Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Securing IIS6: From the OS, Up

The dark side of the Internet can test even the most diligent System Administrator's ability to get, and keep their web server secure. WWW attacks targeted at both web applications and the servers that offer them are growing at an ever-increasing rate. This document provides a detailed look at securing Internet Information Services v6.0 (IIS6), using a combination of security templates and manual techniques. In order to provide the most secure installation of IIS possible, the paper first looks at securing the base ope...

Copyright SANS Institute

Author Retains Full Rights

AD

Securing IIS6: From the OS, Up

GSEC Practical Assignment, Version 1.4b, Option 1

September 23, 2003

By Joey Peloquin

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Contents

Abstract 3
Introduction 4
Physical Security 5
Installing Windows Server 2003 5
Hardening Windows Server 2003 6
Security Templates 6
Security Configuration and Analysis 7
Installing IIS6 9
Securing IIS6 11
Web Service Extensions 12
DCOM 12
Logging 14
Web Site Permissions 14
Manual Tweaks 14
Services 15
Registry 16
Accounts 17
File System 17
Current Security Vulnerabilities 18
Conclusion 19
Bibliography 20
Appendix A 21
Acknowledgements 22

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Abstract
The dark side of the Internet can test even the most diligent System Administrator's ability to get, and keep their web server secure. WWW attacks targeted at both web applications and the servers that offer them are growing at an ever-increasing rate.

This document provides a detailed look at securing Internet Information Services v6.0 (IIS6), using a combination of security templates and manual techniques. In order to provide the most secure installation of IIS possible, the paper first looks at securing the base operating system, Windows Server 2003 (Win2K3). The process will be covered completely; creating a hardened baseline on which to install IIS6, hardening the web server itself, and manually tweaking settings to conform to a custom environment. Finally, the paper also explains methods of analyzing and verifying the prescribed security settings.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Introduction

In the presentation of this document, the assumption is made that the reader has a low to moderate level of familiarity with Windows operating systems (OS) and previous versions of Internet Information Services (IIS).

Windows Server 2003 and Internet Information Services v6.0 continue to expand upon, and improve Microsoft's initiative of Trustworthy Computing. Both products have been designed with a focus on security, shown in part by the lack of IIS's presence in a default installation of Win2K3.

Rather than provide a canned list of security enhancements to the Win2K3 / IIS6 offerings, listed below are some features that stood out during the first installation and configuration of the server:

Windows Server 2003

- Strong password warning for Administrator during installation
- IIS not installed by default
- Low privilege service accounts: Network Service & Local Service
- By default, NTFS gives read-only access to the Everyone group for the \Documents and Settings directory. The group is not included in the ACL for any other directories. Users, get read access as well, but starting from the root (e.g., C:\).
- Password protected screen saver by default (10 minutes inactivity)
- Successful logon and account logon events audited by default
- Internet Explorer is configured in the high-security zone by default.

Internet Information Services 6.0

- Not installed by default
- Configured to serve only static content out-of-the-box
- \Inetpub\AdminScripts only contains adsutil.vbs and synciwam.vbs
- 'Users' get 'read' permission on \Inetpub, 'everyone' is not present
- IUSR is explicitly denied 'write' permission on \wwwroot and children
- FTP and SMTP services are not installed with IIS6

The preceding was merely a drop in the bucket compared to the many changes made "under the hood", as well as user interface and general usability improvements. For example, incoming requests to IIS are now routed through http.sys, which resides in kernel-space, rather than inetinfo.exe (or dllhost, depending on configuration), a user-mode process (Microsoft).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Physical Security

Any document about securing or hardening a server would be lacking without mentioning, at least, minimum requirements for physically securing the box. Ideally, it would be located in a server rack (cage), with chassis lock engaged, and behind a door with an access-card reader. "Mileage" varies according to One's environment and budget, however, so ensure the server is as protected from unauthorized physical access as possible.

Installing Windows Server 2003

A detailed, step-by-step instruction for setting up Win2K3 is beyond the scope of this document. There are sure to be ample documents of that nature in the SANS reading room (http://www.sans.org/rr) and elsewhere on the Internet before too long, therefore, this paper attempts to concentrate on the details essential to the security of the server, and preparing it for installing IIS6.

