



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

**Auditing IIS server, Windows 2000 server
An Independent Auditors Perspective
SANS GSNA V. 2.1 (Option 1)**

Derek Geborek

4 July 2003

Abstract

This paper contains four sections which are related to each other. The first section researches the best practices for auditing Internet Information Server V 5.0 running on Windows 2000 server. It does so by defining control objectives and methods for achieving the objectives with technology. The second section contains a checklist of items that will be tested, the risks involved and detailed instructions on how to go about checking each item. The third section demonstrates the audit of eleven items from the checklist including screen shots. The fourth section presents what was done and how. It communicates the findings, recommendations and costs to management.

Assignment 1 - Research in Audit, Measurement Practice, and Control	4
Identify the system to be audited	4
Evaluate the risk to the system	4
Identified Risks:	5
What is the current state of practice, if any?	6
Assignment 2 - Create an Audit Checklist	9
Check 1- Physical Security	9
Check 2- Change Management	9
Check 3- Service Packs and patches	10
Check 4- NTFS format	11
Check 5- Strong Password	11
Check 6- Unnecessary Services	12
Check 7- Unnecessary Accounts	12
Check 8- Essential programs	13
Check 9- Anomous access to the registry	13
Check 10- Customized UrlScan configuration	14
Check 11- Appropriate ACLs on virtual directories	14
Check 12- Appropriate IIS Log file ACLs	15
Check 13- Sample applications	16
Check 14- Metabase Permissions	17
Check 15- Security template	17
Check 16- Unused Script Mappings	18
Check 17- Antivirus Software and signature file	19
Check 18- Existence of written policies/procedures	19
Check 19- Administrators knowledge/training	20
Check 20- Sufficient Auditing mechanisms	20
Assignment 3 – Audit Evidence	22
Result 1 - Physical Security	22
Result 2 - Service Packs and patches	23
Result 3 - NTFS format	25
Result 4 - Strong Password	25
Result 5 - Unnecessary Services	26
Result 6 - Unnecessary Accounts	30
Result 7- Essential programs	32
Result 8- Customized UrlScan configuration	33
Result 9- Security template	35
Result 10- Unused Script Mappings	37
Result 11- Antivirus Software and signature file	38
Assignment 4 – Audit Report or Risk Assessment	39
Executive summary	39
Audit Finding No. 1 - Missing security updates	40
Background/risk	40
Audit recommendations	40
Costs	40
Audit Finding No. 2 – Strong Password	41
Background/risk	41
Audit recommendations	41
Costs	41
Audit Finding No. 3 – Unnecessary Services	41
Background/risk	42
Audit recommendations	42
Costs	42
Audit Finding No. 4 – Unnecessary Accounts	42
Background/risk	43
Audit recommendations	43
Costs	43
Audit Finding No. 5 – Essential Programs	43
Background/risk	43

Audit recommendations	44
Costs	44
Audit Finding No. 6 – Security Template	44
Background/risk	44
Audit recommendations	45
Costs	45
Audit Finding No. 7 – Unused Script Mappings	45
Background/risk	45
Audit recommendations	45
Costs	45
Audit Finding No. 8 – Anti Virus software and signature file	46
Background/risk	46
Audit recommendations	46
Costs	46
Compensating Controls	47
Ongoing costs	47
References	48
Appendix A	50

© SANS Institute 2003, Author retains full rights.

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

Identify the system to be audited

This paper will document an audit of Microsoft Internet Information Server (IIS), version 5.0 running on a Windows 2000 server.

The role of the device is to publish information, and provide to the public and internal users material on the role, functions and operations of the organisation

Internet Information Server 5.0 (IIS) is fully integrated at the operating system level. Windows 2000 Server lets organizations add Internet capabilities. IIS provides the capability to host Web sites. It is one of the most popular Web hosting servers currently available and a competitor to Apache Web Server.

The IIS server that I will be auditing resides on the DMZ leg, all traffic to the server is required to traverse a parameter router and a firewall before it accesses the IIS server. However, the router and firewall will be outside the scope of this audit paper. The paper will concentrate on the operating system that the server runs on, and the IIS it's self only.

The reason for choosing to audit this server is that the server is exposed to the Internet, its protection against intruders is limited and it has never been audited before. I believe that it is a good material for finding vulnerabilities and providing organisation with findings which will lead to hardening of the server.

Evaluate the risk to the system

The IIS is vulnerable in three major ways: failure to handle unanticipated requests, buffer overflows, and sample applications. The first vulnerability of the IIS resides in the way that the server handles unanticipated requests. An improperly formatted request can provide the hacker with the picture of source code or installation of a backdoor.¹

The second major vulnerability resides in the buffer of the IIS. It is possible to create a request with the help of ISAPI extensions (ASP, HTR, IDQ, PRINTER, and SSI extensions), which will lead towards successful denial of service. That vulnerability was successfully exploited by Code Red and Code Red II worms.¹

¹SANS Institute. "SANS/FBI Top 20 List". Version 3.22. March 3, 2003. <http://www.sans.org/top20/#W1> (15 March. 2003).

Sample applications are another way that provides an attacker with the possibility of creating or overwriting arbitrary files on the server, collect user ids and passwords. Sample applications are usually installed when the server is being built and tested but they should be removed before the server is moved to a production environment.¹

Microsoft produces patches to cater for known vulnerabilities. As new vulnerability becomes known the systems should be patched as required.

A number of risks can be identified. The realisation of any of the risks would not only interfere with daily operations, but also lead to embarrassment to the organisation if the incident was published.

Identified Risks:

What can go wrong	How likely	Consequences
Inappropriate/offensive information published to the IIS server (server got hacked)	High	Exposure to the inadequate security practices of the organisation resulting in public enquiry
Modifications (whether authorised or not) made to the IIS server content or configuration	High	An inability to hold individuals accountable, making it difficult to prevent repeat offences. Individual accountability is also a deterrent
Hardware failure	Low	Internal staff and public unable to access the server, therefore unable to view information
Successful Denial of Service attack	Medium	Public unable to access the information published on the IIS server
Penetration of internal systems, through exploitation of vulnerabilities within the operating system or application configuration. Penetration could be via Internet based attackers or external parties connected to the organisational environment.	Medium	Resulting in unauthorised access to information or the use of organisational resources to attack other external systems. Organisation unable to demonstrate due diligence in protecting personal data stored on internal systems
Virus infection	High	Resulting in service unavailability, compromise of the integrity of the information, or unauthorised

¹ SANS Institute. "SANS/FBI Top 20 List". Version 3.22. March 3, 2003. <http://www.sans.org/top20/#W1> (15 March. 2003).

		disclosure of information.
--	--	----------------------------

What is the current state of practice, if any?

Microsoft is the "big-name" vendor in the Internet Information publishing market. There are a number of resources available that contain information on the current state of practice. Since IIS is a Microsoft product I will begin with the manufacturer. I have run a search on the Microsoft site for IIS server security. I have found an extensive list of vulnerabilities on the Windows 2000 Server Baseline Security Checklist site. The Baseline Security Checklist lists some recommendations and best practices to secure a server on the Web running Internet Information Services IIS. The vulnerabilities refer to the operating system. However, for the IIS to run securely it is important that the operating system is secured also.²

The Secure Internet Information Services 5 Checklist is also a very good source of information for auditors. It concentrates on the vulnerabilities of the IIS server that is incorporated into Windows2000 server. Once the operating system is secure it is important to secure the IIS server.³

SANS Institute also provides a good list of vulnerabilities for an IIS. They provide a good description of the areas where the server may be vulnerable, with an explanation of how to determine if the server is vulnerable and important how to protect the server against the vulnerabilities. I believe it is a good source of information for a check list.¹

I have found another site that looks at the audit from different perspective and may provide a few points that the Microsoft side does not. It talks more about access control, recovery from disaster, best practices for passwords. It has a checklist that is of specific format and may be also implemented.⁴

I have run a search on a number of search engines: www.google.com.au, www.yahoo.com, www.altavista.com, www.hotbot.com for vulnerabilities in IIS or audit check list for IIS. I have come across site which lists 54 CVE entries.

² Microsoft Cooperation. "Windows 2000 Server Baseline Security Checklist" <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/w2ksvrcl.asp> (10 Mar 03)

³ Microsoft Cooperation. "Secure Internet Information Services 5 Checklist" <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/iis5chk.asp> (10 Mar 03)

¹ SANS Institute. "SANS/FBI Top 20 List". Version 3.22. March 3, 2003. <http://www.sans.org/top20/#W1> (15 March. 2003).

⁴ "Risk Assessment/Countermeasure Analysis/Security Test and Evaluation (ST&E) for Microsoft Windows 2000 Computer Systems". October 1, 2002 PART II (V1.5). http://www.nswc.navy.mil/ISSEC/Form/AccredForms/acc_part2_2000.html (17 Mar 03)

Some of these entries may prove to be useful for check list of common vulnerabilities and exposures.⁵

According to SANS, one of the most common vulnerabilities that IIS has is when the server receives an improperly formed HTTP requests. A common tool used to fight these vulnerabilities is the IIS Lockdown tool with the Urlscan. This method allows screening of all incoming requests to the server and filters them based on rules set by the administrator. This secures the server by ensuring that only valid requests are processed. By filtering out all unusual requests, Urlscan prevents them from reaching the server and potentially causing damage.⁶

The Lockdown tool is able to assist the administrator in Un-mapping Unnecessary ISAPI Extensions, Filter HTTP Requests.⁷ The IIS Lockdown tool can be downloaded from:

<http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=DDE9EFC0-BB30-47EB-9A61-FD755D23CDEC>

There are a number of tools which were discussed during the SANS Conference in Sydney 2003, available to assist an auditor in a successful audit. The tools serve different purpose some are easy to use other need to be built as a server on a UNIX platform.

