Using Microsoft's IISlockdown tool to protect your IIS Web Server

Name: Jeff Wichman

Date: 1/4/2002

Version: GSEC 1.2f

Course Attended: Great Lakes Sans

Abstract

The topic of this paper is to give informational instructions on the IISlockdown tool. The paper will include information from the Great Lakes Sans conference, common exploits for IIS servers, best practices for installing the IISlockdown tool and information on tools used to test the server following the installation. The test system is a default installation of Windows 2000 Server current with all service packs and hotfixes.

Introduction

In the past year the hacking community has kept server administrators of Microsoft's Internet Information Service (IIS) busy. In August 2001 Microsoft released the IISlockdown tool, which is an automated wizard used to shutdown unnecessary features that are deployed during a default installation of IIS. The IISlockdown tool can remove unused services, modify file permissions, modify registry settings and remove application mappings that have proven to be vulnerable to attacks. Microsoft is making the tools available to the community, but administrators still must secure their systems.

Before we jump into the IISlockdown tool, let's examine some of the vulnerability facts that relate to IIS servers.

Vulnerability Facts

According to the defacement archive at alldas.de, Microsoft web servers have accounted for sixty-one percent of all defaced web sites since April 2000. IIS is the leading target in web site defacement and server compromises due to default installations, untrained systems administrators and buffer overflows in Microsoft's coding. With OS hardening techniques, trained system administrators and proper configurations of IIS we could have a relatively secure web server.

Table 1.1 lists some of the common vulnerabilities found on an IIS server and the percentages of servers that were found to be vulnerable during NetCraft's Web Server Survey from June 2001 to October 2001. NetCraft polled over 33 million sites for the data in October's survey and found that one in nine IIS servers could be taken over by hackers. Imagine a new worm that could exploit the sites with their administration pages accessible. The worm would install a Trinoo Flood agent and the resulting Distributed Denial of Service (DDoS) that could be performed would contain an estimated 8,000,000 agents attacking any given target.

(Items followed by * are addressed with the IISlockdown tool depending upon the settings chosen)

	June-01	July-01	Aug-01	Sept-01	Oct-01
Administration pages accessible*	35.71 %	11.76 %	10.26 %	17.14 %	24.69 %
Cross-site scripting*	57.14 %	36.47 %	19.23 %	22.86 %	13.58 %
URL Decode bugs*	42.86 %	32.94 %	16.67 %	17.14 %	12.35 %
Sample pages and scripts*	28.57 %	14.12 %	16.67 %	17.14 %	25.93 %
Server path revealed*	50.00 %	22.94 %	6.41 %	8.57 %	9.88 %
Viewing script source code*	21.43 %	11.18 %	3.85 %	11.47 %	4.94 %
WebDAV configuration*	50.00 %	47.65 %	43.59 %	37.14 %	34.57 %
IIS .printer overflow*	21.43 %	10.00 %	2.56 %	2.86 %	1.23 %
Code Red Vulnerable*	14.29 %	34.71 %	2.00 %	0.00 %	2.47 %
Root.exe installed*	7.14 %	10.00 %	12.82 %	8.57 %	11.11 %

Table 1.1

Some of the recent exploits that have made the news that directly affect IIS servers are:

Sadmind/IIS, CodeRed I & II and Nimda

The last item from Table 1.1 (root.exe) refers to the recent IIS worms and is usually found on compromised servers in the C:\Inetpub\scripts directory. The file is a copy of the cmd.exe executable and is used by remote attackers to execute programs on the compromised server.

With the installation of the IISlockdown tool an IIS server will be protected from many of the recent exploits including the top three Windows related vulnerabilities found on the SANS/FBI Top 20 List. It is still highly recommended by Microsoft and the security community to keep servers up to date with service packs and hotfixes.

Pre-Installation

During the Sans Great Lakes Conference, Eric Cole, Director of the SANS CDI (Cyber Defense Initiative) explained four points of system and network security. I personally consider them to be the foundation of security. Each of the foundation items should be examined before performing any type of installation for potential issues with the operations and security of a network.

1. Know your system.
   - What services are running?
   - What ports are open?
   - What type of site(s) does the server provide?
   - Who has physical access? Remote access?
   - What are the other applications that are available on the server?
   - When was the last backup?
2. Defense in depth
   - Filtering ports at the router.
   - Harden the operating system.
   - Follow an IIS Security Checklist.
   - Access controls on server.
   - Physically secure the server.
3. Privilege of least privilege
   - User rights are what they need to complete their job.
4. Prevention is ideal, but protection is a must.
   - There is no one way to prevent attacks, but with good practices you can protect your network, servers and desktops.
   - Keeping up with protection will help in preventing successful attacks.

