guest group.</p> <p>Using Administrator Tools check the local security policy of</p>

	<p>the IIS system and determine if the IUSR and/or IWAN account have any rights.</p> <p>In Local Security Settings, navigate to the leaf of Security Settings, Local Policies, and User Rights Assignments.</p> <p>For example, IUSR and IWAM may have the effective right to “logon as a batch job”. This is valid. However, you would not want these accounts to have the right to “Manage and Audit security log”. These parameters should be examined and a determination of which are reasonable and which represent an exposure.</p> <p>The directory structure should be examined to determine which files and folders IUSR has access to. One key tool to accomplish this is from the Windows 2000 Server Resource Kit and is called showacls.exe. This can generate a massive amount of output and can be refined in a script¹³⁴.</p> <p>Inspection by hand (Stimulus/Response): You can set the IUSR account so that you know the password. Changing the IUSR account to a known password is a simple function. Once you know the password, you can try to log onto the system normally as a user. If you can log on, try to access the files and run programs. How far you can get into the system will be the same if the attacker can achieve a way to execute the same programs and traverse the same directories.</p>
Remediation Procedure	<p>Immediate: Limit excess privileges, rights, and access</p> <p>Long term: Remove excess privileges, rights, and access</p> <p>Inhibitors: As with anything else, this can break running applications. If an application is running today with the excess privilege or rights, removal may prevent the application from running. Detecting which right or privilege an application requires is very difficult. File access may be easier to detect by using a file access monitor, which is a free tool from sysinternals¹³⁵. Downgrading of privileges, rights and permissions has always been a difficult but necessary requirement,</p>

¹³⁴Windows .NET Magazine. Automatically Audit Access to Files and Folders. (June 2003)
URL: <<http://www.windowssitpro.com/Windows/Article/ArticleID/38942/38942.html>>

¹³⁵ Website Homepage. URL: <<http://www.sysinternals.com>>

	especially to achieve principle of least privilege.
Test Nature	Objective
Evidence	Placeholder for artifacts, such as screenshots, logs, etc
Findings	Placeholder
Recommendation	Placeholder

© SANS Institute 2005, Author retains full rights.

IIS 2.13 Service Account Permissions and Rights

Reference	<ul style="list-style-type: none">Grant local and network privileges according to the authentication mechanisms used¹³⁶
Component Tested	IIS
Risk	<p>Vulnerabilities being tested: Verifying the application of least privilege and insuring that the service account does not have too much privilege. If it does, then access and modification of system files may occur.</p> <p>Assets at risk: A major or complete compromise of the IIS component could lead to a major or complete compromise of the application code, or a direct compromise of the application data. In this case all assets listed in section 1.2.1 Assets at risk are controlled by a single application on this IIS web server, all which may be exposed either directly or indirectly. The potential damage of a successful compromise can be rated as high. The types of damage to the assets may be the unauthorized disclosure, modification, or destruction of protected data.</p> <p>Likelihood of threat: High. For Windows 2000 the default service account is localsystem that is a high privilege account.</p> <p>Explanation: The previous checklist item checked the IUSR and IWAM accounts that were the low privilege guest level accounts used for out of process execution. For in-process execution of the web server components, they run under the service account. If an in-process task is compromised, it will have excessive privileges and rights. In several cases IIS may erroneously run an out-of-process type task in-process, exposing that task to excessive privileges.</p>
Test Procedure	<p>Settings: You must first check services and determine the service account of each of the IIS components. If the service account is localsystem, then it may be possible to reduce the privilege and rights. If it is not localsystem, then follow</p>

¹³⁶ Internet Security Systems. Microsoft Windows 2000 Security Technical Reference. Redmond: Microsoft Press, 2000 (ISBN: 0-7356-0858-X) p. 479

	<p>the test procedure for IIS 2.12 checklist item.</p> <p>Inspection by hand (Stimulus/Response): If not localsystem, logon to the account (after getting the password), and then try to log onto the system normally as a user. If you can log on, try to access the files and run programs. How far you can get into the system will be the same if the attacker can achieve a way to execute the same programs and traverse the same directories.</p>
Remediation Procedure	<p>Immediate: If not local system and excess privilege, permissions or rights, then scale down the power of the user account.</p> <p>Long term: If localsystem, then try to replace with a special local account. Reduce privileges, rights and permissions to bare minimum.</p> <p>Inhibitors: It is very difficult to scale down the privilege level of an account. It is a lot of work, very difficult to troubleshoot, and probably not feasible. It may be justified to create a substitute system account that is as powerful as localsystem but does not have the permissions to access critical parts of the file system. This would allow some control on which files and folders may be accessed and limit the attack surface.</p>
Test Nature	Objective.
Evidence	Placeholder for artifacts, such as screenshots, logs, etc
Findings	Placeholder
Recommendation	Placeholder

IIS 2.14 IP Forwarding

Reference	<ul style="list-style-type: none">• Disable IP Routing¹³⁷
Component Tested	TCP/IP Stack
Risk	<p>Vulnerabilities being tested:</p> <p>A multi-homed server (more than one Network Interface Card (NIC)) could unintentionally be converted to a router. As a router, traffic may be routed to sections of the network that is unsafe, or it may allow an attacker to penetrate deeper into the network to bypass protection mechanisms such as a firewall.</p> <p>Assets at risk:</p> <p>A major or complete compromise of the IIS component could lead to a major or complete compromise of the application code, or a direct compromise of the application data. In this case all assets listed in section 1.2.1 Assets at risk are controlled by a single application on this IIS web server, all which may be exposed either directly or indirectly. The potential damage of a successful compromise can be rated as high. The types of damage to the assets may be the unauthorized disclosure, modification, or destruction of protected data.</p> <p>Likelihood of threat:</p> <p>Low because disabling of routing is the default.</p> <p>Explanation:</p> <p>When auditing an IIS server that is Internet facing, i.e. is exposed or bastion to the Internet, the IIS server should be located in a DMZ protected by some firewall configuration.</p> <p>There are many different firewall configurations, but the one configuration that this test applies to is the firewall sandwich, where the web server is placed between two firewalls – one external and one internal. The web server would be multi-homed with two separate Network Interface Card (NIC) connections, one connection to each firewall. The purpose of this configuration is to provide additional defense in depth by putting two firewalls between the Internet and the company network. In a sandwich DMZ it is</p>

¹³⁷ Internet Security Systems. Microsoft Windows 2000 Security Technical Reference. Redmond: Microsoft Press, 2000 (ISBN: 0-7356-0858-X) p. 478

	<p>recommended that the firewalls use different vendors, for example use Checkpoint for External and Cisco PIX for Internal. Now, not only does a hacker have to penetrate two firewalls, but of different technologies and different underlying vulnerabilities.</p> <p>Another part of this layered approach is that in either direction a hacker would have to breach a firewall, a web server, then another firewall before invading a company network. This requires that the web server does not just route traffic through the web server. In this design, it is not the intention for Internet traffic to ever reach the internal firewall or for the company traffic to reach the external firewall. If the web server acts as a router, and using IP forwarding – network traffic will bypass the web server and flow beyond the intended boundaries of the DMZ.</p> <p>The risk of improper configuration is the creation of a network channel that can move an attack closer into the company network.</p>
Test Procedure	<p>Settings: In Windows NT 4.0, this parameter was specified in the TCP/IP properties page. This was removed in Windows 2000, and IP Forwarding is disabled by default. Inspection will require viewing a registry key to see if this was overridden. Microsoft knowledge base article Q230082¹³⁸ from July 2004 indicates how to enable IP Forwarding. Using the registry editor, examine the following HKLM key:</p> <p>SYSTEM\CurrentControlSet\Services\TCPIP\Parameters</p> <p>And look for the value IPEnableRouter, if this has a value of 1, then forwarding is configured.</p> <p>Another setting test is to issue the following command in a command window:</p> <p style="text-align: center;">Ipconfig /all</p> <p>In the output there will be a line that says:</p> <p style="text-align: center;">IP Routing Enabled</p> <p>Followed by either a “Yes” or “No”.</p>

¹³⁸ Microsoft Support Website. How to Enable TCP/IP Forwarding in Windows 2000. URL: <<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q230082>>

	<p>Yes is enabled, No is disabled.</p> <p>Inspection by hand (Stimulus/Response): This is one test that should not be trusted to settings. This will be a complicated test, and will require multiple testing computers, one running a sniffer. The test requires attaching to one interface a machine that can generate traffic (The Generator), and a machine that can see the traffic (The Sniffer) to the other interface. Using the Generator, traffic is sent to addresses on the far interface. If the sniffer sees that traffic, then the web server is routing the traffic. Now swap interfaces and repeat to see if traffic flows in the other direction.</p>
Remediation Procedure	<p>Immediate: Change configuration to disable forwarding. Reboot server.</p> <p>Long term: Change configuration to disable forwarding. Reboot server.</p> <p>Inhibitors: The network configuration could be poorly designed that breaking the forwarding breaks the application. If this occurs, then the problem may be bigger than discovered.</p>
Test Nature	<p>Subjective. Depending on the state of the server, the routing tables, and traffic addressing, the true state of IP Forwarding may be masked.</p>
Evidence	<p>Placeholder for artifacts, such as screenshots, logs, etc</p>
Findings	<p>Placeholder</p>
Recommendation	<p>Placeholder</p>

IIS 2.15 Anonymous FTP Accounts

Reference	<ul style="list-style-type: none">• Securing the Microsoft Internet Information Server Chapter 19¹³⁹ FTP Server.• Dedicate ANY volume accessible by the FTP server explicitly to the FTP service, Section 9.1 Internet Information Services 5¹⁴⁰
Component Tested	IIS – FTP Service
Risk	<p>Vulnerabilities being tested:</p> <p>FTP provides multiple issues for exposure. The largest is exposure of credentials as logon credentials are passed over the Internet (or over any medium) in clear text. The recommendation is to use anonymous FTP. But on that side, anonymous FTP also has its issues. If someone fills up the disk with illegitimate files so that legitimate files cannot be transferred, we have a denial of service. If someone loads the FTP directories with illegal copyrighted materials or even porn, then we have liability issues. If these files are child porn, we may even be in a position for criminal prosecution.</p> <p>Assets at risk:</p> <p>A major or complete compromise of the IIS component could lead to a major or complete compromise of the application code, or a direct compromise of the application data. In this case all assets listed in section 1.2.1 Assets at risk are controlled by a single application on this IIS web server, all which may be exposed either directly or indirectly. The potential damage of a successful compromise can be rated as high. The types of damage to the assets may be the unauthorized disclosure, modification, or destruction of protected data.</p> <p>Likelihood of threat:</p> <p>Anonymous FTP with writable disks is easily found as part of scanning and other reconnaissance. Likelihood of detection is high, and likelihood of compromise is also high.</p> <p>Explanation:</p> <p>When an FTP account is configured for anonymous logon,</p>

¹³⁹ Philip Cox and Tom Sheldon. Windows 2000 Security Handbook. Berkeley: McGraw Hill/Osborne, 2001, (ISBN: 0-07-212433-4) pgs: 598-603

¹⁴⁰ SANS Institute Windows 2000 Security Step By Step Version 1.5, July 1 2001 p. 56

	<p>two possible threats may occur.</p> <p>In one threat, we have successful guest access being established. There is always a possibility of an exploited vulnerability in FTP that could cause privilege escalation. Unless really required, anonymous FTP should be avoided, or if required, should be configured for download only.</p> <p>The other possible threat occurs with anonymous FTP where the directory is enabled for write access. The risk here is high in this situation, and the consequences may also pose legal issues with software piracy. There is a large movement of Warez activity where anonymous FTP sites are sought for illegal hosting and distribution of copyrighted software, music and movies. These sites are made into PUB sites, and scanning techniques are used to find these anonymous FTP sites. A site being caught as a PUB site could be implicated as contributing to software piracy and publicity about this could tarnish the reputation of the company owning the FTP site.</p> <p>Writable anonymous FTP sites could also experience denial of service (DoS) situations were the entire disk can be filled to the point that the Operating System has to shut down. In the case of moving illegal copyright material, such as Warez, complete network bandwidth may also be consumed preventing legitimate traffic from flowing.</p> <p>All of the above is also a risk in the case of non-anonymous configuration, where user credentials can be easily obtained and cracked. This has a much lower probability than allowing anonymous access because credentials have to be captured or cracked.</p>
Test Procedure	<p>Some scanning tools will test to see if anonymous access is configured by sending a login and checking the return code. This is better than just relying on a settings check, but in either case it does not confirm whether the account can do damage (An anonymous FTP server with read-only disks is less of a threat than writable disks). FTP may be required to be defined at the default port (TCP 21) for a scanner to pick this up.</p> <p>Settings: Check the Security Accounts property page for each FTP site (See Figure B13) and examine the anonymous box. If it is checked, then anonymous access is allowed.</p>

	<p>Check the Home Directory property page for each FTP site (see Figure B14) and examine if the write box is checked. If it is checked, then the FTP server will allow the disk to be written.</p> <p>Take note that even if anonymous and write are both checked, the ability to actually write may depend on the file system and the permissions.</p> <p>Inspection by hand (Stimulus/Response): For each FTP site, determine the IP address and Port number being used. The initial IIS tree, as shown in Figure B11, shows each site, IP address and Port number. Since in the sample the IP address is any assigned, you will have to run the tests for ALL IP address and port combinations.</p> <ol style="list-style-type: none"> 1. Determine the IP addresses in use. Open a command window on the target server, run the following command: IPCONFIG 2. From a test machine, other than the target, establish a FTP session: FTP target_ip_address target_port 3. Username is anonymous: anonymous 4. Password can be anything: track7@sans.org 5. If the login fails, no anonymous access. 6. If login is successful, then issue a directory command to see if there are any files in the FTP directory DIR 7. If a non-empty directory is displayed, try to obtain a file: get filename 8. Try to upload your own file: put filename 9. If the upload is successful, test to see if same file can be retrieved: get filename 10. Repeat for each IP/Port combination until complete.
Remediation Procedure	<p>If anonymous write access is absolutely required, then:</p> <ul style="list-style-type: none"> • Disk contents should be monitored on a regular basis. Since detection of such a site by Warez promoters is done via scanning, network based intrusion detection (NIDS) for detection of port scan and ping sweeps can be used to detect possible intrusion activity. • Monitoring of disk and network bandwidth usage should be performed. • Logs should be reviewed more frequently than other system and activity logs. • If possible, change the default port number from 21 to a different port number. • The FTP writable directory should be built in a dedicated partition on the disk solely for that purpose. If this partition should fill up, no other application should be

	<p>affected by a disk full situation. This becomes a forced quota for the disk.</p> <ul style="list-style-type: none"> • If only anonymous read access is required, then make sure that such access is consistent with the data privacy and confidentiality requirements of the data being exposed. • If anonymous is not required, then disable anonymous access. <p>Turning off anonymous is just a check box on the security accounts page (see Figure B13).</p> <p>Turning off write ability is just a check box on the home directory page (see Figure B14). For extra protection, remove write attributes from file system Access Control Lists (ACL).</p> <p>Inhibitors:</p> <p>Use of credentials might not be user-friendly, and because they would be passed in the clear, is also unsafe. IIS does not support SSL/FTP, but if credentials are needed to be used in a non-anonymous scenario, use of non-IIS FTP servers that support SSL may help. Some of the common FTP servers that support SSL are WSFTP¹⁴¹, CuteFTP¹⁴², and ServU¹⁴³. A client that supports SSL is also needed. If anonymous FTP with writable disks must be used, then monitoring of the disk activity and contents is a must.</p>
Test Nature	Objective
Evidence	Placeholder for artifacts, such as screenshots, logs, etc
Findings	Placeholder
Recommendation	Placeholder

¹⁴¹ IPSWITCH Website URL: <http://www.ipswitch.com/products/WS_FTP-Server/index.html>

¹⁴² GlobalScape Website. URL: <<http://www.globalscape.com/gsftps/>>

¹⁴³ ServU Website. URL: <<http://www.serv-u.com/>>

IIS 2.16 Install URLSCAN For Traffic Filtering

Reference	<ul style="list-style-type: none"> • URLSCAN not being used¹⁴⁴ • Two tools are available to secure an IIS server, IIS Lockdown and URLSCAN¹⁴⁵ • User URLSCAN to filter HTTP Requests¹⁴⁶
Component Tested	IIS
Risk	<p>Vulnerabilities being tested: URLSCAN is not a vulnerability, but a compensating control. This utility provides a sort of force field in front of the web server to filter out potentially hazardous html streams. For example, It can compensate for situations where potentially dangerous mappings were not deleted.</p> <p>Assets at risk: A major or complete compromise of the IIS component could lead to a major or complete compromise of the application code, or a direct compromise of the application data. In this case all assets listed in section 1.2.1 Assets at risk are controlled by a single application on this IIS web server, all which may be exposed either directly or indirectly. The potential damage of a successful compromise can be rated as high. The types of damage to the assets may be the unauthorized disclosure, modification, or destruction of protected data.</p> <p>Likelihood of threat: Since the exploits that URLSCAN defends are of high likelihood, this may be rated as high.</p> <p>Explanation: URLSCAN is a parser that examines the data streams (HTML) being presented to the web server. Examining the streams, URLSCAN can look for signatures of potentially hazardous code that may indicate in an attempt to exploit</p>

¹⁴⁴ WEB SERVER CHECKLIST Version 4, Release 1.3 Microsoft IIS Server, NIST/ Computer Security Resource Center (CSRC), May 26, 2004

URL: <http://csrc.nist.gov/pcig/CHECKLISTS/web_checklist_052604.zip> Item: Wi040

¹⁴⁵ Smith, Ben, and Komar, Brian. Microsoft Windows Security Resource Kit. Redmond: Microsoft Press, 2003 (ISBN: 0-7356-1868-2) p. 456

¹⁴⁶ SANS Institute. SANS/FBI Top 20 List for Windows, Oct 8, 2004 URL: <<http://www.sans.org/top20/>>

	<p>the web server. Figure F2 shows some of the options that can be selected to customize the allowable and forbidden operations. Customization of the urlscan.ini file allows tailoring of the IIS filter to meet the organization's needs. The c:\winnt\system32\inet_srv\urlscan folder contains the DLL file, INI files, activity log files, and installation log files. URLSCAN may be installed by hand or as part of the IIS Lockdown tool.</p>
Test Procedure	<p>Settings: Examination of the ISAPI settings in the Master WWW Property Sheet and individual web sites – looking for the URLSCAN.DLL file. Figure B23 shows an example of URLSCAN installed in the Master WWW Properties Sheet.</p> <p>Inspection by hand (Stimulus/Response): Offending commands that the URLSCAN filter will reject may be entered. After entry, check the URLSCAN log and see if the entries are recorded.</p> <p>See Figure F3 for a sample URLSCAN log file. In this sample, URL strings containing strings with .HTW, .IDA and .EXE extensions were entered, filtered, and intercepted by URLSCAN.</p>
Remediation Procedure	<p>Immediate: Determine the value of URLSCAN, and determine a configuration that is compatible with current applications.</p> <p>Long term: Implement URLSCAN to provide an extra layer of protection. This would support defense in depth.</p> <p>Inhibitors: If not done right, URLSCAN could break the application. However, with appropriate testing and determination of configuration parameters, URLSCAN may be tweaked to the point where URLSCAN can be used without breaking the application.</p>
Test Nature	Objective
Evidence	Placeholder for artifacts, such as screenshots, logs, etc
Findings	Placeholder
Recommendation	Placeholder

IIS 2.17 Unused Script Mappings Should be Removed

Reference	<ul style="list-style-type: none"> • Securing the Microsoft Internet Information Server Chapter 19¹⁴⁷ • Managing Web Server Security: Removing Unused Application Mappings¹⁴⁸ • The mappings that the server does not utilize should be removed. This will prevent any potential vulnerability in those .DLL files such as buffer overflows¹⁴⁹ • Remove unused script (MIME) mappings, Section 9.1 Internet Information Services 5¹⁵⁰ • Script mappings have proven to be the source of several IIS vulnerabilities, Appendix D¹⁵¹ • Unused and vulnerable script mapping in IIS are not removed¹⁵² • Unmap all unnecessary ISAPI extensions¹⁵³
Component Tested	IIS
Risk	<p>Vulnerabilities being tested: Many functions are provided by IIS through ISAPI extensions which are DLL files that serve those functions. These filters have been very buggy and have provided many buffer overflow vulnerabilities.</p> <p>Assets at risk: A major or complete compromise of the IIS component could lead to a major or complete compromise of the application code, or a direct compromise of the application data. In this case all assets listed in section 1.2.1 Assets at</p>

¹⁴⁷ Philip Cox and Tom Sheldon. Windows 2000 Security Handbook. Berkeley: McGraw Hill/Osborne, 2001, (ISBN: 0-07-212433-4) p. 579

¹⁴⁸ Staneck, William R. Microsoft Windows 2000 and IIS 5.0 Pocket Reference. Redmond: Microsoft Press, 2001 (ISBN: 0-7356-1024-X) p. 147

¹⁴⁹ Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0, NSA/System and Network Attack Center (SNAC), Oct 29, 2003

URL: <http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/os/win2k/iis_5_v1_4.pdf> p.

89

¹⁵⁰ SANS Institute Windows 2000 Security Step By Step Version 1.5, July 1 2001 p. 56

¹⁵¹ Web Server SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) V5.0, NIST/Computer Security Resource Center (CSRC), Jul 26, 2004

URL: <<http://csrc.nist.gov/pcig/STIGs/WebV5R0.zip>> p. 86

¹⁵² WEB SERVER CHECKLIST Version 4, Release 1.3 Microsoft IIS Server,

NIST/ Computer Security Resource Center (CSRC), May 26, 2004

URL: <http://csrc.nist.gov/pcig/CHECKLISTS/web_checklist_052604.zip> Item: Wi050

¹⁵³ SANS/FBI Top 20 List for Windows, Oct 8, 2004 URL: <<http://www.sans.org/top20/>>

	<p>risk are controlled by a single application on this IIS web server, all which may be exposed either directly or indirectly. The potential damage of a successful compromise can be rated as high. The types of damage to the assets may be the unauthorized disclosure, modification, or destruction of protected data.</p> <p>Likelihood of threat: High. The mappings are enabled by default, and the vulnerabilities have been known for a while, with well crafted exploits in the wild. Even though patching will resolve all known exploits, the ISAPI filters are very buggy and new vulnerabilities are discovered.</p> <p>Explanation: Mappings are extensions that map to a particular function. Some of the file mappings used in IIS, and can be disabled using the IIS Lockdown Tool are (See Figure C6):</p> <ul style="list-style-type: none"> • Active Server Pages (.asp) • Index Server Web Interface (.idq .htw .ida) • Server Side Includes (.shtml, .shtm, .stm) • Internet Data Connector (.idc) • .HTR Scripting (.htr) • Internet Printing (.printer) <p>Buffer overflows of ISAPI filters for IIS have always been problem prone. Here are two overflows from 2001:</p> <ul style="list-style-type: none"> • Internet Printing had an early buffer overflow vulnerability that has been exploited. There is a Hacking Tool called Jill.exe that targets this specific vulnerability¹⁵⁴ MS01-023¹⁵⁵. • The index server (idq.dll) also had its buffer overflow issues in MS01-033¹⁵⁶.
Test Procedure	<p>Settings: The mappings can be viewed in the Application Configuration property sheet (see Figure B7) on the App</p>

¹⁵⁴ Sheridan, John. Microsoft Windows 2000 IIS 5.0 **IPP** ISAPI 'Host:' Buffer Overflow Vulnerability. SANS Institute, GCIH Practical. Jun 19, 2001

URL: <http://www.giac.org/practical/David_Sheridan_GCIH.doc>

¹⁵⁵ Microsoft Support Website. Unchecked buffer in ISAPI extension could enable compromise of IIS 5.0 server. URL: <<http://www.microsoft.com/technet/security/bulletin/MS01-023.mspx>>

¹⁵⁶ Microsoft Support Website. Unchecked Buffer in Index Server ISAPI Extension Could Enable Web Server Compromise.

URL: <<http://www.microsoft.com/technet/security/bulletin/MS01-033.mspx>>

	<p>Mappings tab. They can also be added, modified or deleted from this page.</p> <p>Inspection by hand (Stimulus/Response): An attempt may be made to actually use the mappings and see what type of error is returned. A 404 error may indicate that the mapping was removed by IIS lockdown, or is being intercepted by URLSCAN. The return of a 404 might not be adequately inclusive to indicate removal of the mapping. But a non-404 return where a syntax error is returned would indicate that the mapping is still in effect.</p>
Remediation Procedure	<p>Immediate: Either use the IIS Lockdown Tool or remove the settings directly. Figure B7 shows the Application Configuration App Mappings property sheet for making these modifications.</p> <p>Long term: If the mappings were changed by hand, then using the IIS Lockdown tool is a better method. However, the IIS Lockdown tool can only be run once, so you have to get it right the first time. Otherwise, to rerun the lockdown tool you must reverse the settings from the last run of the IIS lockdown tool, and then start again.</p> <p>Inhibitors: You must make sure that the function is not required. Deleting the .ASP mapping on a server using .ASP pages is going to be a problem. Yet also note that the install of some software products and feature may bring the mapping back – which means that after you delete a mapping it may appear again. When using the IIS Lockdown tool, the tool does not delete the mapping, it re-associates it to a 404 Dll.</p>
Test Nature	Objective
Evidence	Placeholder for artifacts, such as screenshots, logs, etc
Findings	Placeholder
Recommendation	Placeholder

IIS 2.18 SMTP Open Relay Should be Restricted

Reference	<ul style="list-style-type: none">• Securing the Microsoft Internet Information Server Chapter 19¹⁵⁷ – SMTP Server configuration.• An Open Relay web server does not limit email to outbound only¹⁵⁸
Component Tested	IIS –SMTP Service
Risk	<p>Vulnerabilities being tested: Whether the SMTP service will allow the relay of e-mail from different source e-mail domains.</p> <p>Assets at risk: Open relay, if abused – especially for SPAM, can have repercussions on the Brand and can lead to lawsuits in downstream liability. There is also another negative effect. Many organizations use blacklists to filter SPAM e-mail. These blacklists are difficult to impossible to get removed once you get on one. If someone abuses your SMTP server, they could cause you to get blacklisted on one of these servers. This can impact your ability to send legitimate business e-mail to those clients that use these blacklists as filters.</p> <p>Likelihood of threat: High. Automated scanning tools searching for port 25 can be used to find an open relay. Once your site is listed on an open relay, the open relay lists then become a directory that can be used to find your site as a relay candidate.</p> <p>Explanation: Outbound e-Mail that is passed through the SMTP server should only be from authorized users and from authorized domains. Incoming e-mail may come from any domain.</p>
Test Procedure	<p>Settings: Examination of the SMTP property sheets, specifically the Relay Settings. On the SMTP Properties sheet will be a button for Relay. (See Figure B15). The relay property sheet (see Figure B16) allows settings of who may relay. Understanding this property sheet and its values may be</p>

¹⁵⁷ Philip Cox and Tom Sheldon. Windows 2000 Security Handbook. Berkeley: McGraw Hill/Osborne, 2001, (ISBN: 0-07-212433-4) pgs. 603-606

¹⁵⁸ WEB SERVER CHECKLIST Version 4, Release 1.3 Microsoft IIS Server, NIST/ Computer Security Resource Center (CSRC), May 26, 2004
URL: <http://csrc.nist.gov/pcig/CHECKLISTS/web_checklist_052604.zip> Item: WG330

	<p>confusing.</p> <p>Inspection by hand (Stimulus/Response): This can be a fun test. What will be important is that port 25 be open between the tester and the IIS server. Not only must the firewall be open if this is being done from the Internet, but if you are on your home network and using the Internet, you must make sure your ISP does not block port 25. Many ISP's are blocking port 25 because of SPAM issues. (Many of the latest e-mail propagation worms now include their own SMTP server to push e-mail out. ISP's are blocking port 25 to limit the spread of these worms).</p> <p>In this test, we will use telnet to connect to port 25 and enter raw SMTP commands, and check for the response from SMTP. The testing is not complex, but can be burdensome as different authentication scenarios are required. Microsoft Provided a Knowledge Base Q304897¹⁵⁹ article in its support database on how to do this process by hand.</p>
Remediation Procedure	<p>Immediate: Restrict SMTP relay to only authorized users. Relay is required to send outgoing e-mail out to the Internet.</p> <p>Long term: Multiple SMTP virtual servers may be required, one for incoming e-mail that does not allow relay and another for outgoing e-mail that allows relay. Some companies allow employees to use the company SMTP server to send outgoing e-mail, even when the employee is home. In this configuration, the only reasonable way to allow authentication is to remove anonymous authentication on the relay server and only allow use of the server for someone who is successfully logged onto a user account. Since this will not work with incoming e-mail (incoming e-mail will require anonymous credentials) a second server that allows anonymous but disallows relay would be required. Both virtual servers can be installed on the same server, but require different IP addresses.</p> <p>Inhibitors: Relay is needed, but must be controlled. If you force someone to authenticate to a SMTP server with non-anonymous credentials, the e-mail client might not even</p>

¹⁵⁹ Microsoft Support Website. SMTP relay behavior in Windows 2000, Windows XP, and Exchange Server URL: <<http://support.microsoft.com/default.aspx?scid=kb:en-us:304897>>

	support entry of a set of credentials. If it does support this, then the amount of effort will be related to the number of e-mail clients that access the SMTP server. Some Outlook clients have an option that specifies the SMTP server requires authentication, use same credentials as the POP3 server. This can keep a helpdesk very busy, and requires a large amount of administrative work to make a change like this. Keep in mind that unless using a secure protocol (one that uses SSL) the credentials travel across the Internet in clear text and this can expose the user account and password.
Test Nature	Objective
Evidence	Placeholder for artifacts, such as screenshots, logs, etc
Findings	Placeholder
Recommendation	Placeholder

© SANS Institute 2005, Author retains full rights

SECTION 3: RESULTS - AUDIT, MEASUREMENTS, AND CONTROLS

Preparation for Performing the Audit

The act of performing an audit can be very intrusive. Even using non-intrusive tools, the physical act of entering a computer room and plugging into switches is intrusive.

Intrusive scanning is also intrusive. The issues that an auditor will have to deal with are the severity of the intrusive behavior. For example, running various scan tools may try to determine a specific vulnerability by sending a specially crafted data stream and analyze the results. Depending on the actual vulnerability and the data stream, these tests can actually cause the server to crash or may corrupt data.

It is critically important that proper notification and authorization is obtained. The performance of audit should, where possible, be presented within an organization's change control process. If recording systems, such as ARS Remedy service tickets are being used, determine if an ARS ticket should be opened to record the start and stop time of the audit. This becomes part of the official record that the audit was performed.

Coordination with the Business Owners of the Application, Operations, and Development should be performed. If a scan of a server should crash it, then you will need to know who to contact to restore and recover the server. This is a proactive requirement. If you crash a server in the middle of the night, and come morning the server is still down, then the scanning process will be blamed for an outage. If you are prepared and get the problem resolved quickly, then at least you minimize the damage. And the client should be prepared that although you will do your best to not crash the systems, sometimes these audits just might do it. The disclaimer is important, and having the right players in place should there be a problem, will keep the impact of the audit low. It is also possible that business unit owners will want the scanning to be performed off-hours so that the application and users are not impacted.

A preparation list of required items should be built and developed into a jump pack list. This list would include what equipment you would need to perform the onsite audit, which will include a notebook computer containing your tools. On the client side, you may require user credentials with administrator authority, since many scanners do better with administrative rights and MSBA will not scan the machine unless it has those rights.

See Appendix D for instructions on the Install and Execution of MSBA.

IIS 2.1 Service Packs and Security Updates Part 1

Microsoft Baseline Security Analyzer

View security report

Sort Order:

Computer name: BloodLab\SIMBA
IP address: 65.169.18.12
Security report name: BloodLab - SIMBA (2-1-2005 3:45 AM)
Scan date: 2/1/2005 3:45 AM
Scanned with MBSA version: 1.2.4013.0
Security update database version: 2005.1.11.0
Office update database version: 11.0.0.7306
Security assessment: Severe Risk (One or more critical checks failed.)

Security Update Scan Results

Score	Issue	Result
	Office Updates	1 update is missing. What was scanned Result details How to correct this
	Windows Security Updates	5 security updates could not be confirmed. What was scanned Result details How to correct this
	Microsoft VM Security Updates	No critical security updates are missing. What was scanned
	IIS Security Updates	No critical security updates are missing. What was scanned
	Windows Media Player Security Updates	No critical security updates are missing. What was scanned
	Exchange Server Security Updates	No critical security updates are missing. What was scanned
	MDAC Security Updates	No critical security updates are missing. What was scanned
	MSXML Security Updates	No critical security updates are missing. What was scanned

Previous security report Next security report

© 2002-2004 Microsoft Corporation. © 2002-2004 Shavlik Technologies, LLC. All rights reserved.

Artifact 1 Security Update Analysis - Missing Patches

Findings	All critical security patches have been applied to IIS,MDAC and XML
Recommendation	Resolve 5 security updates that could not be resolved.

IIS 2.1 Service Packs and Security Updates Part 2

Microsoft Baseline Security Analyzer - Microsoft Internet Explorer

Microsoft:
Baseline Security Analyzer

5 security updates could not be confirmed.

Result Details

Windows Security Updates

Security updates that the tool cannot confirm as installed on the scanned computer are marked with a blue asterisk

Score	Security Update	Description	Reason
*	MS02-064	Windows 2000 Default Permissions Could Allow Trojan Horse Program (Q327522)	Please refer to 306460 for a detailed explanation.
*	MS03-008	Flaw in Windows Script Engine could allow code execution (814078)	Please refer to 306460 for a detailed explanation.
*	MS03-030	Unchecked Buffer in DirectX Could Enable System Compromise (819696)	Please refer to 306460 for a detailed explanation.
*	MS04-016	Vulnerability in DirectPlay Could Allow Denial of Service (839643)	Please refer to 306460 for a detailed explanation.
*	MS04-028	Buffer Overrun in JPEG Processing (GDI+) Could Allow Code Execution (833987)	Please refer to 306460 for a detailed explanation.

If a service pack is listed, it is recommended that you install it prior to any other items listed.

Artifact 2 Security Update Analysis – Patch Exceptions

Findings	Additional security fixes require extra handling.
Recommendation	Verify items on list. Focus on Windows 2000 Default permissions specifications as these may seriously affect IIS.
Follow-up	Settings have been checked and do not apply.

IIS 2.2 File System Should be NTFS

Microsoft Baseline Security Analyzer

View security report

Sort Order: Score (worst first)

Windows Scan Results

Vulnerabilities

Score	Issue	Result
✗	Restrict Anonymous	Computer is running with RestrictAnonymous = 0. This level prevents basic enumeration of user accounts, account policies, and system information. Set RestrictAnonymous = 2 to ensure maximum security. What was scanned How to correct this
✗	Automatic Updates	Updates are automatically downloaded, but not automatically installed on this computer. What was scanned How to correct this
✗	Administrators	More than 2 Administrators were found on this computer. What was scanned Result details How to correct this
✗	Password Expiration	Some user accounts (35 of 59) have non-expiring passwords. What was scanned Result details How to correct this
ℹ	Windows Firewall	Windows Firewall is not installed or configured properly, or is not available on this version of Windows.
✓	File System	All hard drives (3) are using the NTFS file system. What was scanned Result details
✓	Autologon	Autologon is not configured on this computer. What was scanned
✓	Guest Account	The Guest account is disabled on this computer. What was scanned
	Local Account Password Test	Password checks are not performed on a domain controller. What was scanned

Previous security report Next security report

© 2002-2004 Microsoft Corporation. © 2002-2004 Shavlik Technologies, LLC. All rights reserved.

Artifact 3 MSBA Report Showing Windows Scan Results

Findings	All File Systems NTFS
Recommendation	None. Passed.

IIS 2.3 IIS Should Not be Installed on Domain Controller

IIS 2.4 IIS Lockdown Tool

IIS 2.5 IIS Sample Applications Should be Removed

IIS 2.6 IISADMPWD Virtual Directory

IIS 2.7 IIS Parent Paths Part 1

IIS 2.8 MSADC and Scripts Virtual Directories on IIS

IIS 2.9 IIS Logging Should be Enabled Part 1

IIS 2.10 Remove or Disable Unnecessary Services Part 1

© SANS Institute 2005, Author retains full rights.

Microsoft Baseline Security Analyzer

Microsoft Baseline Security Analyzer

- Welcome
- Pick a computer to scan
- Pick multiple computers to scan
- Pick a security report to view
- View a security report**

See Also

- Microsoft Baseline Security Analyzer Help
- About Microsoft Baseline Security Analyzer
- Microsoft Security Web site

Actions

Print

Copy

View security report

Sort Order: Score (worst first)

Local Account Password Test Password checks are not performed on a domain controller. [What was scanned](#)

Additional System Information

Score	Issue	Result
	Auditing	Logon Success and Logon Failure auditing are both enabled. What was scanned
	Services	Some potentially unnecessary services are installed. What was scanned Result details How to correct this
	Shares	11 share(s) are present on your computer. What was scanned Result details How to correct this
	Windows Version	Computer is running Windows 2000 or greater. What was scanned

Internet Information Services (IIS) Scan Results

Vulnerabilities

Score	Issue	Result
	IIS Lockdown Tool	The IIS Lockdown tool has not been run on the machine. What was scanned How to correct this
	Sample Applications	Some IIS sample applications are installed. What was scanned Result details How to correct this
	Parent Paths	Parent paths are enabled in some web sites and/or virtual directories. What was scanned Result details How to correct this
	MSADC and Scripts Virtual Directories	MSADC virtual directory was found under one or more web sites. What was scanned How to correct this
	IISAdmin Virtual Directory	IISADMPWD virtual directory is not present. What was scanned

Additional System Information

Score	Issue	Result
	Domain Controller Test	IIS is running on a primary or backup domain controller. What was scanned How to correct this
	IIS Logging Enabled	Some web or FTP sites are not using the recommended logging options. What was scanned Result details How to correct this

[Previous security report](#) [Next security report](#)

© 2002-2004 Microsoft Corporation. © 2002-2004 Shavlik Technologies, LLC. All rights reserved.

Artifact 4 MSBA Analysis IIS Scan Results


Findings	<p>IIS on Domain Controller</p> <p>IIS Lockdown Tool Never Run</p> <p>IIS Sample Applications Are Installed</p> <p>IISADMPWD Virtual Directory Removed</p> <p>IIS Parent Paths Part 1 Were Found</p> <p>MSADC and Scripts Virtual Directories on IIS Were Found</p> <p>IIS Logging Enabled</p> <p>Unnecessary Services Part 1 May have been found</p>
Recommendation	<p>Separate IIS and Domain Controller</p> <p>Run IIS Lockdown Tool</p> <p>Remove Samples</p>

	IISADMPWD is OK. Passed. Remove or reduce Parent Paths where possible Scripts directory not found. Passed MSADC located, disable or remove if possible Select more fields for IIS Logging Disable or remove unnecessary services
--	---

© SANS Institute 2005, Author retains full rights.