- **N-Sleath** – is a CGI scanner that has a database of default CGIs and will provide a report on any CGI found. More information can be found on www.nstalker.com/nstealth⁹
- **Brutus** – Tool that allows brute force web authentication. It allows user to include a list of word from different sources. More information can be found on www.hoobie.net/brutus/index.html⁹
- **Achillies** – This tools has the ability to act as a proxy that allows user to redirect Web traffic through it, so you are able to see the code. More information can be found on www.mavensecurity.com and the tool can be downloaded from www.digizen-security.com⁹
- **Screaming Cobra** – It uses URL to get a Web page and parse it in search for links and form elements. More information can be found on www.cobra.lucidx.com⁹
- **Web Sleuth** – It is a very universal Web application tool. It is known as a well kept secret in the auditing world. It is a tools that has plug-ins. It

⁵ “Common Vulnerabilities and Exposures The Key to Information Sharing”. CVE version: 20030402 <http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=iis+5.0> (20 March 03)

⁶ Microsoft Cooperation. “UrlScan Security Tool” <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/urlscan.asp> (7 Mar 03)

⁷ Microsoft Cooperation. “IIS Lockdown Tool”. <http://www.microsoft.com/technet/security/tools/locktool.asp> (10 Mar 03)

⁹ Rhoades, David. “Auditing Web Servers and Applications”. SANS Institute Track 7 – Auditing Networks, Perimeters and Systems. 2002. p. 64, 72, 77, 86

is also known as all in one Web application audit tool. More information can be found on www.geocities.com/dzzie/sleuth⁹

- **Nessus** – Is a scanner that allows plugging in modules depending on the needs of the audit. It runs on different varieties of Unix. The instructions to build the server and client are reasonably good for people that had little to do with Unix OS. More information can be found on www.nessus.org⁹

There are two factors which I will mainly take into account when examining the IIS. The first is the security of the Win 2000 server and then the IIS, which is a service that runs as part of the Win 2000 server. Both have to be examined for security loop holes.

⁹ Rhoades, David. "Auditing Web Servers and Applications". SANS Institute Track 7 – Auditing Networks, Perimeters and Systems. 2002. p. 88, 15

Assignment 2 - Create an Audit Checklist

Check 1- Physical Security

Reference	Personal experience
Control Objective	Access Control
Risk	Unauthorised modifications made to the IIS server content or configuration. The possibility of that risk occurring internally is low. The consequences would be an inability to hold individuals accountable, making it difficult to prevent repeat offences. Depending on the action consequences could be different. Any consequences listed in the risk list in section 1 may occur.
Compliance	The server must be located in an area that has strictly controlled access eg. Security guard at the door to the server room, access by slash card, and area under constant video surveillance.
Testing	Someone who does not have the appropriate access rights should try physically accessing the server room. This exercise should be confirmed with the appropriate management to avoid negative consequences to the person trying to make the illegal entry
Objective/Subjective	Objective

Check 2- Change Management

Reference	Personal experience
Control Objective	Track changes and allow for rollbacks
Risk	Modifications (whether authorised or not) made to the IIS server content or configuration, which may result in application not working correctly or not at all. The likelihood of that risk occurring is high due to the fact that some systems are different in test environment to the production environment and when the change is migrated to the production platform it causes on occasions errors or unpredictable outcomes. The consequence may be an inability to hold individuals accountable, making it difficult to prevent repeat offences.
Compliance	The system is compliant if there is a system in place that spells out the details of the change. Who approves change, who implements change, who verifies that change was implemented correctly, are

	there procedures for a rollback included
Testing	I will check for an existence of change manager. Ask the change manager for change management procedures and policies and then compare these documents to the actions that take place when a change occurs
Objective/Subjective	Subjective

Check 3- Service Packs and patches

Reference	²
Control Objective	Verify that all service packs and patches have been applied.
Risk	Newly discovered security vulnerabilities in components included with Windows 2000 can be used to the benefit of an attacker. The system can be compromised, crushed, data may be changed or access to other devices may be gained through a compromised un-patched device, especially if it is exposed to the internet
Compliance	Run the MBSA against the computer being audited. The results will show all missing components necessary for compliance. The compliance changes regularly, therefore I believe MBSA is a good tool that will save time and is kept up to date by Microsoft
Testing	<ul style="list-style-type: none"> • Download the latest Microsoft Base Line Security Analyser • Run it against the server being audited • The results screen will show all missing service packs and patches • Click on the “results detail” link • Click on the “How to correct this” link • Depending on the findings correct the problem according to the instructions displayed under the “How to correct this” link <p>Appropriate patches can be found and downloaded from: http://www.microsoft.com/downloads/search.aspx?opsysid=1&search=Keyword&value='security_patch'&displaylang=en</p>
Objective/Subjective	Objective

² Microsoft Cooperation. " Windows 2000 Server Baseline Security Checklist"
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/w2ksvrcl.asp> (10 Mar 03)

Check 4- NTFS format

Reference	²
Control Objective	Verify that all disk partitions are formatted with NTFS
Risk	The NTFS offers access control and security that FAT does not have.
Compliance	All partitions need to be checked for format type, they need to exhibit NTFS
Testing	<ul style="list-style-type: none">• Right click on start button• Click on explore• Right click on all local partitions• In the General Tab the file system will be displayed
Objective/Subjective	Objective

Check 5- Strong Password

Reference	²
Control Objective	Verify that the accounts have strong passwords
Risk	The password can be compromised by running Brutus against the server. It may result in unauthorised access to the server with admin rights
Compliance	Longer passwords are harder to break. Passwords with letters, numbers, punctuation marks, and non-printing ASCII characters generated by using the ALT key and three-digit key codes on the numeric keypad are better. The password needs to be minimum nine characters long and include at least one punctuation mark or non-printing ASCII character in the first seven characters
Testing	<ul style="list-style-type: none">• Click on start button• Click on Programs/Administrative tools/local Security Policy• Click on Account Policies• Click on Password Policy• Check that minimum password length is nine characters• Check that password must meet complexity requirements is enabled• Run Brutus against the server for five minutes
Objective/Subjective	Objective

² Microsoft Cooperation. " Windows 2000 Server Baseline Security Checklist"
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/w2ksvrcl.asp> (10 Mar 03)

Check 6- Unnecessary Services

Reference	² Personal experience
Control Objective	Verify that unnecessary services are disabled
Risk	An unnecessary service increases the possibility of compromise of the server
Compliance	<p>The Security Template should disable unwanted services, however a manual check in the services applet should be performed to verify that the following services are disabled:</p> <p>Alerter, ClipBook, Compaq management services (several, disable all), Distributed File System, DHCP Client (needed for test environment, disable for production), Distributed Link Tracking Client, Distributed Link Tracking Server, Distributed Transaction Coordinator, Fax Service, File Replication, FTP Publishing Service, Indexing Service, Internet Connection Sharing, IPSEC Policy Agent, Messenger, Network DDE, Network DDE DSDM, NetMeeting Remote Desktop Sharing, NT LM Security Support Provider, Performance Logs and Alerts, QoS RSVP, Remote Access Auto Connection Manager, Remote Access Connection Manager, RunAs Service, Smart Card, Smart Card Helper, Telephony, Telnet, Uninterruptible Power Supply, Utility Manager</p>
Testing	<ul style="list-style-type: none">• Click on the start button• Click on programs/administrative tools/services• Check that the services listed above are disabled• Run NMap against the server
Objective/Subjective	Objective

Check 7- Unnecessary Accounts

Reference	²
Control Objective	Verify that there are no unnecessary accounts
Risk	Unnecessary accounts may give access to an unwanted intruder to the server; the configuration on the unnecessary account may not be secure. It may result in a compromise of the server or unauthorised changes made to the server.
Compliance	The accounts that are present on the server should

² Microsoft Cooperation. " Windows 2000 Server Baseline Security Checklist"
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/w2ksvrcl.asp> (10 Mar 03)

	be once that active for both users and applications
Testing	<ul style="list-style-type: none"> • Run MBSA, it will show all accounts or • Use Computer Management snap-in <p>Analyse the accounts and confirm that all are necessary.</p> <ul style="list-style-type: none"> • Examine Nessus scanner results <p>The MS Baseline Analyser can be downloaded from http://download.microsoft.com/download/e/5/7/e57f498f-2468-4905-aa5f-369252f8b15c/mbsasetup.msi</p>
Objective/Subjective	Objective

Check 8- Essential programs

Reference	Personal Experience
Control Objective	Verify that there are no non essential programs
Risk	Some programs may expose the server to vulnerabilities. It is good practice to run only programs that are necessary. It may result in unauthorised access to some resources and therefore unauthorised changes to the system or files.
Compliance	The only optional programs ticked in the Add/remove programs should be: Calculator, notepad, WordPad, IIS Common Components, IIS Documentation, IIS management Snap-in, FTP service, World-Wide Web Service.
Testing	<ul style="list-style-type: none"> • Click on Start/settings/control panel • Double click on add/remove programs • Click on Windows components • Check that only the ones that must stay are ticked <p>Terminal Service (Testing only, to be disabled during production)</p>
Objective/Subjective	Objective

Check 9- Anomous access to the registry

Reference	²
Control Objective	Verify that there is no anomous access to the registry
Risk	The only group of people that should be able to

² Microsoft Cooperation. " Windows 2000 Server Baseline Security Checklist"
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/w2ksvrcl.asp> (10 Mar 03)

	access the registry remotely is the administrators. The system when installed by the fault does not limit access to registry. By providing anomous access to the registry the user may change settings in the registry which may stop the server from functioning. Users will not be able to access the server or they will be getting errors on some sites.
Compliance	Winreg value name permissions are set to Full Control, and that no other users or groups are listed.
Testing	<ul style="list-style-type: none"> • The registry contains the following key: Hive - HKEY_LOCAL_MACHINE \SYSTEM. Key - \CurrentControlSet\Control\SecurePipeServers Value Name - \winreg • Select winreg, click the Security menu, and then click Permissions • Check that the Administrators permission is set to Full Control, and that no other users or groups are listed.
Objective/Subjective	Objective

Check 10- Customized UrlScan configuration

Reference	³
Control Objective	Verify that the installed copy of UrlScan file is the one that should be used by organisation
Risk	UrlScan is an ISAPI filter that screens and analyses requests IIS receives. It reduces the risk of potential attacks on the IIS.
Compliance	Compare that the UrlScan file is same as the one that has been approved for usage on that server by the organisations IT security personnel
Testing	<p>The UrlScan file for usage by my organisation has been modified.</p> <ul style="list-style-type: none"> • Make a copy of the file from the server and compare it physically, with the one stored offline (modified one). • Run N-Sleath scanner against the server
Objective/Subjective	Objective

Check 11- Appropriate ACLs on virtual directories

Reference	³
Control Objective	Check that appropriate access levels are applied to

³ Microsoft Cooperation. "Secure Internet Information Services 5 Checklist"
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/iis5chk.asp> (10 Mar 03)

	the directories that contain files with the description listed below in the compliance section
Risk	If an inappropriate access to a directory or file is achieved by an intruder it may result to unauthorised changes made to the files. The consequences may be, changes made to the websites or total failure of the server
Compliance	<ul style="list-style-type: none"> • CGI (.exe, .dll, .cmd, .pl) Everyone (X) Administrators (Full Control) System (Full Control) • Script files (.asp) Everyone (X) Administrators (Full Control) System (Full Control) • Include files (.inc, .shtm, .shtml) Everyone (X) Administrators (Full Control) System (Full Control) • Static content (.txt, .gif, .jpg, .html) Everyone (R) Administrators (Full Control) System (Full Control)
Testing	<p>These permissions should be applied to the directories that the files reside in.</p> <ul style="list-style-type: none"> • Right click on the directory • Click on properties • Click on the security tab • View the permissions
Objective/Subjective	Objective