System Requirements

System Requirements:

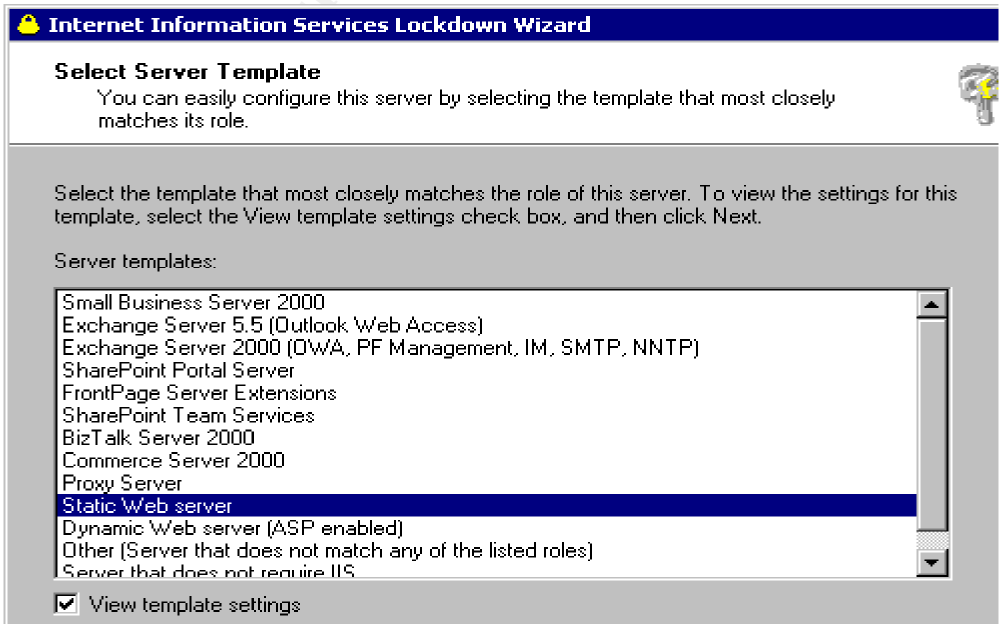
- Operating System
  - Windows NT 4.0 *or*
  - Windows 2000 Professional, Server, or Advanced Server
- IIS Service
  - IIS 4.0 on NT 4.0 *or*
  - IIS 5.0 on Windows 2000
- Latest service packs and hotfixes

As stated in the pre-installation section, the administrator needs to know what type of web sites and services that are running on the server before the installation of the IISlockdown tool. The IISlockdown tool will be modifying settings for the IIS server and could potentially cause the server to stop responding to requests.

Installation

Microsoft has made the installation wizard as simple as possible by providing templates for many of the common Microsoft server roles. Figure 1.1 shows the templates available in version 2.1 of the IISlockdown tool. The templates assist in providing a smooth installation and they attempt to minimize the mistakes that could be made. The templates are a nice addition from the previous versions, but the administrator still must understand what the template script will do to the server.

1) Template options



Internet Information Services Lockdown Wizard

Select Server Template

You can easily configure this server by selecting the template that most closely matches its role.

Select the template that most closely matches the role of this server. To view the settings for this template, select the View template settings check box, and then click Next.

Server templates:

Small Business Server 2000
Exchange Server 5.5 (Outlook Web Access)
Exchange Server 2000 (OWA, PF Management, IM, SMTP, NNTP)
SharePoint Portal Server
FrontPage Server Extensions
SharePoint Team Services
BizTalk Server 2000
Commerce Server 2000
Proxy Server
Static Web server
Dynamic Web server (ASP enabled)
Other (Server that does not match any of the listed roles)
Server that does not require IIS