IIS 2.10 Remove or Disable Unnecessary Services Part 2






Microsoft Baseline Security Analyzer - Microsoft Internet Explorer

 Microsoft:
Baseline Security Analyzer

Some potentially unnecessary services are installed.

Result Details

The following list of services should only be enabled on computers that require their functionality. Services that are not required should be disabled to reduce the attack surface of the system.

Score	Service	State
	Network Associates McShield	Running
	Network News Transport Protocol (NNTP)	Running
	Simple Mail Transport Protocol (SMTP)	Running
	Telnet	Stopped
	World Wide Web Publishing Service	Running

Artifact 5 MSBA Analysis – Unnecessary Services

Findings	SMTP and NNTP are running.
Recommendation	SMTP is required for Exchange. NNTP is usually not required, and would recommend disable and remove of product.

IIS 2.7 IIS Parent Paths Part 2

Microsoft Baseline Security Analyzer - Microsoft Internet Explorer

 Microsoft Baseline Security Analyzer

Parent paths are enabled in some web sites and/or virtual directories.

Result Details

Score	Web Site	Virtual Directory
✗	BloodLab Website	-
✗	BloodLab Website	MSADC
✗	BloodLab Website	_vti_bin
✗	Administration Web Site	-
✗	Administration Web Site	IISAdmin
✗	Administration Web Site	MSADC
✗	Microsoft SharePoint Administration	-
✗	Microsoft SharePoint Search Proxy	OWS_VRoot_4
✗	Microsoft SharePoint Search Proxy	-
✗	OWA	ExchWeb/bin
✗	OWA	Printers
✗	OWA	Exadmin
✗	OWA	Exchange
✗	OWA	public
✗	OWA	ExchWeb
✗	OWA	-
✗	OWA Redirect	-
✗	Project	-
✗	Project	_vti_bin
✗	Project Server Web Site	-
✗	Project Server Web Site	MSADC
✗	Project Server Web Site	ProjectServer

Artifact 6 MSBA Analysis – Parent Paths

Findings	Parent Paths used for many websites. Also observe that SharePoint, Project Server, OWA and Remote Admin Sites are installed.
Recommendation	Determine if SharePoint and Project servers are required for external access. If not (internal only) then move functions to a different server. Change program code for application written internally so that parent paths are no longer required.

IIS 2.9 IIS Logging Should be Enabled Part 2

BloodLab Website Properties

Directory Security | HTTP Headers | Custom Errors

Server Extensions | Server Extensions 2002

Web Site | Operators | Performance | ISAPI Filters | Home Directory | Documents

Web Site Identification

Description: BloodLab Website

IP Address: (All Unassigned) Advanced...

ICP Port: 80 SSL Port: 443

Connections

☒ Unlimited

☐ Limited To: 1,000 connections

Connection Timeout: 900 seconds

☒ HTTP Keep-Alives Enabled

☒ Enable Logging

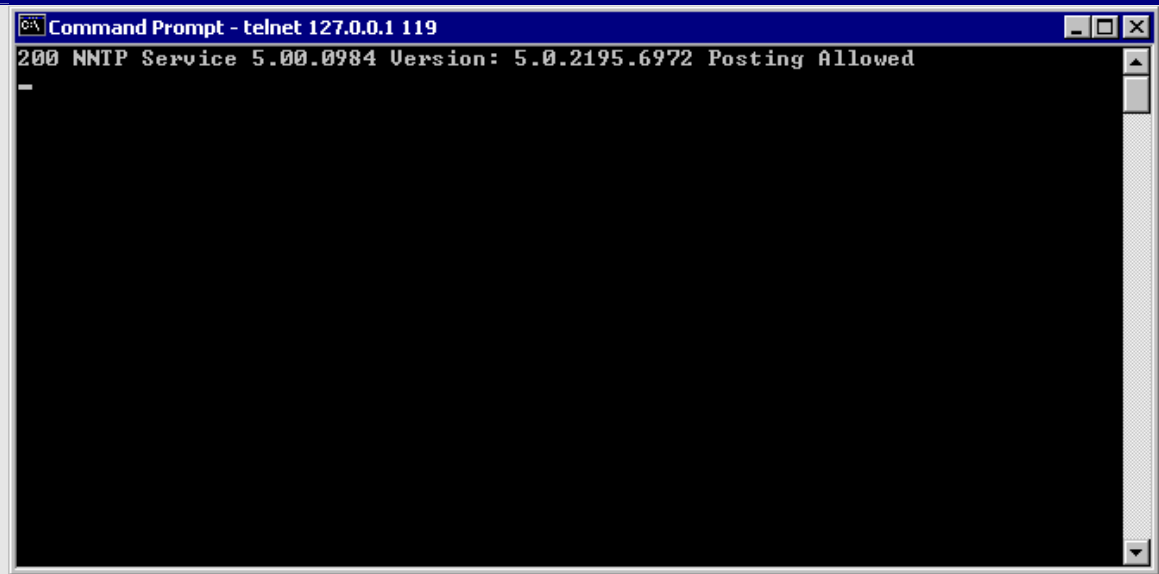
Active log format: W3C Extended Log File Format Properties...

OK Cancel Apply Help

Artifact 7 BloodLab Web Site Property Page

Findings	Logging is Enabled. W3C Extended Logging in effect.
Recommendation	None. Passed.

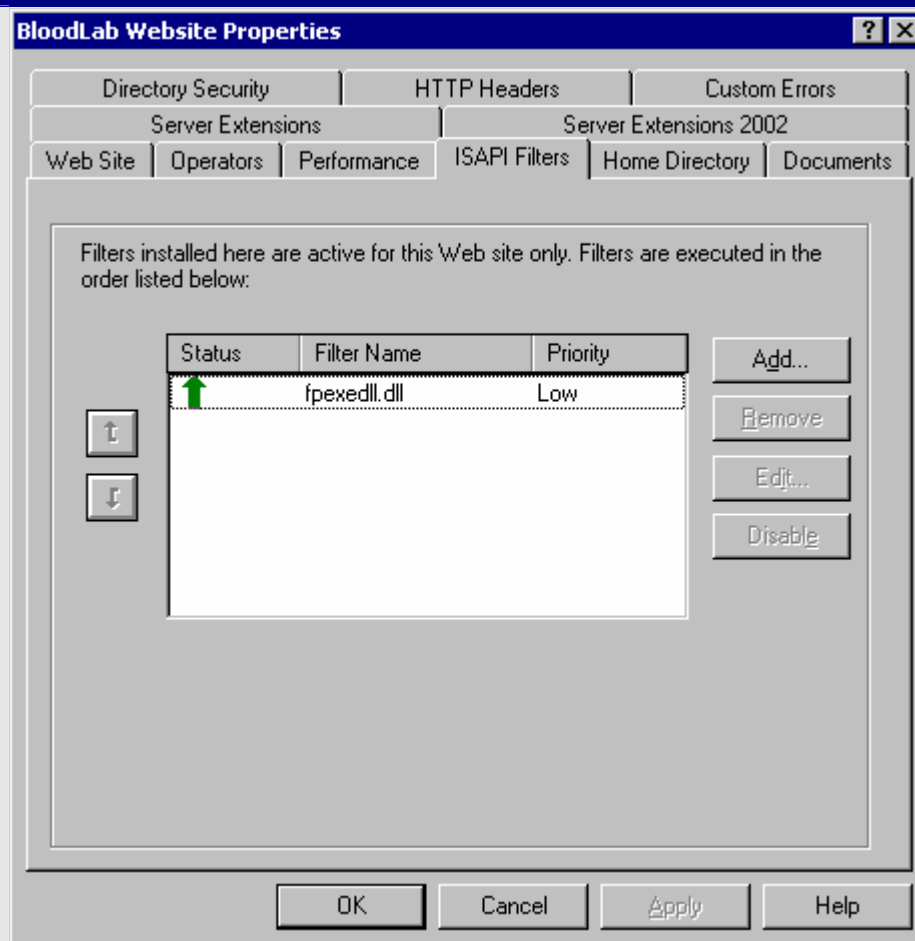
IIS 2.10 Remove or Disable Unnecessary Services Part 3



Artifact 8 Telnet Analysis – Verify NNTP Service Running

Findings	Open Command Window Type "telnet 127.0.0.1 119" NNTP is in use
Recommendation	If NNTP is not required, disable and uninstall software.

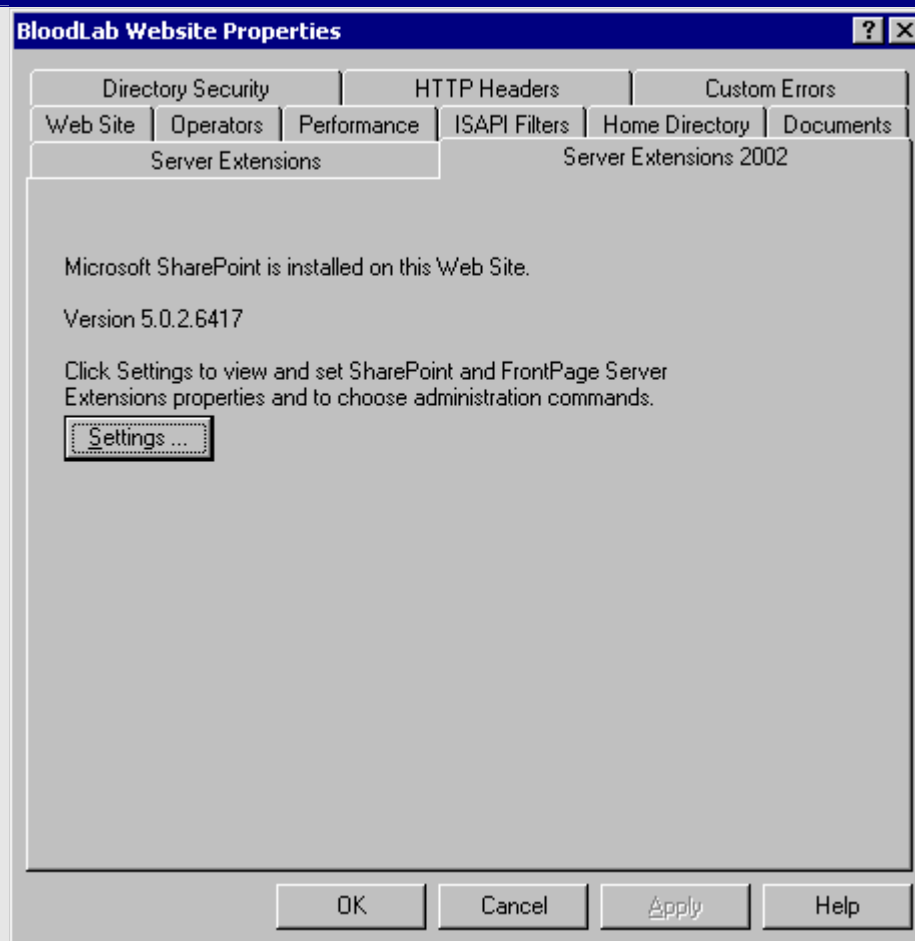
IIS 2.10 Remove or Disable Unnecessary Services Part 4



Artifact 9 ISAPI DLL Found – Front Page Extensions

Findings	FrontPage DLL found in ISAPI table.
Recommendation	Disable/Remove FrontPage if possible. Use the firewall as a compensating control. Restrict ports and functionality to internal network.

IIS 2.10 Remove or Disable Unnecessary Services Part 5



Artifact 10 Server Extensions 2002 – Share Point Installed

Findings	SharePoint and FrontPage server extensions installed.
Recommendation	If SharePoint is not used or access externally, move to different server. Where possible disable or remove service. Use firewall where possible as a compensating control to protect functions from outside.

IIS 2.10 Remove or Disable Unnecessary Services Part 6

BloodLab Website Properties

Directory Security | HTTP Headers | Custom Errors

Web Site | Operators | Performance | ISAPI Filters | Home Directory | Documents

Server Extensions | Server Extensions 2002

☒ **Enable authoring**

Version control: None

Performance: Tune for 100-1000 pages

Client scripting: JavaScript

Options

Specify how mail should be sent: Settings ...

Configure Office Collaboration features: Administer ...

☒ **Don't Inherit Security Settings**

☐ Log authoring actions

☐ Manage permissions manually

☐ Require SSL for authoring

(version 5.0.2.6417)

OK Cancel Apply Help

Artifact 11 Server Extensions

Findings	Server Extensions and WebDav authoring specified for website.
Recommendation	Remove/Disable for this website if possible. If not possible, use firewall to prevent feature from being used from the Internet. Look for other compensating controls. WebDav is needed for Exchange 2000 Mailbox Server. Move Exchange 2000 mailboxes to a separate mailbox server.

IIS 2.11 Directory Browsing Part 1

BloodLab Website Properties

Directory Security | HTTP Headers | Custom Errors

Server Extensions | Server Extensions 2002

Web Site | Operators | Performance | ISAPI Filters | **Home Directory** | Documents

When connecting to this resource, the content should come from:

- ☒ A directory located on this computer
- ☐ A share located on another computer
- ☐ A redirection to a URL

Local Path:

☐ Script source access ☒ Log visits

☒ Read ☒ Index this resource

☐ Write

☐ Directory browsing

Application Settings

Application name:

Starting point:

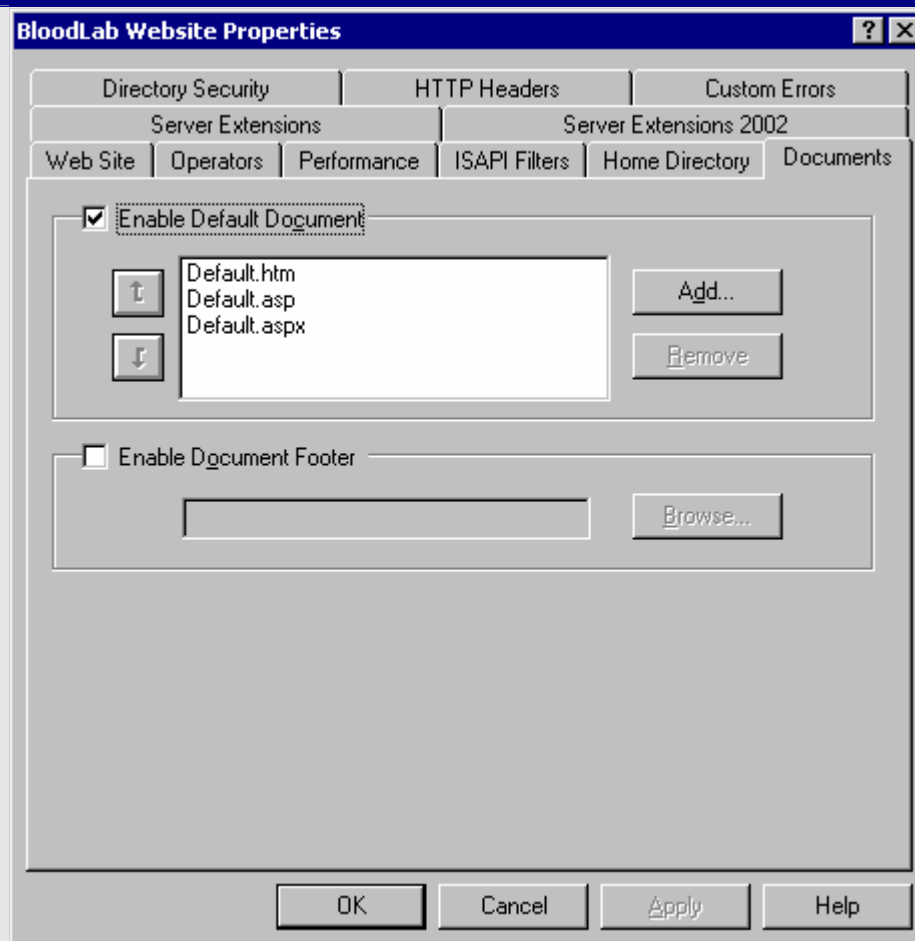
Execute Permissions:

Application Protection:

Artifact 12 BloodLab Web Site Home Directory Property Sheet

Findings	Directory Browsing is disabled
Recommendation	None. Passed.

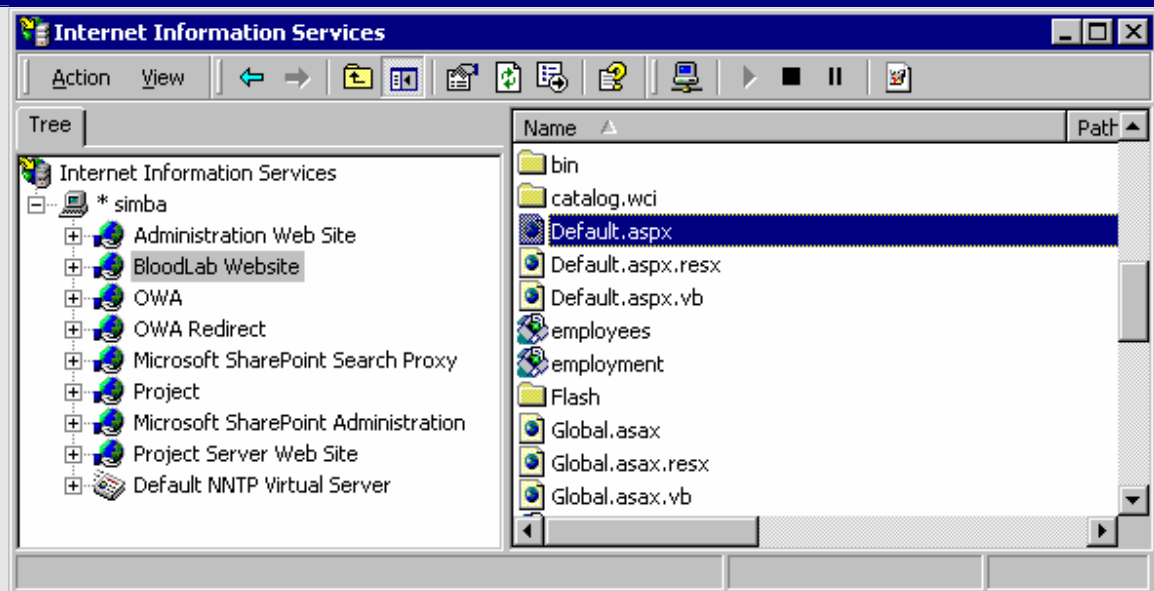
IIS 2.11 Directory Browsing Part 2



Artifact 13 Default Document Search Order

Findings	Three Default Documents Defined
----------	---------------------------------

IIS 2.11 Directory Browsing Part 3



Artifact 14 Internet Information Services – MMC Plug-in

Findings	Default.aspx is the only default document, but is not the first in the search list.
Recommendation	Move Default.aspx to the top of the list. In the current configuration an attacker could add in either a Default.htm or a Default.asp file which would take precedence over the Default.aspx.

IIS 2.12 IUSR_computername Permissions and Rights Part 1

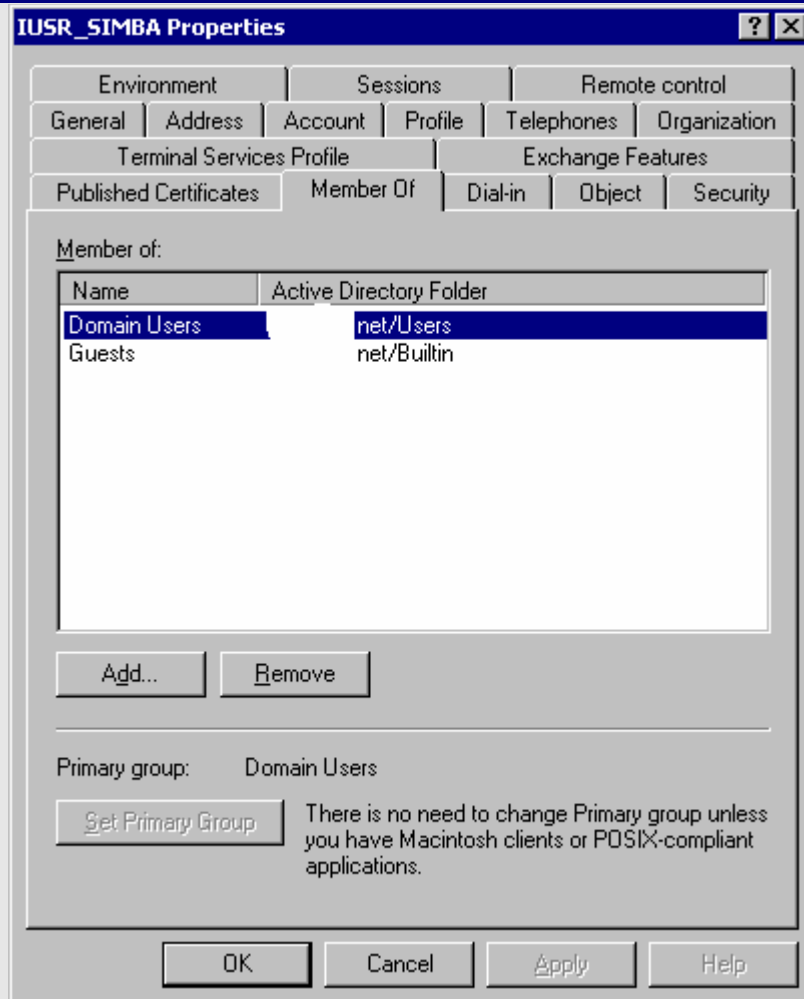


Artifact 15 Anonymous User Accounts – Setting Password

Findings	IIS Anonymous account is using default name
----------	---

© SANS Institute 2005, Author

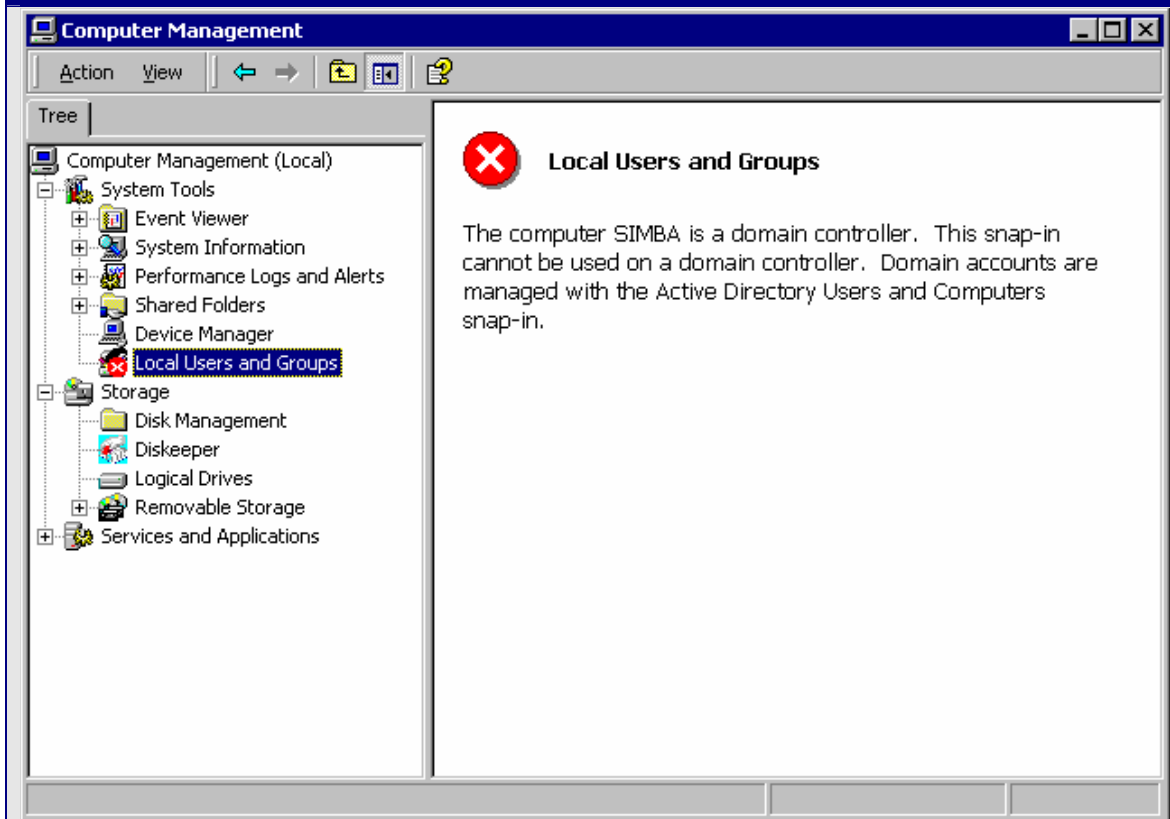
IIS 2.12 IUSR_computername Permissions and Rights Part 2



Artifact 16 Assignment and Password of IUSR Account

Findings	Excess Privilege. IUSR Guest account in Domain Users Group
Recommendation	Remove from Domain Users

IIS 2.12 IUSR_computername Permissions and Rights Part 3



Artifact 17 Computer Management – Local Users And Groups

Findings	Audit Target is a Domain Controller
Recommendation	Demote server to member

IIS 2.13 Service Account Permissions and Rights Part 1

World Wide Web Publishing Service Properties (Local Computer) ? x

General | Log On | Recovery | Dependencies

Service name: W3SVC

Display name: World Wide Web Publishing Service

Description: Provides Web connectivity and administration through t

Path to executable: C:\WINNT\System32\inet_srv\inetinfo.exe

Startup type: Automatic

Service status: Started

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Artifact 18 Services General Tab for WWW Service

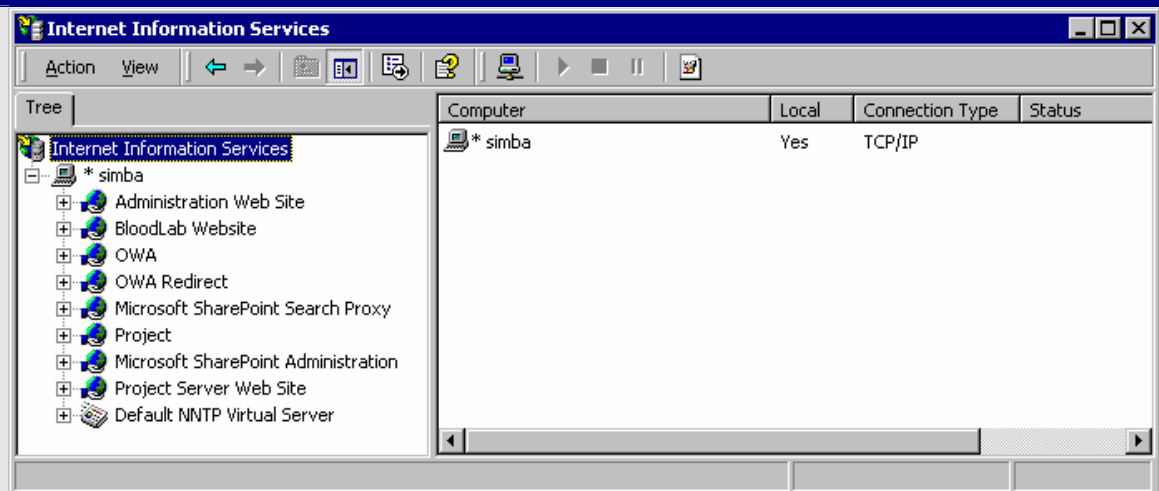
IIS 2.13 Service Account Permissions and Rights Part 2



Artifact 19 Services Properties – Log On Tab – Local System Account

Findings	WWW Service uses localsystem account
Recommendation	Replace with a less privileged account

IIS 2.15 Anonymous FTP Accounts Part 1



Artifact 20 Internet Information Services – MMC Plug-in

Findings	FTP Sites not defined
Recommendation	None, Passed.

IIS 2.15 Anonymous FTP Accounts Part 2

Internet Information Services Lockdown Wizard

Internet Services
Services that are already selected are recommended for this server template.

Select the Internet services to enable on this server. Services not selected will be disabled.

☒ **Web service (HTTP)**
This service uses HTTP to respond to Web client requests on a TCP/IP network.

☐ **File Transfer service (FTP)**
This service supports the creation of File Transfer Protocol (FTP) sites used to transfer files to and from the Internet.

☐ **E-mail service (SMTP)**
This service uses the Simple Mail Transfer Protocol (SMTP) to send and receive e-mail messages.

☐ **News service (NNTP)**
This service uses the Network News Transport Protocol.

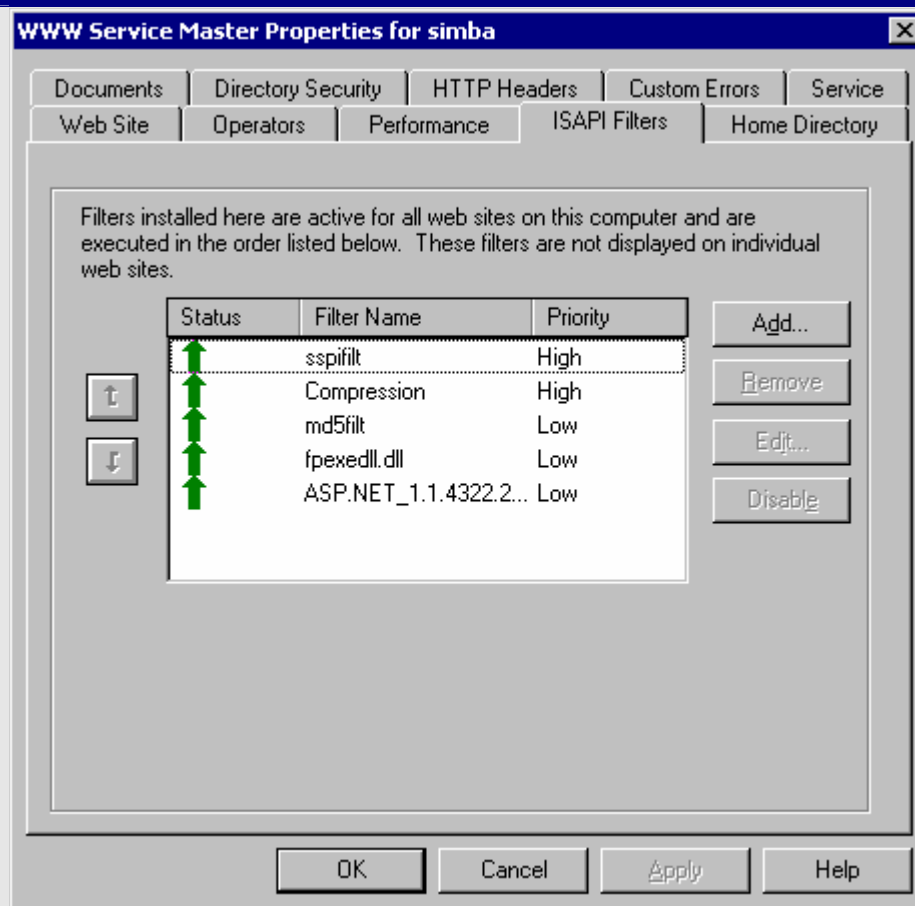
☐ **Remove unselected services**

< Back Next > Cancel Help

Artifact 21 IIS Lockdown Tool Services Template

Findings	FTP Service Not Installed
Recommendation	None, Passed.

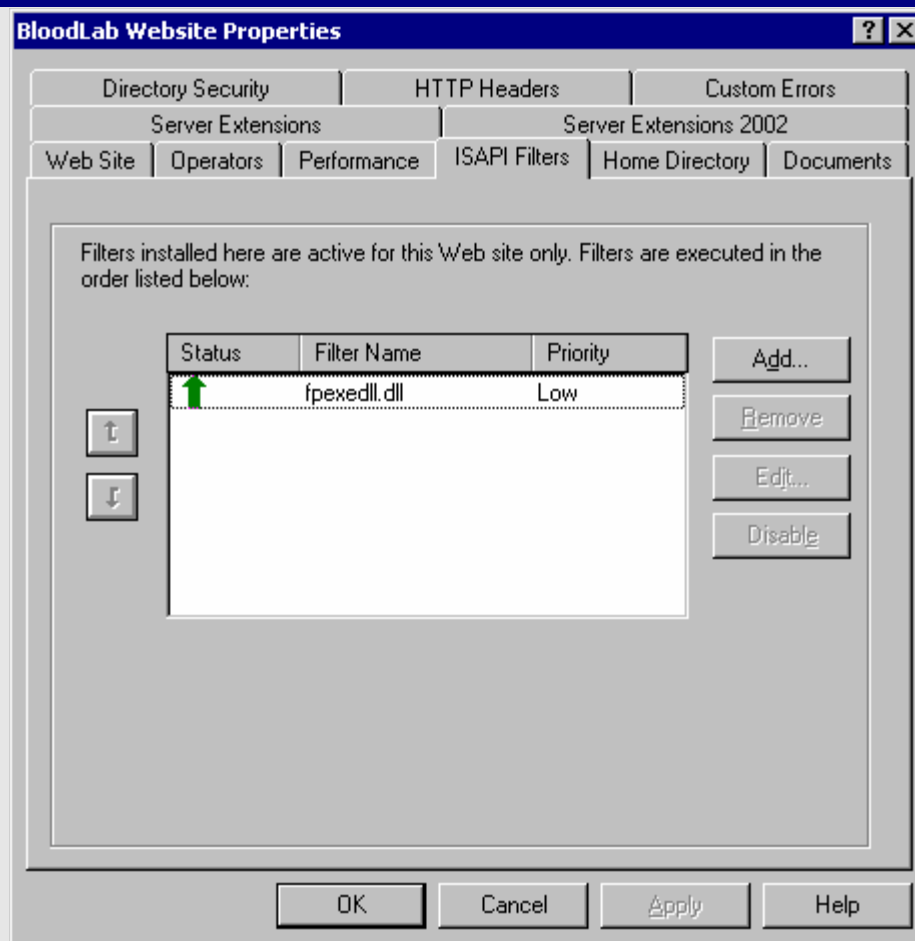
IIS 2.16 Install URLSCAN For Traffic Filtering Part 1



Artifact 22 IIS Master WWW Property Sheet for ISAPI

Findings	URLSCAN is probably not in use, it is not listed in the Master WWW Properties..
Recommendation	Check Local Web Site ISAPI Filter List

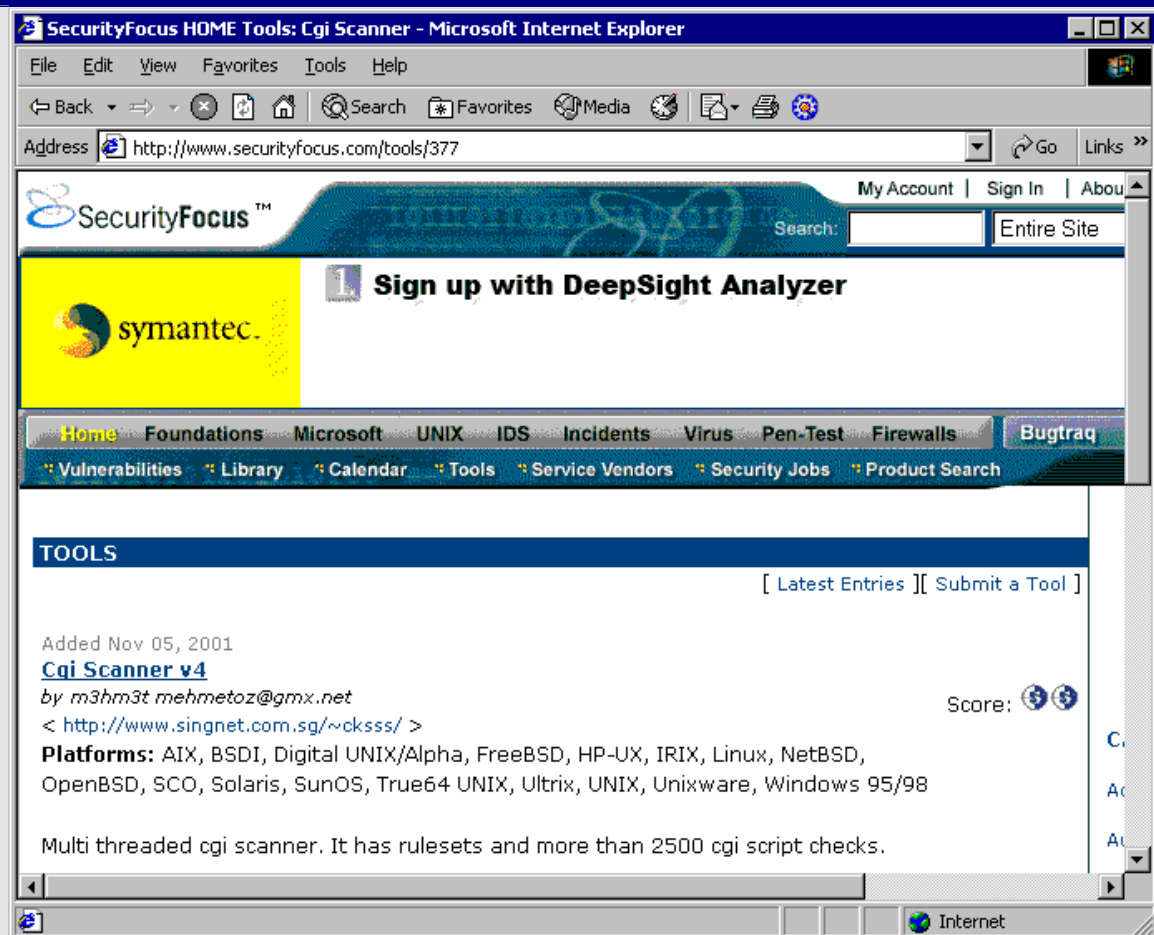
IIS 2.16 Install URLSCAN For Traffic Filtering Part 2



Artifact 23 Web Site Local Property Sheet for ISAPI

Findings	No ISAPI Filters listed. URLSCAN not installed.
Recommendation	Install URLSCAN