Check 12- Appropriate IIS Log file ACLs

Reference	³
Control Objective	Check that ACLs on the IIS-generated log files in (%systemroot%\system32\LogFiles) have appropriate level of access control
Risk	The hacker may delete or edit these files to cover his/her malicious activity.
Compliance	<ul style="list-style-type: none"> • Administrators (Full Control) • System (Full Control) • Everyone (RWC)
Testing	<ul style="list-style-type: none"> • Go to %systemroot%\system32\LogFiles • Right click on properties • Click on security tab • View the security settings

³ Microsoft Cooperation. "Secure Internet Information Services 5 Checklist"
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/iis5chk.asp> (10 Mar 03)

Objective/Subjective	Objective
-----------------------------	-----------

Check 13- Sample applications

Reference	³ 1
Control Objective	Check that no sample applications are present on the server.
Risk	These applications may provide unauthorised access to the server and further serve as tools for malicious activities
Compliance	<p><u>No</u> evidence of:</p> <ul style="list-style-type: none"> • IIS Samples in c:\inetpub\iissamples • IIS Documentation in c:\winnt\help\iishelp • Data Access in c:\program files\common files\system\msadc <p><u>No</u> evidence of below files in the %wwwroot%/scripts directory:</p> <ul style="list-style-type: none"> • code.asp • codebrws.asp • ism.dll • newdsn.exe • viewcode.asp • winmsdp.exe <p>This is a list of some samples. However, an eye should be kept for other sample applications in other locations, the list may vary</p> <p>Sample applications are these that do not get installed by default</p>
Testing	<ul style="list-style-type: none"> • Go to the above listed locations. The names may vary depending on the naming conventions chosen by the administrator that has built and administered the server • Physically check for existence of the above applications and others that should not have been installed by default • Do a search for the above files on all drives <p>It is challenging to list all applications and all locations because an administrator could have</p>

³ Microsoft Cooperation. "Secure Internet Information Services 5 Checklist"
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/iis5chk.asp> (10 Mar 03)

¹ SANS Institute. "SANS/FBI Top 20 List". Version 3.22. March 3, 2003. <http://www.sans.org/top20/#W1> (15 March. 2003).

	installed anything anywhere
Objective/Subjective	Objective

Check 14- Metabase Permissions

Reference	³
Control Objective	Check that appropriate permissions are applied to IIS Metabase file and the back up file
Risk	Security and other IIS configuration settings are maintained in the IIS Metabase file if these permissions are accessed by a hacker the server may be compromised
Compliance	<ul style="list-style-type: none"> • Full control should be granted to Administrator and System • All other removed
Testing	<ul style="list-style-type: none"> • Find the IIS Metabase • Check the permissions
Objective/Subjective	Objective

Check 15- Security template

Reference	³
Control Objective	Check that the security template used on the IIS server is applied correctly and it matches the template that should be used by the organisation. The template should be either a custom made for the specific organisation or one available from Microsoft called "Hisecweb.inf" and may be downloaded from http://support.microsoft.com/support/misc/kblookup.asp?id=Q316347
Risk	The server may be compromised
Compliance	The number of settings that should match the desired template is too big to list. However, after running the Security Configuration and Analysis tool the results should show no differences between the examined template and the one that is installed on the server. The organisation has a security template that was custom made. I will compare it to the one on the server.
Testing	<ul style="list-style-type: none"> • Copy the appropriate template to the %windir%\security\templates directory • Open the Security Templates tool, and look

³ Microsoft Cooperation. "Secure Internet Information Services 5 Checklist"
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/iis5chk.asp> (10 Mar 03)

	<p>over the settings.</p> <ul style="list-style-type: none"> • Open the Security Configuration and Analysis tool, and load the template. • Right-click the Security Configuration and Analysis tool, and choose analyze computer now • Examine the results
Objective/Subjective	Objective

Check 16- Unused Script Mappings

Reference	³
Control Objective	Check that unnecessary script mappings are removed
Risk	Resulting in unauthorised access to information or the use of organisational resources to attack other external systems. Organisation unable to demonstrate due diligence in protecting personal data stored on internal systems
Compliance	<ul style="list-style-type: none"> • If Web-based password reset is not used, the “.htr” entry should not exist • If the Internet Database Connector is not used, the “.idc” entry should not exist • If Server-side Includes is not used, the “.shtml, shtm” entries should not exist • If Internet Printing is not used, the “.printer” entry should not exist • If Index server is not used, the “.ida, idq, .htw” entries should not exist
Testing	<ul style="list-style-type: none"> • Open Internet Services Manager • Right-click the Web server, and choose Properties • Master Properties • Select WWW Service • Click on Edit • Click on Home Directory • Click on Configuration
Objective/Subjective	Objective

³ Microsoft Cooperation. “Secure Internet Information Services 5 Checklist”
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/iis5chk.asp> (10 Mar 03)

Check 17- Antivirus Software and signature file

Reference	²
Control Objective	Verify that antivirus software is installed with the latest signature file
Risk	Resulting in service unavailability, compromise of the integrity of the information, or unauthorised disclosure of the information
Compliance	The anti virus software is installed with up to date signature file. Information on the latest signature files for InoculateIt and Vet can be found on http://support.ca.com/Download/virusig.html#inoc60 The current for Inoculate is 23.61.35
Testing	<ul style="list-style-type: none">• Click on start• Choose programs• Choose .E-Trust Antivirus• Click on Help• View the information
Objective/Subjective	Objective

Check 18- Existence of written policies/procedures

Reference	⁹
Control Objective	Verify that written security policies, procedures exist. Verify any differences between the policies and the IIS server
Risk	The system may not be subject to any policies therefore it may be up to the administrator to configure and update the server which ever way and when ever the administrator feels suitable or when time permits. That may result in server not being configured up to industry best practice on time or at all and therefore be vulnerable to intrusions or the server may become instable.
Compliance	The written policies, procedures must exist The existing policies and procedures must meet the settings/policies on the server.
Testing	Obtain the security policies and procedures documentation from the administrator, and then physically compare them against what is on the server.
Objective/Subjective	Objective

² Microsoft Cooperation. " Windows 2000 Server Baseline Security Checklist"
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/w2ksvrcl.asp> (10 Mar 03)

⁹ Rhoades, David. "Auditing Web Servers and Applications". *SANS Institute Track 7 – Auditing Networks, Perimeters and Systems*. 2002. p. 11

Check 19- Administrators knowledge/training

Reference	10
Control Objective	Sufficient administrator knowledge/training
Risk	Insufficient knowledge or lack of training for administrator may lead to low levels of security being implemented and therefore the server may be compromised.
Compliance	Administrator has completed necessary training for IIS administration
Testing	Evidence of relevant certifications/courses possessed by the administrator
Objective/Subjective	Objective

Check 20- Sufficient Auditing mechanisms

Reference	10
Control Objective	System has sufficient auditing mechanisms enabled
Risk	If the system would become compromised there would be hard to establish what has happened and how. The system may lose its integrity and the only way to make sure that the system is fine again would be a restore from back up or a full reload. That would result in down time of the server. Public and internal staff unable to access information on the server
Compliance	<ul style="list-style-type: none">• System events enabled both success and failure• Privilege use, failure only• Policy change enabled both success and failure• Object access failure only• Logon events enabled both success and failure• Account management enabled both success and failure• Account logon events enabled both success and failure• Logs are copied regularly to a different storage system (for performance and security reasons)
Testing	<ul style="list-style-type: none">• Right click on My Computer on the desktop• Click on Manage• Click on Local Policy• Click on audit Policy• Check the above settings

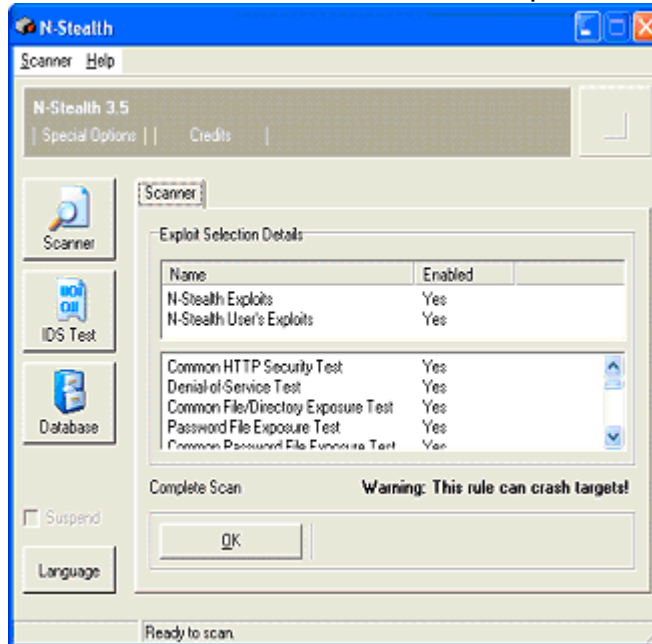
¹⁰ Krasavin, Serge. "IIS 5.0 Web Server Audit Checklist".
www.ccsso-staff-nts.cso.uiuc.edu/skrasavi/Info/IIS%205.0%20checklist.pdf (10 May 03)

Objective/Subjective	Objective
----------------------	-----------

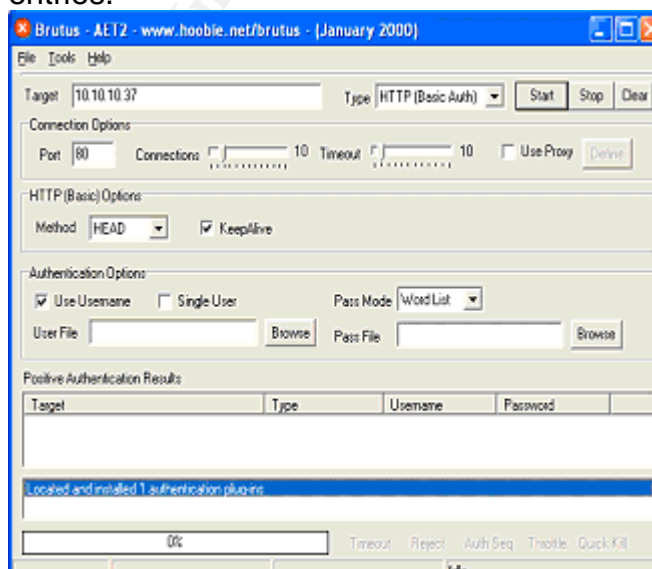
The audit will involve physical examination of the check points as described in the checklist. I will physically check the settings and provide screen dumps of the results.