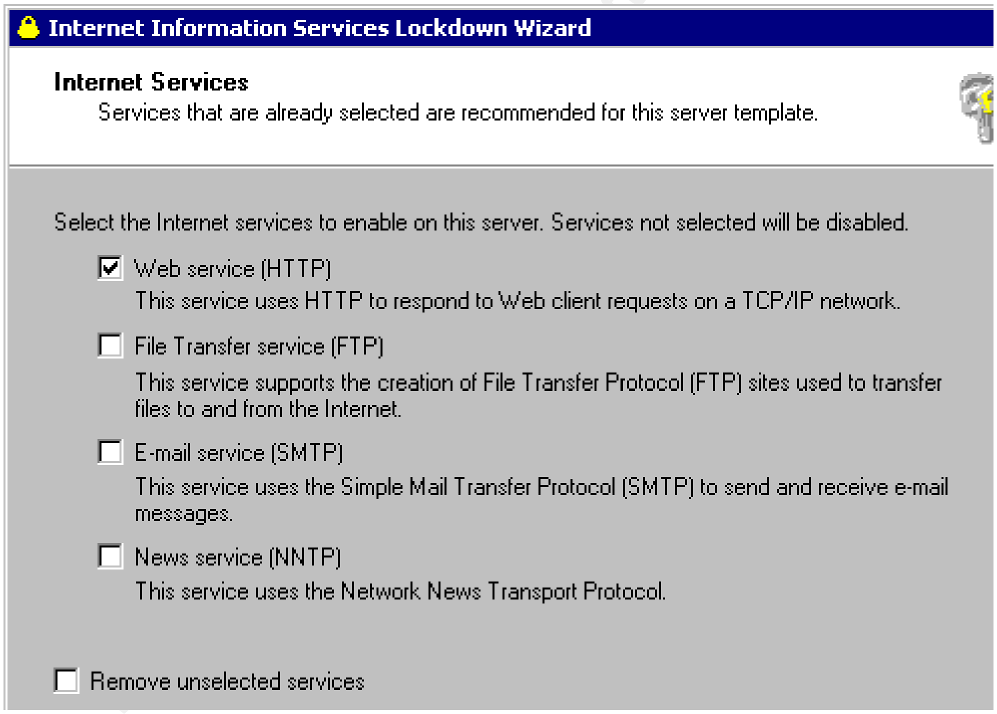
☑ View template settings

Figure 1.1

The administrator should be sure to check the box "view template settings" to allow greater flexibility in the configuration of the installation wizard. By checking that box the administrator will be prompted with the remaining steps of the installation wizard. Otherwise the administrator will jump to step 5 – installing the URLScan utility. This will also allow for modifications to be made, allow for documentation to be completed on the options chosen and, most importantly, keep the administrator knowledgeable about the server.

2) Template settings

As shown in Figure 1.2, during the second step of the installation (if the view *template setting* is chosen) you can choose what types of Internet Services the server is to provide. With a default installation of IIS all of the services below are installed. Any unneeded service should be removed to prevent the services from accidentally or maliciously being started in the future.



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

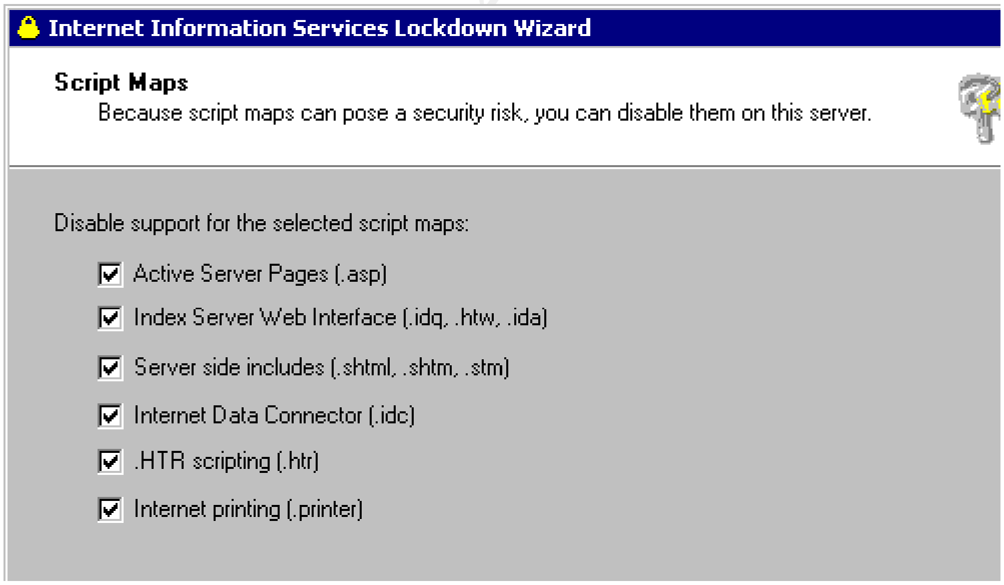
Figure 1.2

3) Removing the script maps

The installation wizard's next step is to remove script maps. These pose a security risk and should be disabled if not specifically needed. Figure 1.3 shows the options that may be removed. Disabling the script maps should be done on servers that are not using those features. The script maps can always be manually added if it is later desired.