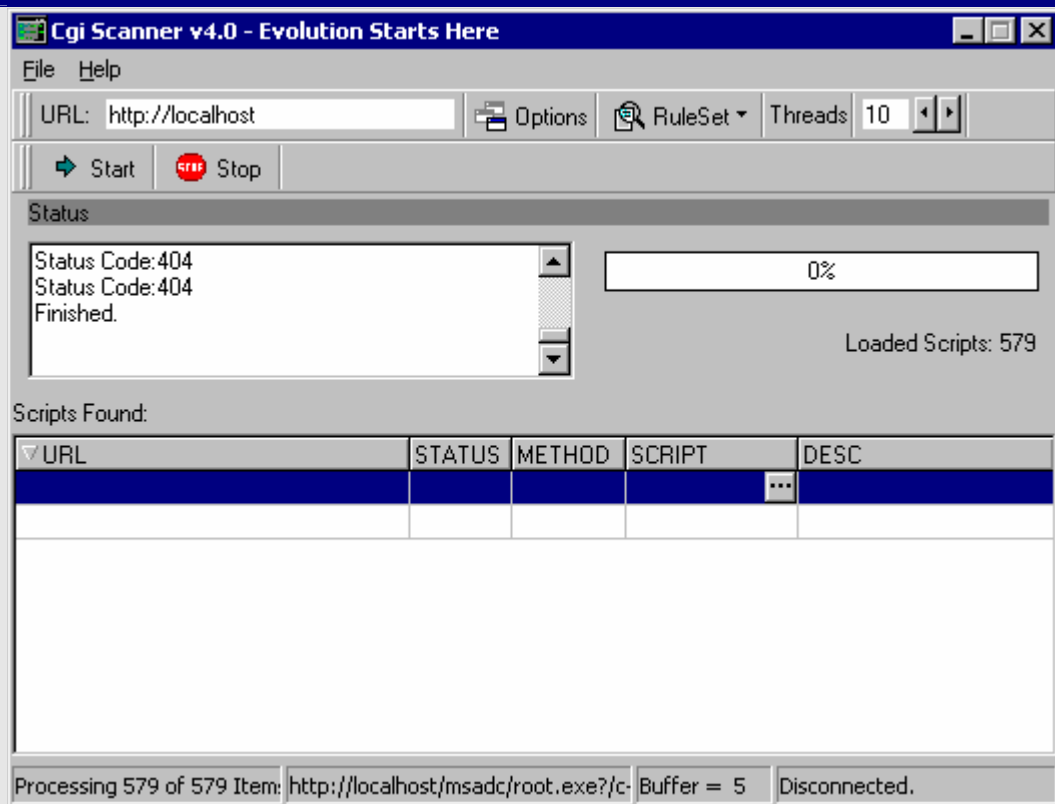
IIS 2.17 Unused Script Mappings Should be Removed Part 1



Artifact 24 Download of Tool CGI Scanner V4

Findings	Use of open source, and freeware hacking tools will help us send some test data to the IIS web server. To test some of the mappings, I will use a tool called CGI Scanner V4.
Recommendation	Find good tools that work for you,

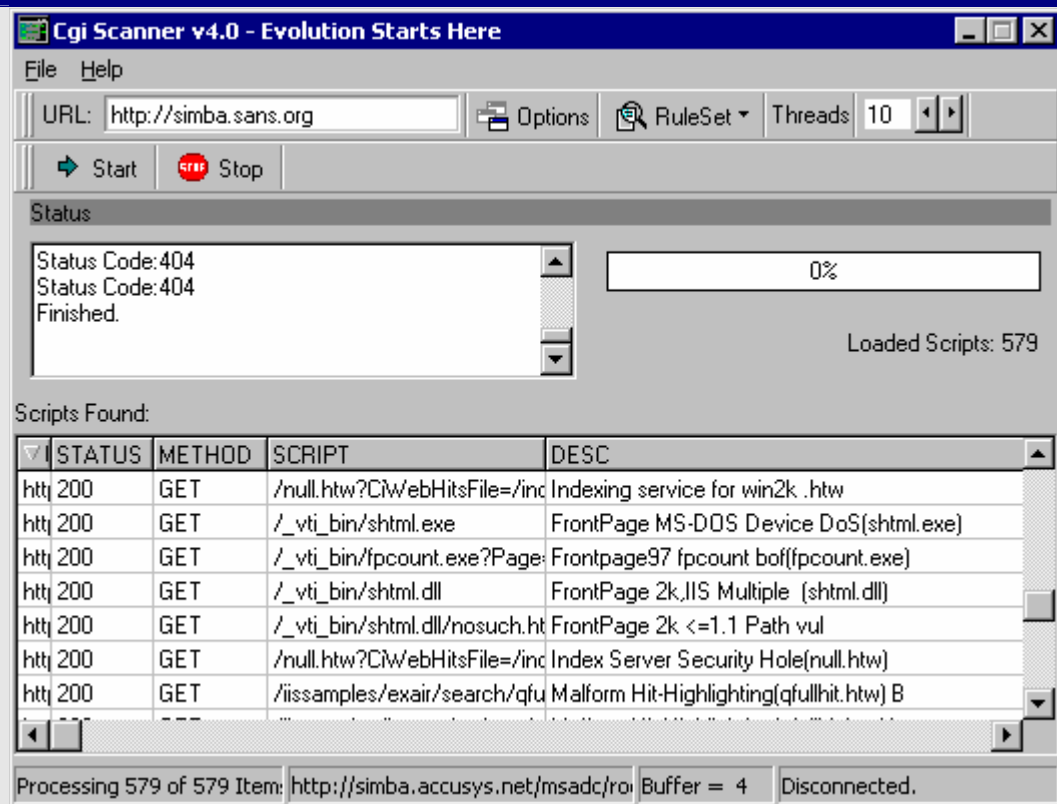
IIS 2.17 Unused Script Mappings Should be Removed Part 2



Artifact 25 CGI Scanner 4.0 – Using localhost

Findings	Running against local host does not provide much help. When we look at the entire web site there are many web sites and they probably use different ports than 80 and some may even use host headers.
----------	---

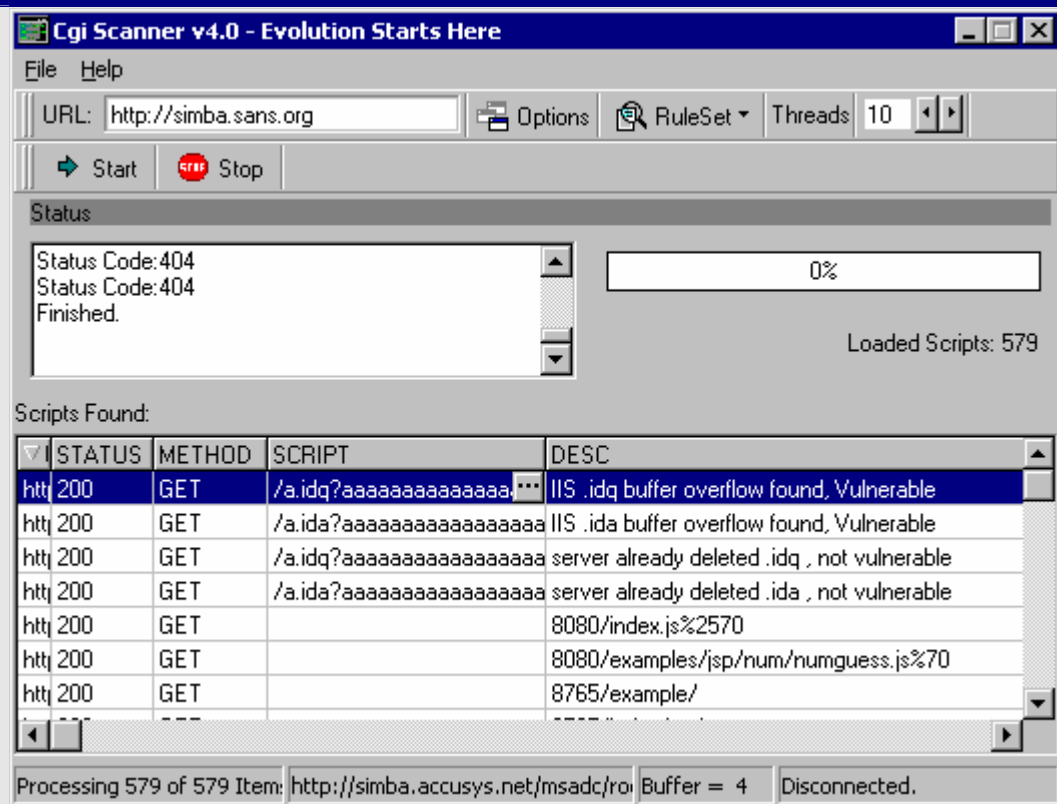
IIS 2.17 Unused Script Mappings Should be Removed Part 3



Artifact 26 CGI Scanner V4.0 Scanning the Website

Findings	Using a Simba URL, we get some successful (code 200) responses.
----------	---

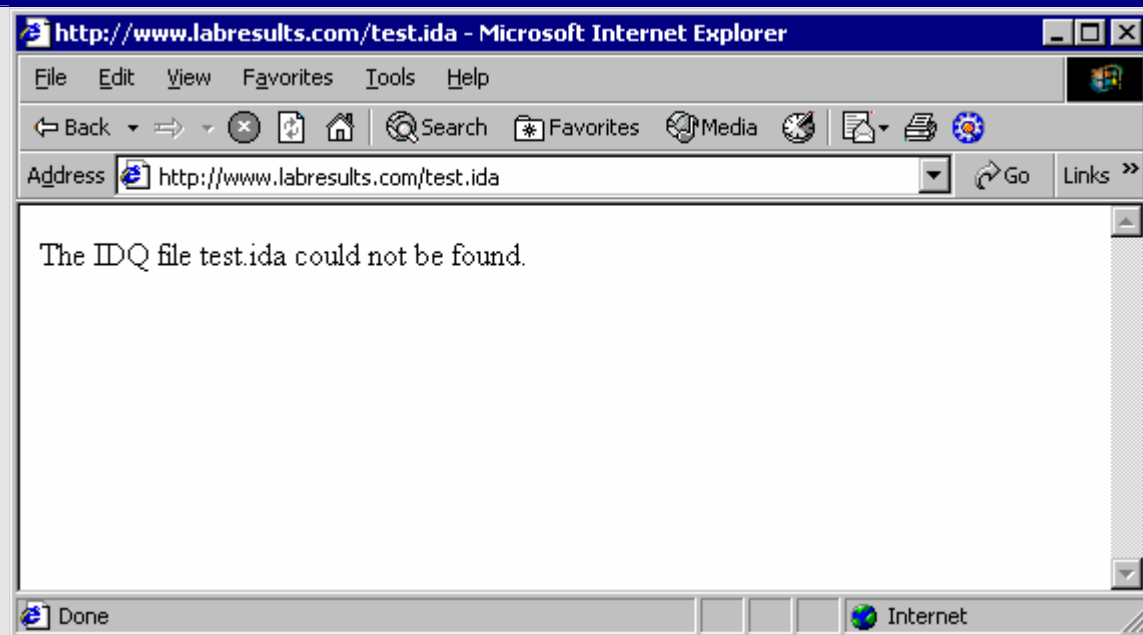
IIS 2.17 Unused Script Mappings Should be Removed Part 4



Artifact 27 CGI Scanner – Scan of SIMBA

Findings	Scanner shows successful (code 200) on commands using extensions of .ida and .idq. Although the reported buffer overflow is not true, there is enough indication that potentially dangerous mappings are in effect.
Recommendation	Mappings should be removed, remapped, or URLSCAN installed and configured to filter these extensions.

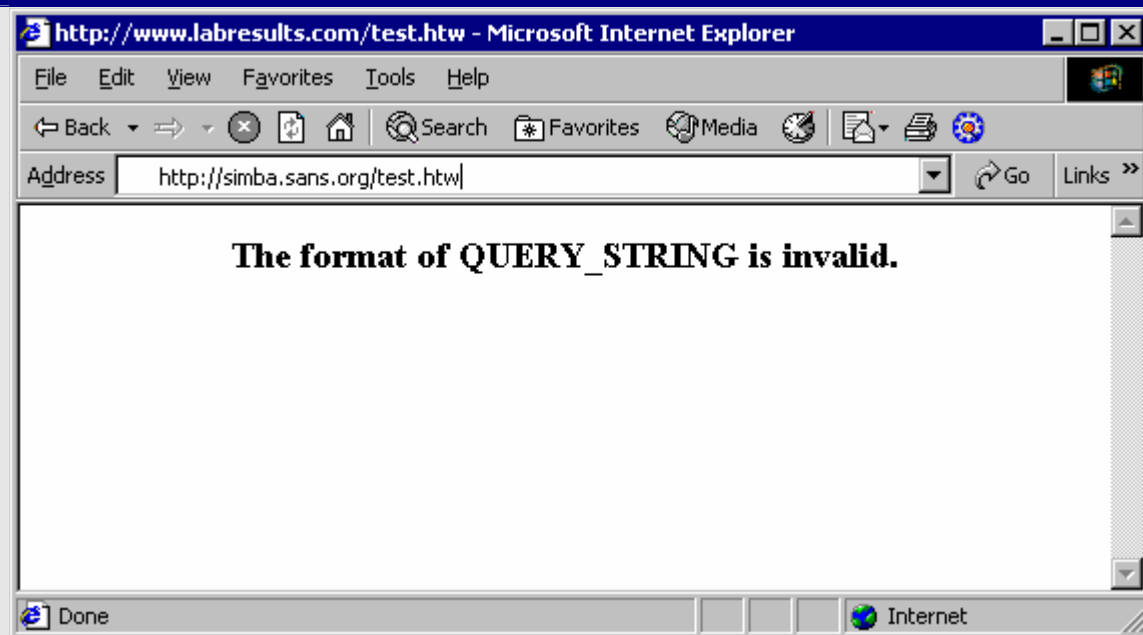
IIS 2.17 Unused Script Mappings Should be Removed Part 5



Artifact 28 Test of IDA scripting extension mapping.

Findings	<p>The CGI scanner is easier, but you could just try the raw command yourself.</p> <p>Here, we did not get a 404 page. We got a response. Files ending with .ida may get processed.</p>
Recommendation	<p>Mappings should be removed, remapped, or URLSCAN installed and configured to filter these extensions.</p>

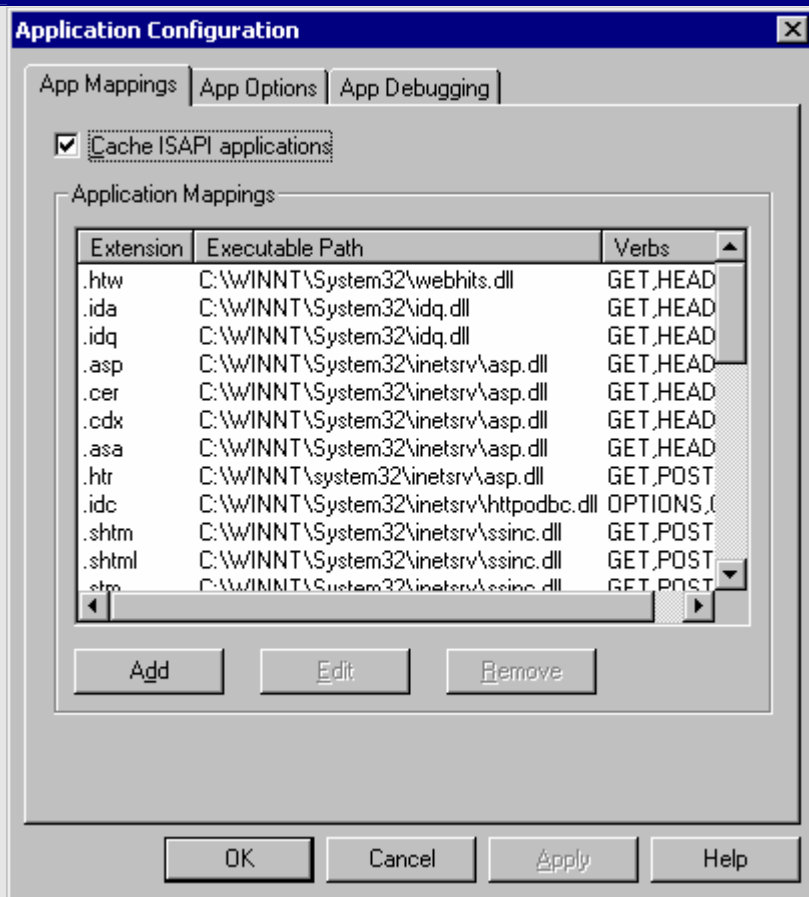
IIS 2.17 Unused Script Mappings Should be Removed Part 6



Artifact 29 Test of HTW scripting extension mapping.

Findings	<p>The CGI scanner is easier, but you could just try the raw command yourself.</p> <p>Here, we did not get a 404 page. We got a response. Files ending with .htw may get processed.</p>
Recommendation	<p>Mappings should be removed, remapped, or URLSCAN installed and configured to filter these extensions.</p>

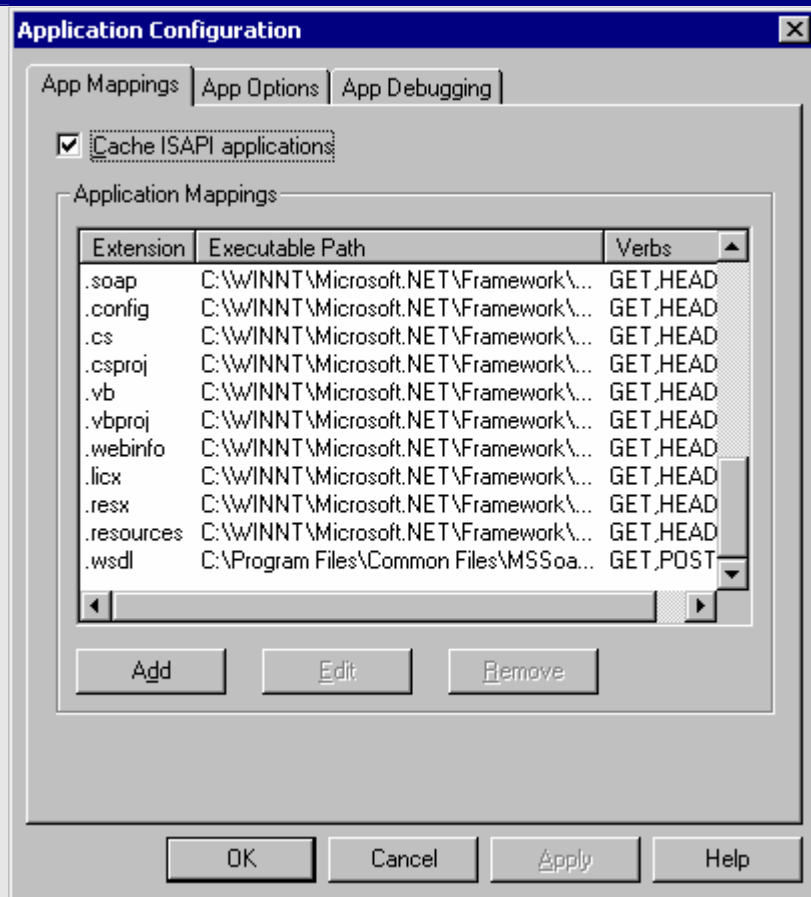
IIS 2.17 Unused Script Mappings Should be Removed Part 7



Artifact 30 Inspection of Script Mappings Part A

Findings	Visual inspection shows the mappings that are active. HTW, IDA, IDQ, and others are active.
Recommendation	Mappings should be removed, remapped, or URLSCAN installed and configured to filter these extensions.

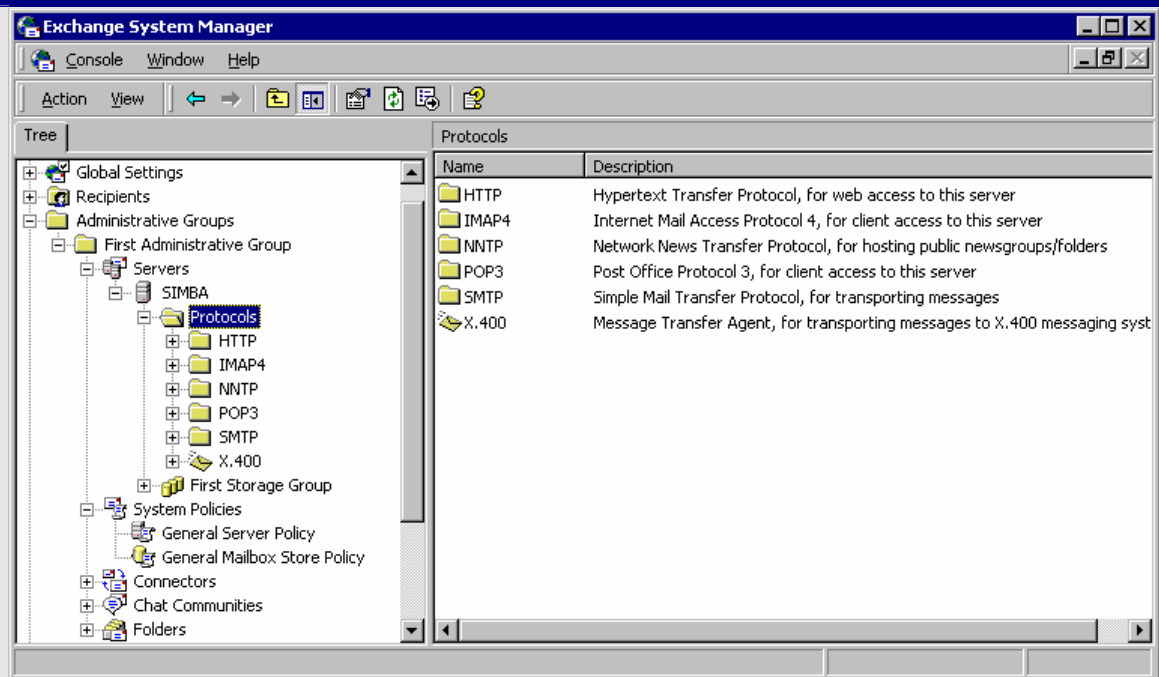
IIS 2.17 Unused Script Mappings Should be Removed Part 8



Artifact 31 Inspection of Script Mappings Part B

Findings	Additional mappings introduced by the Microsoft.NET framework are installed.
Recommendation	None at this time. These mappings should be checked to see if they are all required, and if any can be removed, it should be considered.

IIS 2.18 SMTP Open Relay Should be Restricted



Artifact 32 Display of Exchange 2000 Services

Findings	<p>SMTP was moved from IIS to Exchange as part of the Exchange 2000 Install. Not seen is that there are two virtual SMTP servers, one requiring authentication (relay server) and one that uses anonymous authentication (incoming mail).</p> <p>This test will be skipped and the Exchange 2000 audit will cover this.</p>
Recommendation	<p>None. Skipped, and should be covered in the Exchange 2000 audit.</p>

Summary Matrix

The following table summarizes the 18 Checklist Items.

Checklist Item	P/F	Severity ¹⁶⁰
IIS 2.1 Service Packs and Security Updates	P	High
IIS 2.2 File System Should be NTFS	P	High
IIS 2.3 IIS Should Not be Installed on Domain Controller	F	Medium
IIS 2.4 IIS Lockdown Tool	F	Medium
IIS 2.5 IIS Sample Applications Should be Removed	F	High
IIS 2.6 IISADMPWD Virtual Directory	P	Medium
IIS 2.7 IIS Parent Paths	F	High
IIS 2.8 MSADC and Scripts Virtual Directories on IIS	F	High
IIS 2.9 IIS Logging Should be Enabled	P	Low
IIS 2.10 Remove or Disable Unnecessary Services	F	High
IIS 2.11 Directory Browsing	P	High
IIS 2.12 IUSR_computername Permissions and Rights	F	Medium
IIS 2.13 Service Account Permissions and Rights	F	Medium
IIS 2.14 IP Forwarding	N/A	High
IIS 2.15 Anonymous FTP Accounts	P	Low
IIS 2.16 Install URLSCAN For Traffic Filtering	F	Low
IIS 2.17 Unused Script Mappings Should be Removed	F	Critical
IIS 2.18 SMTP Open Relay Should be Restricted	N/A	Medium

Table 3-1: Summary Table

P/F Column

P – Pass

F – Fail

N/A – test was not performed

¹⁶⁰ Severity is a subjective assessment of the criticality of the failed item, and determined by taking into account the risk in relation to the targeted organization. Its purpose is to aid in prioritizing the order of remediation and resolution.

SECTION 4: RISK ASSESSMENT

4.1 Executive Summary

Evaluation of BloodLab's corporate assets, as described in Section **1.2.1 Assets At risk** can be divided into a quadrangle of likelihood vs. magnitude. Figure 4.2 shows a mapping of BloodLab's 13 identified assets.

The main assets at risk, which include the Brand, Customer Support (CS), Patient Records (PR) and the Laboratory License (LIC) fall into the Likely / High quadrant. Security controls in this quadrant can be technical, but heavily rely on Procedural and Training. These assets are the most critical as each one standing by itself could determine whether the business will survive or go into bankruptcy. The integrity of patient records could literally mean life or death, and the confidentiality of patient records requires compliance with regulatory laws.

By indicating that one main control in this quadrant is procedural is an indication of the main threat being personnel, and a high probability of the threat being insider. Although BloodLab maintains a staffing that is medical oriented and not computer savvy, it doesn't take a computer genius to use the computer to manipulate the system. In a joint study of the Secret Service's National Threat Assessment Center and the CERT/CC of Carnegie Mellon University's Software Engineering Institute, "Most incidents required little technical sophistication. Only 23 percent of perpetrators held technical positions, and 87 percent of the incidents used only simple, legitimate user commands"¹⁶¹.

Symantec quotes a survey (2003 Computer Crime and Security Survey) jointly released by the Computer Security Institute and the FBI, "that 62% of the number of respondents reported a security incident involving an insider"¹⁶². The article then indicated that the first action item is to "Create an effective security policy".

4.1-A Assets at Risk / Risk Management

Quadrant	Type Of Control
Unlikely / Low	Acceptance
Unlikely / High	Financial/Insurance
Likely / Low	Technical
Likely / High	Procedural/Training

Figure 4-1: Mitigating Controls for Likelihood/Cost Quadrants

¹⁶¹ Government Computer News – GCN.COM. Jackson, William. Secret Service and CERT analyze insider threats August 26, 2004

URL: <http://www.gcn.com/vol1_no1/daily-updates/27074-1.html>

¹⁶² Symantec Small Business Website. Protect Yourself from Insider Threats.

URL: <<http://www.symantec.com/smallbiz/library/insider.html>>

4.1-B Assets at Risk Likelihood/Cost

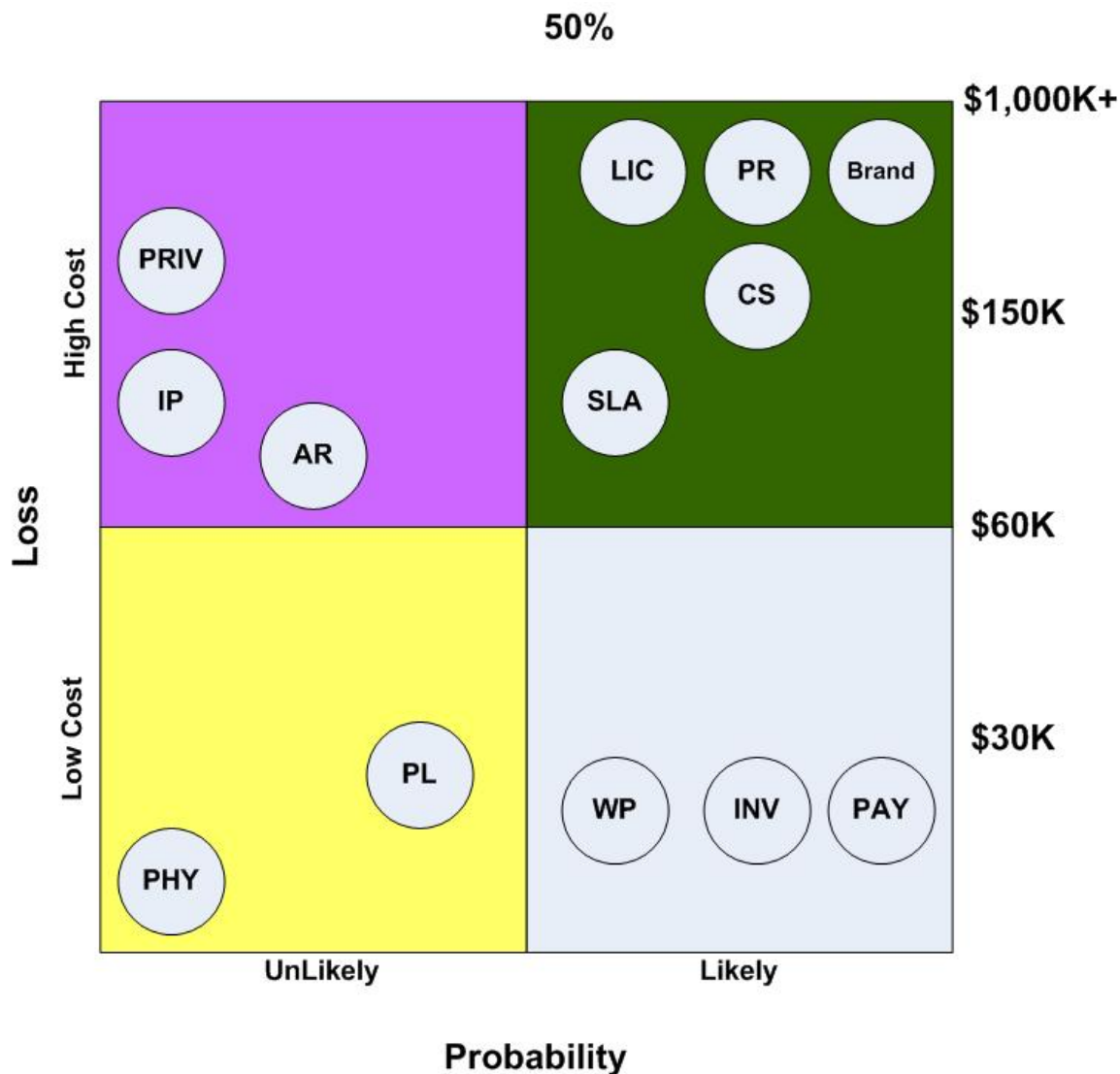


Figure 4-2 – Likelihood/Costs for Assets at Risk

The vulnerability assessment that was requested had a scope and goals of reviewing technical controls, specifically the configuration of the IIS component of the main web server. This would provide a measurement of the existing condition compared to the desired state. That desired state, the state where the measurement “bar” has been set, is determined by the security policy. Without a security policy, the desired state cannot be determined.

Before presentation of the technical findings, the following is a procedural recommendation:

Development of an Information Protection Program

At a minimum, the following needs to be established:

- A person responsible for security, whether it be a CSO, CISO or a VP/Director of Security
- Written Security Policy, Based on an ISO17799/BS7799 Standard
- Security Awareness Program
- Incident Response Team

Being a small to medium size company (staffing at 100+), the costs of the above program may be relatively substantial. A major reason for this assessment is due to startup costs since none of the above elements exist today for BloodLab. However, BloodLab may be forced to move forward just to achieve compliance with HIPAA.

- A security professional, with the above skills and the skills to take care of the technical details, with benefits and training will run \$100K-\$150K per year.
- A written security policy will vary in cost based on how customized the policy is required to be. There are ready-made policies available¹⁶³ that can be used as-is, or may be customized as needed. These “fill-in” forms offerings run from \$200 to \$1,000. I recommend finding one of these ready-made policies that is geared for the medical field and can match compliance with HIPAA regulations. I’d estimate an additional 120 man hours (3 man weeks) to review, update, and publish the final document. At \$50/Hour and \$1K for the ready-made materials, the cost is \$7K
- Security awareness program is also costly, but also depends on how much you want to do. The program cannot commence until the written policy is approved by senior management and published. There are companies that can aid in the building and development of such a program. There are even government programs¹⁶⁴ that can be tailored, used and followed. Preparation of a simple program, including materials, and loss of employee use (while in class salary is being paid but laboratory work is not being done) can be done for \$100 per employee,

¹⁶³ One example is the RUSecure URL: <<http://www.information-security-policies.com/>>

¹⁶⁴ United States. National Institute of Standards and Technology. Wilson, Mark and Hash, Joan. NIST SP800-50 Building an Information Technology Security Awareness and Training Program October 2003. URL: <<http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf>>

assuming a half day class of 3-4 hours. For 100 personnel, that is a cost of \$10,000.

- Assembling an Incident Response Team, which would consist of selected current employees, will also vary, based on the responsibilities and technical expertise of the team. For a team of 5 people, meeting 5 hours per month, at a blended rate of \$50/Hour is \$15K per year. This would only cover minor incidents and security alerts.

Summary Annual Costs to Generate a Information Security Program

Action Item	Annual Cost
Dedicated Security Professional	\$150,000
Written Security Policy	\$7,000
Security Awareness Program	\$10,000
Incident Response	\$15,000
	\$182,000.00

Table 4-1 Estimated Cost for Security Program Startup

Note: Costs may and will vary, based on the commitment to information security and the resources available. The above table is only to give one possible scenario at achieving an information security program.

4.2 Audit Findings

4.2.1 Audit Objectives

This is a technical vulnerability assessment of the IIS component of Windows 2000. The target server is the web server hosting the Laboratory Information System (LIS) of BloodLab Inc. The objective of this audit is to determine insecure settings in the IIS configuration and to provide recommendations on how to improve the security of the target.

4.2.2 Audit Scope

The audit will only focus on this one single server and its IIS configuration. Out of scope includes all network components including firewalls, switches and routers, the Operating System and Application Layers of the server, Physical security of the server, and any other installed applications residing on the target server.

4.2.3 Audit Checklist Result Summary

The following checklists represent the findings of the technical audit, the audit of the IIS configuration.

Checklist Items That Passed

Checklist Item – Passing Items
IIS 2.1 Service Packs and Security Updates
IIS 2.2 File System Should be NTFS
IIS 2.6 IISADMPWD Virtual Directory
IIS 2.9 IIS Logging Should be Enabled
IIS 2.11 Directory Browsing
IIS 2.15 Anonymous FTP Accounts

Table 4-2 Passing Checklist Tests

Checklist Items That Did Not Pass

Checklist Item – Failing Items	Severity
IIS 2.17 Unused Script Mappings Should be Removed	Critical
IIS 2.5 IIS Sample Applications Should be Removed	High
IIS 2.7 IIS Parent Paths	High
IIS 2.8 MSADC and Scripts Virtual Directories on IIS	High
IIS 2.10 Remove or Disable Unnecessary Services	High
IIS 2.16 Install URLSCAN For Traffic Filtering	Low
IIS 2.3 IIS Should Not be Installed on Domain Controller	Medium
IIS 2.4 IIS Lockdown Tool	Medium
IIS 2.12 IUSR_computername Permissions and Rights	Medium
IIS 2.13 Service Account Permissions and Rights	Medium

Table 4-3 Failing Checklist Tests

The following pages will examine each of the “Did not pass” items in table 4-3, explaining the results and remediation costs associates to each checklist item.

4.3 Recommendations and Costs Detail

An interview process was performed with both the CEO and the Senior Software Developer. The interview was conducted after the audit but before developing the following recommendations. This provided a point of input from the client to allow more precise recommendations based on the needs of the organization. The information that was provided during the interview process will be noted in *italics*.

IIS 2.17 Unused Script Mappings Should be Removed

Interview:

“With the exception of the .asp mappings, we are not aware of any other script mapping that is required. We believe that these can be removed without breaking the application”

Findings:

Many unused script mappings were in effect. These mappings pose a threat because some of them have been used in the past to breach IIS. Determined from inspection of IIS mappings and independent testing using crafted URL's.

Recommendation:

Use IIS Lockdown Tool to remove script mappings, other than .asp.

Estimate: 1 Hr @ \$50/Hr **[\$50]**

IIS 2.5 IIS Sample Applications Should be Removed

Interview:

“The IIS Sample Applications and IIS Remote Admin Website are not being used, and they are not part of the application. We believe that these can be removed without breaking the application”

Findings:

The IIS Sample Application Virtual Directory and IIS Remote Admin Website were installed. These pose a threat because the sample applications are well known by the hacking community and can be exploited to compromise the server. Remote Administration poses a threat because a breach of the admin functionality would allow a hacker to reconfigure the entire IIS server to his/her liking. Determined from the MSBA report and visual inspection of the website properties by using the IIS Manager.

Recommendation:

Use IIS Lockdown Tool to remove script mappings, other than .asp. *For Step-by-Step instructions for removal without using IIS Lockdown, see Appendix A – 5324.*

Estimate: 1 Hr @ \$50/Hr **[\$50]**

IIS 2.7 IIS Parent Paths

Interview:

“We do not yet know the impact of disabling parent paths. The application code will require a code review and possible changes”

Findings:

Parent paths are enabled on many of the websites. The ability to use parent paths to navigate the directory tree may expose data or code that should not be access or executed. Determined from the MSBA report.

Recommendation:

Remove Parent Paths by hand. Application code should be evaluated and tested to insure that this will work. *For Step-by-Step instructions for removal without using IIS Lockdown, see Appendix A – 5326.*

Estimate: 2 Hr @ \$50/Hr, including testing **[\$100]**

Estimate: 26Hr @ \$50/Hr, including coding changes and testing. **[\$1300]**

IIS 2.8 MSADC and Scripts Virtual Directories on IIS

Interview:

“The Scripts Virtual Directory is empty and not used by the application. MSADC may be required because MS SQL is in use. The application code will require a code review and possible changes”

Findings:

The Scripts and MSADC virtual directories are installed. These directories are similar to sample directories and are well known and documented. The installation of these virtual directories poses a threat where a hacker can exploit code in these directories to compromise the IIS server. Determined from MSBA report.

Recommendation:

Remove Scripts Virtual Directory. *For Step-by-Step instructions for removal without using IIS Lockdown, see Appendix A – 5327.*

Estimate: 1Hr @ \$50/hr **[\$50]**

Evaluate MSADC requirement, remove if not needed

Estimate: 4Hr @ \$50/hr **[\$200]**

IIS 2.10 Remove or Disable Unnecessary Services

Interview:

"It was never our intention to make Simba an Exchange Mailbox server. This was forced as a temporary solution because the old Exchange server hardware was constantly failing. We already have a server built and ready to go to move the Exchange Mailbox functionality"

"Network News Transmission Protocol (NNTP) was never installed on Simba. When we needed to add Exchange, NNTP was a prerequisite requirement. We do not need nor use NNTP"

"We had a design where Project 2003 and SharePoint Portal Services 2003 would be used, and would require external access. However, that functionality did not work out for us, although we may wish to revisit the use of those products in the future. They are not being used, and if need be, can be removed from Simba"

Findings:

Network News Transmission Protocol, SharePoint Portal Services, and Project Server 2003, were discovered as installed on this IIS server. Outlook Web Access (OWA) was also installed, but was expected and may be required. Services that do not require external access should be moved to another server. Simba was also discovered to be a Mailbox server, and in this configuration probably should be a Front-End server. Discovered from MSBA reports, different sections.

Recommendation:

Remove NNTP, Remote Admin Website, SharePoint Portal Services and Project Server 2003. If needed, SharePoint Portal Services or Project Server 2003 should be installed onto a different physical server. Estimate does not include redeployment, only uninstall. *For Step-by-Step instructions for removal without using IIS Lockdown, see Appendix A – 53116.*

Estimate: 8 Hours @ \$50/Hr [**\$400**]

Mailboxes should be moved to new Exchange Mailbox server, Simba to be changes to a Front-End server.

Estimate: 48 Hours @ 50/Hr [**\$2400**] including removal of all other unnecessary services.

IIS 2.16 Install URLSCAN For Traffic Filtering

Findings:

URLSCAN utility was not installed. Although not necessary, this utility can provide substantial control to mitigate other findings by filtering the HTTP traffic. Determined from inspection of installed ISAPI filters, lack of URLSCAN install directory and lack of URLSCAN logs.

Recommendation:

Install and customize URLSCAN.