Secondary I will use different tools to confirm the findings and make sure that the audit is performed to a high standard. The tools that will be used during this audit are:

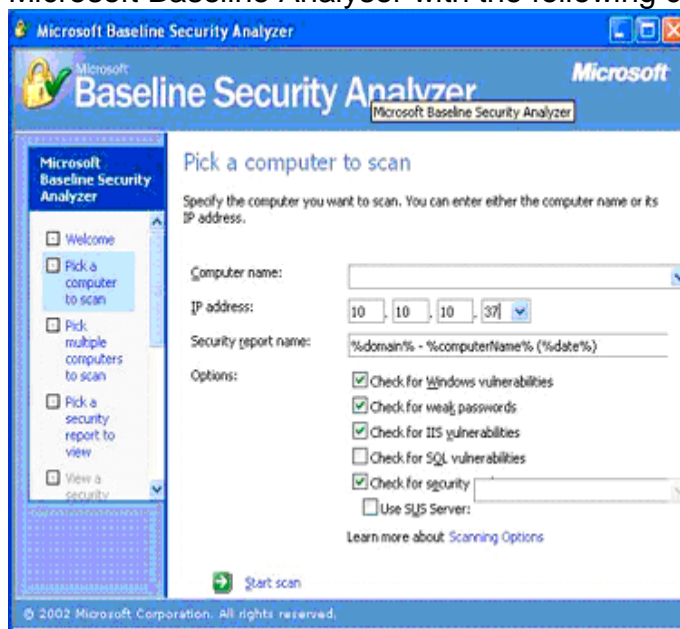
- N-Sleath scanner with scan rule complete on port 80.



- Brutus with the following configuration found below and two files that contain user names and passwords which were provided in the SANS Conference in Sydney 2003. I will edit the files by adding additional entries.



- Microsoft Baseline Analyser with the following configuration



- Nessus scanner will be build on a Linux Red Hat platform. I will use all the plug-ins. Nessus client which will be built on the Linux computer same as the server and will be run from there.

Assignment 3 – Audit Evidence

Result 1 - Physical Security

Reference Check No. 1. p.9

The test has shown that sufficient security measures are in place.

In order to access the server physically any person entering the building has to go through security check point, where I was asked to produce my security pass which was scanned and my details with my picture were displayed.

Following that in order to access the server room there is another security measure in place where unauthorised personnel are not able to pass because a security pass has to be scanned for the door to open.

Third level of security is that the server is behind another door where an officer authorised to do so may grant the visitor access subject to prior clearance with management.

The residual risk to the system is low. I believe there is no need for further improvements. The controls in place make it very hard for anyone without

appropriate access rights to access the server physically. The control objective was achieved.

Result 2 - Service Packs and patches

Reference Check No. 3. p.10


The examination of the service packs and patches has revealed that there are nine security updates missing. The residual risk to the server in this case is high because the server is exposed to the Internet and may be attacked. Missing patches provide attacker with the ability to execute code of their choice.

The vulnerabilities found can be fixed by downloading the relevant patches listed below in the results and the patches should be applied to the server in a test domain. Following substantial testing the change can be moved to the production server.

It is necessary for the servers that are exposed to the Internet to be patched as soon as possible to avoid unnecessary risks. The security patches present known vulnerabilities to Microsoft, they are free.

The control objective has been achieved, in the sense that I have verified that all service packs have been applied but not all security patches have been applied to the server.


The system is auditable. The audit was conducted using Microsoft Baseline Analyser and the cut down version of results is present below

 Microsoft
Baseline Security Analyzer

9 security updates are missing or could not be confirmed.
Result Details

Windows Security Updates

Security updates confirmed as missing are marked with a red X


[MS03-011](#)
Flaw in Microsoft VM Could Enable System Compromise (816093)
File \\xxxxxxx\C\$\WINNT\system32\msjava.dll has a file version [5.0.3809.0] that is less than what is expected [5.0.3810.0].



[MS03-013](#)

Buffer Overrun in Windows Kernel Message Handling could Lead to Elevated Privileges (811493)
File \\xxxxxxx\C\$\WINNT\system32\cmd.exe has a file version [5.0.2195.4803] that is less than what is expected [5.0.2195.6656].



[MS03-015](#)

Cumulative Patch for Internet Explorer (813489)
The registry key **SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\{06DD38D3-D187-11CF-A80D-00C04FD74AD8}** should have a value of 1024. It has a value of 32.

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



[MS01-022](#)

WebDAV Service Provider Can Allow Scripts to Levy Requests as User
Please refer to Q306460 for a detailed explanation.



[MS02-008](#)

XMLHTTP Control Can Allow Access to Local Files
Please refer to Q306460 for a detailed explanation.



[MS02-053](#)

Buffer Overrun in SmartHTML Interpreter Could Allow Code Execution (Q324096)
Please refer to Q306460 for a detailed explanation.



[MS02-064](#)

Windows 2000 Default Permissions Could Allow Trojan Horse Program (Q327522)
Please refer to Q306460 for a detailed explanation.



[MS02-065](#)

Buffer Overrun in Microsoft Data Access Components Could Lead to Code Execution (Q329414)
Please refer to Q306460 for a detailed explanation.



[MS03-008](#)

Flaw in Windows Script Engine could allow code execution (814078)
Please refer to Q306460 for a detailed explanation.

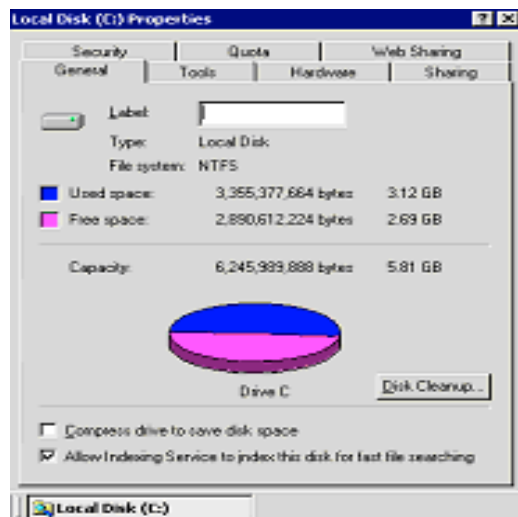
Result 3 - NTFS format

Reference Check No. 4. p.11

The examination of all disk partitions has shown that all partitions are formatted with NTFS. The residual risk is low. In this test no vulnerabilities were discovered.

The control objective has been achieved. All partitions on this server have been confirmed to have NTFS.

The system is auditable the cut down version of the results are presented below.



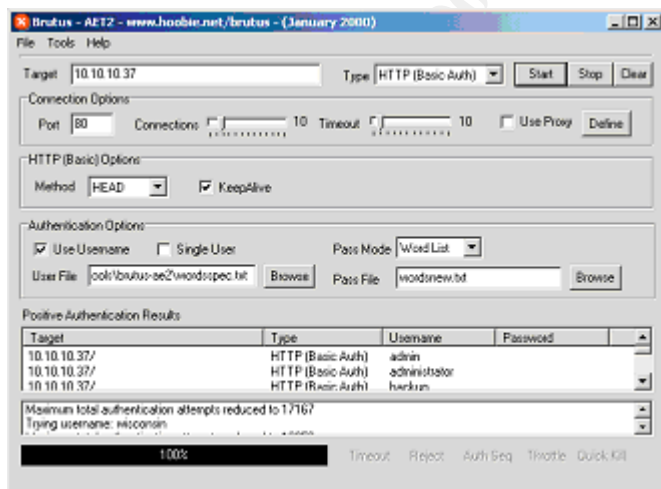
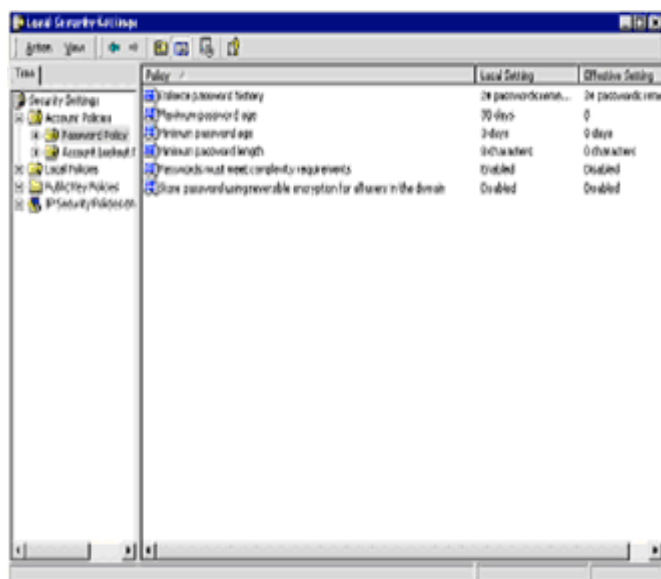
Result 4 - Strong Password

Reference Check No. 5. p.11

Password strength examination has revealed that the minimum password length is set to eight characters. The password complexity requirements is disabled, therefore the users can enter weak passwords which can be broken easier, the residual risk in this case is medium.

My recommendations would be to change the minimum length for the password to nine characters and enable password complexity requirements. The other choice would be to apply the customised security template which will automatically fix both problems.

The system is auditable and the control objective was achieved; the accounts have not got strong passwords policies applied to them. However, Brutus was unable to get the passwords in five minutes. The administrator may be using strong passwords anyway. The results of the physical examination and Brutus are visible below.



Result 5 - Unnecessary Services

Reference Check No. 6. p.12

The examination of the unnecessary services has revealed that there are three unnecessary services running on the server which increases the possibility of compromise of the server. The three services running are:

- Compaq system shutdown service
- Compaq version control agents
- DHCP client

The fourth service in question is “performance logs and alerts” which is set to manual.

The residual risk is high because as mentioned above these services provide attacker with more ways to compromise the server. The services are unnecessary. My recommendations would be to disable the three unnecessary services that are running and the fourth one that is set to manual.