Virtually any guide for hardening Windows server advises to start with a clean installation of the OS, rather than upgrading from a previous version. This ensures the Administrator is able to take advantage of any new technologies, and provides the opportunity to install only what is needed. Agreeing the advice of Phil Cox and the security consultants of First Base Technologies, in their guides for hardening Windows 2000, the author elected to begin with a fresh install of Win2K3 (3, 3). Although it is becoming less of a task to upgrade the Windows family of server operating systems, experience has proven the value of starting with a fresh copy whenever possible.

To protect against Directory Traversal attacks, ensure two partitions are created. The directory where web server content is stored, \Inetpub, by default resides on the C drive. Exploiting the web application on the server can lead to the ability to execute files in its partition. Moving \Inetpub to another partition will prevent the execution of OS system files and utilities.

During the installation of Win2K3, the user will be prompted to create an Administrator password. It is subject to a strict password creation policy by default, and the system will complain if two few, or a too-easy-to-guess or crack combination of characters is used. Take heed to this warning, and set a strong password before continuing.

One of the last interactive portions of the Win2K3 installation presents an opportunity to configure network settings for the server. This is a step that should be skipped, unless the machine is being built on an isolated network, or is disconnected altogether. Once the latest service pack and hotfixes have been applied, and the box has been hardened against attack, it can safely be connected to the network or Internet. Although it was a RedHat machine, and not Windows, the Honeynet Project documented, "the fastest time ever for a system to be compromised was 15 minutes" (Honeynet). It's likely that a Windows machine running IIS could squash that record today, considering the

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

likes of Nimda, CodeRed, Blaster, and Welchia/Nachi running loose on the Internet.

Microsoft states, "The product will be shipped to customers in a locked-down state, with more than 20 services turned off by default or running with reduced privileges to help IT Administrators run the most secure configurations" (Microsoft). Statistics for the services installed by default are as follows:

83 Services are present out-of-the-box
49 Services running
10 Services controlled by Local Service
06 Services controlled by Network Service

This is an improvement over previous releases of the Windows Server OS. However, any services not required for a system to fulfill its role should be disabled. This is part of the hardening process; the next step.

Hardening Windows Server 2003

The comprehensive "Windows Server 2003 Security Guide" (SG) presents a set of guidelines for securing Win2K3 servers, with categorized levels of security based on the function of the server (Microsoft). The best method for utilizing the guide is to download it in its entirety, as this provides the Administrator with several supporting documents such as the Testing, Supporting, and Delivering Windows Server 2003 guides. The "kit" also includes the security templates referred to throughout the SG.

A companion document, called "Threats and Countermeasures Guide", was produced to supplement the information contained in the Win2K3 and Windows XP security guides (Microsoft). It provides detailed information on the settings available in these two operating systems. This guide is also available for download.

Security Templates

The "Windows Server 2003 Security Guide" examines the Administrator's security needs based on the function of the server she is locking down. There are three top-level environments used in the document; Legacy Client, Enterprise Client, and High Security. The guide provides an explanation of these environments:

> The Legacy Client settings are designed to work in an Active Directory domain running on Windows Server 2003 domain controllers with Windows 98, Windows NT 4.0, and later client computers and member servers.
>
> The Enterprise Client settings are designed to work in an Active Directory domain running on Windows Server 2003 domain controllers with

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Windows 2000, Windows XP, and later client computers and member servers.

The High Security settings are also designed to work in an Active Directory domain running on Windows Server 2003 domain controllers with Windows 2000, Windows XP, and later client computers and member servers. However, the High Security settings are so restrictive that many applications may not function, performance of the servers may be noticeably slower, and managing the servers will be more challenging (Microsoft).

The security templates used for this paper, Enterprise Client - Member Server Baseline.inf and Enterprise Client - IIS Server.inf, are provided in the downloaded "Windows Server 2003 Security Guide" kit. As advised in the SG, the first step will be to apply the Enterprise Client - Member Server Baseline.inf. Next, the server will be analyzed to ensure the settings were implemented correctly. Once the baseline settings have been verified, IIS6 will be installed, the Enterprise Client - IIS Server.inf template applied, and a final analysis conducted. Finally, the IIS template only provides settings for the services and anonymous account installed with IIS6, therefore some additional tweaking by hand may be necessary to bring the server to the level of security desired.