Estimate: 4 Hours @ \$50/Hr [**\$200**] if URLSCAN requires minor configuration changes.

Estimate: 16 Hours @ \$50/Hr [**\$800**] if major configuration changes and testing is required.

IIS 2.3 IIS Should Not be Installed on Domain Controller

Interview:

“We already have at least four domain controllers, and didn’t realize that Simba was also one. The application does not depend on being resident on a domain controller”

Findings:

The IIS server is also a domain controller. Determined from MSBA report.

Recommendation:

Run DCPROMO, remove Simba as a Domain Controller.

Estimate: 4 Hours @ \$50/Hr [**\$200**]

IIS 2.4 IIS Lockdown Tool

Findings:

IIS Lockdown Tool was never used to harden this IIS server. Determined from MSBA report.

Recommendation:

Run IIS Lockdown Tool, using the Exchange template. Remove sample programs and virtual directories as per previous recommendations.

Estimate: 4 Hours @ \$50/Hr [**\$200**] Time for evaluation and testing is included in other estimates.

IIS 2.12 IUSR_computername Permissions and Rights

Findings:

Found excessive permissions on the IUSR and IWAM user accounts. These accounts were members of the Domain Users Global Security Group. Determined from visual inspection using Administrator Tools – Active Directory Users and Computers.

Recommendation:

Remove IUSR and IWAM accounts from Domain Users Global Security Group.

Estimate: 1 Hours @ \$50/Hr [**\$50**] to remove from global groups.

Estimate: 16 Hours @ \$50/Hr [**\$800**] to remove from global groups and change ACL permissions to minimum required (“Least Privilege”).

IIS 2.13 Service Account Permissions and Rights

Findings:

IIS running under “localsystem” account. Account may possess more permission than necessary for running IIS. The threat is that a hacker who compromises IIS would own the server quicker, with less need to escalate privileges. Determined from inspection of the Services MMC snap in.

Recommendation:

Leave the “localsystem” account setting for now. Any adjustment at this time may be excessive. Adjusting this value without breaking IIS may be difficult.

4.4 Recommendations and Costs Summary

Cost to remediate failed checklist items

Checklist Item – Failing Items	Cost
IIS 2.17 Unused Script Mappings Should be Removed	\$50
IIS 2.5 IIS Sample Applications Should be Removed	\$50
IIS 2.7 IIS Parent Paths	\$100-\$1300
IIS 2.8 MSADC and Scripts Virtual Directories on IIS	\$50-\$200
IIS 2.10 Remove or Disable Unnecessary Services	\$400-\$2400
IIS 2.16 Install URLSCAN For Traffic Filtering	\$200-\$800
IIS 2.3 IIS Should Not be Installed on Domain Controller	\$200
IIS 2.4 IIS Lockdown Tool	\$200
IIS 2.12 IUSR_computername Permissions and Rights	\$50-\$800
IIS 2.13 Service Account Permissions and Rights	\$0

Table 4-4 Estimated Cost for Failing Checklist Items

4.5 Long Term Recommendation

A substantial effort may be required to fix current problems and issues. However, a program needs to be put into place to insure that whatever changes are made to resolve those problems and issues remain fixed, and that future new deployments occur in a safe manner.

Server building should be standardized for both internal and external servers. By developing a set of documentation that contains Standard Server Build & Hardening procedures, Standard Operating Procedures, and Hardening Templates, servers may be built in a secure manner for future servers to be deployed.

A self audit program, using vulnerability scanning software, should be developed for self assessment. A quarterly assessment/audit will periodically measure policy compliance and help insure that once the servers are secured, they remain secured.

Implementation of change control procedures for server build and deployment is required. Use of change control will provide a “gate” function where deployment of new servers can be controlled. At the point of change control, it can be established whether the server was properly built to standards, and deficiencies rectified before proceeding with the deployment.

4.6 Additional Controls

The installation and use of URLSCAN will provide a filter and help reduce the attack surface. Possible exploits may be detected and averted before reaching application code.

Implementation of intrusion detection on the network level, with analysis of the logs, may alert BloodLab of scanning and probing activity, which is usually a precursor to an attack. Open source solution such as Snort can be used, but there will still be costs for hardware and personnel to analyze the logs.

Conversion of the firewall configuration from a dual-homed to a tri-homed configuration, placing the external Internet facing servers in a screened network (DMZ) will provide the ability to better protect the critical servers.

Additional ports on the firewall should be blocked. Currently an optimistic firewall configuration is in use where only certain ports are blocked while all others are open. BloodLab should convert to a pessimistic firewall configuration, where all ports are closed unless explicitly open, as this will provide for a more secure DMZ.

REFERENCES

Bragg, Roberta.

Hardening Windows Systems. Emeryville: McGraw Hill/Osborne, 2004, (ISBN: 0-07-225354-1)

Bragg, Roberta.

Windows 2000 Security. Indianapolis: New Riders Publishing, 2001 (ISBN: 0-7357-0991-2)

California State Senate

Official California Legislative Information Bill Information

URL: <http://info.sen.ca.gov/cgi-bin/postquery?bill_number=sb_1386&sess=PREV&house=B&site=sen>

Centers for Medicare & Medicaid Services

URL: <<http://www.cms.hhs.gov/hipaa/>>

CERT/CC Website.

CERT® Advisory CA-2001-12 Superfluous Decoding Vulnerability in IIS. May 15, 2001.

URL: <<http://www.cert.org/advisories/CA-2001-12.html>>

CERT/CC Website.

CERT® Advisory CA-2001-26 Nimda Worm. Revised September 2001.

URL: <<http://www.cert.org/advisories/CA-2001-26.html>>

Commonwealth Agency of the Australian Government

Website and Internet System Security Checklist V1.1 Dec 2003 URL:

<http://www.agimo.gov.au/data/assets/file/9043/security_checklist.pdf>

Garfunkel, Wild & Travis, P.C. New York Health Law Update, Jan 2002

URL: <<http://www.gwtlaw.com/gwt/healthlawjan2002.html>>

GlobalScape Website.

URL: <<http://www.globalscape.com/gsftps/>>

Government Computer News – GCN.COM.

Jackson, William. Secret Service and CERT analyze insider threats August 26, 2004

URL: <http://www.gcn.com/vol1_no1/daily-updates/27074-1.html>

HIPAA Complete

Avoid HIPAA non-compliance penalties

URL: <<http://www.hipaacomplete.com/penalties.asp>>

Internet Security Systems.

Microsoft Windows 2000 Security Technical Reference. Redmond: Microsoft Press, 2000 (ISBN: 0-7356-0858-X)

IPSWITCH Website

WS FTP Server Homepage

URL: <http://www.ipswitch.com/products/WS_FTP-Server/index.html>

Krutz, Ronald L. and Vines, Russell Dean.
The CISSP Prep Guide – Mastering the Ten Domains of Computer Security, New York:
Wiley Computer Publishing 2001 (ISBN: 0-471-41356-9)

Maryland Department Of Health and Mental Hygiene Website.
FAQ – Clinical Laboratories.
URL: <<http://www.dhmd.state.md.us/ohca/faq/labfaq.htm#2>>

Microsoft Download Site
Microsoft Baseline Security Analyzer 1.2.1 August 16 2004
URL: <<http://www.microsoft.com/technet/security/tools/mbsahome.msp>>

Microsoft MSDN Website.
Securing Your Web Server. Microsoft Corporation, January 2004
URL: <<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/secmod/html/secmod89.asp>>

Microsoft Security Website.
Checklist: Securing Your Web Server. Microsoft Corporation, January 2004
URL: <<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/secmod/html/secmod104.asp>>

Microsoft Support Site.
Disabling Parent Paths Breaks User Interface.
URL: <<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q288309>>

Microsoft Support Website.
How to Change Windows NT Account Passwords Using Internet Information Server (IIS) 4.0
URL: <<http://support.microsoft.com/default.aspx?scid=kb;en-us;184619>>

Microsoft Support Website.
How to Disable or Remove Unnecessary IIS Services.
URL: <<http://support.microsoft.com/default.aspx?scid=kb;en-us;321141>>

Microsoft Support Website.
How to Enable TCP/IP Forwarding in Windows 2000.
URL: <<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q230082>>

Microsoft Support Website.
SMTP relay behavior in Windows 2000, Windows XP, and Exchange Server
URL: <<http://support.microsoft.com/default.aspx?scid=kb;en-us;304897>>

Microsoft Support Website.
Unchecked Buffer in Index Server ISAPI Extension Could Enable Web Server Compromise.
URL: <<http://www.microsoft.com/technet/security/bulletin/MS01-033.msp>>

Microsoft Support Website.
Unchecked buffer in ISAPI extension could enable compromise of IIS 5.0 server.
URL: <<http://www.microsoft.com/technet/security/bulletin/MS01-023.msp>>

Microsoft TechNet Security Site.
Security Update for Microsoft Windows (835732)
URL: <<http://www.microsoft.com/technet/security/bulletin/MS04-011.msp>>

Microsoft TechNet Security Site.

Buffer Overrun In RPC Interface Could Allow Code Execution (823980)

URL: <<http://www.microsoft.com/technet/security/bulletin/MS03-026.msp>>

Microsoft TechNet Security Site.

Buffer Overruns in SQL Server 2000 Resolution Service Could Enable Code Execution (Q323875)

URL: <<http://www.microsoft.com/technet/security/bulletin/MS02-039.msp>>

Microsoft TechNet Security Site.

Buffer Overrun in JPEG Processing (GDI+) Could Allow Code Execution (833987)

URL: <<http://www.microsoft.com/technet/security/bulletin/ms04-028.msp>>

Microsoft TechNet Security Site.

Microsoft Security Baseline Analyzer (MSBA).

URL: <<http://www.microsoft.com/technet/security/tools/mbsahome.msp>>

Microsoft TechNet Security Site.

Microsoft Security Response Center Security Bulletin Severity Rating System (Revised, November 2002).

URL: <<http://www.microsoft.com/technet/security/bulletin/rating.msp>>

Microsoft Website.

System Management Server (SMS).

URL: <<http://www.microsoft.com/smserver/default.asp>>

Microsoft Website.

Windows Update Services (SUS).

URL: <<http://www.microsoft.com/windowsserversystem/sus/default.msp>>

Mitre CVE Website

CAN-2004-0200

URL: <<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0200>>

NIST/ Computer Security Resource Center (CSRC)

WEB SERVER CHECKLIST Version 4, Release 1.3 Microsoft IIS Server. May 26, 2004

URL: <http://csrc.nist.gov/pcig/CHECKLISTS/web_checklist_052604.zip>

NIST/Computer Security Resource Center (CSRC)

Web Server SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) V5.0. Jul 26, 2004

URL: <<http://csrc.nist.gov/pcig/STIGs/WebV5R0.zip>>

NSA/System and Network Attack Center (SNAC).

Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0, , Oct 29, 2003

URL: <http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/os/win2k/iis_5_v1_4.pdf>

OWASP Website.

The Open Web Application Security Project

URL: <www.owasp.net>

OWASP Website.

OWSAP Top Ten Project

URL: <<http://www.owasp.net/documentation/topten.html>>

Paul, Brooke.

Calculate Your Risk. *Secure Enterprise* Jan 2005: pp: 16-22.

Philip Cox and Tom Sheldon.

Windows 2000 Security Handbook. Berkeley: McGraw Hill/Osborne, 2001, (ISBN: 0-07-212433-4)

Philips, Robert MD.

Laboratory Safety and Quality in Primary Care: Evidence and Revolution

URL: <<http://www.phppo.cdc.gov/mlp/QIConference/Presentations/Phillips-Quality%20Institute.pdf>>

SANS Institute

Audit of a Corporate Security Systems Domain Controller Steve Graham, November 12, 2004

URL: <http://www.giac.org/practical/GSNA/Steven_Graham_GSNA.pdf>

SANS Institute

Auditing a File Server - Microsoft® Windows Server™ 2003 Tamer Eltoni, May 2004

URL: <http://www.giac.org/practical/GSNA/Tamer_Eltoni_GSNA.pdf>

SANS Institute

Auditing a IIS Microsoft Windows 2000 Server Beverly Pfaff, November 11, 2004

URL: <http://www.giac.org/practical/GSNA/Beverly_Pfaff_GSNA.pdf>

SANS Institute

Auditing a Microsoft Windows 2000 Terminal Server William Driskell, January 6, 2005

URL: <http://www.giac.org/practical/GSNA/William_Driskell_GSNA.pdf>

SANS Institute

Steganography In the Corporate Environment Joann Kennedy April 9, 2004

URL: <http://www.giac.org/practical/GSEC/Joann_Kennedy_GSEC.pdf>

SANS Institute

Windows 2000 Security Step By Step Version 1.5, July 1 2001

SANS Institute.

SANS/FBI Top 20 List for Windows, Oct 8, 2004

URL: <<http://www.sans.org/top20/>>

Securiteam Website.

Microsoft IIS Remote Denial of Service Attack.

URL: <<http://www.securiteam.com/windowsntfocus/5BP0C151FU.html>>

Sheridan, John.

Microsoft Windows 2000 IIS 5.0 IPP ISAPI 'Host:' Buffer Overflow Vulnerability. SANS Institute, GCIH Practical. Jun 19, 2001

URL: <http://www.giac.org/practical/David_Sheridan_GCIH.doc>

Smith, Ben, and Komar, Brian.

Microsoft Windows Security Resource Kit. Redmond: Microsoft Press, 2003 (ISBN: 0-7356-1868-2)

SPAMLAWS Website.

CAN-SPAM Act of 2003.

URL: <<http://www.spamlaws.com/federal/108s877.html>>

Staneck, William R.

Microsoft Windows 2000 and IIS 5.0 Pocket Reference. Redmond: Microsoft Press, 2001 (ISBN: 0-7356-1024-X)

STAT – Statim (Latin: immediately [medical]) using Google acronym finder

URL: <<http://www.acronymfinder.com/af-query.asp?String=exact&Acronym=stat&Find=Find>>

Symantec Security Response Website.

W32.Blaster.Worm

URL: <<http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.html>>

Symantec Security Response Website.

W32.Sasser.Worm

URL: <<http://securityresponse.symantec.com/avcenter/venc/data/w32.sasser.worm.html>>

Symantec Security Response Website.

W32.SQLExp.Worm

URL: <<http://securityresponse.symantec.com/avcenter/venc/data/w32.sqlexp.worm.html>>

Symantec Small Business Website.

Protect Yourself from Insider Threats.

URL: <<http://www.symantec.com/smallbiz/library/insider.html>>

Symantec Website.

Symantec Internet Security Threat Report, Volume IV. September 2004.

URL: <<http://enterprisesecurity.symantec.com/content.cfm?articleid=1539>>

Todd, Chad.

Hack Proofing Windows 2000 Server. Rockland: Syngress, 2001, (ISBN: 1-931836-49-3)

United States. National Institute of Standards and Technology.

Engineering Principles for Information Technology Security (A Baseline for Achieving Security) NIST Special Publication SP800-27 June 2001

United States. National Institute of Standards and Technology.

Risk Management Guide for Information Technology Systems NIST Special Publication SP800-30 January 2002.

United States. National Institute of Standards and Technology.

Generally Accepted Principles and Practices for Securing Information Technology Systems NIST Special Publication SP800-14 September 1996

Webopedia Definition.

Steganography

URL: <<http://www.webopedia.com/TERM/S/steganography.html>>

Webopedia Definition.

Warez

URL: <<http://www.webopedia.com/TERM/w/warez.html>>

Website Homepage.

eEye Digital Security. Retina Network Security Scanner.

URL: <<http://www.eeye.com/html/products/retina/index.html>>

Website Homepage.

GFI Languard Network Security Scanner.

URL: <<http://www.gfi.com/languard/>>

Website Homepage.

ServU FTP Server Homepage.

URL: <<http://www.serv-u.com/>>

Website Homepage.

NIST/ Computer Security Resource Center (CSRC) Homepage

URL: <<http://csrc.nist.gov>>

Website Homepage.

Microsoft Developer Network Homepage.

URL: <<http://msdn.microsoft.com/>>

Website Homepage.

eEye Digital Retina Network Security Scanner.

URL: <<http://www.eeye.com/html/products/retina/index.html>>

Website Homepage.

GFI Languard Network Security Scanner.

URL: <<http://www.gfi.com/lannetscan/>>

Website Homepage.

Internet Security Systems Network Security Scanner.

URL:

<http://www.iss.net/products_services/enterprise_protection/vulnerability_assessment/scanner_internet.php>

Website Homepage.

Redmond Magazine (Formerly MCP Magazine) Homepage.

URL: <<http://www.mcpmag.com>>

Website Homepage.

Microsoft Security Homepage.

URL: <<http://www.microsoft.com/security/guidance/default.aspx>>

Website Homepage.

Microsoft TechNet Homepage.

URL: <<http://www.microsoft.com/technet/default.aspx>>

Website Homepage.

Nessus Network Scanner.

URL: <<http://www.nessus.com/>>

Website Homepage.

National Institute of Standards and Technology Homepage.

URL: <<http://www.nist.gov>>

Website Homepage.

National Security Agency.

URL: <<http://www.nsa.gov/snac/>>

Website Homepage.

Harris Software STAT network Scanner.

URL: <http://www.stat.harris.com/solutions/vuln_assess/scanner_index.asp>

Website Homepage.

Sysinternals Homepage.

URL: <<http://www.sysinternals.com>>

Website Homepage.

Windows IT Pro Magazine Homepage.

URL: <<http://www.winntmag.com>>

Website Homepage. ISC²

URL: <<http://www.isc2.org>>

Windows .NET Magazine.

Automatically Audit Access to Files and Folders. June 2003.

URL: <<http://www.windowsitpro.com/Windows/Article/ArticleID/38942/38942.html>>

APPENDIX A – MSBA 1.2.1 Help Messages

Messages from Microsoft Baseline Security Analyzer Version 1.2.1

Help text from the tool are provided in this appendix as a reference.

© SANS Institute 2005, Author retains full rights.



[5311] Service Packs and Security Updates

Check Description

This check determines which available service packs and security updates are not installed on the scanned computer.

Service packs are tested collections of updates that focus on a variety of customer-reported concerns with a Microsoft product. Service packs provide fixes for issues that have been reported after the product has become generally available. They are cumulative, that is, each new service pack contains all the fixes in previous service packs, plus any new fixes. They are designed to ensure platform compatibility with newly released software and drivers, and contain updates that fix issues discovered by customers or by internal testing.

Security updates, on the other hand, are interim updates that usually address a specific bug or security vulnerability. All security updates offered during a service pack's lifetime are combined into the subsequent service pack. Each security update identified by this tool has an associated Microsoft security bulletin that contains more information about the fix. The results of this check identify which security updates are missing, and provides a link to the Microsoft Web site to view the details of each security bulletin.

Microsoft® Baseline Security Analyzer (MBSA) checks to ensure that you have the latest service packs and security updates for the following products and components:

- Microsoft® Windows NT® 4.0, Windows 2000, Windows XP, Windows Server 2003
- Internet Information Server (IIS) 4.0, IIS 5.0, IIS 6.0
- SQL Server™ 7.0, SQL Server 2000 (including Microsoft Data Engine 1.0 and 2000)
- Internet Explorer 5.01 and later
- Windows Media Player 6.4 and later
- Exchange Server 5.5, Exchange Server 2000, Exchange Server 2003 (including Exchange Admin Tools)
- Microsoft Data Access Components (MDAC) 2.5, MDAC 2.6, MDAC 2.7, MDAC 2.8

- Microsoft Virtual Machine (VM)
- MSXML 2.5, MSXML 2.6, MSXML 3.0, MSXML 4.0
- Content Management Server 2001, Content Management Server 2002
- Commerce Server 2000, Commerce Server 2002
- BizTalk® Server 2000, BizTalk Server 2002, BizTalk Server 2004
- SNA Server 4.0, Host Integration Server 2000, Host Integration Server 2004
- Microsoft Office ([View the list of Office products supported in the tool and scanning limitations](#))

This check is performed by using information obtained from Microsoft.com in the form of a signed .cab or .xml file (Mssecure.xml). The tool downloads this information from Microsoft.com each time it is run. If it is not able to contact Microsoft.com, it will use a version of the database cached on the local machine. There is also an option to perform this check against an approved updates list from a local Software Update Services (SUS) server, rather than against the complete list of available updates from Microsoft.com.

Default Settings. Security update scans executed from the Microsoft Baseline Security Analyzer (MBSA) graphical user interface (GUI) or from Mbsacli.exe (MBSA-style scan) will scan and report missing updates marked as critical security updates in Windows Update (WU), also referred to as *baseline* critical security updates. When a security update scan is executed from Mbsacli.exe using the /hf switch (HFNetChk-style scan), all security-related security updates will be scanned and reported. A user running an HFNetChk-style scan can choose to scan for WU critical security updates only, and can suppress notes or warnings, if not desired, through the command-line parameters.

SUS Scan Option. This option will search for missing security updates included in an approved items list on the SUS server, rather than from the full list of available security updates in the Mssecure.xml file from the Microsoft Web site. When this option is selected in the GUI, MBSA attempts to automatically obtain the local SUS server name from the local registry. Otherwise, MBSA will use the SUS server name that is entered by the user. MBSA connects over HTTP to the specified SUS server and reads the Approveditems.txt file to identify security updates that have been explicitly approved by the SUS administrator. MBSA notes the approved security updates and then looks at a mapping table in the Mssecure.xml file to match the SUS security updates to the updates in the XML file. MBSA will then perform the security updates scan based on the selected updates in the Mssecure.xml file, which is mapped to the approved updates on the local SUS server.

Additional Resources

[Microsoft Hotfix and Security Bulletin Service](#)

[Microsoft Strategic Technology Protection Program](#)

[Microsoft Software Update Services](#)

©2002-2004 Microsoft Corporation. All rights reserved.

© SANS Institute 2005, Author retains full rights.



[5311] Service Packs and Security Updates

Issue

To ensure that the most recent security updates are applied, you need to install all of the latest service packs and individual updates on your system.

Solution

The scan report identifies which service packs and security updates are missing on your computer. Users can click the link in the security report to view the Microsoft security bulletin or download page, which includes the install location for the security update. The [Windows Update](#) Web site also has the latest service pack and security update releases available for you to download for the Microsoft® Windows® operating system and its components.

In order to obtain and install the latest updates and to effectively use the MBSA results, please observe these guidelines:

- Register with the [Microsoft Security Notification Service](#) to ensure you are notified when new security bulletins become available.
- When updating your computer, remember that changes in configuration may require additional use of Windows Update or MBSA to check the new configuration for compliance. This is particularly true when installing applications, or adding new optional components such as Internet Information Services (IIS) which may install programs that have not been updated with the latest fixes.
- By clicking on **Result Details** in the report you will be able to identify the update as being under one of the following 3 headings:

Security updates confirmed as missing are marked with a red X

These updates require immediate installation to ensure the strongest security of your computer.

Products using a service pack not at the latest version or have other warnings are marked with a yellow X

Service packs: If the description for an item is “The latest service pack for this product is not installed.”, you should obtain and install the latest service pack by using [Windows Update](#) or the [Microsoft Download Center](#) prior to installing other updates. When using the download center, simply enter the name of the service pack at the Keywords prompt, and follow the instructions on the page.

Updates: Other items in this page will typically have a newer than expected file version and are usually of strong security. Because the installed file(s) having a greater than expected version may have been provided directly from Product Support Services or from an update or product that was not security related, these items may require additional confirmation to ensure the specific security fix has been included. Addressing such items is an ongoing aspect of the release process for Microsoft, and allows MBSA to become updated automatically with understanding of the newer file versions.

Security updates that the tool cannot confirm as installed on the scanned computer are marked with a blue asterisk

These updates cannot be detected with adequate precision due to the complexity of the updates or platform configurations. You should refer to the bulletin details for file versions, registry keys, or the Add or Remove Programs entries to confirm these updates have been installed. Because these updates cannot be exhaustively detected, they will remain in the MBSA results even after you have installed them.

Notes

- Windows Update does not carry non-Windows security updates such as Microsoft® SQL Server™ or Microsoft Exchange updates, and users should view the Microsoft security bulletins for these product security updates using the links provided in the Microsoft Baseline Security Analyzer (MBSA) scan report. Users can also download Microsoft Office security updates from the [Office Product Updates](#) Web site.
- Please visit the following site for details on Office products supported in MBSA 1.2 and scanning limitations: [MBSA Version 1.2 Support for Microsoft Office Products](#).

Customers can also subscribe to the Microsoft Security Notification Service, a free service that sends e-mail messages to users when new security bulletins are released.

Additional Resources

[Microsoft Security Bulletin Search](#)

[Microsoft Strategic Technology Protection Program](#)

[Microsoft Software Update Services](#)

©2002-2004 Microsoft Corporation. All rights reserved.

© SANS Institute 2005, Author retains full rights.

Message 5313 – Description

Printed from Microsoft Security Baseline Analyzer 1.2.1 Help HTML Files



[5313] File System

Check Description

This check determines the file system of each hard drive, to ensure that the NTFS file system is being used. NTFS is a secured file system that allows you to control or restrict access to individual files or directories. For example, if you want to allow your coworkers to view your files, but not change them, you can do this by using the access control lists (ACLs) provided by NTFS.

Note

- For this check to succeed, the drive must be shared using administrative drive shares.

Additional Information

[Choosing between NTFS, FAT, and FAT32](#)

[How to Restore the Default NTFS Permissions for Windows 2000](#)

©2002-2004 Microsoft Corporation. All rights reserved.



[5313] File System

Issue

If you are running the FAT file system, which is not a secured file system, you should consider converting to the NTFS file system.

Secured file systems, such as NTFS, are a key component of security, because they restrict user access to data. By using file system security, you can specify which users are allowed to access individual files and what type of access they are allowed (for example, read or modify). NTFS protects your data by preventing unwanted user access to it.

Note

- You need to manually secure your files by using access control lists (ACLs). To do this, right-click the file or folder to which you want to control, click **Properties**, click the **Security** tab, and then specify the appropriate access restrictions for the file.

Solution

Convert your system from FAT to NTFS. For more information, view the documentation below on using NTFS and how to convert drives to NTFS.

Additional Information

[Choosing between NTFS, FAT, and FAT32](#)

[How to Restore the Default NTFS Permissions for Windows 2000](#)

©2002-2004 Microsoft Corporation. All rights reserved.

Message 5321 – Description

Printed from Microsoft Security Baseline Analyzer 1.2.1 Help HTML Files



[5321] IIS on Domain Controller

Check Description

This check determines whether Internet Information Services (IIS) is running on a system that is a domain controller. This is flagged in the scan report as a high-level vulnerability, unless the computer being scanned is running Small Business Server.

We recommend that you do not run an IIS Web server on a domain controller. Domain controllers contain sensitive data, such as user account information, and they should not be used in another role. If you run a Web server on a domain controller, you increase the complexity involved in securing the server and preventing attacks.

©2002-2004 Microsoft Corporation. All rights reserved.



[5321] IIS on Domain Controller

Issue

We recommend that you do not run an Internet Information Services (IIS) Web server on a domain controller. Domain controllers contain sensitive data such as user account information, and they should not be used in another role (unless you are running Small Business Server). If you run a Web server on a domain controller, you increase the complexity involved in securing the server and preventing attacks.

Solution

We recommend that you run Web servers and domain controllers on separate, dedicated computers.

©2002-2004 Microsoft Corporation. All rights reserved.

Message 5323 – Description

Printed from Microsoft Security Baseline Analyzer 1.2.1 Help HTML Files



[5323] IIS Lockdown Tool

Check Description

This check determines whether version 2.1 of the Internet Information Services (IIS) Lockdown tool, part of the [Microsoft Security Tool Kit](#), has been run on the scanned computer.

The IIS Lockdown tool works by turning off unnecessary features in IIS, thereby reducing the attack surface available to attackers. Using the IIS Lockdown tool should be one of the first steps administrators take in securing their Web servers.

Note

- The IIS Lockdown tool was developed for IIS 4.0, 5.0, and 5.1, and is not needed for new Microsoft® Windows® Server 2003 installations running IIS 6.0. If an upgrade is being performed from IIS 5.0 to IIS 6.0, then the lockdown tool should be run.

Additional Resources

[IIS Lockdown Tool](#)

©2002-2004 Microsoft Corporation. All rights reserved.



[5323] IIS Lockdown Tool

Issue

By default, when you install and run Internet Information Services (IIS) on a Microsoft® Windows® 2000 or Windows NT® 4.0 computer, all of the available features and services of the Web server are started. Only those features and services required for the particular Web server should be enabled on the computer to ensure that the least amount of code is running on the server. In addition, all available IIS security updates should be installed on the server to patch any known vulnerabilities.

Solution

We recommend that you download the [IIS Lockdown tool](#) and run it on all IIS computers. The tool works by turning off unnecessary features and services, thereby reducing the attack surface available to attackers. To provide defense in depth, [UriScan](#), has been integrated into the IIS Lockdown tool.

Note

- The IIS Lockdown tool was developed for IIS 4.0, 5.0, and 5.1, and is not needed for new Windows Server 2003 installations running IIS 6.0. If an upgrade is being performed from IIS 5.0 to IIS 6.0, then the lockdown tool should be run.

Additional Resources

[The Microsoft Security Tool Kit](#)

[IIS Lockdown Tool](#)

©2002-2004 Microsoft Corporation. All rights reserved.

Message 5324 – Description

Printed from Microsoft Security Baseline Analyzer 1.2.1 Help HTML Files



[5324] IIS Sample Applications

Check Description

This check determines whether the following Internet Information Services (IIS) sample file directories are installed on the scanned computer:

- \inetpub\iissamples
- \Winnt\help\iishelp
- \Program Files\common files\system\msadc

The sample applications typically installed with IIS illustrate dynamic HTML (DHTML) and Active Server Pages (ASP) scripting, and provide online documentation.

©2002-2004 Microsoft Corporation. All rights reserved.



[5324] IIS Sample Applications

Issue

The Internet Information Services (IIS) sample applications are useful learning tools, but they can be exploited by hackers to break into an IIS system because they contain sample scripts. A production Web server should not have any sample code or scripts on the system.

Solution

Remove the IISsamples, IISHelp, and MSADC virtual directories which map to the following folders:

- \inetpub\iissamples
- \Winnt\help\iishelp
- \Program Files\common files\system\msadc

Note

- New installations of IIS 6.0 do not have virtual directories mapped to these folders by default. Upgrades of IIS 5.0 to IIS 6.0 may still have these virtual directories if they were not manually removed after the upgrade or through the IIS Lockdown Tool.

Instructions

To remove the IISsamples, IISHelp, and MSADC virtual directories in Microsoft® Windows® Server 2003 (if upgraded from previous computers running IIS 5.0)

1. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
2. In Internet Information Services Manager, expand the Computer Name, then expand Web Sites, and expand the Default Web Site.
3. Right-click **IISAMPLES** (if listed), and then click **Delete**. Repeat this step to delete the **IISHELP** and **MSADC** virtual directories, if listed.

To remove the IISsamples, IISHelp, and MSADC virtual directories in Windows XP Professional

1. Click **Start**, point to **Control Panel**, point to **Administrative Tools**, and then click **Internet Information Services**.
2. In Internet Information Services Manager, expand the Computer Name, then expand Web Sites, and expand the Default Web Site.
3. Right-click **IISSAMPLES** (if listed), and then click **Delete**. Repeat this step to delete the **IISHELP** and **MSADC** virtual directories, if listed.

To remove the IISsamples, IISHelp, and MSADC virtual directories in Windows 2000

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Internet Services Manager**.
2. In Internet Information Services Manager, right-click **IISSAMPLES**, and then click **Delete**. Repeat this step to delete the **IISHELP** and **MSADC** virtual directories.

To remove the IISsamples, IISHelp, and MSADC virtual directories in Windows NT®

1. Click **Start**, point to **Programs**, point to **Windows NT 4.0 Option Pack**, point to **Microsoft Internet Information Server**, and then click **Internet Service Manager**.
2. In Internet Information Services Manager, right-click **IISSAMPLES**, and then click **Delete**. Repeat this step to delete the **IISHELP** and **MSADC** virtual directories.

©2002-2004 Microsoft Corporation. All rights reserved.

Message 5325 – Description

Printed from Microsoft Security Baseline Analyzer 1.2.1 Help HTML Files



[5325] IISADMPWD Virtual Directory

Check Description

This check determines whether the IISADMPWD directory is installed on the scanned computer.

Internet Information Server (IIS) 4.0 enables users to change their Windows® passwords and to notify users that their passwords are about to expire. The IISADMPWD virtual directory that installs as part of the default Web site in IIS 4.0 contains files that are used by this feature. This feature is implemented as a set of .htr files located in the <system>\System32\Inetsrv\Iisadmpwd directory and an ISAPI extension named lsm.dll.

Additional Information

[How to Change Windows NT Account Passwords Using Internet Information Server \(IIS\) 4.0 \(184619\)](#)

[IISADMPWD Virtual Directory Is Not Created During Clean Install of IIS 5.0 \(269082\)](#)

©2002-2004 Microsoft Corporation. All rights reserved.



[5325] IISADMPWD Virtual Directory

Issue

Internet Information Server (IIS) 4.0 provides the IISADMPWD virtual directory so that users can change their Microsoft® Windows® passwords. This feature was designed primarily for intranet scenarios. If you allow users to change passwords over the Internet, you create a potential security risk. You should not use the IISADMPWD virtual directory on production servers that have Internet access.

Solution

Remove the **IISADMPWD** virtual directory.

Note

- This directory is not installed as part of Internet Information Services (IIS) 5.0, but it is not removed if you upgrade from IIS 4.0.

Instructions

To remove the IISADMPWD virtual directory in Windows XP Professional

1. Click **Start**, point to **Control Panel**, point to **Administrative Tools**, and then click **Internet Information Services**.
2. In the Internet Information Services Manager, right-click **IISADMPWD**, and then click **Delete**.

To remove the IISADMPWD virtual directory in Windows 2000

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Internet Services Manager**.
2. In the Internet Information Services Manager, right-click **IISADMPWD**, and then click **Delete**.

To remove the IISADMPWD virtual directory in Windows NT®

1. Click **Start**, point to **Programs**, point to **Windows NT 4.0 Option Pack**, point to **Microsoft Internet Information Server**, and then click **Internet Service Manager**.
2. In the Internet Information Services Manager, right-click **IISADMPWD**, and then click **Delete**.

Additional Information

[How to Change Windows NT Account Passwords Using Internet Information Server \(IIS\) 4.0 \(184619\)](#)

[IISADMPWD Virtual Directory Is Not Created During Clean Install of IIS 5.0 \(269082\)](#)

©2002-2004 Microsoft Corporation. All rights reserved.

Message 5326 – Description

Printed from Microsoft Security Baseline Analyzer 1.2.1 Help HTML Files



[5326] IIS Parent Paths

Check Description

This check determines whether the **AspEnableParentPaths** setting is enabled on the scanned computer.

By enabling parent paths on Microsoft® Internet Information Services (IIS), pages in Active Server Pages (ASP) can use relative paths to the parent directory of the current directory (that is, paths that use the .. syntax).

Additional Information

[AspEnableParentPaths MetaBase Property Should Be Set To False \(184717\)](#)

©2002-2004 Microsoft Corporation. All rights reserved.



[5326] IIS Parent Paths

Issue

If **ASPEnableParentPaths** is enabled and the parent directories have execute access, a script could run an unauthorized program in a parent directory.

Solution

Disable the **ASPEnableParentPaths** option on Internet Information Services (IIS).

Note

- Microsoft Project Central and Project Server 2002 require parent paths to be enabled. Additional information is available in KB article 316398.

Instructions

To disable the ASPEnableParentPaths option in Microsoft® Windows® XP Professional

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Internet Information Services**.
2. In the Internet Information Services Manager, right-click the root of the Web site that you want to secure, and then click **Properties**.
3. In the **Default Web Site Properties** dialog box, click the **Home Directory** tab, and then click **Configuration**.
4. In the **Application Configuration** dialog box, click the **Options** tab, and then clear the **Enable parent paths** check box.

To disable the ASPEnableParentPaths option in Windows 2000

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Internet Services Manager**.

2. In the Internet Information Services Manager, right-click the root of the Web site that you want to secure, and then click **Properties**.
3. In the **Default Web Site Properties** dialog box, click the **Home Directory** tab, and then click **Configuration**.
4. In the **Application Configuration** dialog box, click the **App Options** tab, and then clear the **Enable parent paths** check box.

To disable the `ASPEnableParentPaths` option in Windows NT®

1. Click **Start**, point to **Programs**, point to **Windows NT 4.0 Option Pack**, point to **Microsoft Internet Information Server**, and then click **Internet Service Manager**.
2. In the Internet Information Services Manager, right-click the root of the Web site that you want to secure, and then click **Properties**.
3. In the **Default Web Site Properties** dialog box, click the **Home Directory** tab, and then click **Configuration**.
4. In the **Application Configuration** dialog box, click the **App Options** tab, and then clear the **Enable parent paths** check box.

To disable the `ASPEnableParentPaths` option if you are running Microsoft Small Business Server 2000

1. Follow the previous steps for Windows 2000.
2. Click **OK**. The **Inheritance Overrides** dialog box appears.

Note

- The following three nodes should be listed in the Child Nodes section: Public, Exchange, and Exadmin. If none of these child nodes are listed, run the IIS Lockdown tool, and then re-run the Microsoft Baseline Security Analyzer.
3. Click **OK** to close the **Inheritance Overrides** dialog box.
 4. Click **OK** to close the **Web Site Properties** dialog box.

Important

- If done incorrectly, Exchange (specifically Outlook Web Access) will no longer function. If this occurs, run the IIS Lockdown tool again and after verifying the three child nodes in the previous steps appear in the Inheritance Overrides dialog box, click OK to accept these settings.

Additional Information

[ASPEnableParentPaths MetaBase Property Should Be Set To False \(184717\)](#)

©2002-2004 Microsoft Corporation. All rights reserved.

© SANS Institute 2005, Author retains full rights.

Message 5327 – Description

Printed from Microsoft Security Baseline Analyzer 1.2.1 Help HTML Files



[5327] MSADC and Scripts Virtual Directories on IIS

Check Description

This check determines whether the MSADC (sample data access scripts) and Scripts virtual directories are installed on a scanned server running Internet Information Services (IIS). These directories typically contain scripts that, if not required, should be removed to help reduce the attack surface of the computer.

Additional Resources

[IIS Lockdown Tool](#)

©2002-2004 Microsoft Corporation. All rights reserved.



[5327] MSADC and Scripts Virtual Directories on IIS

Issue

This check determines whether the MSADC (sample data access scripts) and Scripts virtual directories are installed on a scanned computer running Internet Information Services (IIS). These directories typically contain scripts that, if not required, should be removed to help reduce the attack surface of the computer.

Solution

We recommend that you remove these virtual directories if they are not required on the computer running IIS.

Note

- All versions of Microsoft Project Server (Project Central, Project Server 2002 and Project Server 2003) require the MSADC virtual directory. Project Server setup will create the MSADC virtual directory if not already created and will set minimum permissions required for Project Server functionality. Additional information is available in KB article 316398.