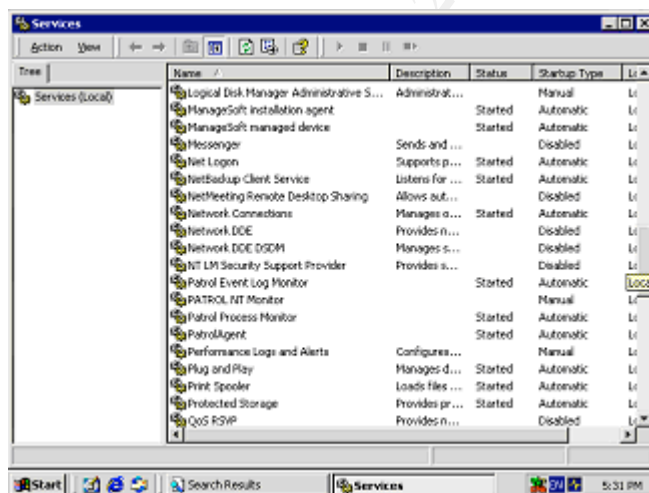
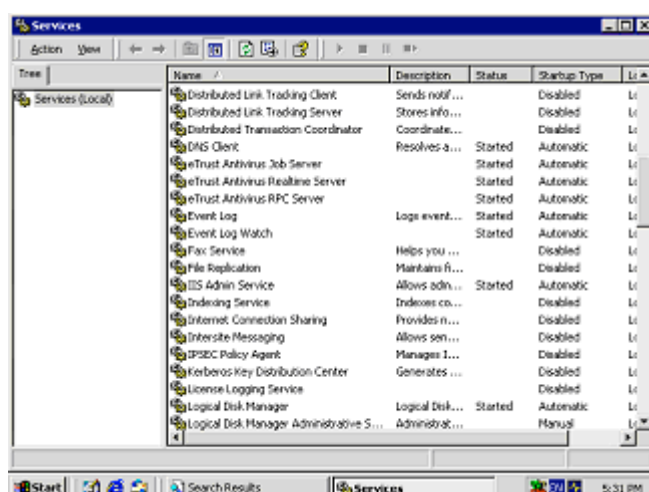
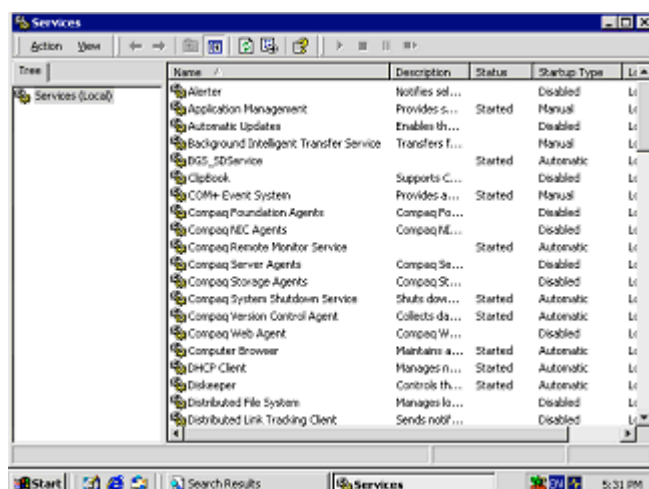
Nmap examination has revealed also that there are a number of services that are accessible from the inside of the network. These may provide an internal attacker with increased possibility to compromise the system. These are:

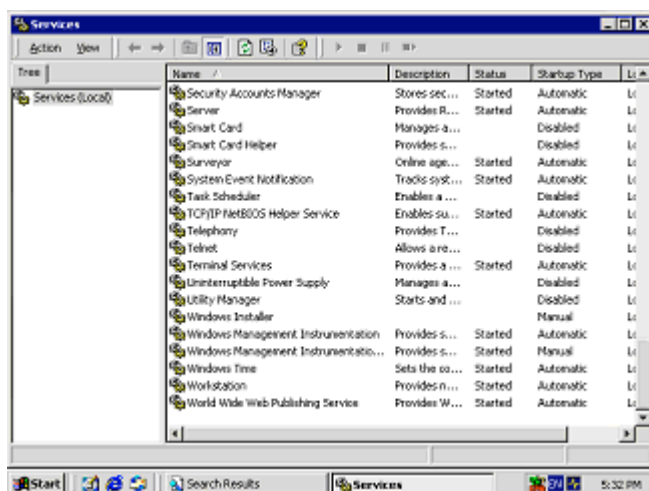
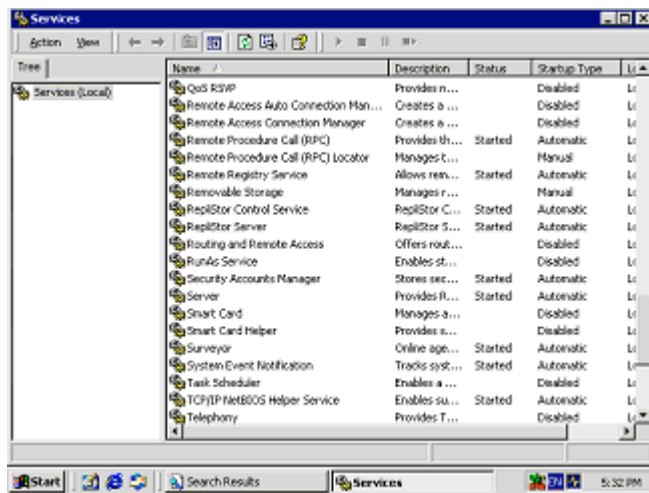
- 199/tcp open smux
- 443/tcp open https
- 445/tcp open microsoft-ds
- 1026/tcp open LSA-or-nterm
- 1027/tcp open IIS
- 1033/tcp open netinfo
- 2301/tcp open compaqdiag
- 3389/tcp open ms-term-serv
- 13782/tcp open VeritasNetbackup
- 49400/tcp open compaqdiag

My recommendation would be to implement a measure that limits access to these ports to employees and services that absolutely need to access these ports, eg administrators. That measure would reduce the risk of the server being compromised from the inside of the organisation. The additional control could be achieved by creating additional entries in the access control list on the firewall which would limit the access to these ports to the necessary users and services.

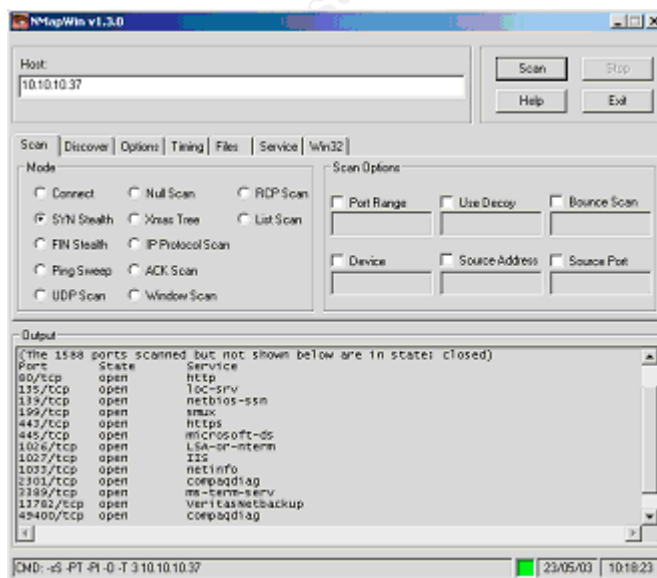
The control objective was achieved and the verification has shown that unnecessary services were running on the server and there are a number of ports open with services advertising themselves to everyone on the inside of the organisation.

The system is auditable and the services were validated as unnecessary. The results of the physical examination are listed below.





NMap Examination



(The 1588 ports scanned but not shown below are in state: closed)

Port	State	Service
80/tcp	open	http
199/tcp	open	smux
443/tcp	open	https
445/tcp	open	microsoft-ds
1026/tcp	open	LSA-or-nterm
1027/tcp	open	IIS
1033/tcp	open	netinfo
2301/tcp	open	compaqdiag
3389/tcp	open	ms-term-serv
13782/tcp	open	VeritasNetbackup
49400/tcp	open	compaqdiag

Remote operating system guess: Win XP Pro or Windows 2000 Pro SP2+
Nmap run completed -- 1 IP address (1 host up) scanned in 7 seconds

Result 6 - Unnecessary Accounts

Reference Check No. 7. p.12

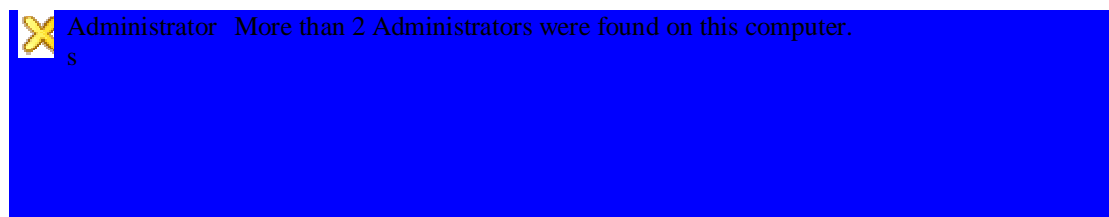
The examination of unnecessary accounts has revealed that there are:




- More than two administrative accounts
- Four accounts have non-expiring passwords
- One account has blank password
- The guest account is disabled

The residual risk is medium because the number of accounts is more than necessary and the passwords never expire. There is an account that has never been logged into and an account that has been disabled. All these unnecessary accounts may provide intruder with a mean to break-in.

I would recommend deleting one administrative account and leaving only one with a password that expires every one month. The guest account should be deleted completely from the server. The unused accounts should be disabled for a short period of time for the purpose of testing, to make sure that nothing is using them, and then deleted. The account that is used by applications (IWAM_YYYYYYYYYYY) should be left as it is. Future account practice should introduce passwords with limited lifetime

The control objective was achieved. I have verified that there are unnecessary accounts present on the server. The system is auditable and the cut down results from Microsoft Baseline Analyser and Nessus scanner are present below.



	Password Expiration	Some unspecified user accounts (4 of 6) have non-expiring passwords.
	Local Account Password Test	Some user accounts (1 of 6) have blank or simple passwords, or could not be analyzed.
	Guest Account	The Guest account is disabled on this computer.