Security Configuration and Analysis

Like Windows 2000, Win2K3 provides several tools to assist Administrators in managing security settings. Probably the best-known tool is the Security Configuration and Analysis (SCA) snap-in for the Microsoft Management Console (MMC). To utilize the tool on a fresh installation of Win2K3, open, or create a security database, and import the security template that will be used to analyze and secure the machine. For this document, the MemberBaseline.sdb security database has been created, using the Enterprise Client - Member Server Baseline.inf template. Now that the security database is populated with the desired security settings, two options are available; analyze the computer or configure it. Prior to the initialization of either function, a window will prompt for a path name to a text file for logging.

To view how the default security configuration of Win2K3 stacks up to the settings implemented by the member server baseline template, right-click 'Security Configuration and Analysis: Analyze Computer Now'. The left panel expands to display the same type of tree shown in the Local Security Policy administrative tool. For example, expand Local Policies, and click on Audit Policy (Fig. 1). This displays the values contained in the security template / database versus the current setting of the machine. The defined policies are marked with specific icons after the analysis, denoting compliance – green check mark, non-compliance – red 'x', or a question mark (?). The question mark denotation was only present on the test system in the Account Lockout Policy

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

console tree, under the ‘account lockout duration’ and ‘reset account lockout after’ policies.

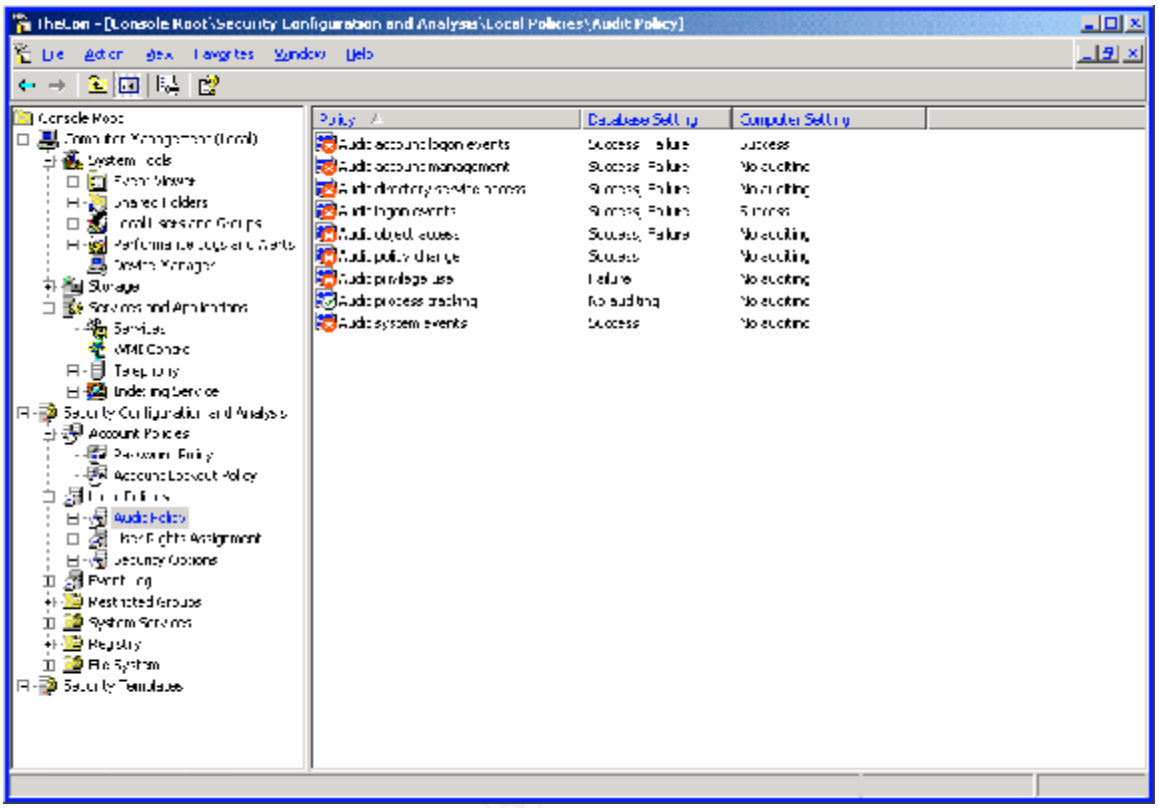

Figure 1

For the command-line inclined, a utility called SECEDIT is installed on Win2K3 systems by default. This tool contains all the functionality of the SCA console application, but offers the flexibility of automation using scripts. It also produces a text file log of the same format. The syntax for all of secedit’s functions is available in the help system.