Instructions

To remove these virtual directories in Microsoft® Windows® XP Professional

1. Click **Start**, point to **Control Panel**, point to **Administrative Tools**, and then click **Internet Information Services**.
2. In the Internet Information Services Manager, right-click the virtual directories to remove, and then click **Delete**.

To remove these virtual directories in Windows 2000

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Internet Services Manager**.
2. In the Internet Information Services Manager, right-click the virtual directories to remove, and then click **Delete**.

To remove these virtual directories in Windows NT®

1. Click **Start**, point to **Programs**, point to **Windows NT 4.0 Option Pack**, point to **Microsoft Internet Information Server**, and then click **Internet Service Manager**.
2. In the Internet Information Services Manager, right-click the virtual directories to remove, and then click **Delete**.

Additional Resources

[IIS Lockdown Tool](#)

©2002-2004 Microsoft Corporation. All rights reserved.

© SANS Institute 2005, Author retains full rights.

Message 5328 – Description

Printed from Microsoft Security Baseline Analyzer 1.2.1 Help HTML Files



[5328] IIS Logging

Check Description

This check determines whether Internet Information Services (IIS) logging is enabled, and if the W3C Extended Log File Format is used.

IIS logging goes beyond the scope of the event logging or performance monitoring features of Windows. The logs can include information, such as who has visited your site, what the visitor viewed, and when the information was viewed last. You can monitor attempts, either successful or unsuccessful, to access your Web sites, virtual folders, or files. This includes events such as reading the file or writing to the file. You can choose which events you want to audit for any site, virtual folder, or file. By regularly reviewing these files, you can detect areas of your server or your sites that may be subject to attacks or other security problems. You can enable logging for individual Web sites and choose the log format. When logging is enabled, it is enabled for all the site's folders, but you can disable it for specific directories.

Additional Information

[HOW TO: Enable IIS Logging Site Activity \(300390\)](#)

©2002-2004 Microsoft Corporation. All rights reserved.



[5328] IIS Logging

Issue

It is essential to log your Web site events regularly to find invalid usage or identify malicious user activity and access.

Solution

Enable logging on your server running Internet Information Services (IIS) and use the W3C Extended Log File Format to log additional event properties.

Instructions

To enable IIS event logging in Microsoft® Windows Server® 2003

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Internet Services Manager**.
2. Double-click your server, right-click the Web site or FTP site, and then click **Properties**.
3. On the **Website or FTP Site** tab, select the **Enable Logging** check box.
4. In the **Active log format** list, click **W3C Extended Log File Format**.
5. Click **Properties**.
6. In the **Extended Logging Properties** dialog box, enable extended properties by selecting the check box, and then select the following: **Client IP Address**, **User Name**, **Method**, **URI Stem**, **Protocol Status**, **Win32 Status**, **User Agent**, **Server IP Address**, and **Server Port**.

To enable IIS event logging in Microsoft Windows XP Professional

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Internet Information Services**.
2. Double-click your server, right-click the Web site or FTP site, and then click **Properties**.
3. On the **Website or FTP Site** tab, select the **Enable Logging** check box.
4. In the **Active log format** list, click **W3C Extended Log File Format**.
5. Click **Properties**.

6. In the **Extended Logging Properties** dialog box, enable extended properties by selecting the check box, and then select the following: **Client IP Address, User Name, Method, URI Stem, Protocol Status, Win32 Status, User Agent, Server IP Address, and Server Port.**

To enable IIS event logging in Windows 2000

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Internet Services Manager**.
2. Double-click your server, right-click the Web site or FTP site, and then click **Properties**.
3. On the **Website or FTP Site** tab, select the **Enable Logging** check box.
4. In the **Active log** format list, click **W3C Extended Log File Format**.
5. Click **Properties**.
6. In the **Extended Logging Properties** dialog box, select the following check boxes: **Client IP Address, User Name, Method, URI Stem, HTTP Status, Win32 Status, User Agent, Server IP Address, and Server Port.**

To enable IIS event logging in Windows NT®

1. Click **Start**, point to **Programs**, point to **Windows NT 4.0 Option Pack**, point to **Microsoft Internet Information Server**, and then click **Internet Service Manager**.
2. Double-click your server, right-click the Web site or FTP site, and then click **Properties**.
3. On the **Website or FTP Site** tab, select the **Enable Logging** check box.
4. In the **Active log** format list, click **W3C Extended Log File Format**.
5. Click **Properties**.
6. In the **Extended Logging Properties** dialog box, select the following check boxes: **Client IP Address, User Name, Method, URI Stem, HTTP Status, Win32 Status, User Agent, Server IP Address, and Server Port.**

Additional Information

[HOW TO: Enable IIS Logging Site Activity \(300390\)](#)

©2002-2004 Microsoft Corporation. All rights reserved.



[53116] Unnecessary Services

Check Description

This check determines whether any services contained in the Services.txt file are installed on the scanned computer, and lists the files with their current state (enabled or disabled). The Services.txt file is a configurable list of services to be checked on the scanned computers. The Services.txt file, installed by default with the tool, contains the following services:

MSFTPSVC (FTP)

TlntSvr (Telnet)

W3SVC (WWW)

SMTPSVC (SMTP)

In Microsoft® Windows® XP, Windows 2000 and Windows NT® 4.0, a service is a program that runs in the background whenever the computer is running the operating system. It does not require a user to be logged on. Services are needed to perform user-independent tasks, such as a fax service that waits for incoming faxes.

©2002-2004 Microsoft Corporation. All rights reserved.



[53116] Check for Unnecessary Services

Issue

Services that are listed in the security report are contained in the Services.txt file and were found to be installed on the scanned computers. The state of each of these services (enabled or disabled) is listed in the Results Details page. The user should determine whether the services found to be installed or running are necessary. If unnecessary, they should be disabled. For example, if the Telnet service is found to be installed and enabled, but users are not required to remotely connect through Telnet to that specific computer, this service should be disabled.

The Services.txt file, included with Microsoft® Baseline Security Analyzer (MBSA) in the installation folder, can be edited such that the tool will check the status of each service listed in the file. To add or change services from the default list, edit the Services.txt file with Notepad or Microsoft Word and type the service name for each service you would like to scan. The service names can be found by viewing the properties of a service in the Services Control Panel applet.

Solution

Use the Services Control Manager to disable the running services that the user confirms should not be running on the computer. Services that are enabled but not required can pose a security risk to the computer.

Important:

- If you are running Small Business Server (SBS), there are services listed in MBSA that are core to your server functionality. These are the Simple Mail Transport Protocol (SMTP) and World Wide Web Publishing services. Do not disable these services on computers running SBS.

Instructions

To disable services in Windows® Server 2003, Windows XP, or Windows 2000

1. Open the **Control Panel**.
2. Double-click **Administrative Tools**, and then click **Services**.
3. Double-click the service that you want to disable.
4. Click **Stop** to stop the service.
5. Under **Startup type**, click **Disabled**.

To disable services in Windows NT® 4.0

1. Click **Start**, point to **Programs**, click **Settings**, and then click **Control Panel**.
2. In Control Panel, double-click **Services**.
3. Double-click the service that you want to disable.
4. Click **Stop** to stop the service.
5. Under **Startup type**, click **Disabled**.

©2002-2004 Microsoft Corporation. All rights reserved.

© SANS Institute 2005, Author retains full rights.

APPENDIX B – Inspecting Web Property Sheets

In this appendix are screenshots of property pages for IIS.

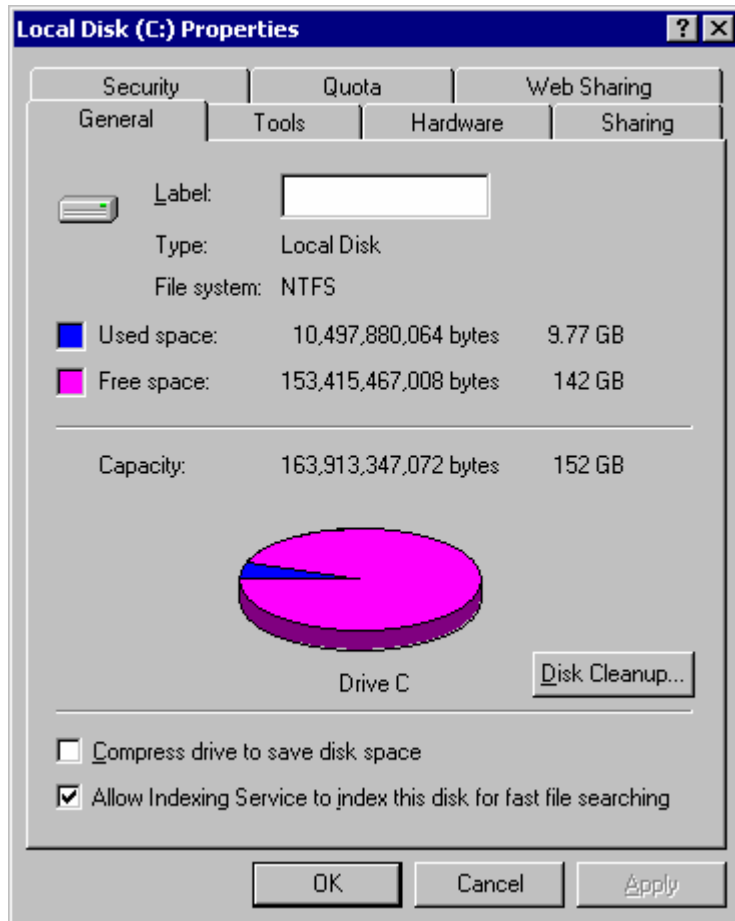


Figure B1: Local Disk Properties to determine file system in use

The file system in use is NTFS. It is 152GB in size, with 9.77 GB in use and 142GB of free space.

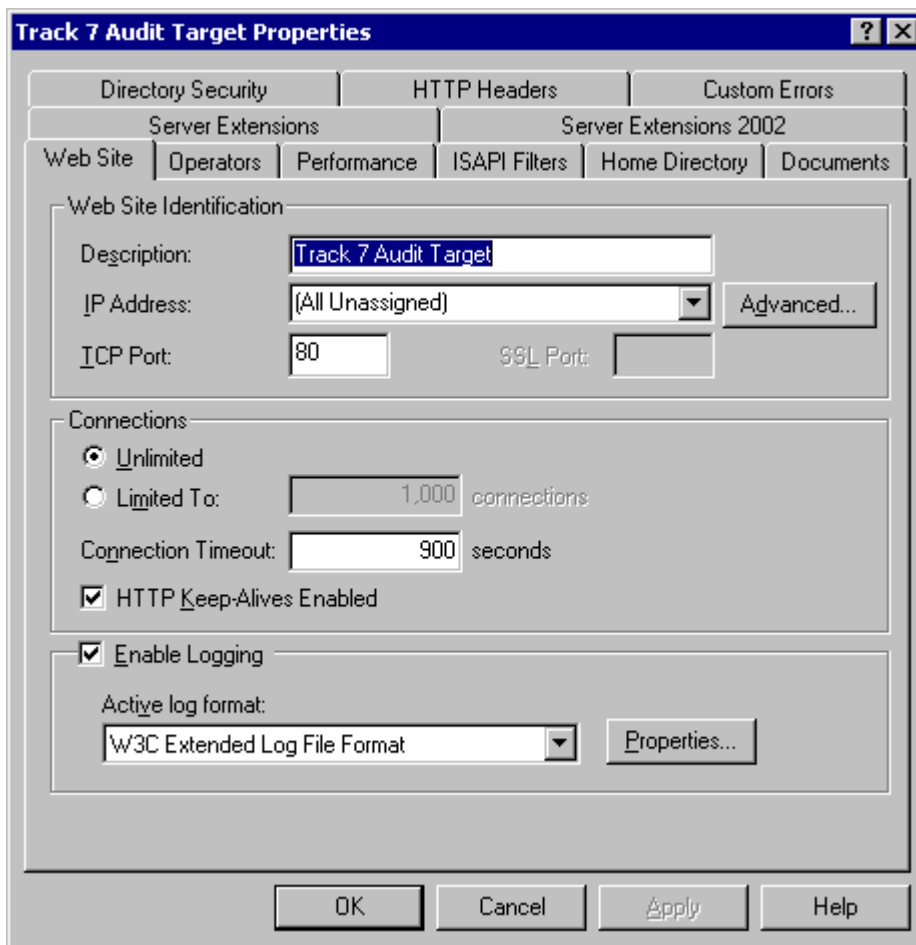


Figure B2: Web Site Properties Page

The web site is running the default port (Port 80) from any IP address found on the interface. Logging is enabled, and W3C log file format is being used.

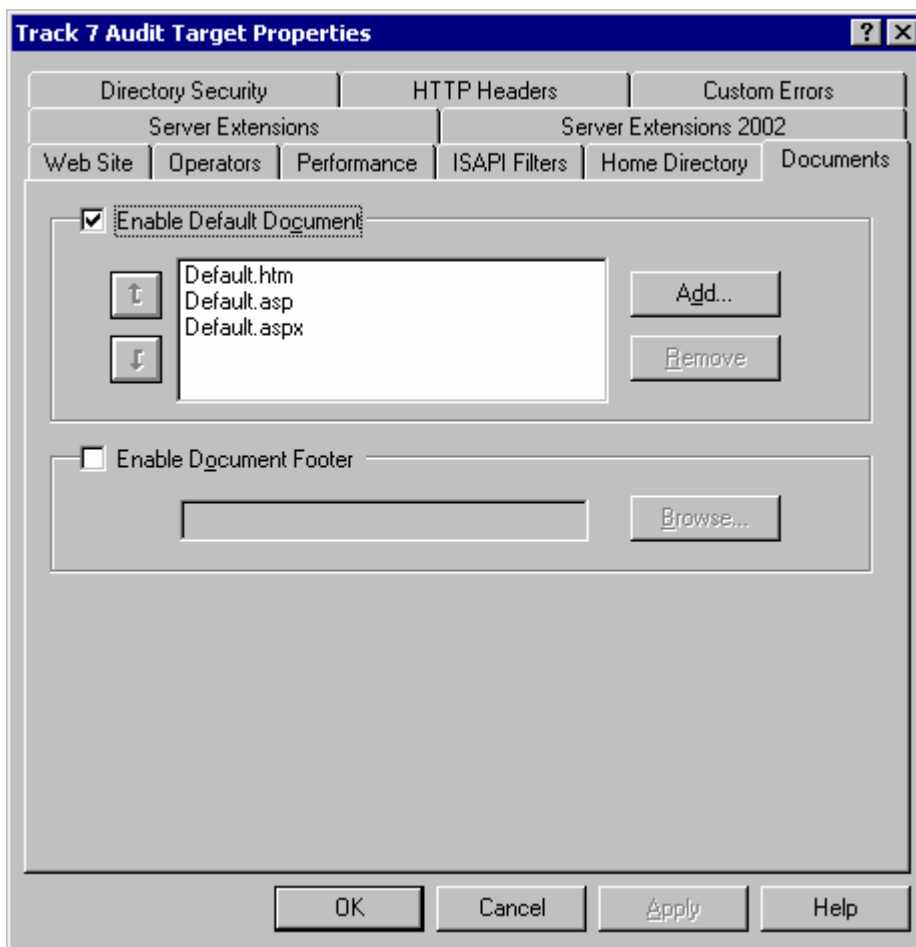


Figure B3: Default Document Properties Page

The document property indicates the default filename of the start page when a page is not indicated in the URL. There are three document names specified in the sample above, and they are tried in order from top to bottom. If a document is not specified on the URL, and default document is not specified or none of the default documents can be found, a page not found condition will occur. This would be a standard 404 error, but the page not found can be customized in the web site configuration.

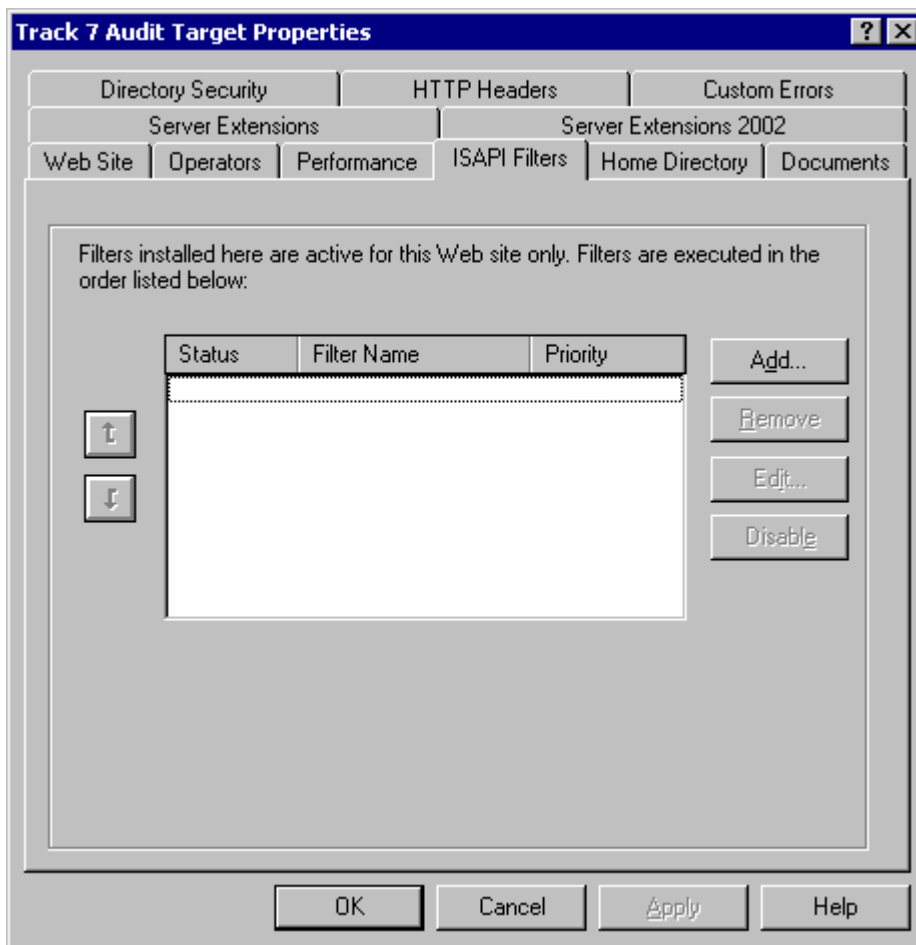


Figure B4: Installed ISAPI Filters

This property page would list any ISAPI filters, if installed. Any ISAPI filters found should be further researched to determine if they are in use, and identify which application they serve.

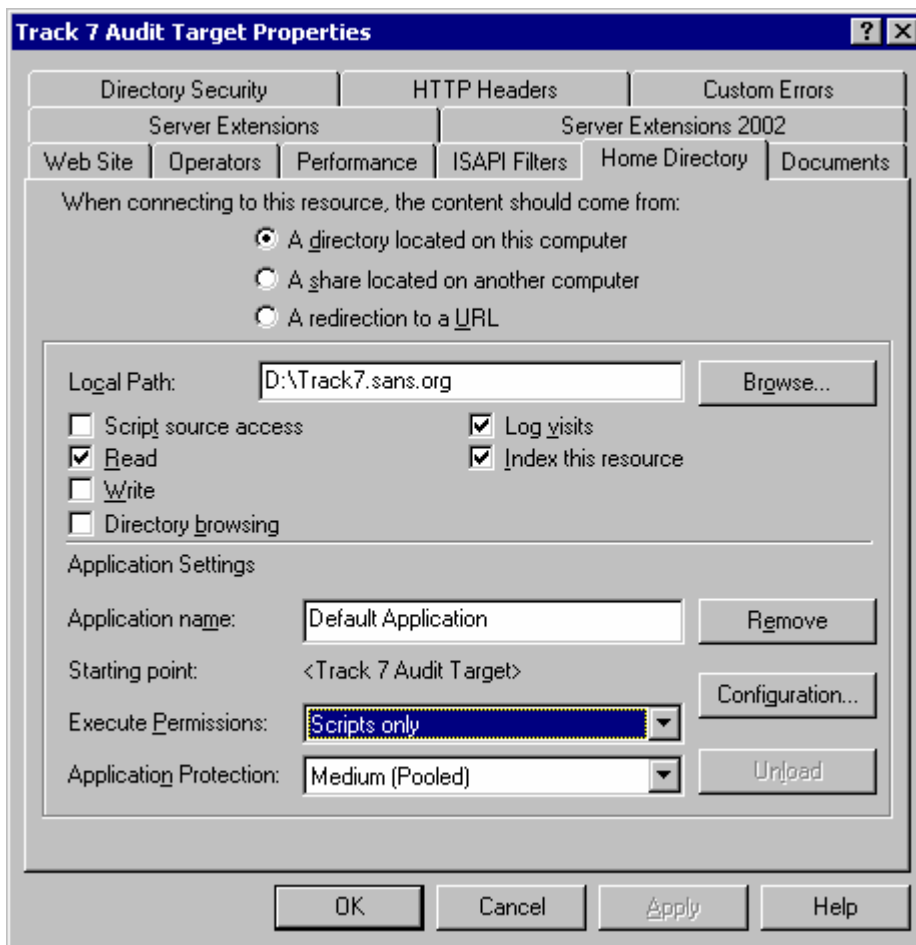


Figure B5: Home Directory Page

The home directory for this website is specified in the logical path. Permissions for disk access only allow read access. Visits are logged, and the resource is indexed. Execute permissions are for script only.

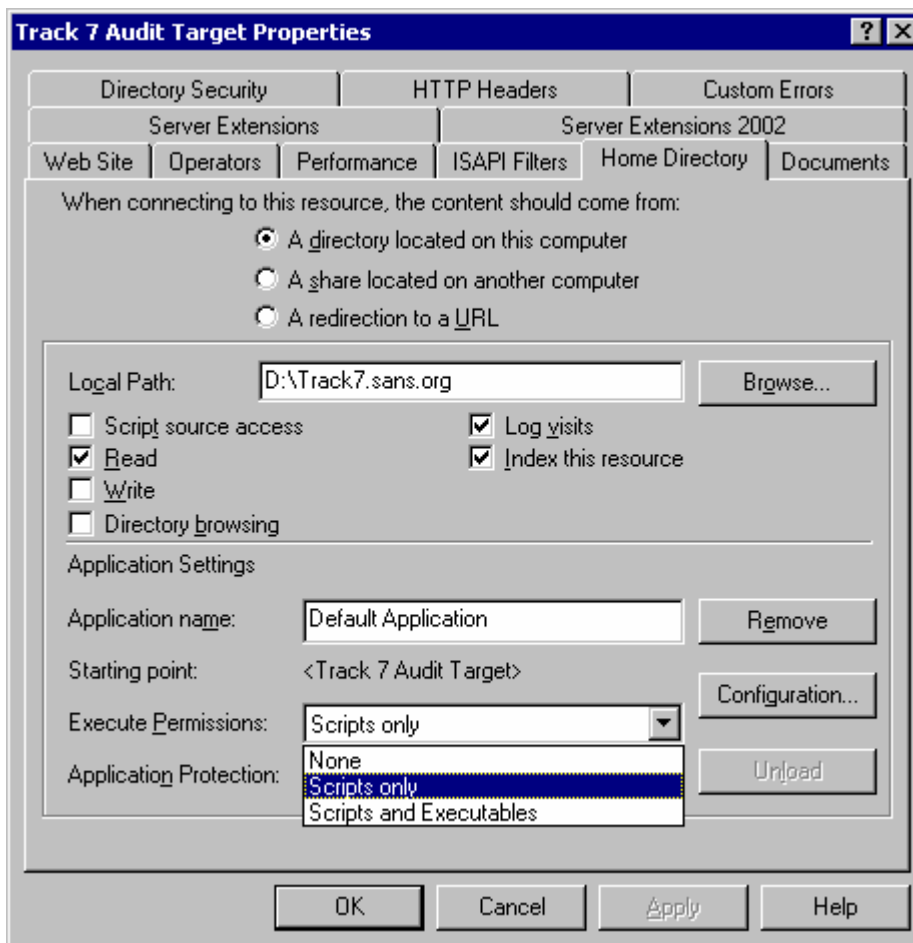


Figure B6: Home Directory Page – Execute Permissions

Execute permissions may be none, scripts only, or scripts and executables. None provides the safest environment because scripts and programs cannot be executed. Executables provides the highest risk as executable programs could be run, and these may be executable programs that were never expected to run. On example is cmd32.exe which is the command prompt. Several worms, including the Nimda worm, were able to access cmd32.exe and execute commands on the web server. For this to be successful, execute permissions was required to be set.

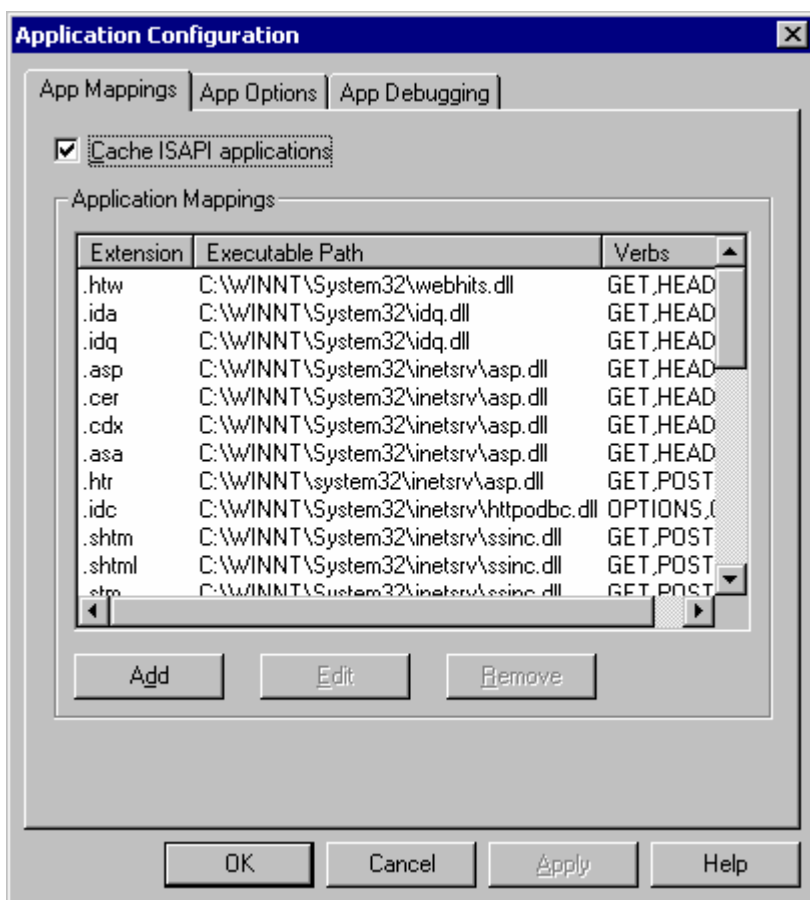


Figure B7: Application Configuration – Application Mapping

Application mappings are used to map the extension to a DLL file. Running IIS Lockdown may remove or remap some of the extensions. To determine the remaining extensions, and how they are mapped, this property sheet will show it. It is also helpful to look here for nonstandard mappings that may have been added for an application or as part of a software package.

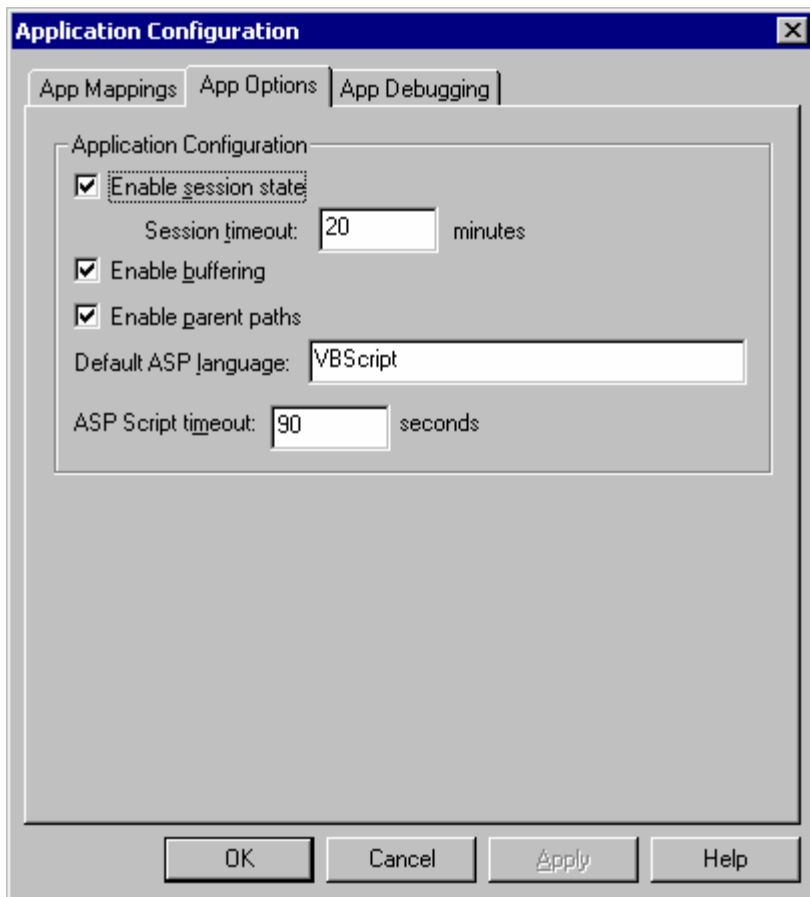


Figure B8: Application Configuration – Application Configuration

This is the property sheet that parent paths are specified. Here it is enabled, and this setting may produce vulnerability for the web server and application.

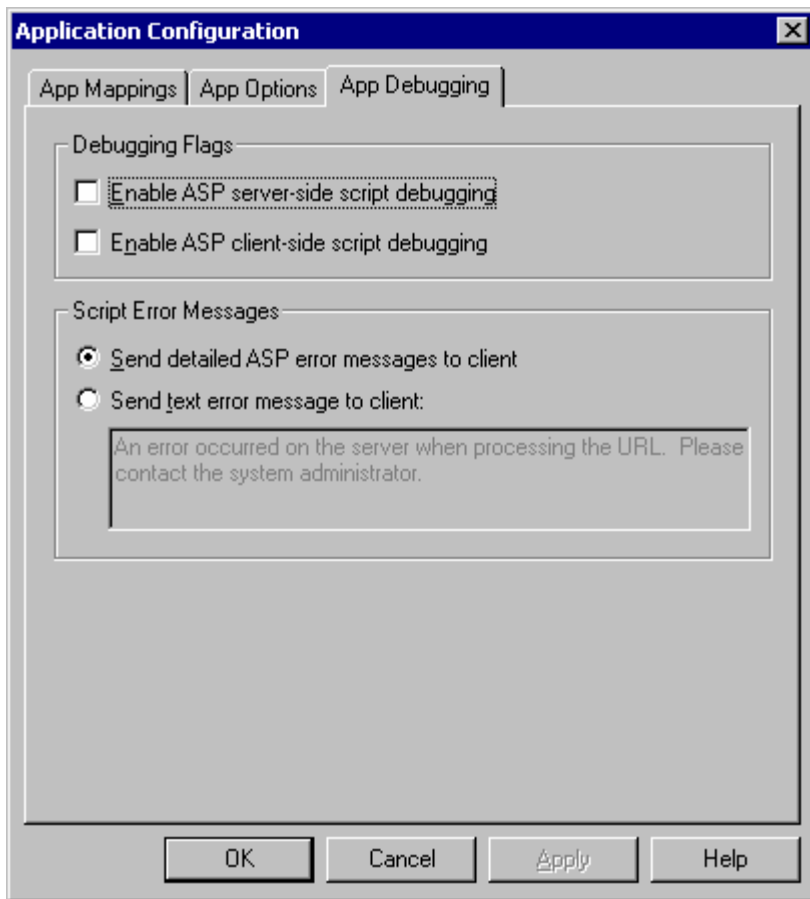


Figure B9: Application Configuration – Application Debugging

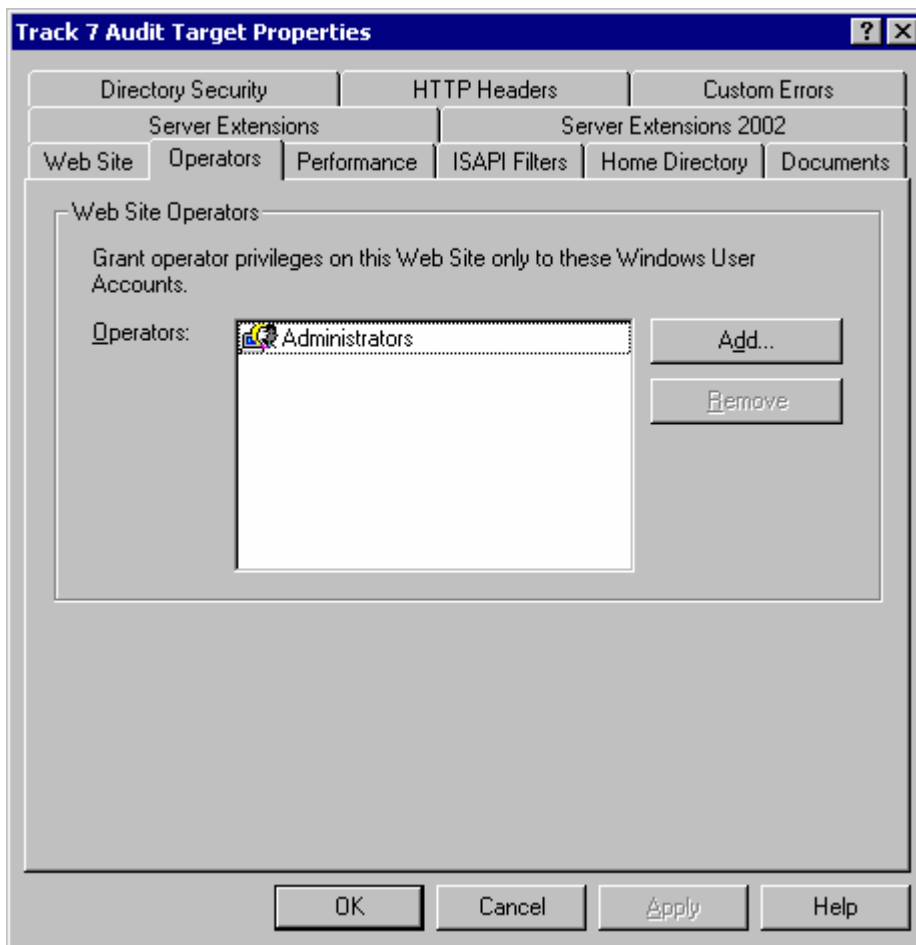


Figure B10: Web Site Operators

This is a list of the Web Server Operators for IIS. This list should be small and properly controlled.

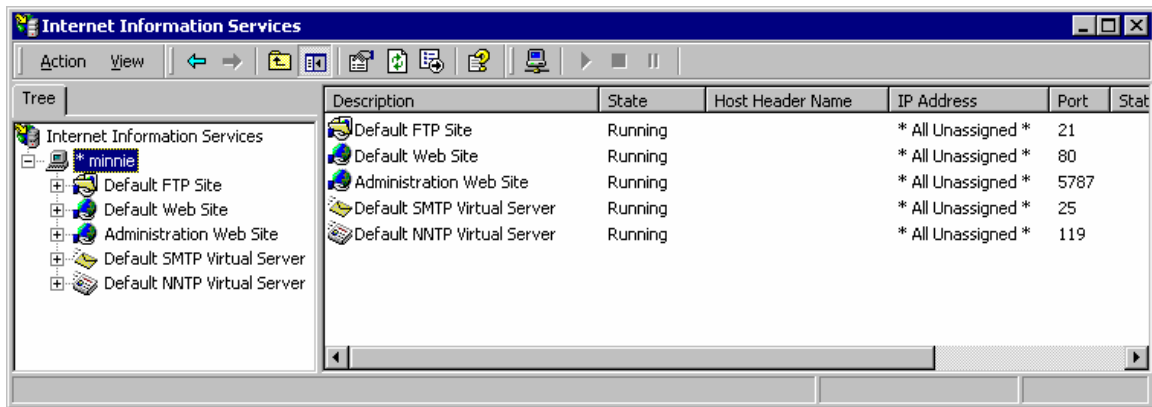


Figure B11: Simple Tree of Default Web Sites

A full default install of IIS creates 5 sites, Default FTP and Web Sites, an Administration Web Site, and SMTP & NNTP virtual servers.

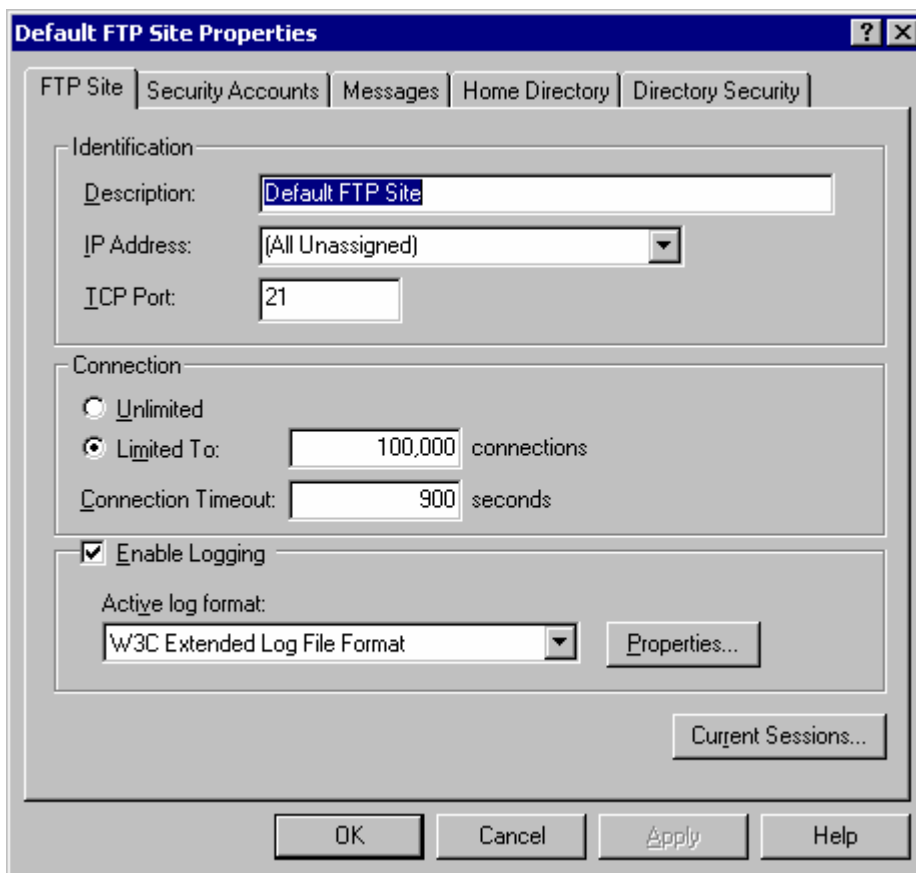


Figure B12: Default FTP Site Properties

The default FTP site has less tabs and options than the Web site.