Nessus Scan Report

```
-----
. Warning found on port netbios-ssn (139/tcp)

- Administrator account name : XXXXXXXXXXXXadmin (id 500)
- Guest account name : nobody (id 501)
- ZZZZZZZZnetUser (id 1000)
- IUSR_AAAAAAAAAA (id 1001)
- IWAM_YYYYYYYYYY (id 1002)
- Web Anonymous Users (id 1003)
- Web Applications (id 1004)

The following local accounts have never changed their password :

XXXXXXXXXXXXadmin
nobody
ZZZZZZZZnetUser
IUSR_AAAAAAAAAA
```


IWAM_YYYYYYYYYYY

To minimize the risk of break-in, users should
change their password regularly

Warning found on port netbios-ssn (139/tcp)

The following local accounts have passwords which never expire :

XXXXXXXXXXXXadmin
nobody
ZZZZZZZnetUser
IUSR_AAAAAAAAAAAA
IWAM_YYYYYYYYYYY

Password should have a limited lifetime
Solution : disable password non-expiry
Risk factor : Medium

. Warning found on port netbios-ssn (139/tcp)

The following local accounts have never logged in :

nobody
ZZZZZZZnetUser
IWAM_XXXXXXXXXXXX

Unused accounts are very helpful to hacker
Solution : suppress these accounts
Risk factor : Medium

. Information found on port netbios-ssn (139/tcp)

The following local accounts are disabled :

nobody

To minimize the risk of break-in, permanently disabled accounts
should be deleted
Risk factor : Low

Result 7- Essential programs

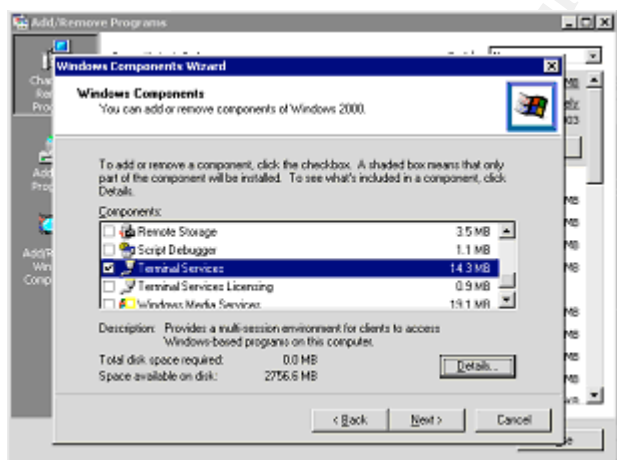
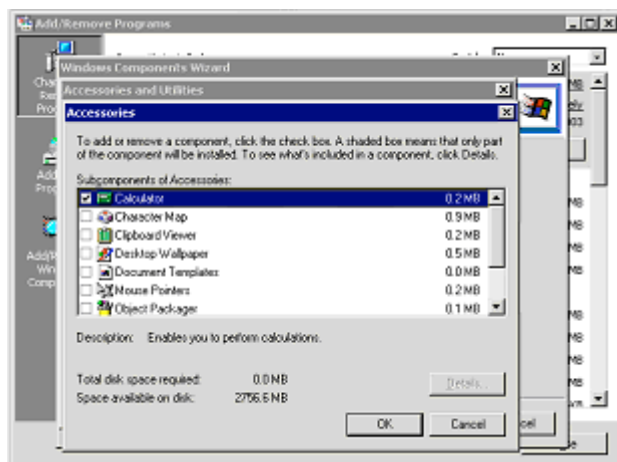
Reference Check No. 8. p.13

The examination of essential programs has revealed that Terminal Service is
present on the server. There are no other non-essential programs present.

The residual risk is medium. Terminal Service may provide unauthorised access to some resources and therefore unauthorised changes to the system or files. It is good practice to run only programs that are necessary.

I would recommend removing Terminal Service from the server.

The control objective was achieved. I have verified that there are non essential programs present on the server. The system is auditable the programs are clearly visible as not present except for Terminal Services. The shutdown version of results is visible below.



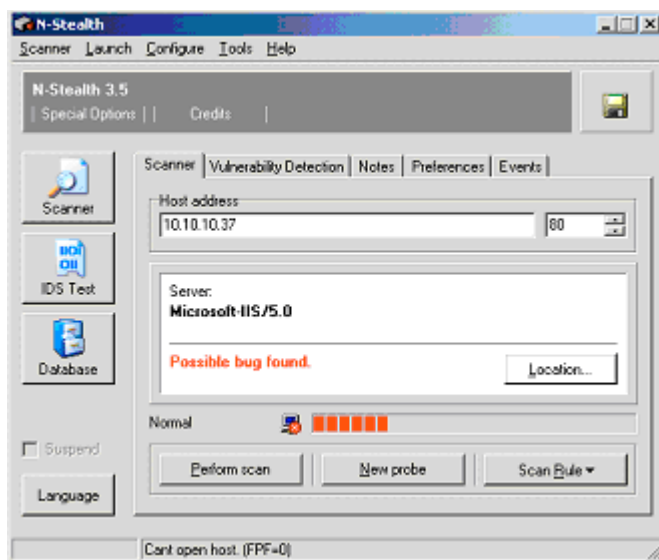
Result 8- Customized UrlScan configuration

Reference Check No. 10. p14.

The physical examination of the UrlScan file has revealed that the file matches the customised UrlScan file for this organisation. All possible high vulnerabilities presented by NSleath scan were examined. Attempts to execute unwanted files with prohibited extensions and Unicode failed on all attempts during this audit.

The residual risk in this case is low. The benefit to the organisation of having a correct up to date UrlScan file is paramount.

The system is auditable. The tests conducted involved a physical check of the UrlScan file, and the use of an NSleath 3.5 Built 55 tool to confirm that the system is compliant. The NSleath tool was obtained during the SANS conference in Sydney 2003. The number of possible vulnerabilities was 337. All possible high vulnerabilities were tested. The cut down version of the results are shown below.



N-Stealth Report

N-Stealth report for - (10.10.10.37)

Date: 5/23/2003 9:34:37 AM

Scan Rule: Normal

10.10.10.37

Host name: -

Port: 80

Server: Microsoft-IIS/5.0

Server may have HTTP vulnerabilities/exposures. 337 item(s)

Special Request

Risk Level: High

Location: <http://10.10.10.37/sek->

[bin/login.gas.bat?Template=../../../../../../../../etc/hosts&LOCALE=en_US&AUTHMETHOD=UserPassword](http://10.10.10.37/bin/login.gas.bat?Template=../../../../../../../../etc/hosts&LOCALE=en_US&AUTHMETHOD=UserPassword)

Common File Exposure - Possible bug or misconfiguration problem in the web server that allow unauthorized remote users to gain information about the web server's host machine that will allow them to break into the system.

My recommendation would be that the server is configured with the correct template, tested for an appropriate amount of time and the change moved to production.

The residual risk to the system is high because the responsibility to apply the appropriate settings to the server is with the administrator only. There is a need for another body to confirm these and any other security settings on regular basis especially on critical devices that are exposed to the Internet. Additional confirmation of the settings could for example occur through regular audits.

The control objective was achieved and the system is auditable. The audit has shown that the security template applied to the server is not the correct one. A cut down version of the results are presented below.

Security Configuration and Analysis tool results

```
View Log File
?-----
05/23/2003 15:41:34
----Analysis engine is initialized successfully.----

----Reading Configuration info...

----Analyze User Rights...

Mismatch - SeNetworkLogonRight.
Mismatch - SeTcbPrivilege.
Mismatch - SeMachineAccountPrivilege.

----Analyze Registry Keys...

Mismatch - machine\software\Policies.
Mismatch - machine\software\classes.

----Analyze File Security...
Mismatch - c:\documents and settings\administrator\Application
Data\Microsoft\Internet Explorer\UserData\index.dat.
Mismatch - c:\documents and settings\administrator\Local

----Analyze General Service Settings...
Mismatch - Wmi.

----Analyze Security Policy...
Mismatch - MinimumPasswordLength.
Mismatch - MaximumPasswordAge.
Mismatch - MinimumPasswordAge.
Mismatch - PasswordComplexity.
```

Result 10- Unused Script Mappings

Reference Check No. 16. p18.

The examination has revealed that there are a number of unused script mappings present. They are:

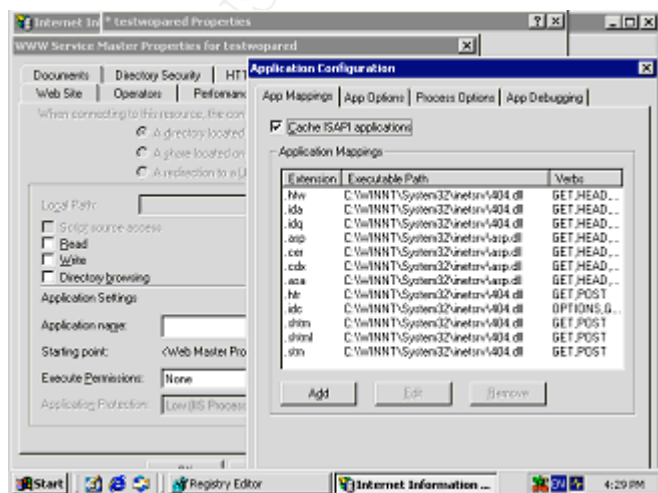
- .htr
- .shtml
- .stm
- shtm
- .ida
- .idq
- .htw

The residual risk is medium. The mappings of the unused scripts may result in unauthorised access to information or the use of organisational resources to attack other external or internal systems.

I would recommend that all the above listed mappings will be removed. The listed mappings should have been removed by the IIS Lockdown wizard. The above extensions are listed in the customised Urlscan.ini file as denied extensions; therefore these mappings should not exist, unless they have been remapped manually.

The control objective was achieved. The inspection has revealed unnecessary script mappings present.

The system is auditable to the extent that, unnecessary mappings have been found. However, it still needs to be determined why the denied extensions exist when they are listed in the Urlscan.ini as denied extensions. The audit was performed as detailed in the checklist and the results are visible below.



Result 11- Antivirus Software and signature file

Reference Check No. 17. p19.

The examination of the antivirus software has revealed that the software is well out of date. The last time the signature file was updated is 12/09/02; the version found on the server is InoculateIT 23.58.34, the product version is 6.0.

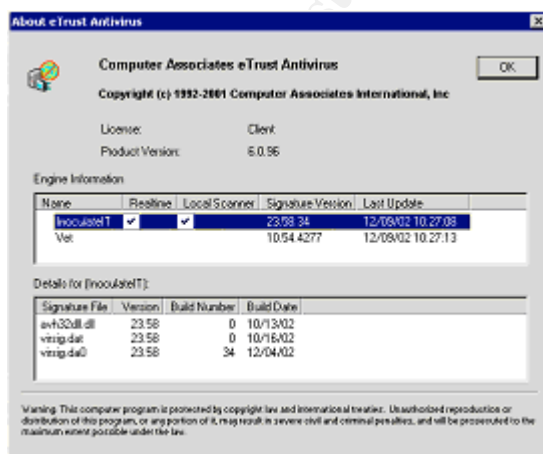
The residual risk is high. The examination has revealed that for months there was no updates to the antivirus software. The server is vulnerable to a number of latest viruses, which may result in the destruction of data on the server or compromise through a virus, which has been a very popular method in the latest past.