To analyze a system, type:
secedit /analyze /db <path to db file name> /cfg <path to config file you are using (template)> /log <path to log file> /overwrite /quiet <suppress further complaints>

The ‘overwrite’ switch clears the database prior to importing the security template (/cfg). If this switch isn’t used, and settings in the database conflict with the template settings, the template settings will be used. Other functions available with secedit include:

/configure – applies a security template
/import – imports a template into a security database
/export – exports settings in a database to a template
/validate – validates a template to ensure the syntax is correct

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

/generaterollback – basically creates a snapshot of current system settings that can be reapplied if problems arise with modified settings.

'Validate' is the only function not available to SCA. The /refreshpolicy switch, used to refresh the security policy on a machine after changes have been made, no longer exists as an option in secedit. To refresh a security policy via command-line, one must now use the utility gpupdate.exe.

To rollback to default, out-of-the-box settings using SCA or secedit, create a rollback.sdb security database, and import the setup security.inf template located in c:\windows\security\templates. This file actually contains ALL the settings for the system, down to permissions of the files installed during the setup of Win2K3.

Installing IIS6

There are two different methods of installing IIS6. First, when 'add a role' is selected (clicked) from the Manage Your Server interface, the Configure Your Server wizard is spawned (Fig. 2). Next, one of two options needs to be selected, which will almost always turn out to be 'custom configuration'. As the name implies, this option allows the Administrator granular control over the set up of the server. Choosing 'typical configuration for a first server' automatically sets the machine up as a domain controller, with several other typical options.