Reasons are listed below as to why each should be removed:

- **Active Server Pages (.asp)** – Could allow attackers to view the source code of your web site and there are Active Server Pages located in the Samples directory that could be used to exploit the server.
- **Index Server Web Interface (.idq, .htw, .ida)** – The .ida script map is what was used in connection with the CodeRed, CodeBlue and Nimda exploits. The Index Server contained a buffer overflow that allowed the remote system to gain system level access. Refer to MS01-033 for further information.
- **Server Side Includes (.shtml, .shtm, .stm)** – Contain an unchecked buffer overflow that would allow attackers to run arbitrary code. Refer to MS00-028 for further information.
- **Internet Data Connector (.idc)** – There is no known exploit for the Internet Data Connector, but the script map should still be removed if not necessary.
- **.HTR scripting (.htr)** – This script map is used to do web-based password resets and is a default mapping. Refer to MS00-031 for more information.
- **Internet Printing (.printer)** – A DDoS is known to exist that would allow attackers to send endless streams of data to your printer. Refer to MS01-023 for more information.



Internet Information Services Lockdown Wizard

Script Maps

Because script maps can pose a security risk, you can disable them on this server.

Disable support for the selected script maps:

☑ Active Server Pages (.asp)

☑ Index Server Web Interface (.idq, .htw, .ida)

☑ Server side includes (.shtml, .shtm, .stm)

☑ Internet Data Connector (.idc)

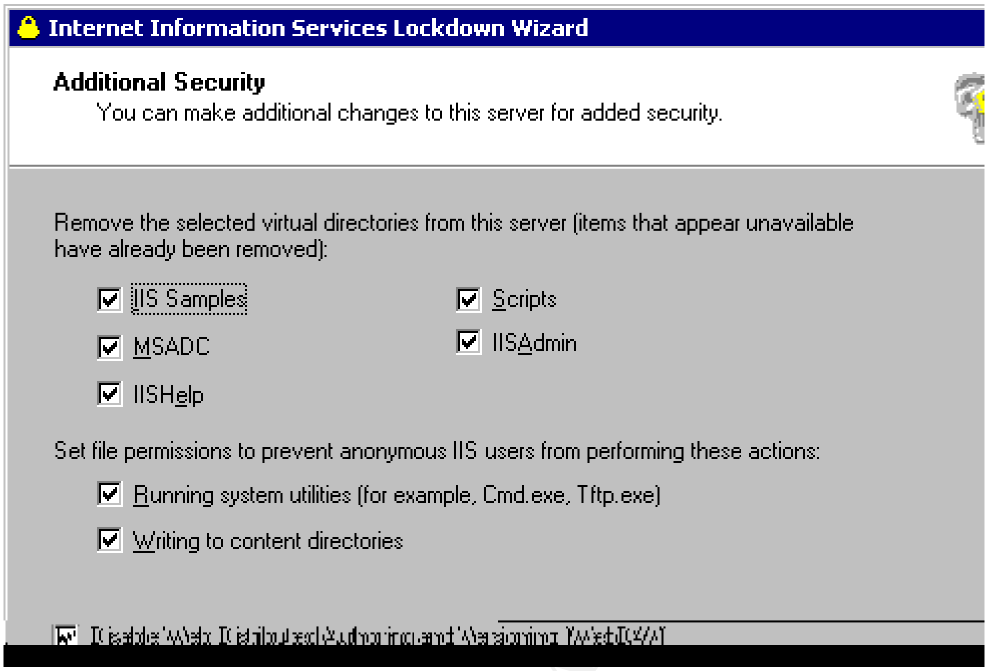
☑ .HTR scripting (.htr)

☑ Internet printing (.printer)

Figure 1.3

4) Additional Security Settings

The additional security settings screen shown in Figure 1.4 will allow extra security configuration to the IIS server. Many of the unnecessary add-ons that are installed during a default installation are removed during this step. Removing these items will eliminate the remaining vulnerabilities that are listed in the NetCraft Web Server Survey.