I would recommend that a newest version of antivirus software be applied, that is 23.61.35. In the nearest future the organisation should look at upgrading product to version 7.0, and newest signature file found at that time. Before product update is applied sufficient testing should be performed.

The organisation has paid for the licence of antivirus software so the costs are significantly reduced. However, mechanisms that check for latest file updates are misplaced in the process. The organisation should once again deploy a secondary mechanism that checks these and any other security settings. The mechanism could be in the form of regular audits.

The control objectives were achieved. I have confirmed that antivirus software is installed but the latest signature file is missing.

The system is auditable, the audit was performed as per the checklist and the results are visible below.



Assignment 4 – Audit Report or Risk Assessment

Executive summary

This paper documents an audit of Microsoft Internet Information Server (IIS), version 5.0 running on a Windows 2000 server.

The server publishes information, and provides public and internal users material on the role, functions and operations of the organisation

The scope of the audit was to determine if the server's security settings meet industry best practice. The focus of the audit was limited to the operating system that the server runs on, and the IIS it's self only.

The audit of the IIS server has revealed that while the organisation pays attention to the physical security of the server, the level of preventative measures to protect the server from intruders and viruses is low.

The following vulnerabilities were found on the IIS server:

- 1) Missing security updates
- 2) Weak password policy
- 3) Unnecessary services running on the server
- 4) Unnecessary accounts are present on the server
- 5) Non-essential programs are present on the server
- 6) Incorrect security template used for configuration
- 7) Unused script mappings present on the server
- 8) Antivirus software out of date

In its present state the server presents numerous vulnerabilities which can result in it being compromised.

An attacker could delete files, edit files or place embarrassing material that would be visible to the public. The server could also be used as a tool to attack other internal or external devices.

If the server were to be compromised it could embarrass the professionalism and confidence of the public in the organisation.

Regular audits of the server and training is recommended for parties responsible for maintenance of the IIS server.

Audit Finding No. 1 - Missing security updates

Reference Result No. 2. p.23

The examination of the service packs and patches has revealed that there are nine security updates missing. It is important to have the server patched up to date. Microsoft regularly informs of new known vulnerabilities and provides patches to prevent these vulnerabilities from being exploited.

Background/risk

The attacker could exploit this vulnerability by running arbitrary code on a user's system.

It is possible for an attacker to create a URL that would inject script during the rendering of a third party file format and cause the script to execute in the security context of the user.

The vulnerability would provide the attacker with the capability to read files of the hard drive. The attacker would find sufficient information there to make changes which could result as a public embarrassment to the organisation. The server after compromise of this nature would most probably have to be re-imaged from backup due to the fact that it would take longer to determine if this and any other possible vulnerabilities have fully been removed than re-imaging it.

Audit recommendations

Relevant patches should be downloaded from Microsoft Cooperation. Patches should be applied to the server in a test domain. Following substantial testing the relevant patches can be applied to the production server.

Costs

Downloading and research of the patches – 1 day at \$250 per day
Installation and testing – 4 days at \$250 per day

Total = \$1250

Audit Finding No. 2 – Strong Password

Reference Result No. 4. p.25

The minimum password length is set to eight characters. The password complexity requirements is disabled, therefore the account holders can enter weak passwords which can be broken easier.

Background/risk

Weak password provides attackers with an easy way to get access to the server. By breaking the administrator's password, the attacker could do anything they like on the server. The attacker could delete files, edit files or place embarrassing material that would be visible by the public. This could result in a public embracement and evidence that the organisation is unable to sustain sufficient security measures. The server would have to be re-imaged to make sure there are no vulnerabilities left by the attacker.

Audit recommendations

Change the minimum length for the password to nine characters and enable password complexity requirements

Costs

Change of password length – 10min at \$250 per day = \$5

Enable password complexity – 10min at \$250 per day = \$5

Change passwords to suit the new policy – 30min at \$250 per day = \$15

Total = \$25

Audit Finding No. 3 – Unnecessary Services

Reference Result No. 5. p.26

There are three unnecessary services running on the server: Compaq system shutdown service, Compaq version control agents, DHCP client

The fourth service "performance logs and alerts" is set to manual.

Further examination has shown that there are services accessible from the inside of the network. These are:

- 199/tcp open smux
- 443/tcp open https
- 445/tcp open microsoft-ds
- 1026/tcp open LSA-or-nterm

- 1027/tcp open IIS
- 1033/tcp open netinfo
- 2301/tcp open compaqdiag
- 3389/tcp open ms-term-serv
- 13782/tcp open VeritasNetbackup
- 49400/tcp open compaqdiag

Background/risk

The services that are advertising themselves to the inside of the network may provide an internal attacker with increased possibility to compromise the system. Unnecessary services may provide internal attacker also with another way to compromise the server. Depending on the compromise the attacker may gain partial or full control of the server.

The risk of internal attack is low because each employee has to go through security clearance. However, if it did happen the results may be loss of data or unwanted material published on the server. The result once again could cost the organisation, public embracement and the server being out of action because it would have to be rebuilt if it was not clear how the attacker got in and what was done to the server.

Audit recommendations

Disable Compaq system shutdown service, Compaq version control agents, DHCP client and performance logs and alerts.

Implement a control that limits access to these ports to employees and services that absolutely need to access these services on these ports. Create additional entries in the access control list on the firewall which would limit the access to these ports to the necessary users and services.

Costs

Disabling and testing of the four above services – 2hrs at \$250 per day = \$63
 Creating new entries on the firewall and testing – 2days at \$250 per day = \$500

Total = \$563

Audit Finding No. 4 – Unnecessary Accounts

Reference Result No. 6. p.30

The examination of unnecessary accounts has revealed that there are more than two administrative accounts and the number of accounts is more than necessary. There is an account that has never been logged into and account that has been disabled.

Background/risk

All these unnecessary accounts may provide intruder with a possible way to break-in. If an account is compromised, being a local account, it will provide attacker with sufficient access to do a lot of damage (files edited/deleted, unapproved material placed for public viewing). This could result in a public embracement and evidence that the organisation is unable to sustain sufficient security measures. The server would have to be re-imaged to make sure there are no vulnerabilities left by the attacker.

Audit recommendations

I would recommend deleting one administrative account and leaving only one. The guest account should be deleted completely from the server. The unused accounts should be disabled for a short period of time for the purpose of testing, to make sure that no applications or services are using them, and then deleted. It is good practice to delete accounts which are disabled for a long period of time. If it is not needed it is safer to delete it. The account that is used by applications (IWAM_YYYYYYYYYY) should be left as it is

Costs

Deletion, disabling of accounts – 30min at \$250 per day = \$15
Making sure applications are not using disabled accounts – 4hrs at \$250 per day = \$125

Total = \$140

Audit Finding No. 5 – Essential Programs

Reference Result No. 7. p. 32

Terminal Service is present on the server.

Background/risk

Terminal Service should only be used during testing. It could provide attacker with additional possible way to break in.

Audit recommendations

Remove Terminal Service from the server

Costs

Remove the Terminal Service from the server - 15min at \$250 per day = \$8

Audit Finding No. 6 – Security Template

Reference Result No. 9. p. 35

The server was not configured using the correct security template. The test has revealed 215 mismatches between the current security configuration and the template that should be used for this IIS server. The security template that should be used was present on the server but it was not used.

Background/risk

An incorrect security template reduces the security of the server in number of areas. Other vulnerabilities listed previously would not exist eg. Weak passwords if the correct template was applied because the template enforces strong security policies. There are 213 different security settings between the template that the server is configured with and the template that it should be configured with. Keeping that in mind the risk of the server being compromised is high.

There are a number of areas that make the server more vulnerable

- The password policy would not prevent the use of weak passwords and the passwords would never expire.
- The accounts would not lock out if an attacker was trying to use it to log into the server and the password was incorrect.
- The audit policy is set incorrectly. It does not cater for appropriate events which would provide sufficient information to audit the server in case of a suspicion of break in.
- The user rights policy allows unauthorised users to bypass traverse checking and take ownership of files and objects.
- The security settings policy provides user with the ability to shut down the server without logging on and it does not display the text for users attempting to log on, warning them of consequences of un-authorised access.
- Service policy does not disable DHCP client.
- The registry permissions policy allows for inappropriate access to the registry.

Audit recommendations

Organisation had a security template created by an external contractor and tested especially for this IIS server. Deploy the security template that was designed for this IIS server.

Costs

The template already exists so the costs in creating custom template to suit the organisation will be \$0

Deploying the template and testing – 5 days at \$250 per day = \$1250

Total = \$1250

Even that the template was already tested before, I still recommend testing it again before the change is moved into production server.

Audit Finding No. 7 – Unused Script Mappings

Reference Result No. 10. p. 37

The audit has revealed the following unused script mappings.

- .htr
- .shtml
- .stm
- shtm
- .ida
- .idq
- .htw

Background/risk

Unused script mappings may result in unauthorised access to information or the use of organisational resources to attack other external or internal systems.

Audit recommendations

Remove all the above unused script mappings on a test IIS server and after substantial testing do the same on the production server.

Costs

Removal and testing 2 days at \$250 per day

Total = \$500

Audit Finding No. 8 – Anti Virus software and signature file

Reference Result No. 11. p. 38

Antivirus software is present on the server but the signature file is well out of date. The last time the signature file was updated is 12/09/02; the version found on the server is InoculateIT 23.58.34, the engine version is 6.0.

Background/risk

The server is vulnerable to a number of latest viruses, which may result in the destruction of data on the server or compromise through a virus, which has been a very popular method in the latest past.

For further details about the viruses that the server is vulnerable to please refer to Appendix A.

Further more some of the Trojans make requests to specific Web-sites to download additional malicious software in which case the firewall would not be able to stop because it would assume that the request is genuine and it comes from the inside.

Audit recommendations

The server may be infected with a virus, backdoor or a Trojan. Some of these viruses disable antivirus software. Therefore, the system should be scanned from another computer possibly connected to the server only, using two different antivirus applications.

Update the signature file to the latest one which is 23.61.35.

Find out why the management software has failed to deploy the signature files to the server and also why it did not find out about the out of date signature for months. There is a possible failure in the configuration of antivirus management software.

Costs

Scan, download and apply up to date signature file 2hrs at \$250 per day = \$63

Research and correct antivirus management software 2 days at \$250 per day = \$500

Total = \$563

Organisation holds current licence for antivirus software so the costs in purchasing software are nil.

Organisation has antivirus management software which should deploy and check the deployment success rate of new signature files, therefore the costs of purchasing this software is nil.

Compensating Controls

The organisation has the relevant sections to look after the different aspects of configuration and security. However, there are no controls in place that would check whether the work is done up to the industry best practice.