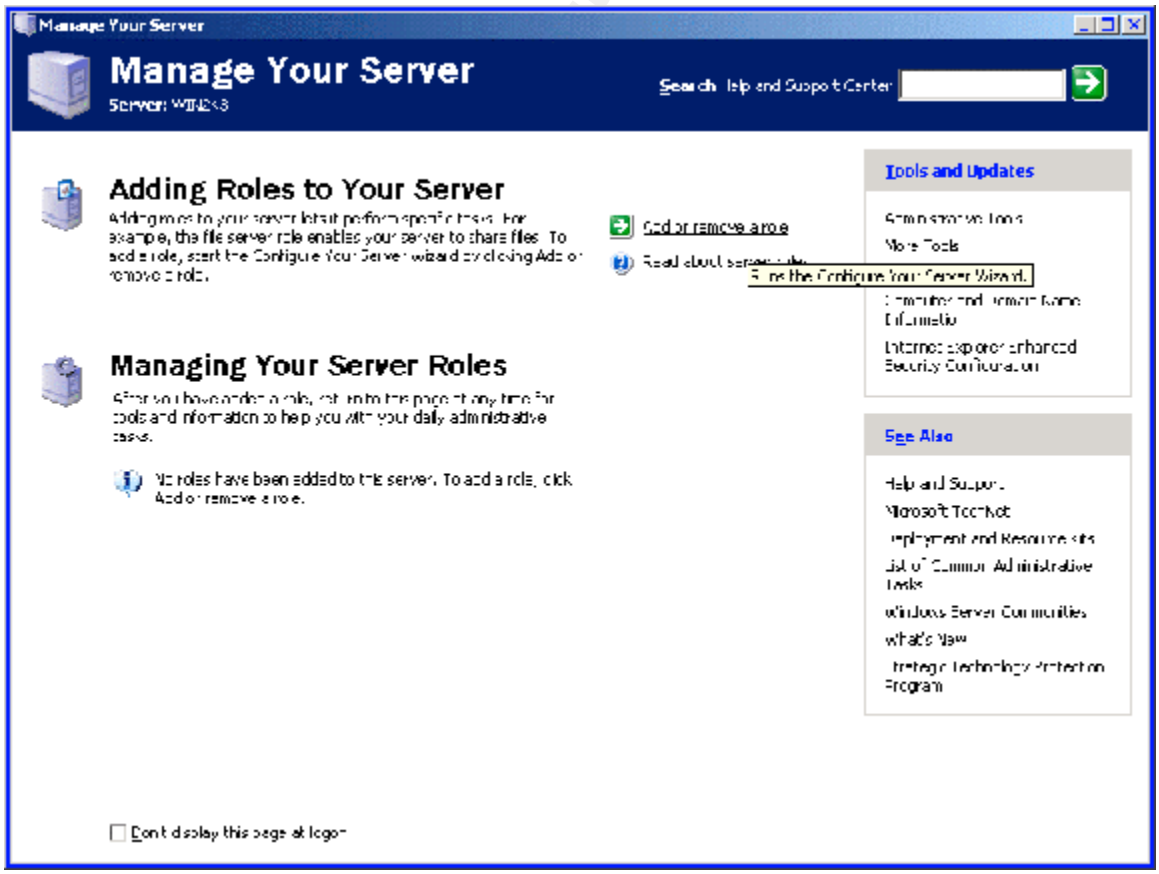

Figure 2

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The first step after choosing to customize the server is to assign it a role. IIS6 is an Application server; choose this role and the optional components on the following page applicable to the server's function (Fig. 3). A summary of selections is displayed, followed by the installation of IIS6 and the options chosen. Manage Your Server is located in the Start>Programs>Administrative Tools program group.

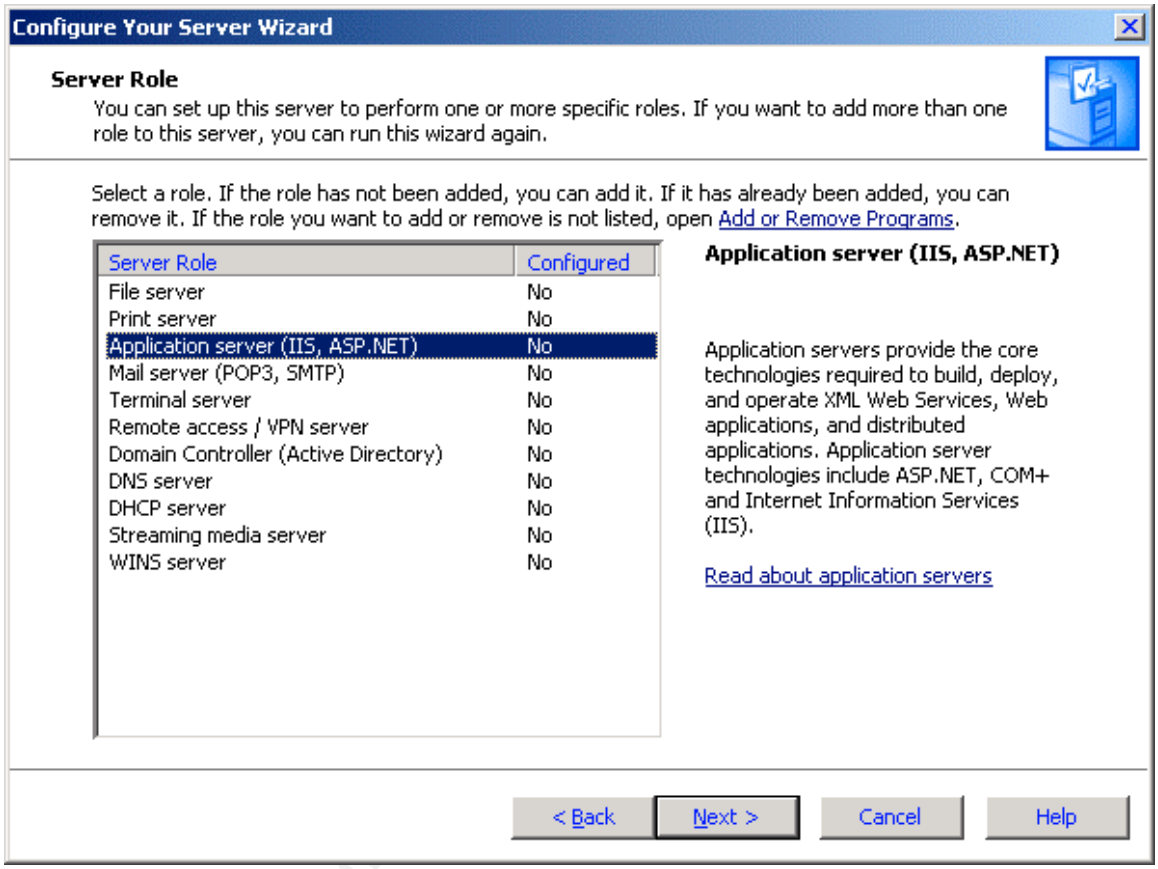

Figure 3

The WWW Publishing Service (WWWsvc) doesn't start immediately after installation. One of the services it is dependant on was disabled by the member baseline template used in the security templates phase of securing Win2K3. The HTTPSSL service must be enabled (started) before the web server can be started. The WWWsvc is configured to start automatically when the server boots up, however it can also be started from the services control manager, or by right-clicking the Internet Information Services Manager (IISM) and accessing the tasks menu.