Internet Information Services Lockdown Wizard

Additional Security

You can make additional changes to this server for added security.

Remove the selected virtual directories from this server (items that appear unavailable have already been removed):

☑ IIS Samples ☑ Scripts

☑ MSADC ☑ IISAdmin

☑ IISHelp

Set file permissions to prevent anonymous IIS users from performing these actions:

☑ Running system utilities (for example, Cmd.exe, Tftp.exe)

☑ Writing to content directories

☑ Disable Web Distributed Authoring and Versioning (WebDAV)

Figure 1.4

The following are reasons why these items should be removed or checked:

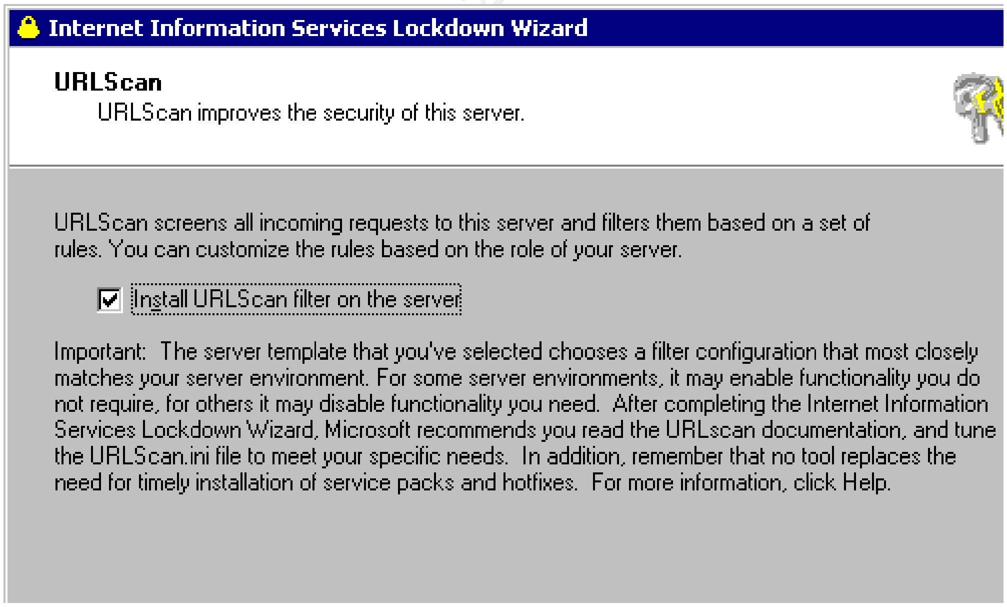
- **Sample Scripts** have known issues with the coding of some of the scripts. If a hacker was doing reconnaissance work on a server and found the sample scripts, they would know the server was probably a default installation.
- **MSADC** components should be removed if they are not in use. Rain Forest Puppy (RFP) is credited with the discovery of the MSADC RDS exploit. Please refer to RFP's site for detailed information on the exploit.
- **IIS Admin** files pose a security threat since a hacker could attempt to brute force passwords or read file fragments if the .HTR mappings have not been removed. For the .HTR script mappings bulletin please refer to MS00-044.
- **IIS Help** files should be removed as suggested by Microsoft in the IIS Security Checklist and the NSA's IIS Security Checklist.
- The **Scripts** virtual directory should be removed if it is not used. If the scripts directory is used, the folder should not allow anonymous users read access.
- **Running system utilities** should be checked to prevent anonymous users from executing system utilities via URL's.
- **Writing to content directories** should be prevented to keep the anonymous user from writing to the directories containing the content for the web site. This will help prevent web site defacement.
- **WebDAV** components should be removed if not used. The WebDAV component contains multiple vulnerabilities that could result in a Denial of Service against the server. More information can be found by searching the securityfocus.com website.

5) Installing the URLScan option.

In Figure 1.5 the installation wizard will install the URLScan filter on the server if chosen. The URLScan.dll will assist with your IIS server security by intercepting, analyzing and filtering incoming requests according to the configuration. Set by the administrator. As a result the server will only reply to legitimate requests.