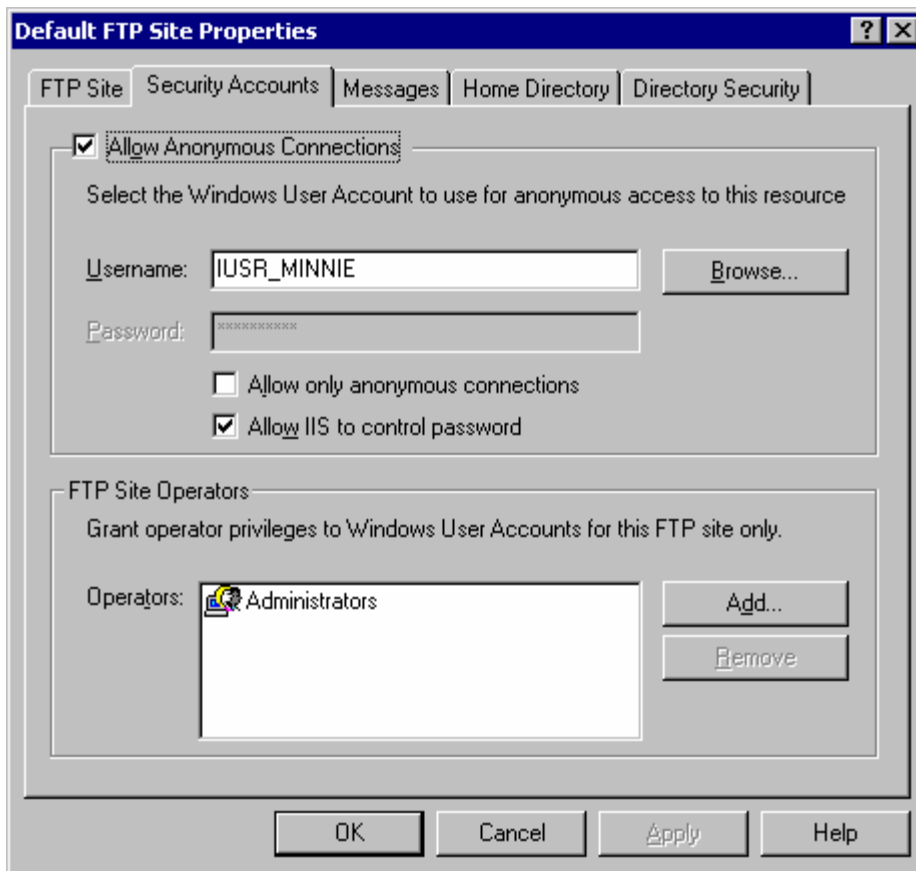


Figure B13: Security Accounts Tab for FTP Sites

Here the default username for mapping the Anonymous account is specified. The check box on top indicates if this site will allow anonymous connections.

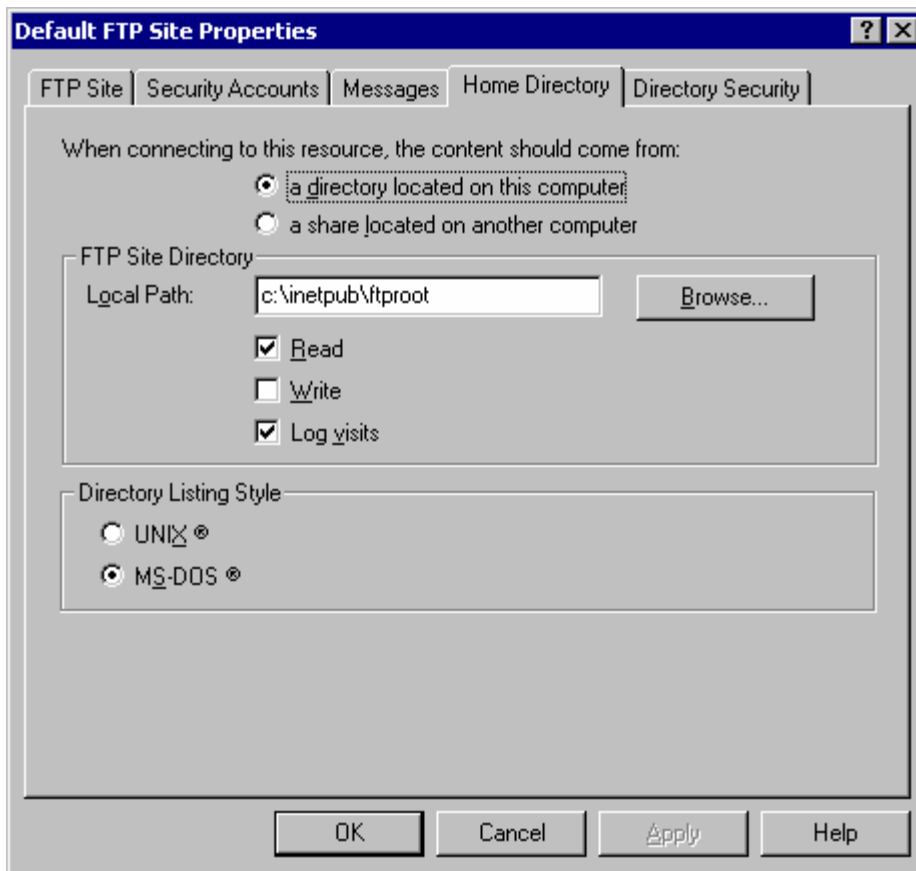


Figure B14: Home Directory and Permissions Page

There are less permissions and options. Read, Write and Log. FTP sites do not provide a method to execute scripts and programs.



Figure B15: Default SMTP Virtual Server Properties

The relay button will take you into a configuration screen to specify relay.

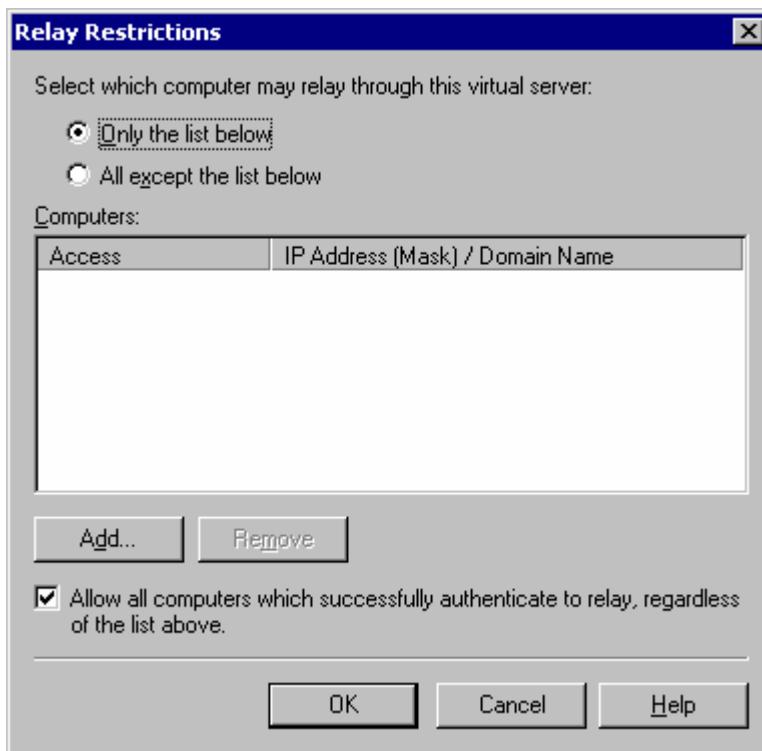


Figure B16: Relay Restrictions

The effect of the relay restrictions in this sample is that only authenticated computers may relay. This will prevent outside sites from connecting to the SMTP server and using it as an open relay unless they can authenticate. However, if the SMTP server is configured for anonymous SMTP login, then anyone can authenticate. Another way that this system could be made into a full open relay is to change the radio button above and specify all except the list below.

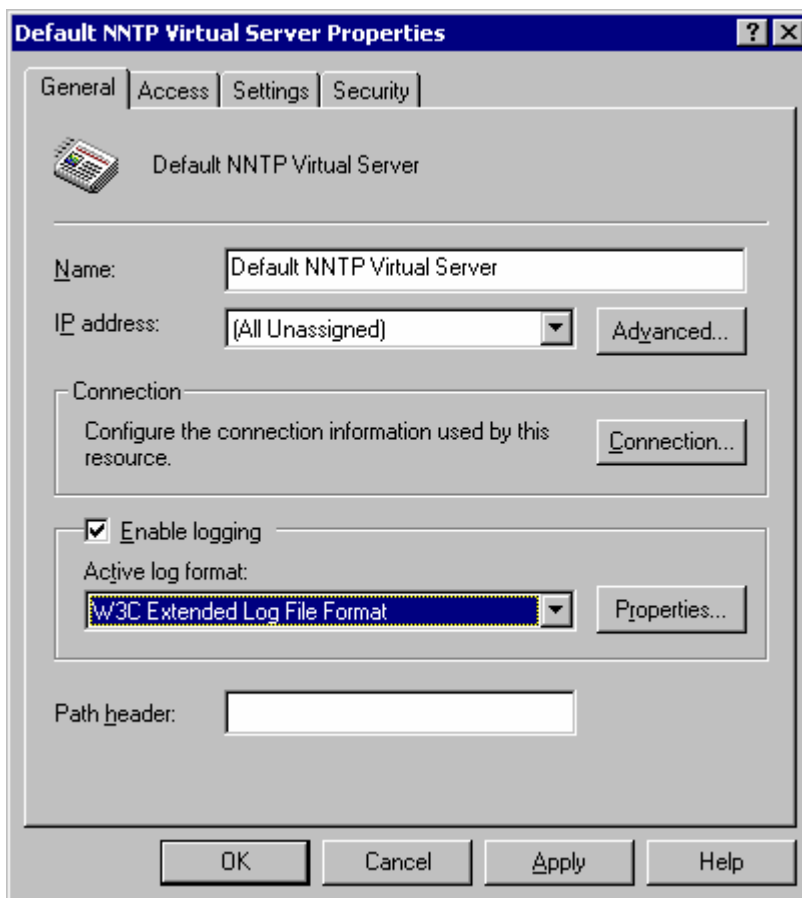


Figure B17: Default NNTP Virtual Server Properties – General Tab

This property sheet shows default NNTP properties. Similar to other property sheets of FTP and Web, logging may be enabled and the format specified here.

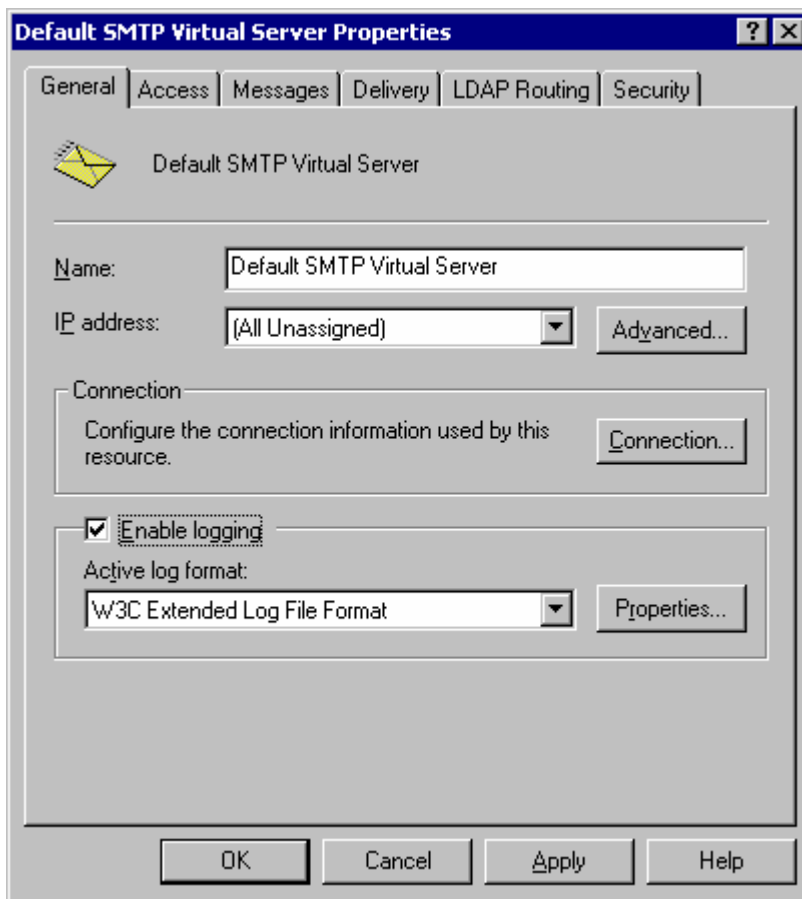


Figure B18: Default SMTP Virtual Server Properties – General Tab

This property sheet shows default SMTP properties. Similar to other property sheets of FTP and Web, logging may be enabled and the format specified here.

Navigation to SMTP properties will be different in Exchange 2000 or 2003 environment. In Exchange, the SMTP server is modified and belongs to Exchange. If Exchange 2000 or above is installed on the server, then you will not see SMTP in the Internet Information Services MMC snap-in, you have to go to Exchange Manager and look under the SMTP protocol.

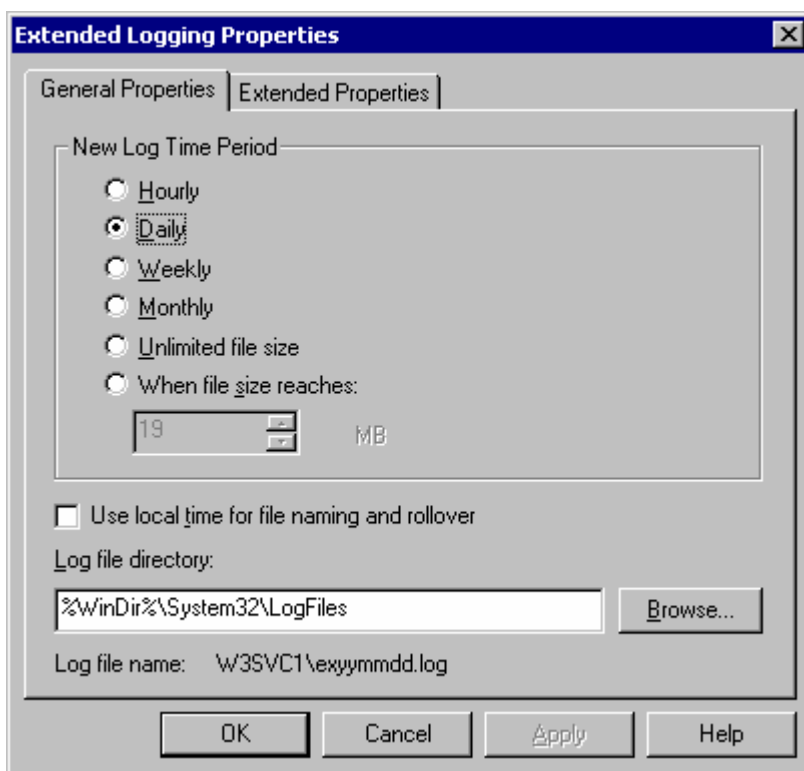


Figure B19: Extended Logging Properties

This property sheet allows overriding the location of where the log files are to be stored. Log files will be stored in the appropriate directory and will use a date stamp as part of the naming convention. Logs can be broken down into hourly, daily, weekly, etc. periods – this is where that period is specified. The use of local time forces the entries in the logs to be local time, otherwise GMT/UTC is used by default.

The extended properties tab allows selection of fields to be logged. Additional data fields may be captured in the log if more detail is required.

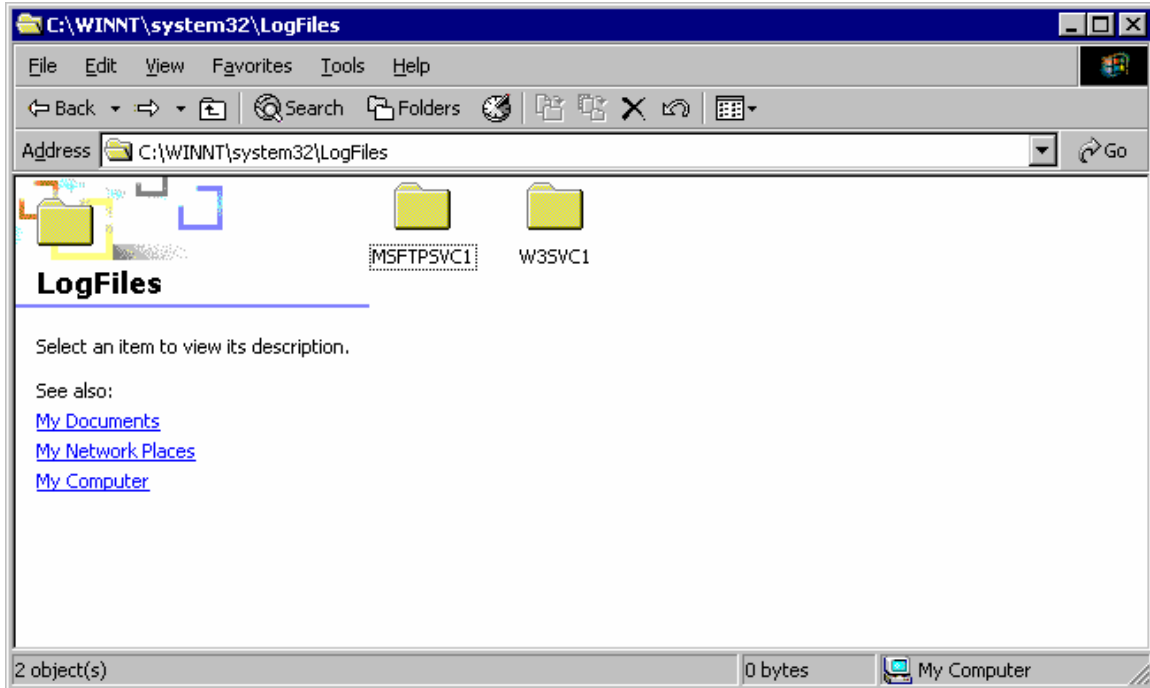


Figure B20: Default Folder for IIS Log files

When logging is enabled, IIS Logs will be placed in the winnt\system32\LogFiles folder. (Note that drive letter and name of windows directory may be different).

In the above example, there are logs for the Default FTP Site (MSFTPSVC1) and the Default Web Site (W3SVC1). A second web or ftp site would be followed by a "2" (i.e. MSFTPSVC2 or W3SVC2).

The locations of the logs, naming of folders and files, etc. may be configured in the property sheet that enables logging.

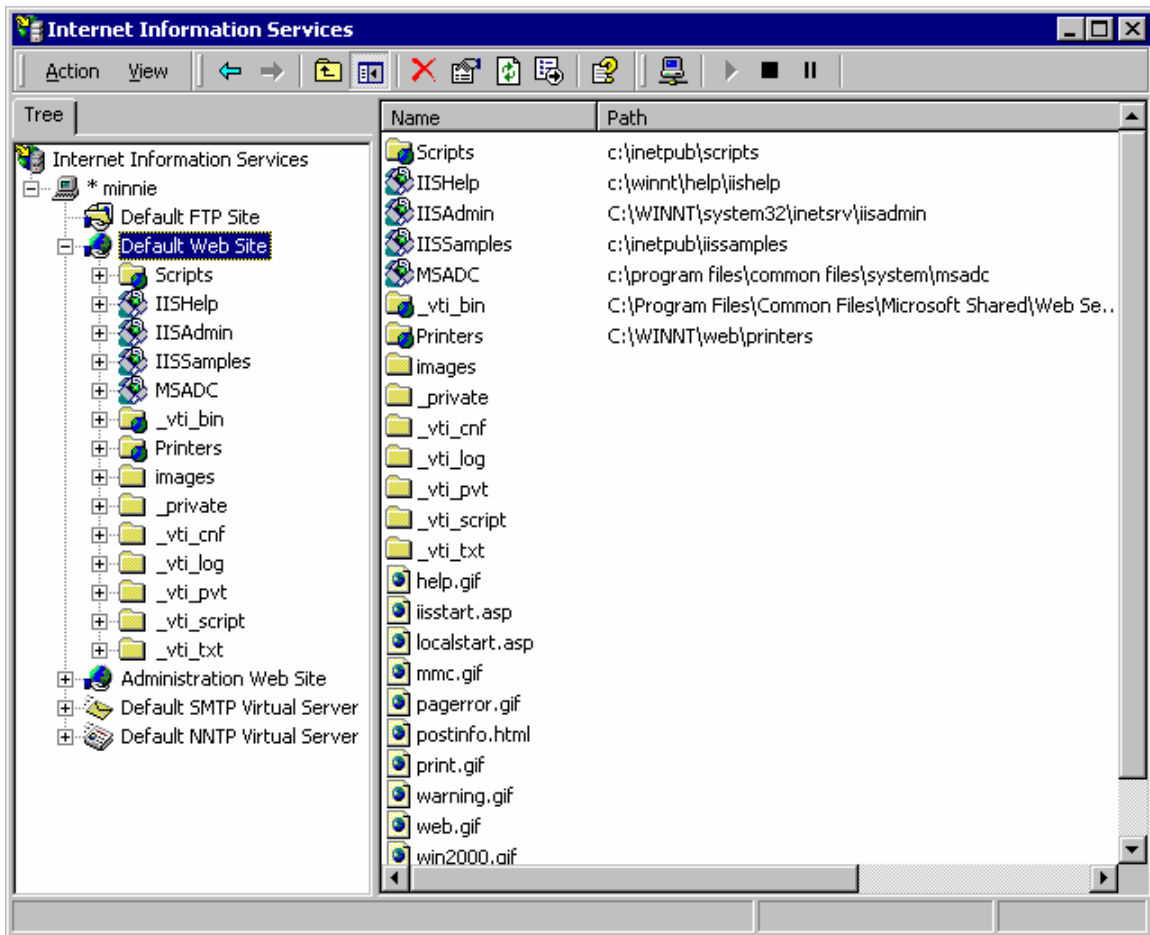


Figure B21: Expanded Default Web Site to Expose Virtual Directories

Selecting the default website shows all the virtual directories and the directory tree that begins at the home directory as root. Directories that are not within the default web site root tree are virtual directories. A virtual directory will be rooted at its own home directory the root is shown in the right pane.

Example: The Virtual Directory Scripts is located at c:\inetpub\Scripts

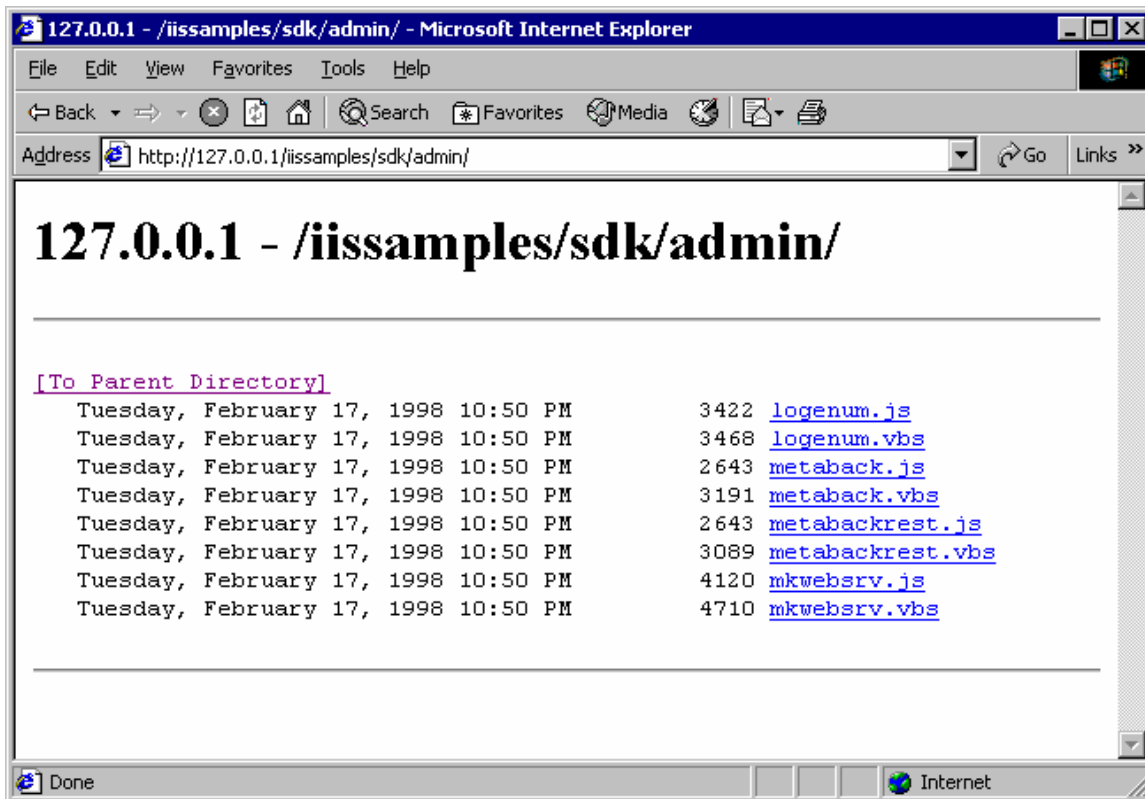


Figure B22: Sample of Browse Directory Screen

If browsing is enabled and there is no default document defined, a directory listing appears. The above is a sample of what a directory listing would look like. By default, the IISSAMPLES directory has browsing enabled and has no default document defined.

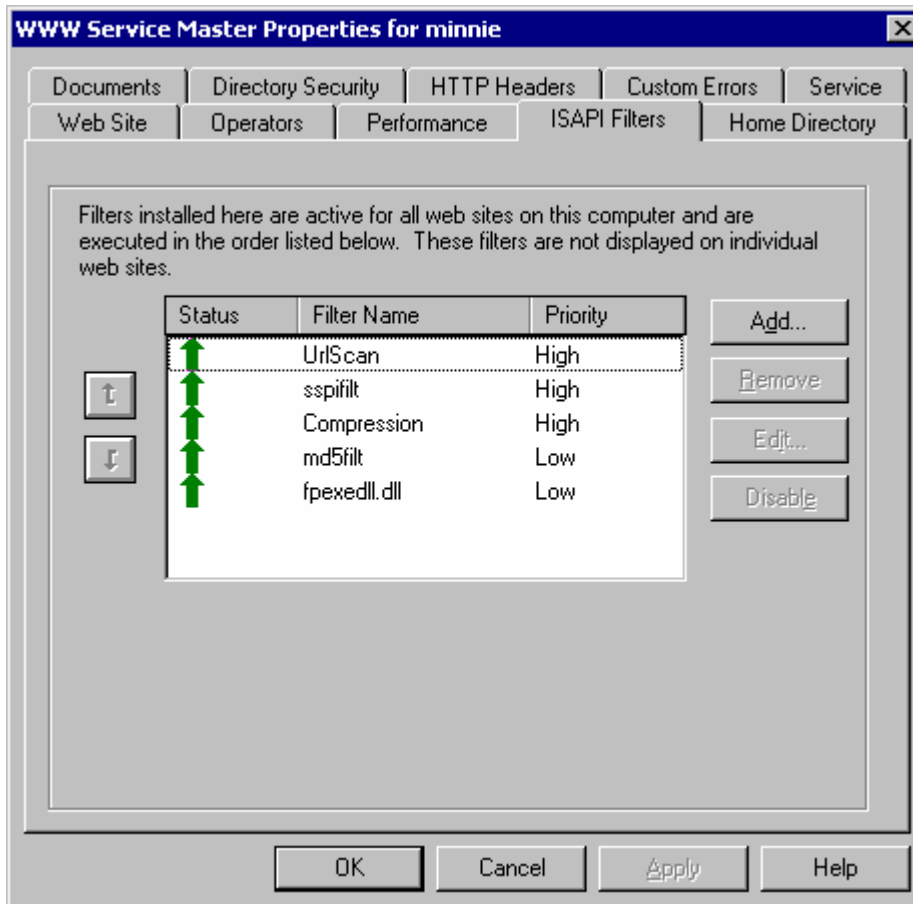


Figure B23: Sample Master Properties ISAPI Screen with URLSCAN

ISAPI filters may be specified on the IIS server as a whole (Global) or for each individual website (local). Examination of global and local ISAPI filters property sheets need to be checked. The above shows a master property sheet ISAPI filter mapping with URLSCAN.DLL installed and enabled.

Other DLLs:

An article from Windows .NET Magazine¹⁶⁵ explains the functions of the other filters. Here is a copy of those explanations from that article:

Sspifilt. The Sspifilt filter provides the ability to use Secure Sockets Layer (SSL) sessions on the server. I suggest that you leave this filter installed.

Compression. The Compression filter, found in IIS 5.0 only, lets you use HTTP compression for specific extensions and tune the compression cache. However, the Compression filter has had a few problems with cache management, it doesn't work with some third-party Web applications, and it's useful only with Microsoft Internet Explorer (IE) 5.x or later clients.

UrlScan. UrlScan is installed on IIS 5.0 and IIS 4.0 machines as part of Microsoft's IIS Lockdown tool and is an important part of IIS security. You can edit the urlscan.ini file, which the installation process creates, to configure this filter. Be aware, however, that improper configuration can disable server functionality. If your server is functioning properly, I would leave the filter in place.

Md5filt. The Md5filt filter provides Digest authentication capability—an IIS 5.0 capability. Digest authentication is a much better authentication method than Basic authentication, but it's not in widespread use. For more information about Digest authentication, see the IIS 5.0 online Help files.

Fpexedll.dll. The fpexedll.dll filter provides backward compatibility from Microsoft FrontPage Server Extensions to the FrontPage 97 client. You can find this filter on both IIS 5.0 and IIS 4.0 installations.

¹⁶⁵ Hill, Bret. Informant: Disabling ISAPI Filters. Windows .NET Magazine March 2002
URL: <<http://www.winnetmag.com/Article/ArticleID/23817/23817.html>>

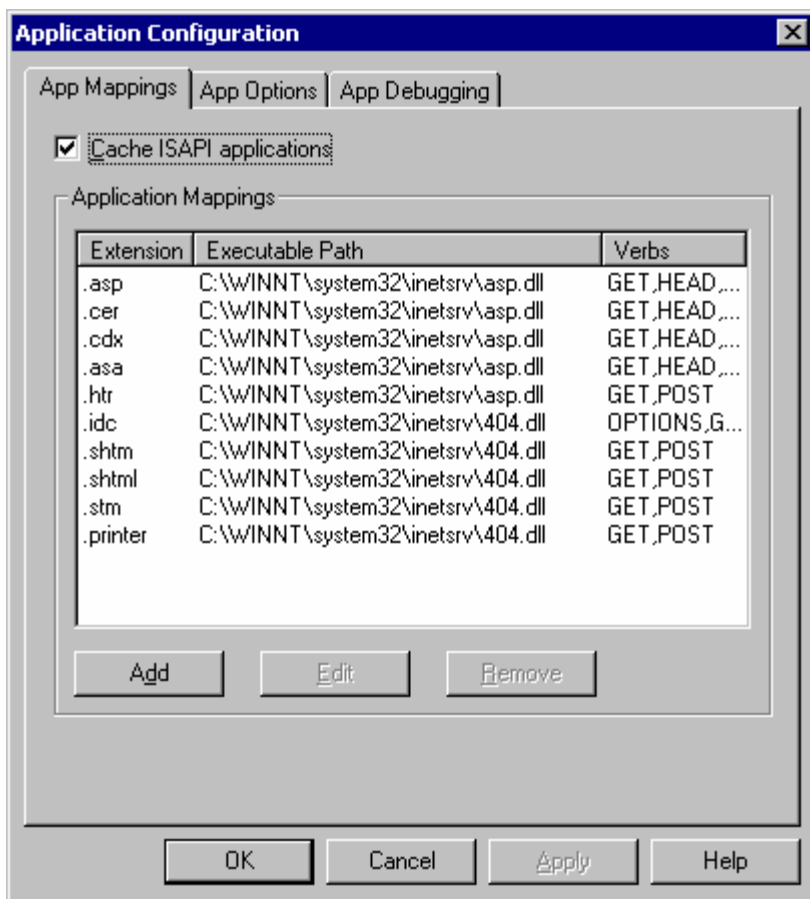


Figure B24: Sample Extension Mappings after IIS Lockdown

After IIS Lockdown completes, as part of removal of script mappings, IIS Lockdown does not delete the mappings, but associates them to a 404.dll.

APPENDIX C – IIS Lockdown Tool V2.1 Sample

Running the IIS lockdown tool is a hardening function to harden the IIS server. This is not part of the audit; the audit will verify settings that may be made by the lockdown tool. The running of the tool is being provided here as a reference to indicate one hardening tool that may be used.



Figure C1: IIS Lockdown Welcome

This is the first screen for running the lockdown tool. This may be considered the splash screen. This tool is a wizard and will present a series of questions and options.

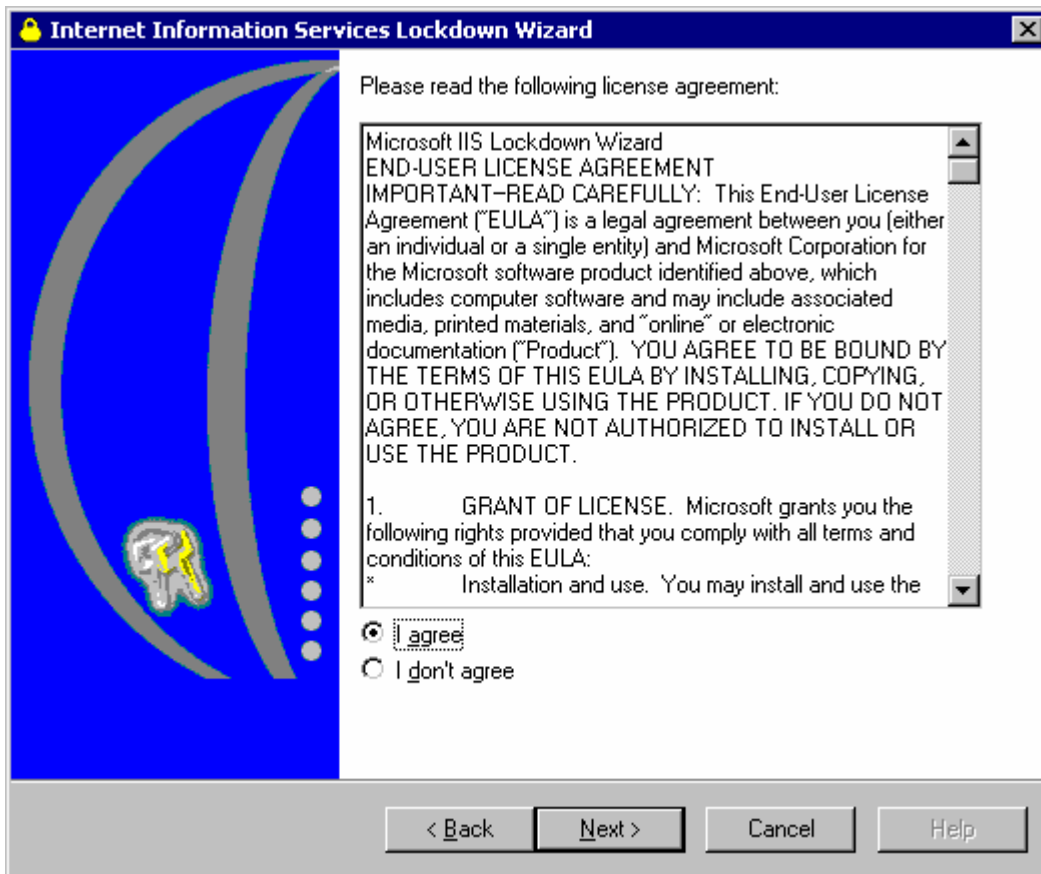


Figure C2: IIS Lockdown EULA

This is the End User License Agreement (EULA) acceptance screen.

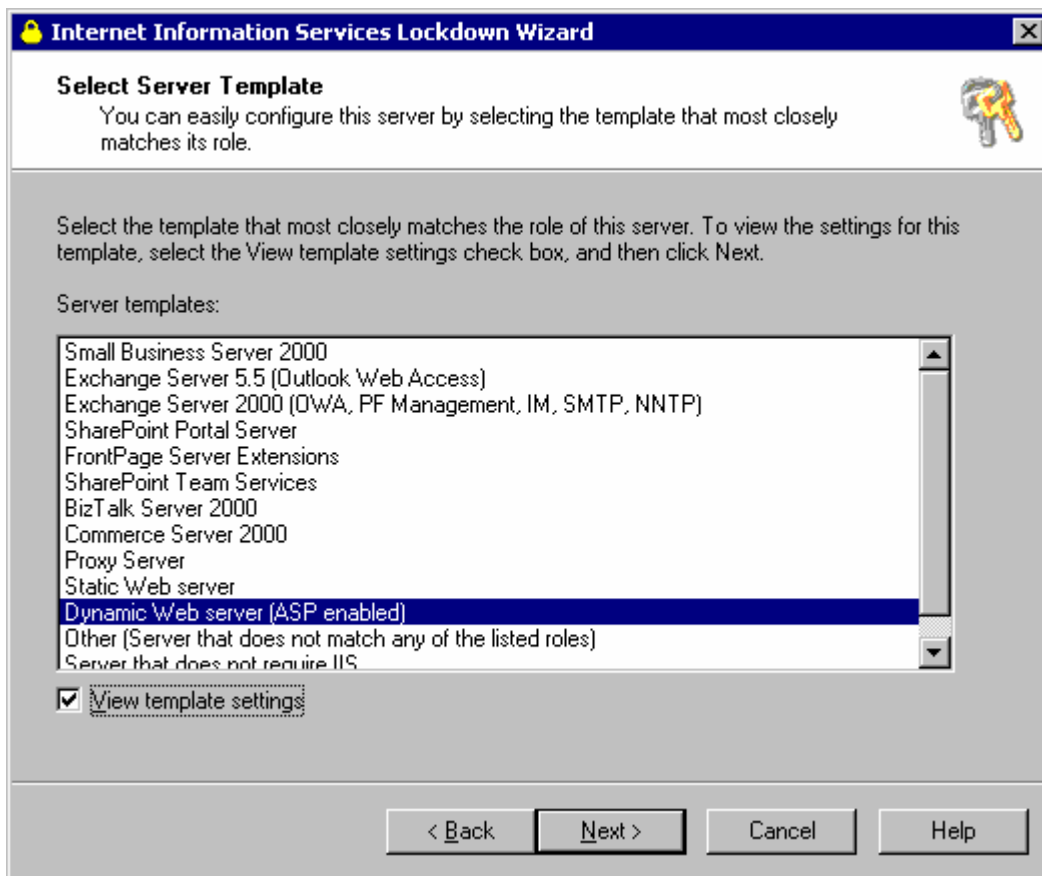


Figure C3: IIS Lockdown Template Selection Screen

This is the template selection screen. There are different IIS configurations that can be selected. By checking the view template settings check box, the wizard will provide additional screens to allow further customization of the template.