Finally, the second method to install IIS6 is through the control panel, with 'add or remove programs'. Choose the familiar 'add or remove windows components' to spawn the Windows Component wizard. This provides an excellent opportunity to remove any accessories installed by default that aren't needed. Before exploring the Application Server options, browse 'details' of the Accessories

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

group and remove clipboard viewer, calculator, and wallpaper. Next, remove chat from 'details' of the communications subgroup, and acknowledge the 'OK'. Terminal Server may also be installed after returning to the Windows Component wizard.

Now, select the Application Server group, and access 'details', exposing a number of options available (Fig. 4). Choose the options applicable to the server's function and environment. The lab system runs lean, with only ASP.NET and the World Wide Web Service selected. If other web services are required for the target server's function, they can be added now and/or later. Installation begins after the services and options chosen have been acknowledged.

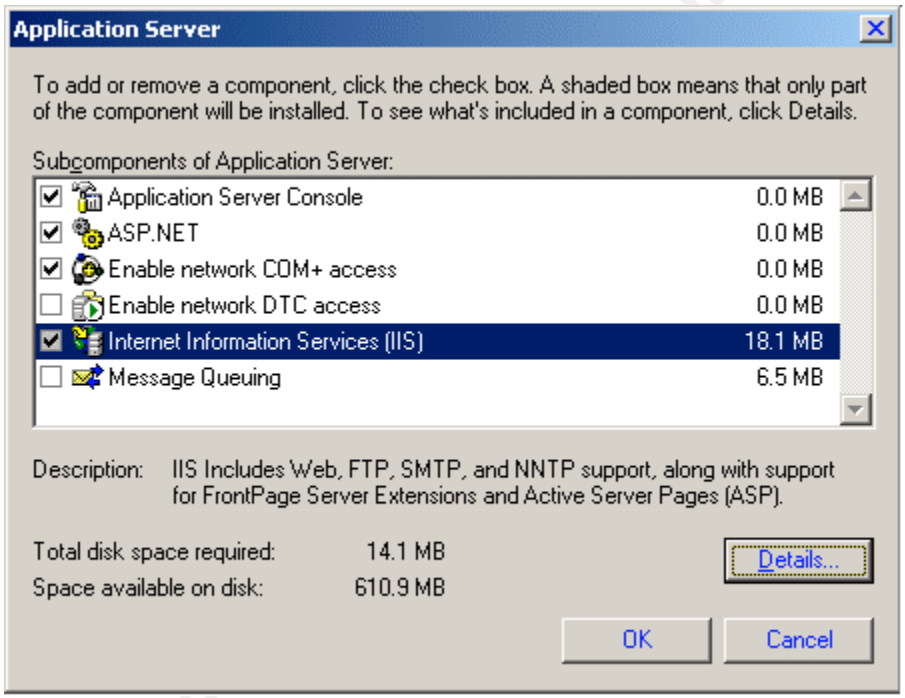

Figure 4

Securing IIS6

Locking down IIS is smoother and less time consuming than before. Many tasks have been eliminated by a combination of the new architecture and the more secure by default approach Microsoft employed in designing it. To begin the process of securing IIS6, apply any security updates available. Next, import and apply the Enterprise Client – IIS Server.inf template. Keep in mind, this template is intended to supplement the member baseline template applied earlier; as such, it applies only four settings:

IIS Admin Service – sets it to type 2, automatic start
WWW Publishing Service – sets it to type 2, automatic start
HTTPFilter (HTTP SSL) – sets it to type 2, automatic start
DenyNetworkLogonRight – denies network logon access to Anonymous User

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Anonymous User is the low privilege account that runs worker processes, which process requests routed through http.sys.