URLScan is an ISAPI filter that analyzes and screens HTTP requests being made to IIS. When URLScan is properly configured. It is effective at reducing the exposure of an IIS server to potential attacks (Q307608). As stated in Track 5.4 Securing Internet Information Server 5.0, HTTP requests can be rejected based upon any of the following criteria:

- HTTP verb user in the request, e.g., GET, HEAD, OPTIONS, PUT, etc...
- Extension of the file requested e.g., ".asp", ".ida", ".exe", etc...
- Double-encoded characters, e.g., "%252e" → %2e" → "."
- Presence of non-ASCII characters in the URL.
- Presence of more than a single period (".") in a requested URL.
- Presence of any user-definable character sequences in the URL
- Presence of any user-definable headers in the request.



URLScan

URLScan improves the security of this server.

URLScan screens all incoming requests to this server and filters them based on a set of rules. You can customize the rules based on the role of your server.

☑ Install URLScan filter on the server

Important: The server template that you've selected chooses a filter configuration that most closely matches your server environment. For some server environments, it may enable functionality you do not require, for others it may disable functionality you need. After completing the Internet Information Services Lockdown Wizard, Microsoft recommends you read the URLscan documentation, and tune the URLScan.ini file to meet your specific needs. In addition, remember that no tool replaces the need for timely installation of service packs and hotfixes. For more information, click Help.

Figure 1.5

When a request is denied, the requestor receives a "404 Object not found" response or is redirected to a URL specified by the administrator in the configuration file. The system then logs the request with the date, time, source IP address, URL and reason why the request was rejected. You will want to add the URLScan logs to the list of other logs that are monitored on the server. Here is a sample of the urlscan log file during a test attack from a Nessus server:

```
[12-30-2001 - 09:42:09] Client at 111.222.333.444: URL contains extension '.idq', which is disallowed.
Request will be rejected.  Site Instance='1', Raw URL='/iissamples/exair/search/query.idq'
```

Finishing the setup

Finally, the script will run and your configuration will be implemented into the server. There is an undo option available if the wizard is run a second time, but the undo option will only reverse the changes made the last time the IISlockdown tool was run. It is best to have the information needed before beginning the installation and to document the steps you are taking.

Once the installation is complete you will want to restart the server and test the settings. Testing will depend upon the settings that the administrator chose during the setup. There are many freeware and evaluation tools available to test your server's security. A few are listed below:

- Nessus Project
- Retina Nimda Scanner
- Retina CodeRed Scanner
- ISS Internet Scanner
- RFP's Whisker
- Patchwork by GRC
- Microsoft's Personal Security Advisor
- Microsoft's Hotfix Checking Tool

Conclusion

This paper has briefly covered the installation and configuration of the IISlockdown tool. It would be impossible for any paper to cover every configuration of an IIS server and the reader is encouraged to prototype their configuration on a non-production server before introducing the IISlockdown tool into a production environment. Microsoft has provided the tool and the templates, but administrators need to take time to ensure that this product is the right solution for their network. Microsoft's IIS server is one of the dominant web servers on the Internet; it is clear that administrators using it will be attacked by Trojans, worms and viruses. With operating system hardening, training and proper configuration of the IIS server administrators can minimize their risks of a compromise. But do not let yourself or management be fooled into the false sense of security that any vendor offers. Securing a server or network is not a one-time procedure, but a process that is ever evolving. As security professionals we have the responsibility to keep ourselves up to date with the latest security holes, patches, hotfixes, concepts and trends that are happening in the hacker community.

References

Alldas.de, Defacement Archive "*OS Statistics.*" November 30, 2001
http://defaced.alldas.de/

Cole, Eric, Track 1: Sans Security Essentials. November 5-10, 2001. Sans Great Lakes Conference

Costello, Sam, "*Survey reveals one in nine IIS servers could be taken over by hackers*" November 2, 2001
http://www.infoworld.com/articles/hn/xml/01/11/02/011102hnsurvey.xml

Dougherty, Chad, et al. "*CERT Advisory CA-2001-11 sadmind/IIS Worm*" May 10, 2001
http://www.cert.org/advisories/CA-2001-11.html

Fossen, et al. "*Track 5.4 Securing Internet Information Server 5.0*" Last Modified October 3, 2001, Document version 12.0

Howard, Michael, "*Secure Internet Information Services 5.0 Checklist*" June 29, 2000
http://www.microsoft.com/technet/

NetCraft, "*NetCraft Web Server Survey*" October 1, 2001
http://www.netcraft.com/survey/index-200110.html

The Sans Institute, Information Security Reading Room
http://www.sans.org/

Walker, William E. IV *"Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0" version 1.2* August 20 2001
http://nsa2.www.conxion.com/win2k/guides/w2k-14.pdf