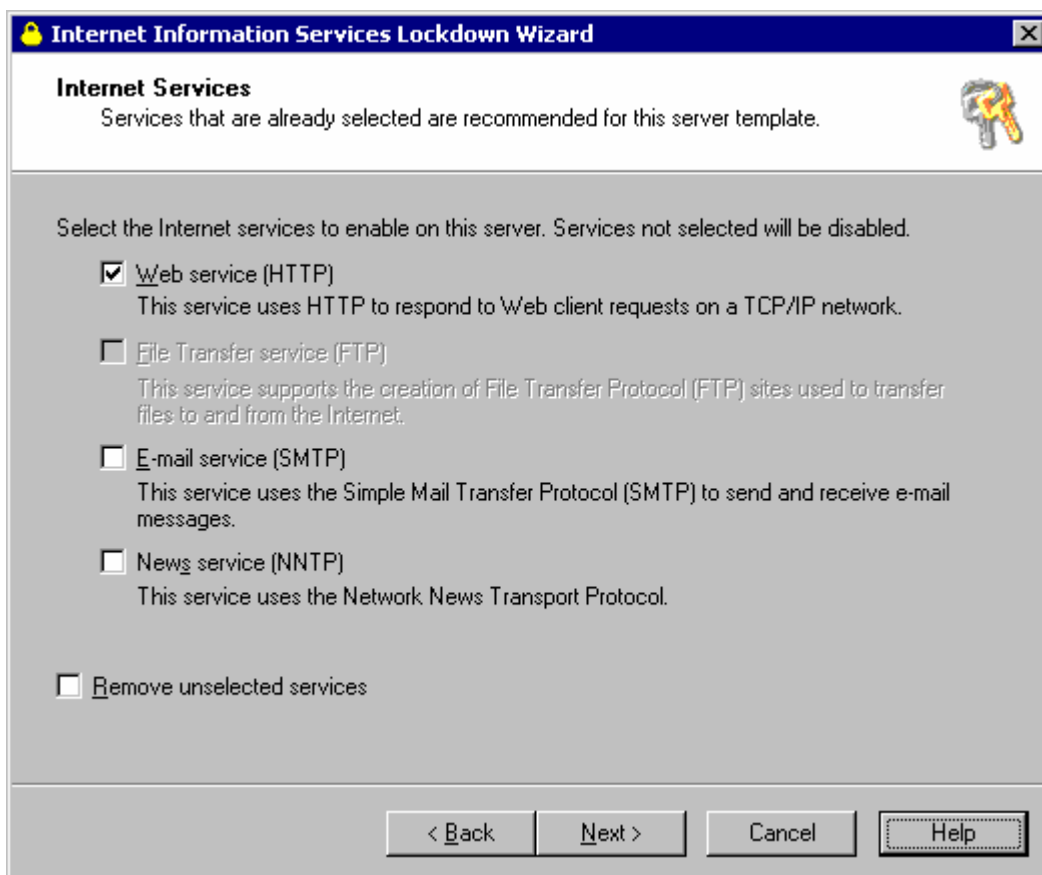


Figure C4: IIS Lockdown Services Selection

For the server that the tool is being run for this example, Web, E-Mail and Network News are installed. For the template selected, which in this sample was dynamic web server, (ASP enabled), only the web server is required and has a check box. If we proceed, the E-Mail and News services will be disabled. If we also were to check the box remove unselected services, E-Mail and News would actually be uninstalled.

This sample was being run on a web server that also runs Exchange and OWA. Leaving E-Mail and News unchecked will break the Exchange server. This would result from using the wrong template, which probably should have been one of the Exchange selections. This is an example where hardening with the wrong parameters can break applications and render them dysfunctional.

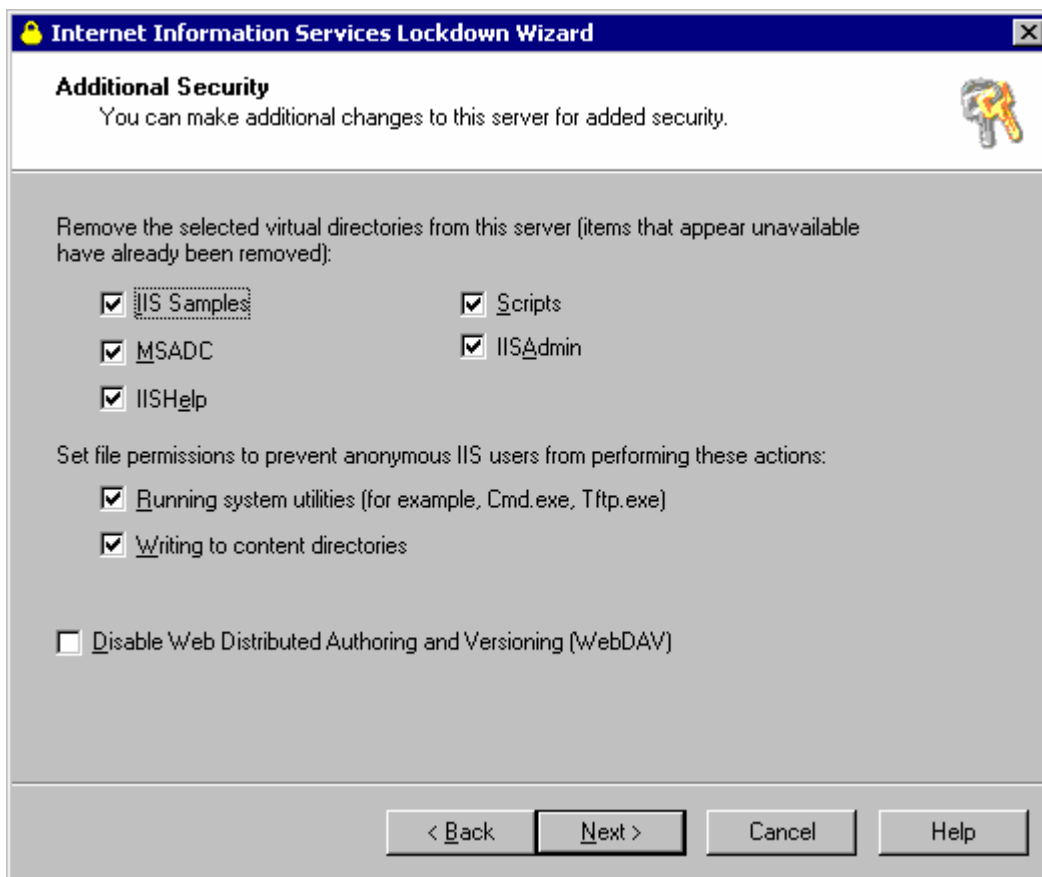


Figure C5: IIS Lockdown Remove Samples

This screen allows changes to be made to select which sample directories are to be removed. Some permission changes can be enforced for system utilities, and WebDav may also be disabled.

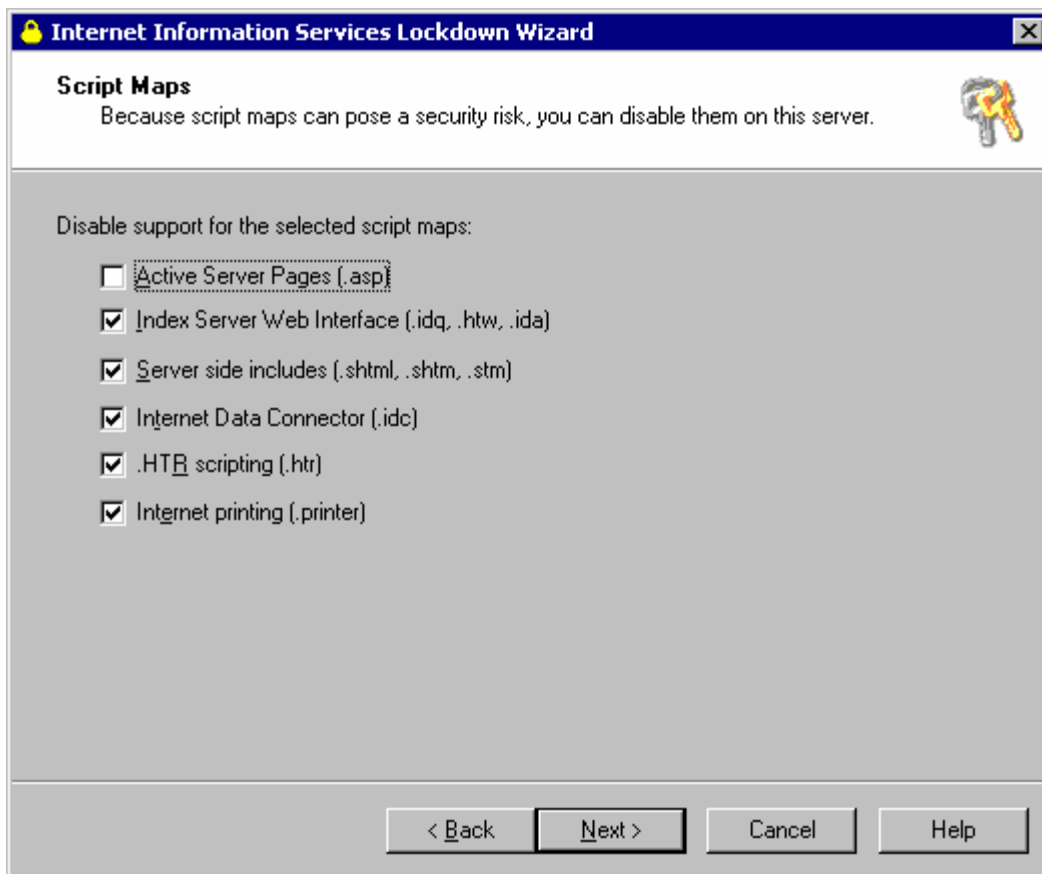


Figure C6: IIS Lockdown Script Mapping Selection

Script mappings will be disabled for the above listed scripts (Except .asp). If you examine Figure B7, the property sheets show the mappings. There are other mappings besides the ones listed above, but the lockdown wizard is built for disabling a specific subset of script mappings. Use the property sheet to check the settings of script mappings.

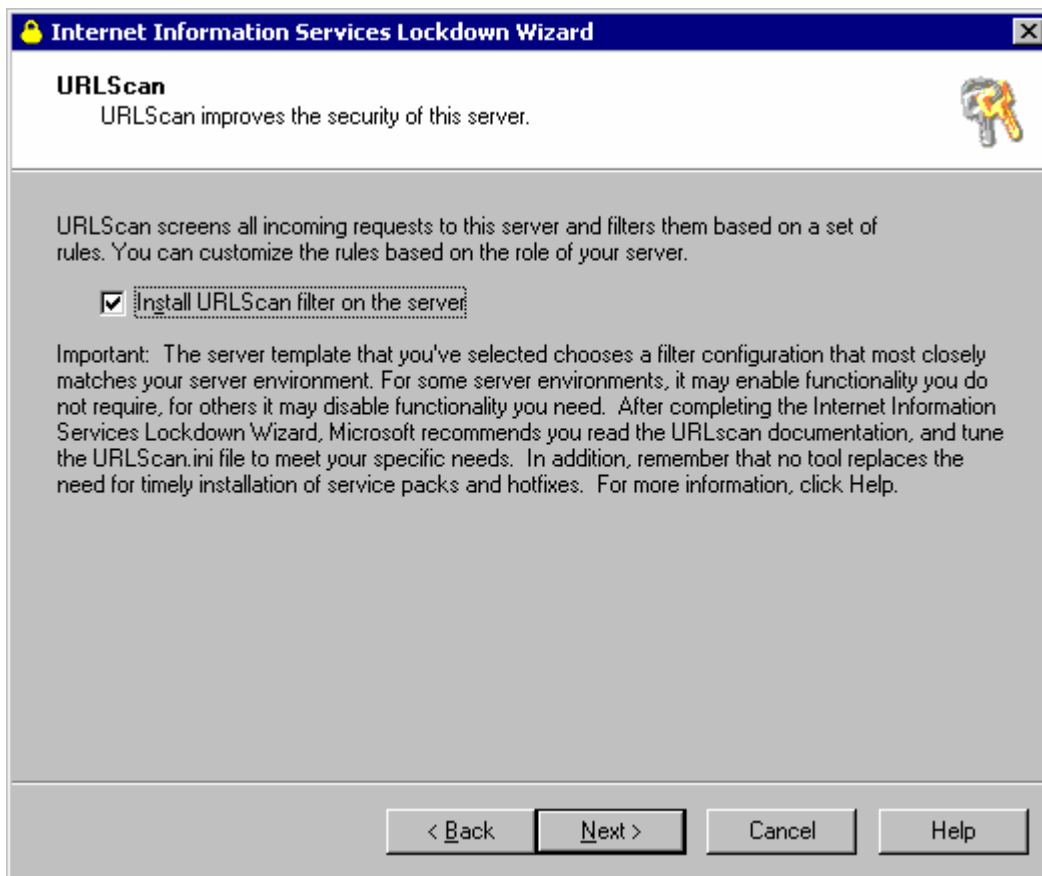


Figure C7: IIS Lockdown URLSCAN Option

URLSCAN is a Microsoft add-on that acts sort of like a host based IDS. It examines the web requests and filters out potentially harmful streams.

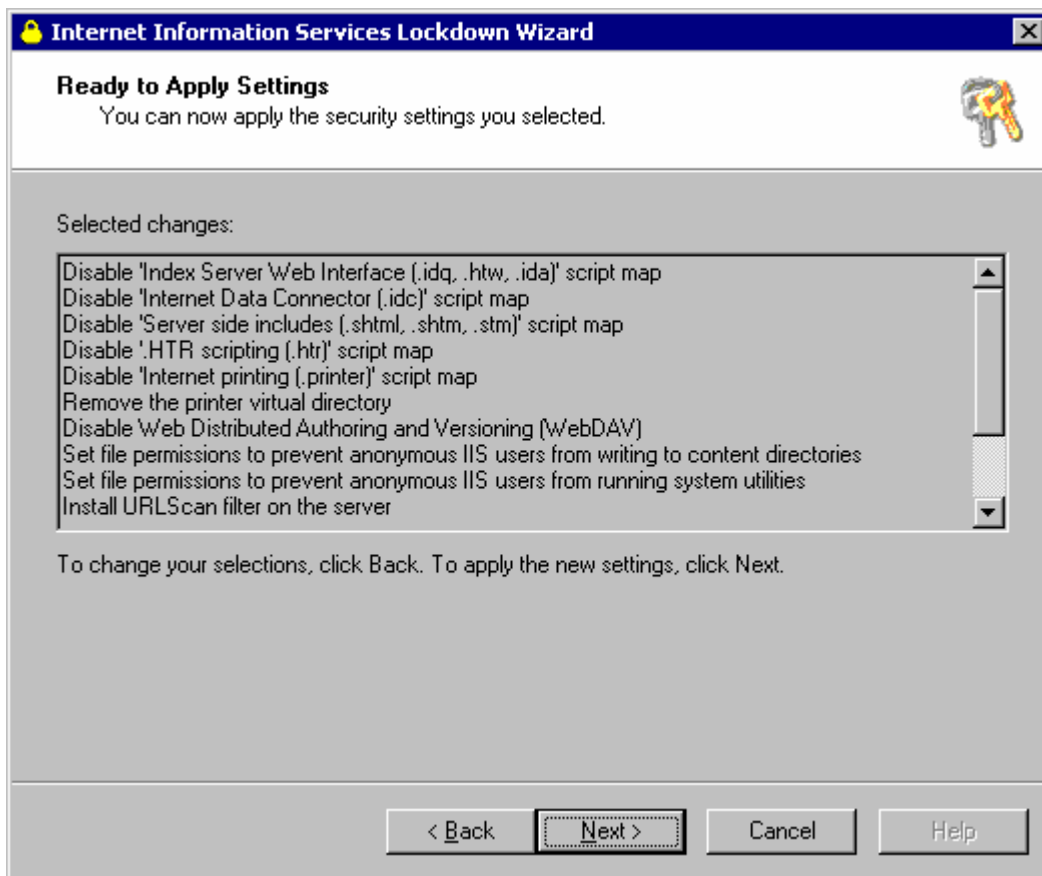


Figure C8: IIS Lockdown Ready To Apply Settings

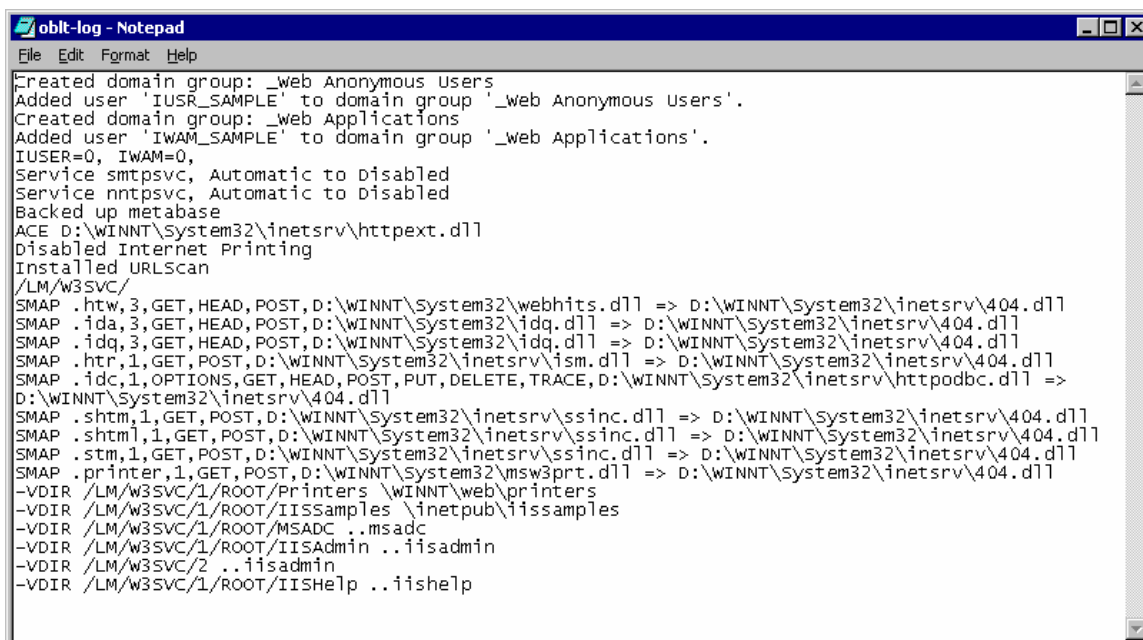
This is a verification screen. This is the last screen showing what will be done if you proceed with the wizard.



Figure C9: IIS Lockdown Already Configured

The wizard can only be run once and it cannot be run for incremental changes. Running the wizard a second time will allow you to back out the settings and restore the configuration.

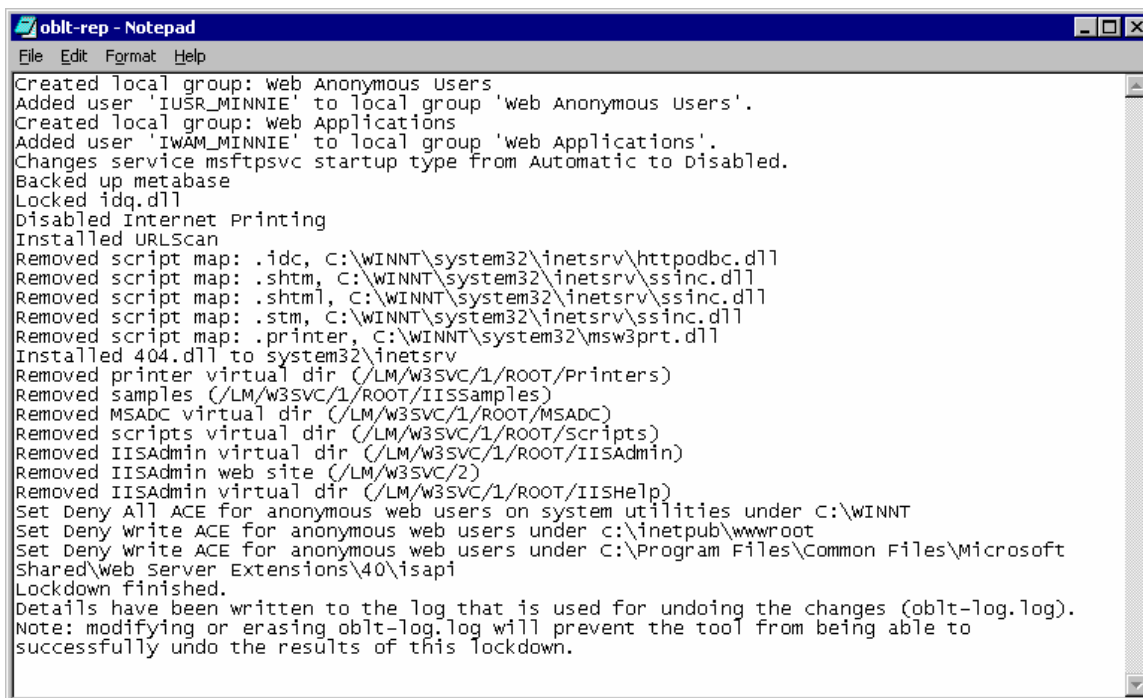
To see the changes made by the lockdown wizard – for a system where the wizard was actually run and changes committed – examine the Oblt-log.log file stored in the inetsrv directory.



```
oblt-log - Notepad
File Edit Format Help
Created domain group: _web Anonymous Users
Added user 'IUSR_SAMPLE' to domain group '_web Anonymous Users'.
Created domain group: _web Applications
Added user 'IWAM_SAMPLE' to domain group '_web Applications'.
IUSER=0, IWAM=0,
Service smtpsvc, Automatic to Disabled
Service nntpsvc, Automatic to Disabled
Backed up metabase
ACE D:\WINNT\System32\inetrv\httpext.dll
Disabled Internet Printing
Installed URLScan
/LM/W3SVC/
SMAP .htw,3,GET,HEAD,POST,D:\WINNT\System32\webhits.dll => D:\WINNT\System32\inetrv\404.dll
SMAP .ida,3,GET,HEAD,POST,D:\WINNT\System32\idq.dll => D:\WINNT\System32\inetrv\404.dll
SMAP .idq,3,GET,HEAD,POST,D:\WINNT\System32\idq.dll => D:\WINNT\System32\inetrv\404.dll
SMAP .htr,1,GET,POST,D:\WINNT\System32\inetrv\ism.dll => D:\WINNT\System32\inetrv\404.dll
SMAP .idc,1,OPTIONS,GET,HEAD,POST,PUT,DELETE,TRACE,D:\WINNT\System32\inetrv\httpodbc.dll =>
D:\WINNT\System32\inetrv\404.dll
SMAP .shtm,1,GET,POST,D:\WINNT\System32\inetrv\ssinc.dll => D:\WINNT\System32\inetrv\404.dll
SMAP .shtm,1,GET,POST,D:\WINNT\System32\inetrv\ssinc.dll => D:\WINNT\System32\inetrv\404.dll
SMAP .stm,1,GET,POST,D:\WINNT\System32\inetrv\ssinc.dll => D:\WINNT\System32\inetrv\404.dll
SMAP .printer,1,GET,POST,D:\WINNT\System32\msw3prt.dll => D:\WINNT\System32\inetrv\404.dll
-VDIR /LM/W3SVC/1/ROOT/Printers \WINNT\web\printers
-VDIR /LM/W3SVC/1/ROOT/IISamples \inetpub\iissamples
-VDIR /LM/W3SVC/1/ROOT/MSADC ..msadc
-VDIR /LM/W3SVC/1/ROOT/IISAdmin ..iisadmin
-VDIR /LM/W3SVC/2 ..iisadmin
-VDIR /LM/W3SVC/1/ROOT/IISHelp ..iishelp
```

Figure C10: Sample OBLT-LOG.LOG File

This is an example Oblt-log.log file.



```
File Edit Format Help
Created local group: web Anonymous Users
Added user 'IUSR_MINNIE' to local group 'web Anonymous Users'.
Created local group: web Applications
Added user 'IWAM_MINNIE' to local group 'web Applications'.
Changes service msftpsvc startup type from Automatic to Disabled.
Backed up metabase
Locked idq.dll
Disabled Internet Printing
Installed URLScan
Removed script map: .idc, C:\WINNT\system32\inetrv\httpodbc.dll
Removed script map: .shtm, C:\WINNT\system32\inetrv\ssinc.dll
Removed script map: .shtml, C:\WINNT\system32\inetrv\ssinc.dll
Removed script map: .stm, C:\WINNT\system32\inetrv\ssinc.dll
Removed script map: .printer, C:\WINNT\system32\msw3prt.dll
Installed 404.dll to system32\inetrv
Removed printer virtual dir (/LM/W3SVC/1/ROOT/Printers)
Removed samples (/LM/W3SVC/1/ROOT/IISamples)
Removed MSADC virtual dir (/LM/W3SVC/1/ROOT/MSADC)
Removed scripts virtual dir (/LM/W3SVC/1/ROOT/Scripts)
Removed IISAdmin virtual dir (/LM/W3SVC/1/ROOT/IISAdmin)
Removed IISAdmin web site (/LM/W3SVC/2)
Removed IISAdmin virtual dir (/LM/W3SVC/1/ROOT/IISHelp)
Set Deny All ACE for anonymous web users on system utilities under C:\WINNT
Set Deny Write ACE for anonymous web users under c:\inetpub\wwwroot
Set Deny Write ACE for anonymous web users under C:\Program Files\Common Files\Microsoft
Shared\Web Server Extensions\40\isapi
Lockdown finished.
Details have been written to the log that is used for undoing the changes (obl-log.log).
Note: modifying or erasing obl-log.log will prevent the tool from being able to
successfully undo the results of this lockdown.
```

Figure C11: Sample IIS Lockdown LOG File

After running the IIS Lockdown tool, you can look at the log of actions taken. The above figure is the results of locking down one of the test systems.

APPENDIX D – MSBA 1.2.1 Install & Run

One part of doing the audit will be checking settings. The Microsoft Security Baseline Analyzer, a free tool from Microsoft, can be used for this function. The software has to be installed on a machine, but does not have to be installed on the machine being audited. If the tool is installed on a different machine, then network access will be required to the target, as well as credentials which have administrative privilege on the target machine.

A compatible version of XML is also required to run the tool. If the tool was run on a NT 4.0 machine, not only would the tool have to be installed, but XML may need to be installed or upgraded. In order to reduce the amount of change to the target machine and to limit being intrusive, the tool is better installed on an “audit” machine and targets scanned across the network.

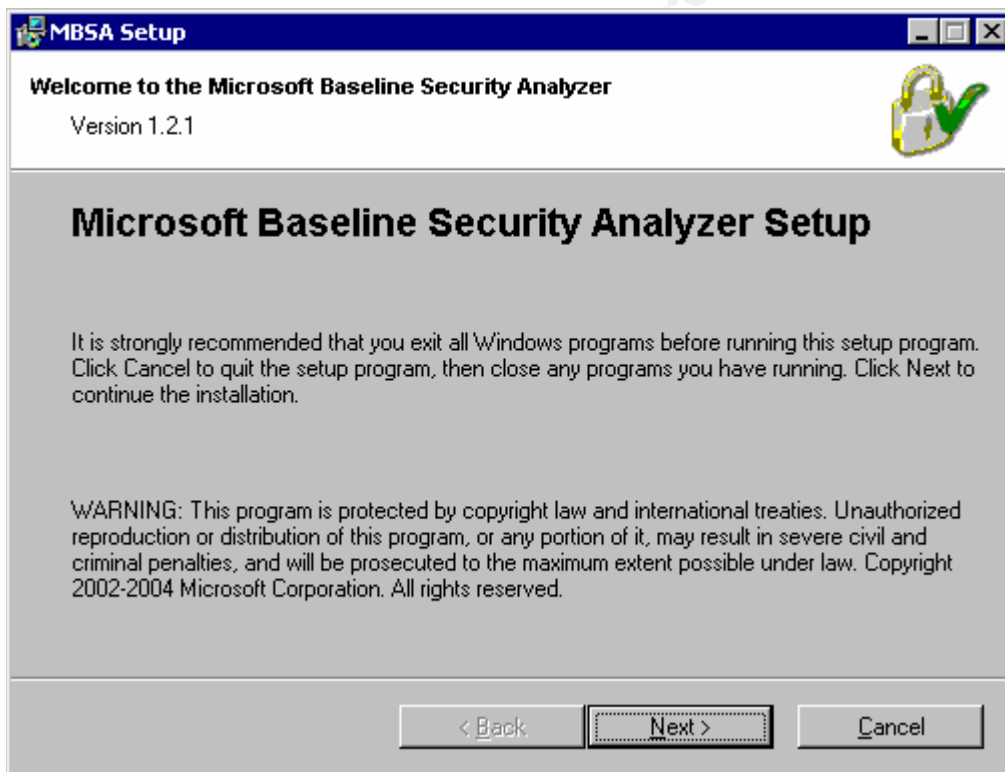


Figure D1: MSBA Splash Screen

Install of the tool got better. In prior releases, when a new release came out, a complete uninstall of the old release was required before upgrade.



Figure D2: MSBA EULA

End User License Agreement (EULA) acceptance screen.

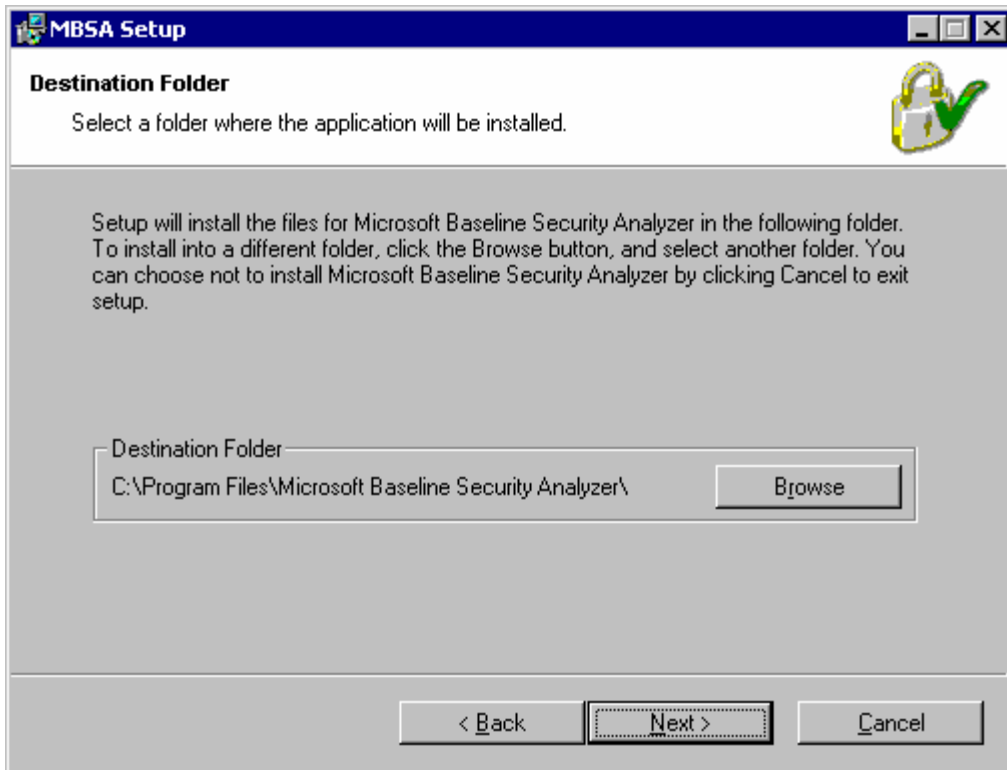


Figure D3: MSBA Destination Folder Selection

Indicate where to install the software.

© SANS Institute 2005, Author

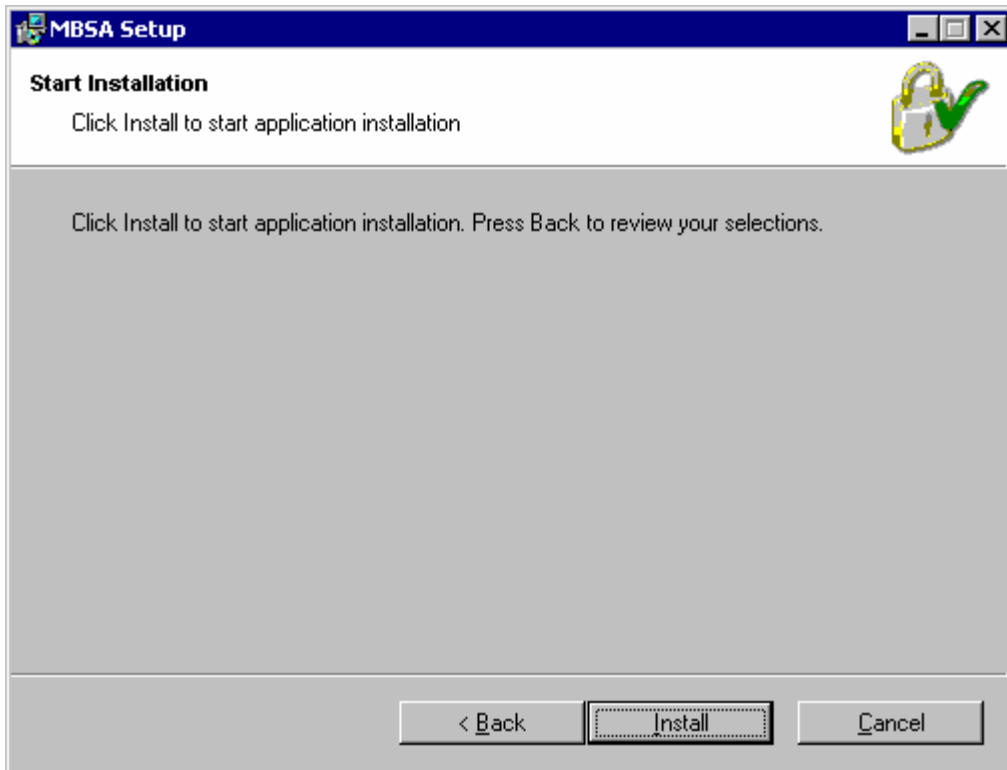


Figure D4: MSBA Setup – Start Installation

Ready, set, go!

© SANS Institute 2005, Author

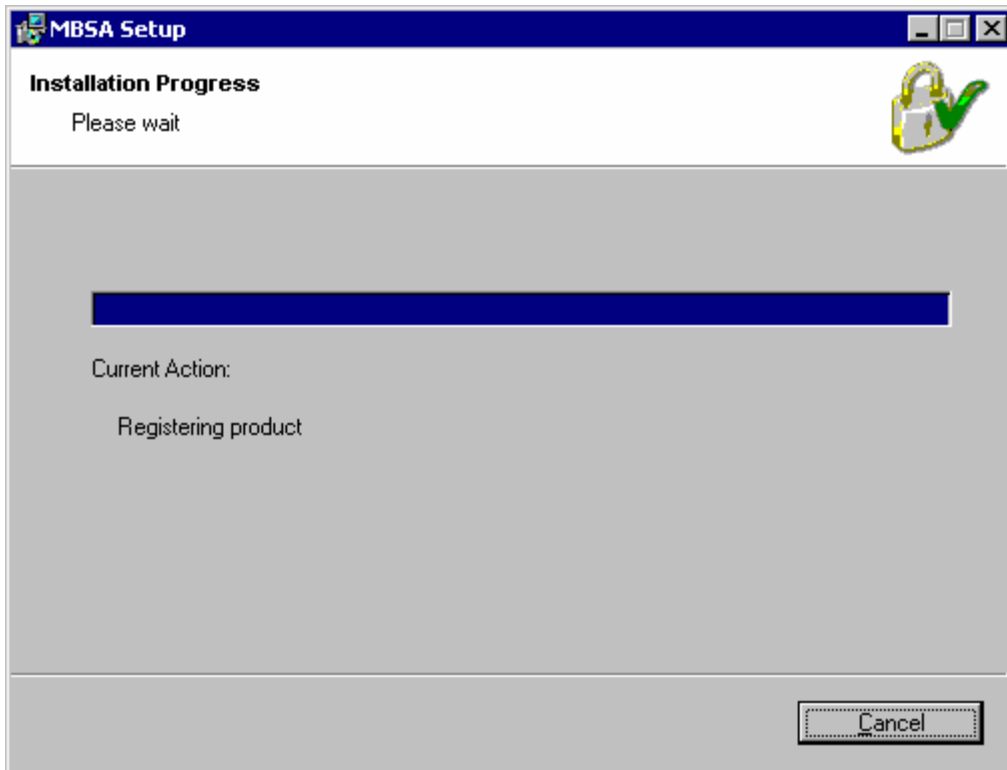


Figure D5: MSBA Installation In Progress, Please Wait

Going!

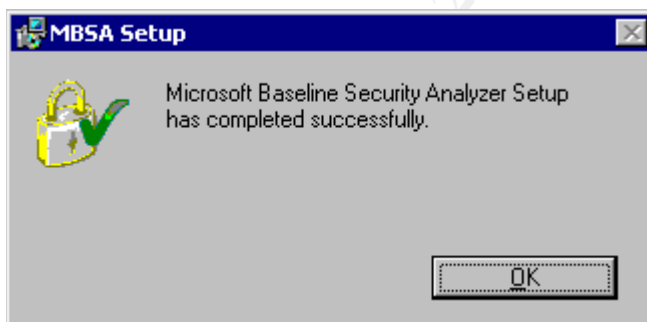


Figure D6: MSBA Install Complete!

Install Complete!