There is a need for the employees to receive regular training, so they can be kept up to date eg SANS Conferences, receive regular news and have access to Web broadcasts that inform of the newest vulnerabilities, best practices, and preventive measures.

I believe that there is a strong need for regular audits so the devices which are used by the organisation can be kept up to the highest level of security and parties responsible for corrections of these devices can be informed and the required improvements can be made. I believe that method would introduce a stronger preventative controls that may prevent the server from being compromised.

Employment of one additional staffer for one week every three months would cater for an audit that could be performed in that time every three months. From that audit, organisation would benefit such that the server would be kept up to industry best practice, vulnerability free. However, it still would be up to the relevant section to test and implement the changes. Each following audit would reveal whether the changes have been implemented correctly.

Ongoing costs

One auditor at \$350 per day, 20 days work in a year = \$7000
Administrator/Security officer training cost = \$5000

Total cost = \$12000

Training of this magnitude should provide with time, sufficient knowledge to keep the IIS server up to industry best practice.

Total immediate and ongoing cost – AUS \$16299

References

- 1) SANS Institute. "SANS/FBI Top 20 List". Version 3.22. March 3, 2003. <http://www.sans.org/top20/#W1> (15 March. 2003).
- 2) Microsoft Cooperation. "Windows 2000 Server Baseline Security Checklist"
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/w2ksvrcl.asp> (10 Mar 03)
- 3) Microsoft Cooperation. "Secure Internet Information Services 5 Checklist"
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/iis5chk.asp> (10 Mar 03)
- 4) "Risk Assessment/Countermeasure Analysis/Security Test and Evaluation (ST&E) for Microsoft Windows 2000 Computer Systems". October 1, 2002 PART II (V1.5).
http://www.nswc.navy.mil/ISSEC/Form/AccredForms/acc_part2_2000.html (17 Mar 03)
- 5) "Common Vulnerabilities and Exposures The Key to Information Sharing". CVE version: 20030402 <http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=iis+5.0> (20 March 03)
- 6) Microsoft Cooperation. "UrlScan Security Tool"
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/urlscan.asp> (7 Mar 03)
- 7) Microsoft Cooperation. "IIS Lockdown Tool".
<http://www.microsoft.com/technet/security/tools/locktool.asp> (10 Mar 03)
- 8) Computer Associates. "Newly Detected Viruses Since the Last Virus Signature Update ", Document Number: 31033b
<http://support.ca.com/techbases/ilnt/31033b.html> (14 June 2003)
- 9) Rhoades, David. "Auditing Web Servers and Applications". SANS Institute Track 7 – Auditing Networks, Perimeters and Systems. 2002. p(s). 15, 64, 72, 77, 86, 88, 11
- 10) Krasavin, Serge. "IIS 5.0 Web Server Audit Checklist". www.ccsostaff-nts.cso.uiuc.edu/skrasavi/Info/IIS%205.0%20checklist.pdf (10 May 03)

Download Sources

- 11) IIS Lockdown tool - <http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=DDE9EFC0-BB30-47EB-9A61-FD755D23CDEC>
- 12) N-Sleath - www.nstalker.com/nstealth/
- 13) Brutus - www.hoobie.net/brutus/index.html
- 14) Achilles - www.mavensecurity.com, www.digizen-security.com
- 15) Screaming Cobra - www.cobra.lucidx.com
- 16) Web Sleuth - www.geocities.com/dzzie/sleuth/
- 17) Nessus - www.nessus.org
- 18) Appropriate Windows 2000 and IIS patches - http://www.microsoft.com/downloads/search.aspx?opsysid=1&search=Keyword&value='security_patch'&displaylang=en
- 19) Microsoft Baseline Analyser - <http://download.microsoft.com/download/e/5/7/e57f498f-2468-4905-aa5f-369252f8b15c/mbsasetup.msi>
- 20) Anti virus software up to date signature files (InoculateIt and Vet) - <http://support.ca.com/Download/virussig.html#inoc60>

Appendix A

Viruses/backdoors that the IIS server is vulnerable to at present time

Virus Signature:

eTrust Antivirus / eTrust InoculateIT Engine 6.0,
Version 23.61.50 (Engine version 23.61.00)

Newly detected viruses since last update:

23.61.50	REG/IRC.FLOOD.NETBUSTER
DETECTION	
23.61.50	W97M/GOEN
DETECTION/CURE	
23.61.50	W97M/JISHE.F
DETECTION/CURE	
23.61.50	WIN32/HLLP.JEEFO.A
DETECTION	
23.61.50	WIN32/LABIRINTO
DETECTION/SYSTEM CURE	
23.61.50	WIN32/LOVGATE.M
DETECTION/SYSTEM CURE	
23.61.50	WIN32/MOFEI.A.DLL
DETECTION/SYSTEM CURE	
23.61.50	WIN32/MOFEI.C
DETECTION	
23.61.50	WIN32/MOFEI.C.BACKDOOR
DETECTION	
23.61.50	WIN32/MOFEI.C.DLL
DETECTION/SYSTEM CURE	
23.61.50	WIN32/MOFEI.C.MIS
DETECTION/SYSTEM CURE	
23.61.50	WIN32/MOFEI.D
DETECTION	
23.61.50	WIN32/MOFEI.D.BACKDOOR
DETECTION	
23.61.50	WIN32/MOFEI.D.DLL
DETECTION/SYSTEM CURE	
23.61.48	BACKDOOR/KATHERDOOR.305.D
DETECTION	
23.61.48	WIN32/BACKZAT.G
DETECTION/SYSTEM CURE	
23.61.48	WIN32/BACKZAT.H
DETECTION/SYSTEM CURE	
23.61.48	WIN32/NACO.F
DETECTION/CURE/SYSTEM CURE	
23.61.47	HTML/FORTNIGHT.C
DETECTION/SYSTEM CURE	
23.61.47	JSCRIPT/CODEBASE.EXPLOIT
DETECTION/CURE	
23.61.47	WIN32/4HORSEMAN.B
DETECTION/SYSTEM CURE	
23.61.47	WIN32/KIRBO.A
DETECTION	
23.61.47	WIN32/PWS.WMPATCH.E.DOWNLOADER
DETECTION/SYSTEM CURE	
23.61.47	WIN32/QAGAT.A
DETECTION/SYSTEM CURE	

23.61.47	WIN32/QAGAT.B
DETECTION/SYSTEM CURE	
23.61.47	WIN32/SPYBOT.44064
DETECTION	
23.61.47	WIN32/THAPROG.C
DETECTION	
23.61.46	BAT/ENERGY
DETECTION	
23.61.46	WIN32/FLOR
DETECTION/SYSTEM CURE	
23.61.46	WIN32/MOFEI.B
DETECTION/SYSTEM CURE	
23.61.46	WIN32/MOFEI.B.DLL
DETECTION/SYSTEM CURE	
23.61.46	WIN32/SUPERWAY.A
DETECTION/SYSTEM CURE	
23.61.46	WIN32/TRYTOO
DETECTION/SYSTEM CURE	
23.61.46	WIN32/VALLA.2048
DETECTION/CURE	
23.61.44	BACKDOOR/AHS.SERVER
DETECTION	
23.61.44	BACKDOOR/ASV.SERVER
DETECTION	
23.61.44	BACKDOOR/DEBUT
DETECTION	
23.61.44	BACKDOOR/DECEPTION.30
DETECTION	
23.61.44	BACKDOOR/DECEPTION.30.CLIENT
DETECTION	
23.61.44	BACKDOOR/DELF.F
DETECTION	
23.61.44	BACKDOOR/DELF.FD
DETECTION	
23.61.44	BACKDOOR/DELF.FE
DETECTION	
23.61.44	BACKDOOR/DELF.FI
DETECTION	
23.61.44	BACKDOOR/DELF.FO
DETECTION	
23.61.44	BACKDOOR/DELF.FT
DETECTION	
23.61.44	BACKDOOR/DELF.FU
DETECTION	
23.61.44	BACKDOOR/DELF.FV
DETECTION	
23.61.44	BACKDOOR/EGGDROP
DETECTION	
23.61.44	BACKDOOR/FERAT.10.A.CLIENT
DETECTION	
23.61.44	BACKDOOR/FERAT.10.A.PLUGIN
DETECTION	
23.61.44	BACKDOOR/FERAT.10.A.SERVER
DETECTION	
23.61.44	BACKDOOR/FERAT.10.A.SERVERBUILDER
DETECTION	
23.61.44	BACKDOOR/GWBOY
DETECTION	
23.61.44	BACKDOOR/IISINFECT.IRC
DETECTION	

23.61.44	BACKDOOR/IISINFECT.MIRC
DETECTION	
23.61.44	BACKDOOR/IRC.MOX
DETECTION	
23.61.44	BACKDOOR/IRC.RHY
DETECTION	
23.61.44	BACKDOOR/JINMOZE.180
DETECTION	
23.61.44	BACKDOOR/KATHERDOOR.305.E
DETECTION	
23.61.44	BACKDOOR/LITHIUM
DETECTION	
23.61.44	BACKDOOR/MAGICLINK.22
DETECTION	
23.61.44	BACKDOOR/MASSAKER.12.A
DETECTION	
23.61.44	BACKDOOR/MHTSERV.B
DETECTION	
23.61.44	BACKDOOR/MONATOR
DETECTION	
23.61.44	BACKDOOR/NETHIEF.46.CLIENT
DETECTION	
23.61.44	BACKDOOR/NETHIEF.46.SERVER
DETECTION	
23.61.44	BACKDOOR/OPTIXDDOS
DETECTION	
23.61.44	BACKDOOR/PEEPVIEWER.201
DETECTION	
23.61.44	BACKDOOR/PEERS.C
DETECTION	
23.61.44	BACKDOOR/POINTEX
DETECTION	
23.61.44	BACKDOOR/Q8.BAT.A
DETECTION	
23.61.44	BACKDOOR/QUIMERA
DETECTION	
23.61.44	BACKDOOR/RATEGA
DETECTION	
23.61.44	BACKDOOR/RECERV
DETECTION	
23.61.44	BACKDOOR/SNOWDOOR
DETECTION	
23.61.44	BACKDOOR/SRVCMD.B
DETECTION	
23.61.44	BACKDOOR/SYSKBOT
DETECTION	
23.61.44	BACKDOOR/TURKOJAN
DETECTION	
23.61.44	BACKDOOR/VB.EX
DETECTION	
23.61.44	BACKDOOR/VB.FC

This is a cut down list. For full list (59 pages) refer to the link below.

Computer Associates. "Newly Detected Viruses Since the Last Virus Signature Update ", Document Number: 31033b

<http://support.ca.com/techbases/ilnt/31033b.html> (14 June 2003)