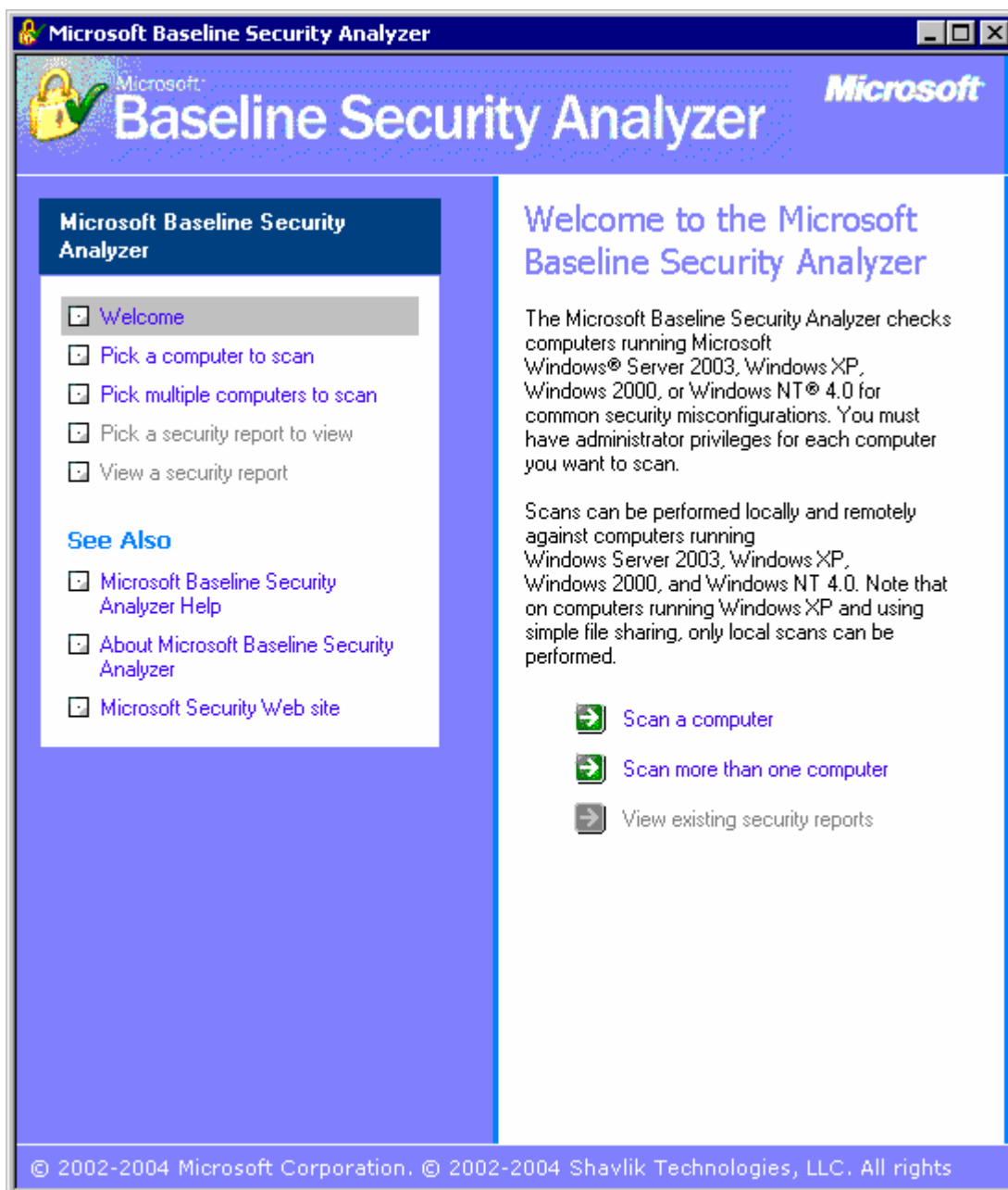


Figure D7: MSBA Function Selection Screen

Let's run a scan, this is the startup screen.

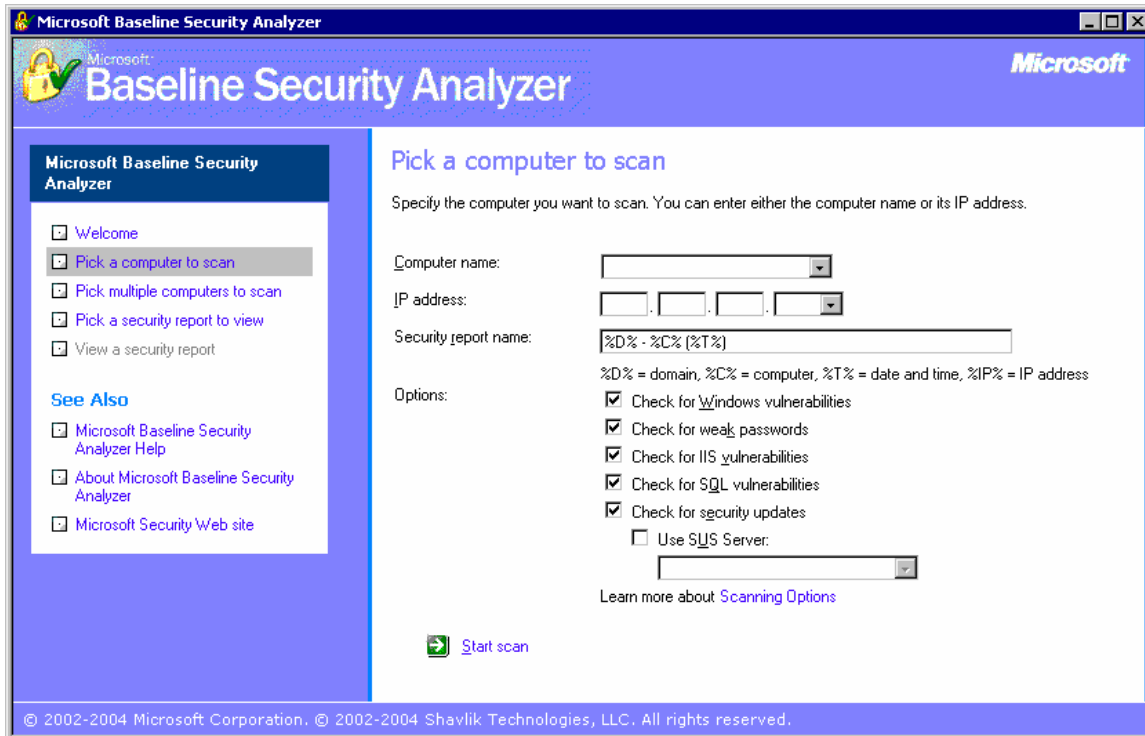


Figure D8: MSBA Scan One Computer

For this example, we will run a scan of one computer.

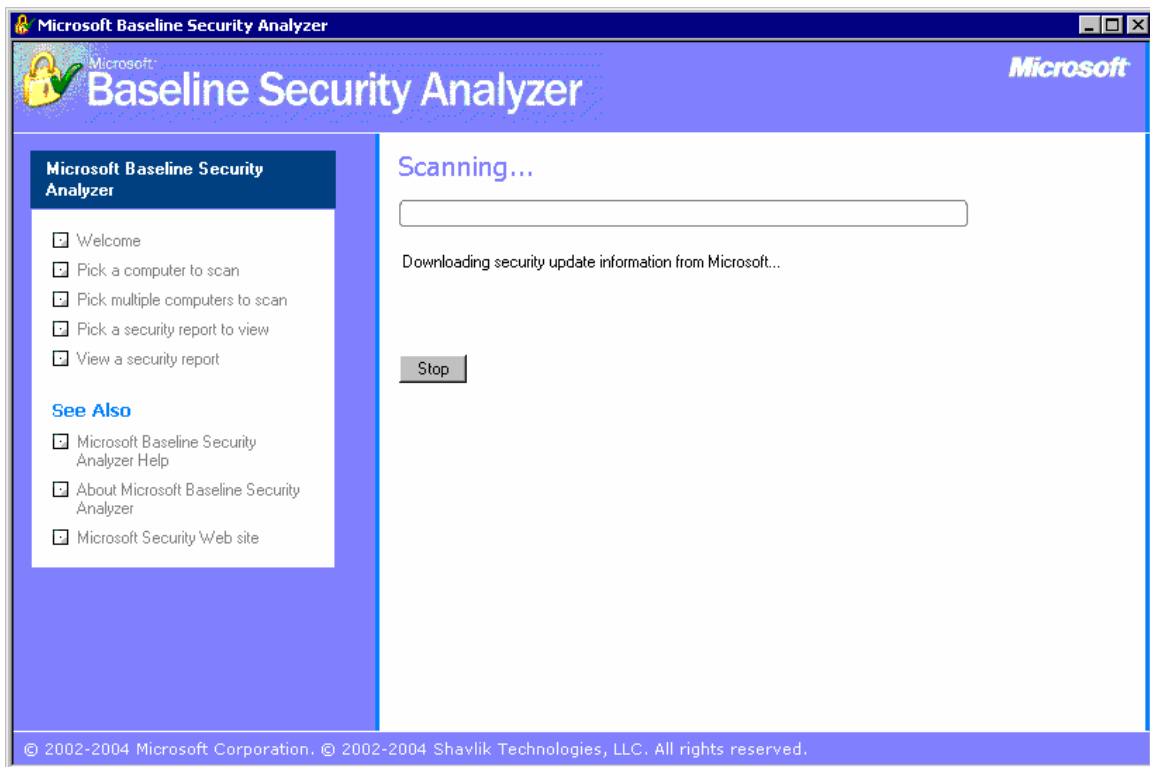


Figure D9: Downloading MSSecure.XML File

Scanning is now in progress. As part of the scan, an XML file known as mssecure.xml is downloaded from the Microsoft site. This will be a zipped version of the file, which will be unzipped in the process.

Mssecure.xml is a database of the security fixes, including hash codes, module version numbers, and other data needed to verify if the security patch has been applied.

In general, when running the tool, a connection to the Internet is required. When this is not possible, the download will fail and the older version resident on the disk will be used. This allows other mechanisms to be used to keep the database up to date when a live Internet connection is not feasible.

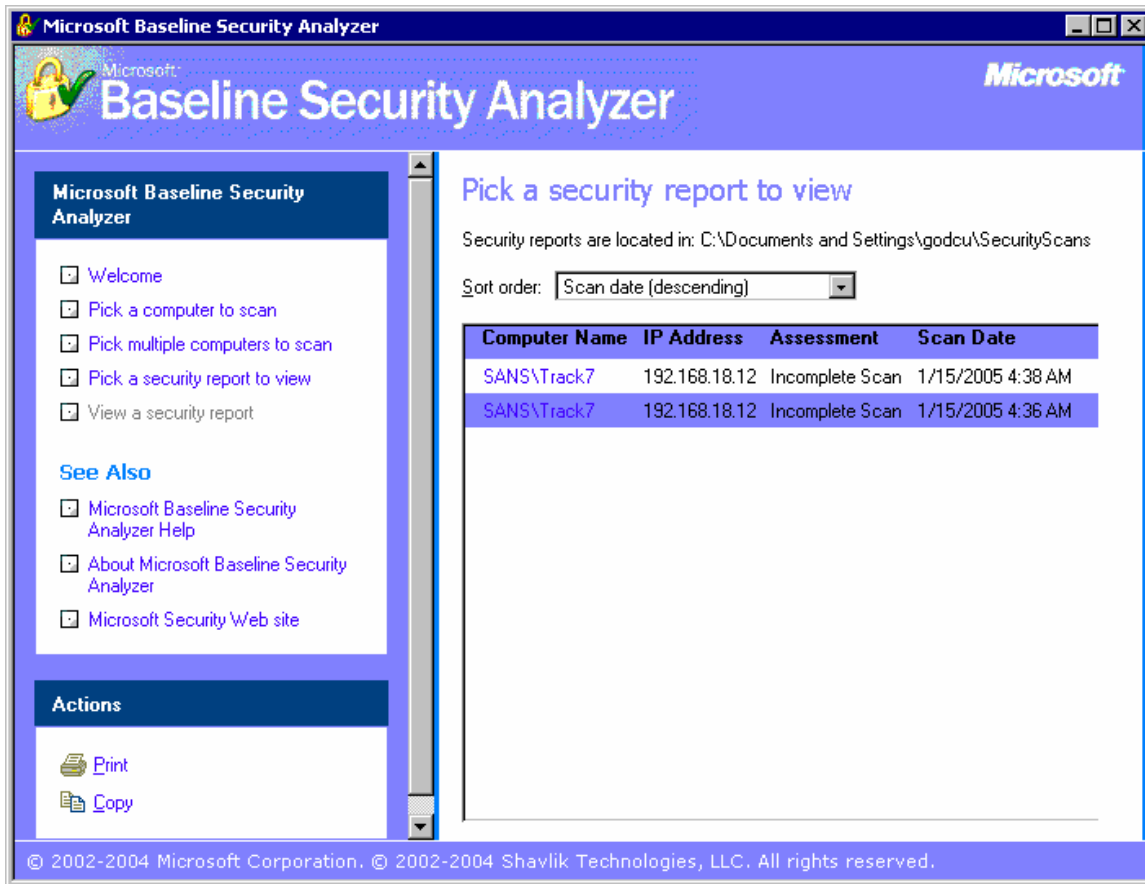


Figure D10: Security Reports Selection Screen

Scans that are run are stored on the system. Older scans can be retrieved at a later time for review. We use the option Pick a security report to view.



Figure D11: Sample MSBA Scan Report

This is sample output from a MSBA scan. One important piece of information is the Security Update Database Version, which in this case is 2005.1.11.0 and is the version of the mssecure XML database. Mssecure contains patch information for security fixes, including hash verification codes. In order to check the installation of the latest versions of the security fixes, the latest version of the mssecure file is required.

If an audit is required of a DMZ server, which is protected via firewalls, you may not have access to the Internet to obtain the latest database. It is recommended that a MSBA be run from while connected to the Internet at least once and very recent to the DMZ scan, before actually going into the DMZ zone. This will insure that the latest, or closest to latest, database will be used.

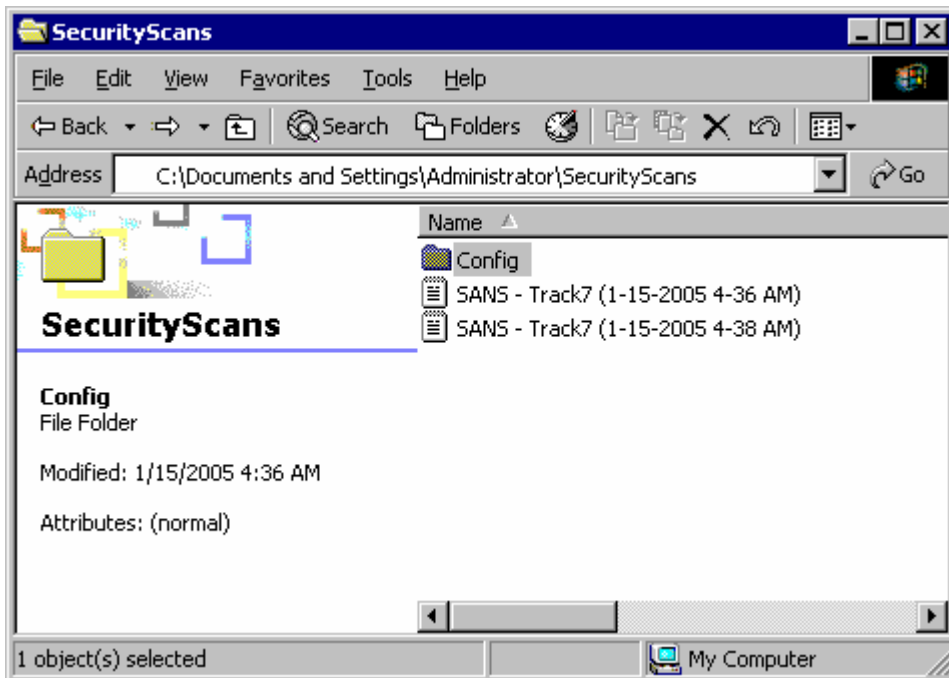


Figure D12: Looking at RAW MSBA XML Files

In D10 above, we saw that there were two security reports that could be reviewed. Each security report is an XML file, saved in the Directory SecurityScans, under the user within documents and settings. These files can be moved to different systems and analyzed there. For example, several computers may be used for scanning large subnets or networks. Each scan will have a XML file. When the scanning is complete, all the XML files can be copied (or moved) to one directory and analysis and reports can be run there.

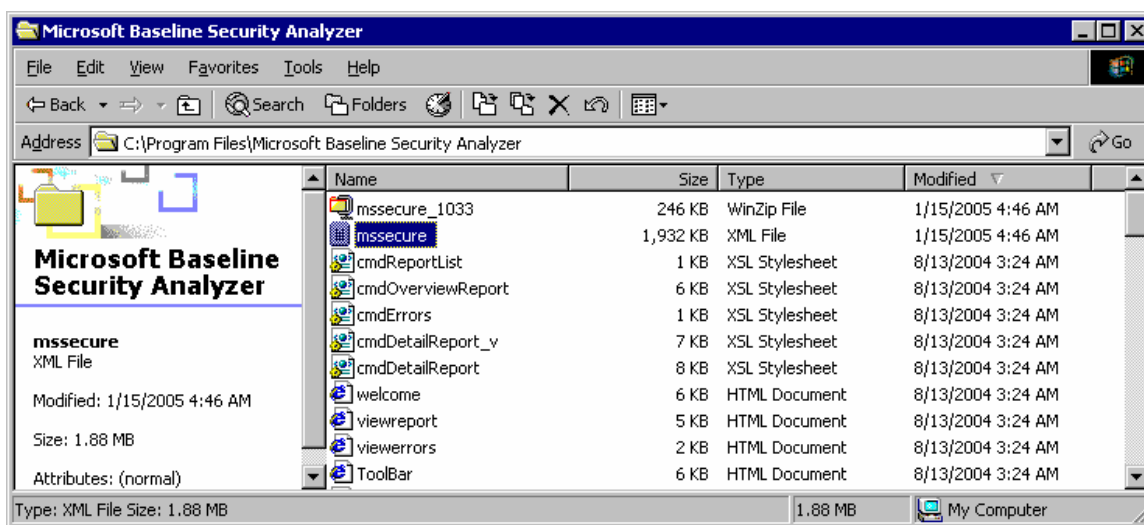


Figure D13: Location where MSSecure.XML file is saved

The mssecure file is located in the Program Files directory where MSBA is installed.

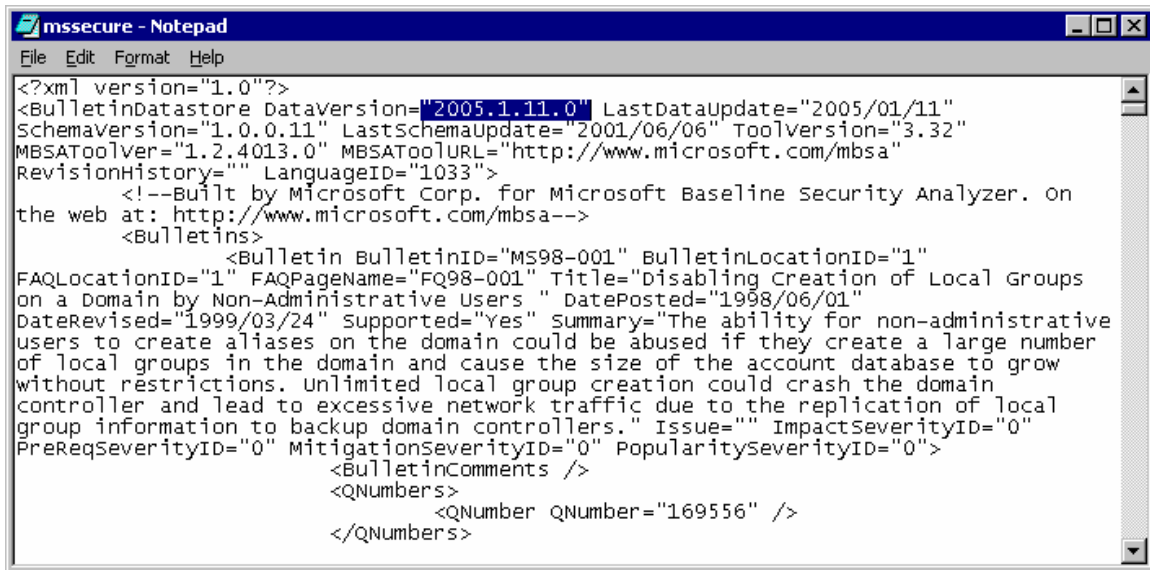


Figure D14: Contents of MSSecure.XML file

This is the mssecure XML file open in notepad. Notice the highlight database version number, which is: 2005.1.11.0 which may also be observed in Figure D11.

APPENDIX E – Target System Characteristics

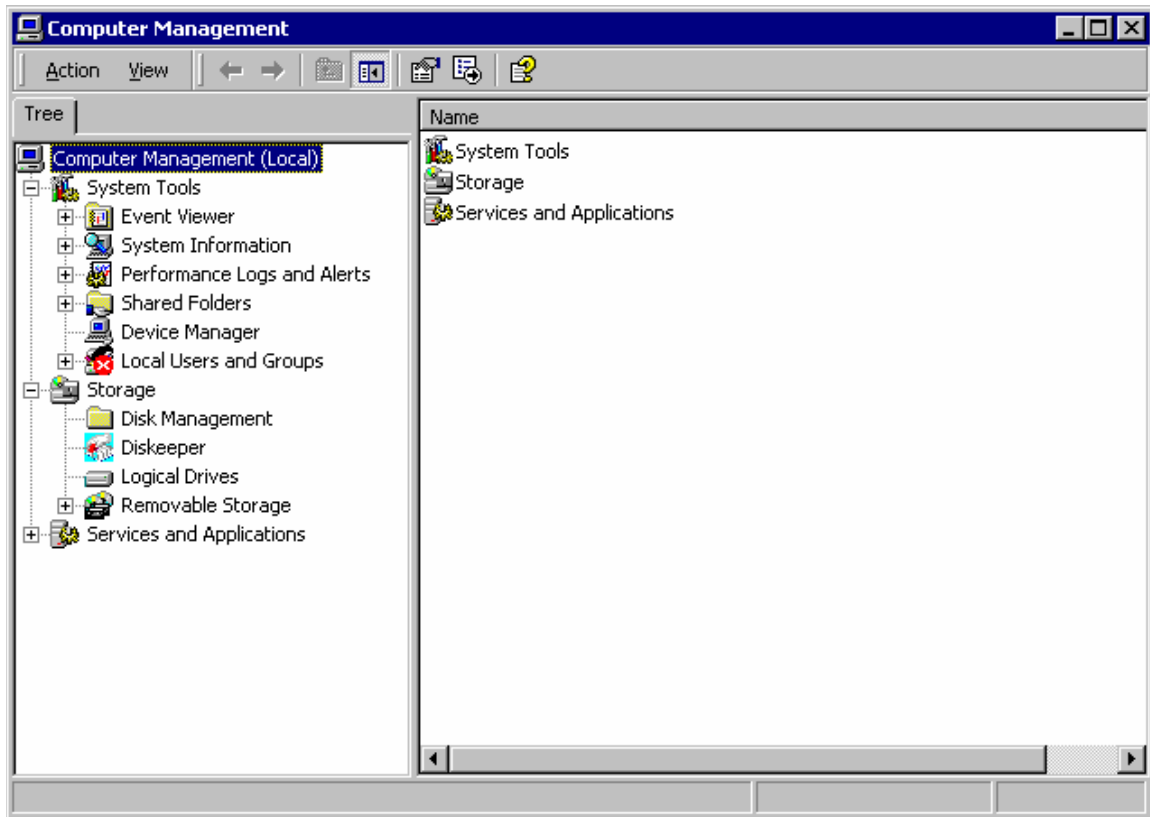


Figure E1: Computer Management

With Windows 2000 and above, the Computer Management console provides system information in the system tools tree. Computer Management is accessed from the Administrator Tools menu.

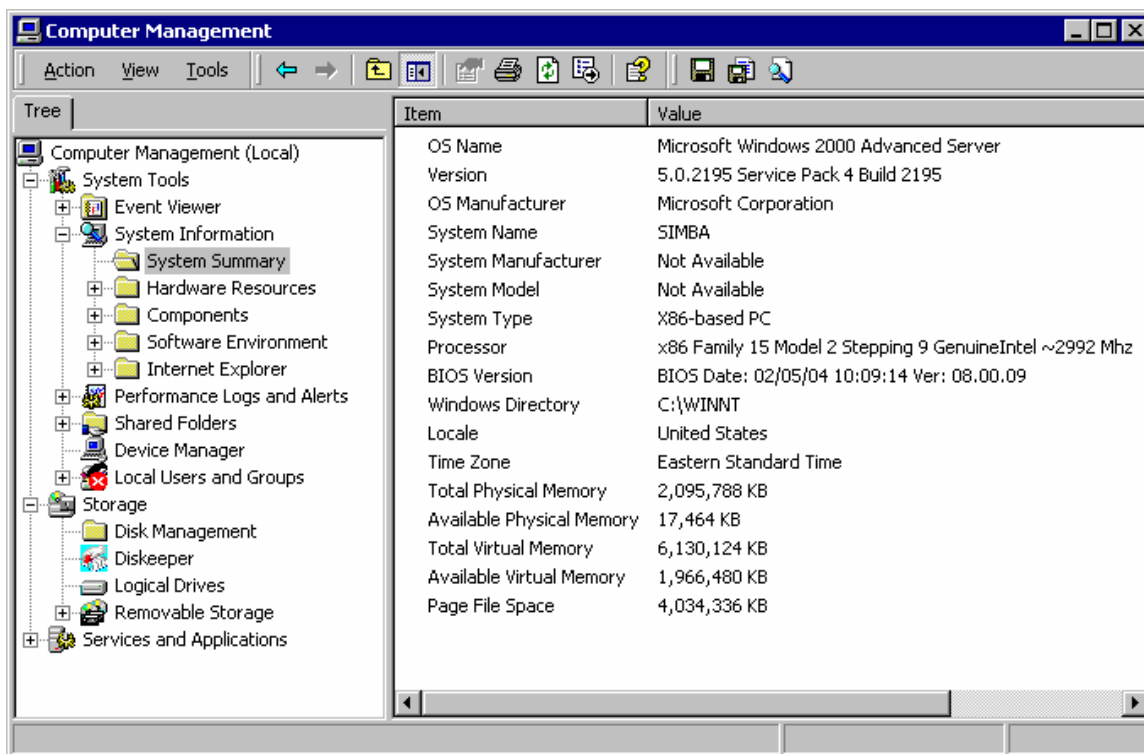
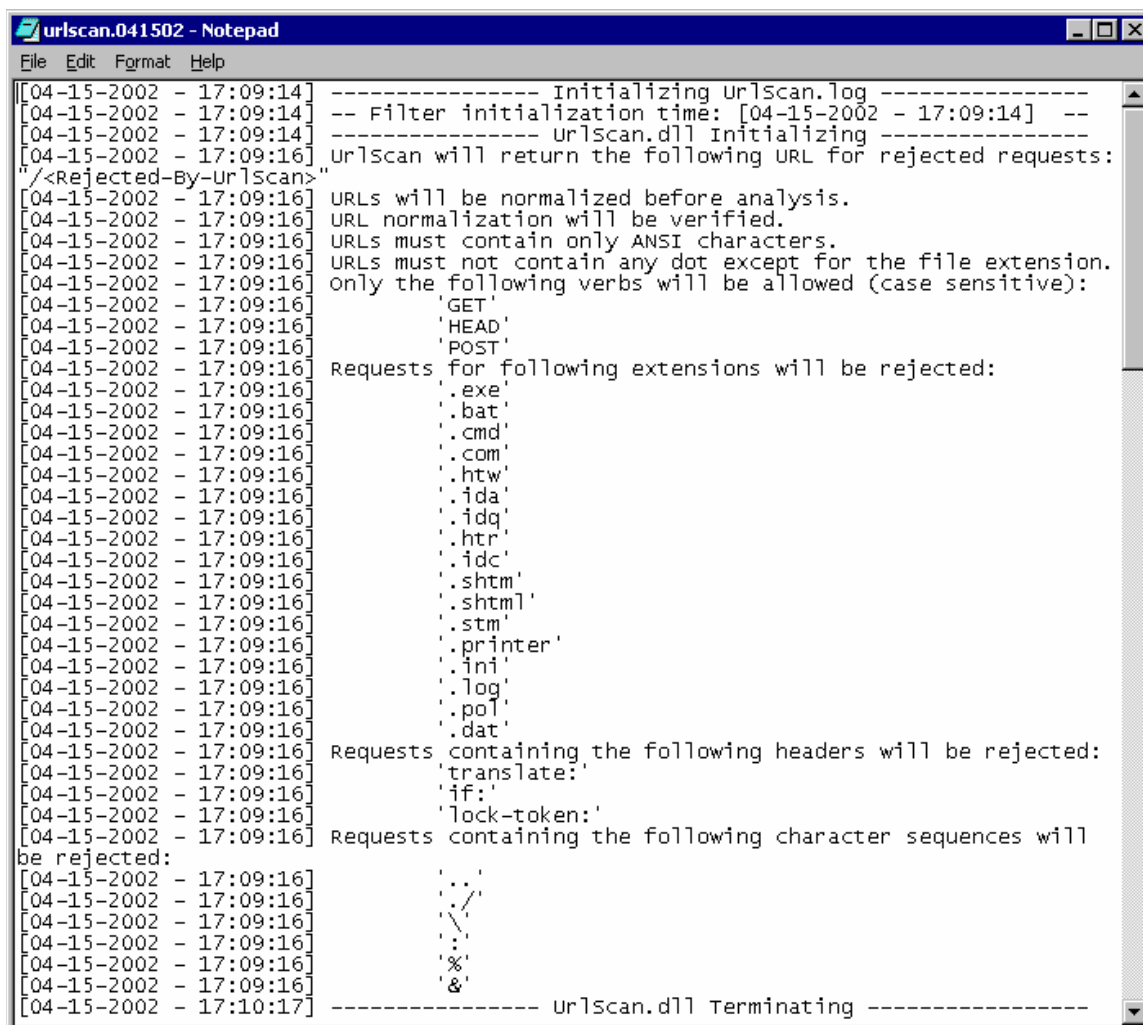


Figure E2: Computer Management – System Summary

System information provides details about the current hardware configuration. A command line version may also be used, WINMSD. Older releases of Windows may just require MSD. MSD stands for Microsoft System Diagnostics.

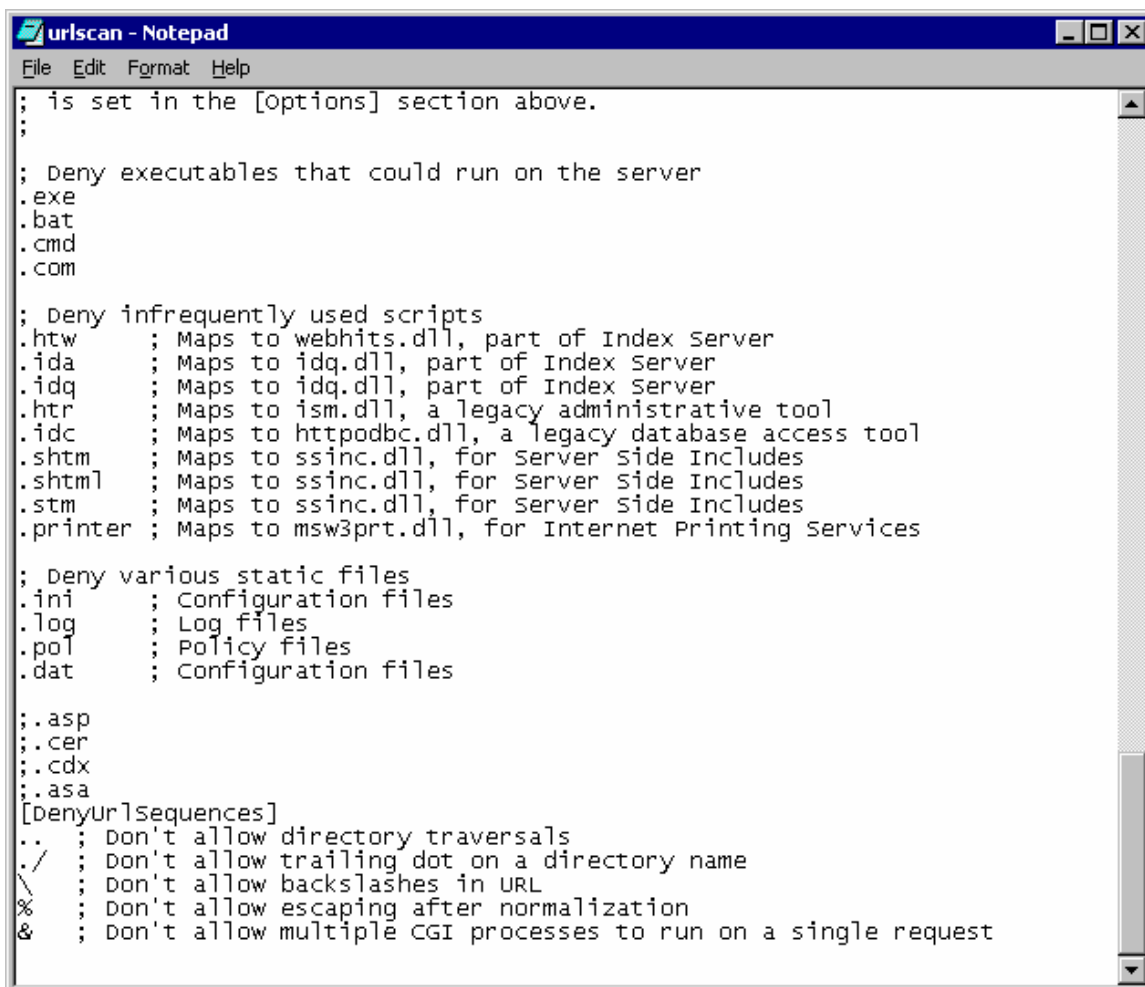
APPENDIX F – URLScan



```
[04-15-2002 - 17:09:14] ----- Initializing Urlscan.log -----
[04-15-2002 - 17:09:14] -- Filter initialization time: [04-15-2002 - 17:09:14] --
[04-15-2002 - 17:09:14] ----- Urlscan.dll Initializing -----
[04-15-2002 - 17:09:16] Urlscan will return the following URL for rejected requests:
"/<Rejected-By-Urlscan>"
[04-15-2002 - 17:09:16] URLs will be normalized before analysis.
[04-15-2002 - 17:09:16] URL normalization will be verified.
[04-15-2002 - 17:09:16] URLs must contain only ANSI characters.
[04-15-2002 - 17:09:16] URLs must not contain any dot except for the file extension.
[04-15-2002 - 17:09:16] only the following verbs will be allowed (case sensitive):
[04-15-2002 - 17:09:16] 'GET'
[04-15-2002 - 17:09:16] 'HEAD'
[04-15-2002 - 17:09:16] 'POST'
[04-15-2002 - 17:09:16] Requests for following extensions will be rejected:
[04-15-2002 - 17:09:16] '.exe'
[04-15-2002 - 17:09:16] '.bat'
[04-15-2002 - 17:09:16] '.cmd'
[04-15-2002 - 17:09:16] '.com'
[04-15-2002 - 17:09:16] '.htw'
[04-15-2002 - 17:09:16] '.ida'
[04-15-2002 - 17:09:16] '.idq'
[04-15-2002 - 17:09:16] '.htr'
[04-15-2002 - 17:09:16] '.idc'
[04-15-2002 - 17:09:16] '.shtm'
[04-15-2002 - 17:09:16] '.shtml'
[04-15-2002 - 17:09:16] '.stm'
[04-15-2002 - 17:09:16] '.printer'
[04-15-2002 - 17:09:16] '.ini'
[04-15-2002 - 17:09:16] '.log'
[04-15-2002 - 17:09:16] '.pol'
[04-15-2002 - 17:09:16] '.dat'
[04-15-2002 - 17:09:16] Requests containing the following headers will be rejected:
[04-15-2002 - 17:09:16] 'translate:'
[04-15-2002 - 17:09:16] 'if:'
[04-15-2002 - 17:09:16] 'lock-token:'
[04-15-2002 - 17:09:16] Requests containing the following character sequences will
be rejected:
[04-15-2002 - 17:09:16] '...'
[04-15-2002 - 17:09:16] '...'
[04-15-2002 - 17:09:16] '...'
[04-15-2002 - 17:09:16] '...'
[04-15-2002 - 17:09:16] '...'
[04-15-2002 - 17:10:17] ----- Urlscan.dll Terminating -----
```

Figure F1: Sample URLSCAN.LOG Initialization

The comments in the log provide information on actions that will be taken by the filter.



```
; is set in the [options] section above.
;
; Deny executables that could run on the server
.exe
.bat
.cmd
.com

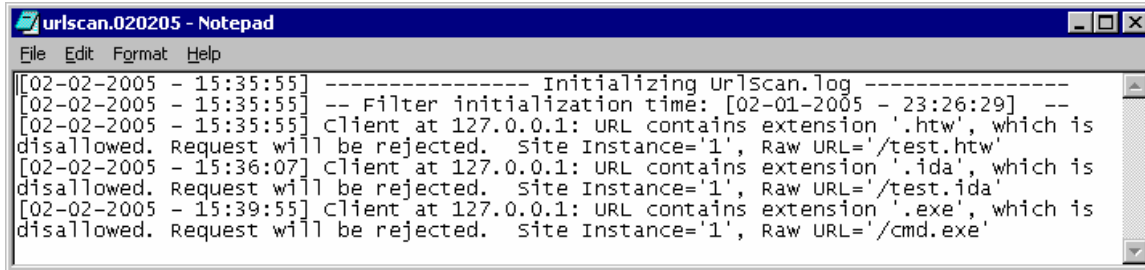
; Deny infrequently used scripts
.htw      ; Maps to webhits.dll, part of Index Server
.ida      ; Maps to idq.dll, part of Index Server
.idq      ; Maps to idq.dll, part of Index Server
.htr      ; Maps to ism.dll, a legacy administrative tool
.idc      ; Maps to httpodbc.dll, a legacy database access tool
.shtm     ; Maps to ssinc.dll, for Server Side Includes
.shtml    ; Maps to ssinc.dll, for Server Side Includes
.stm      ; Maps to ssinc.dll, for Server Side Includes
.printer  ; Maps to msw3prt.dll, for Internet Printing Services

; Deny various static files
.ini      ; Configuration files
.log      ; Log files
.pol      ; Policy files
.dat      ; Configuration files

;.asp
;.cer
;.cdx
;.asa
[Denyurlsequences]
..      ; Don't allow directory traversals
./      ; Don't allow trailing dot on a directory name
\       ; Don't allow backslashes in URL
%       ; Don't allow escaping after normalization
&       ; Don't allow multiple CGI processes to run on a single request
```

Figure F2: Sample URLSCAN.INI File

The file is large. However, this screenshot shows that script mappings and other extensions (i.e. exe, bat, com & cmd) can be filtered and addressed by the URLSCAN function.



```
urlscan.020205 - Notepad
File Edit Format Help
[02-02-2005 - 15:35:55] ----- Initializing UrlScan.log -----
[02-02-2005 - 15:35:55] -- Filter initialization time: [02-01-2005 - 23:26:29] --
[02-02-2005 - 15:35:55] Client at 127.0.0.1: URL contains extension '.htw', which is
disallowed. Request will be rejected. Site Instance='1', Raw URL='/test.htw'
[02-02-2005 - 15:36:07] Client at 127.0.0.1: URL contains extension '.ida', which is
disallowed. Request will be rejected. Site Instance='1', Raw URL='/test.ida'
[02-02-2005 - 15:39:55] Client at 127.0.0.1: URL contains extension '.exe', which is
disallowed. Request will be rejected. Site Instance='1', Raw URL='/cmd.exe'
```

Figure F3: Sample URLSCAN.LOG File

If URLSCAN is installed, how do you know if it is actually working? Well, you can feed suspect URL's and see if URLSCAN bites. I ran three sample commands, each one ending in .HTW, .IDA and .EXE. And for each attempt, there is a log entry in the URLSCAN log file. This indicates that URLSCAN is at least filtering those commands from the URL strings. If these are not filtered, then it does not immediately indicate a failure of URLSCAN until you can make sure that the URLSCAN.INI file (See Figure F2 above) is enabled for those extensions.