Web Service Extensions

IIS6 serves only static content by default, therefore, any type of dynamic content must be enabled by explicitly 'allowing' its use (Fig. 5). For example, to allow ASP, access the Web Services Extensions console tree, under Internet Information Services Manager (IISM). Next, highlight Active Server Pages, and select Allow. Alternatively, right-clicking Active Server Pages from the 'standard' tab in the right pane produces the same options: allow, prohibit, properties. Enabling only the web service extensions needed for the server to function reduces the attack surface.

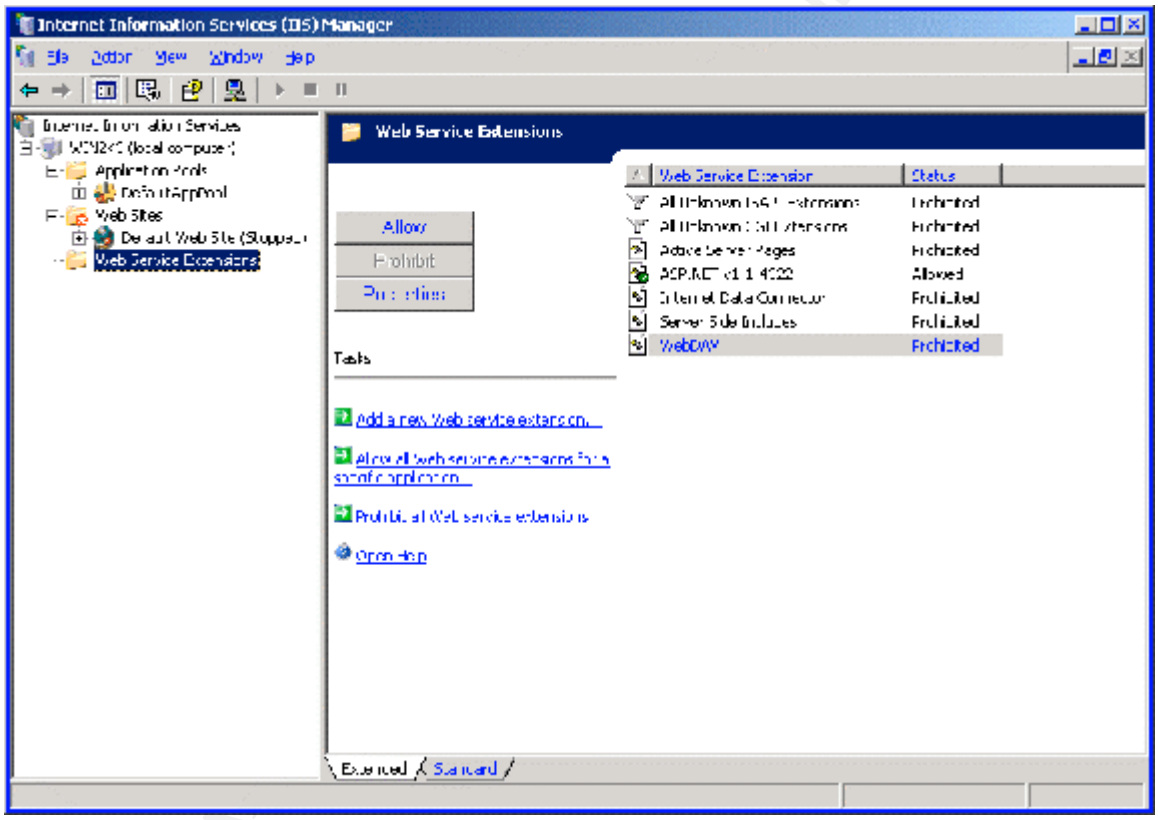

Figure 5

DCOM

If Distributed Component Object Model is utilized on the server, it will need to be enabled. DCOM can not be configured before enabling / starting its dependant services: COM+ System Applications (COM+SysApps) and Distributed Transaction Coordinator (DTC). The latter is not mentioned by Microsoft's help files as being a requirement for DCOM to run, but is needed none-the-less. DTC, which is dependant on the Security Accounts Manager service, seems to be involved with authentication and security for DCOM. COM+ SysApps is installed

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

with a start mode of 'manual' by default; DTC starts automatically by default, but is disabled with the member baseline security template.

After the dependant services have been started, the properties sheet for the local computer, which provides the means to enable or disable DCOM, immediately, becomes available (Fig. 6). In addition to Default COM+ Security, set from this page, the DCOM Config folder provides a means to control security at the application level.

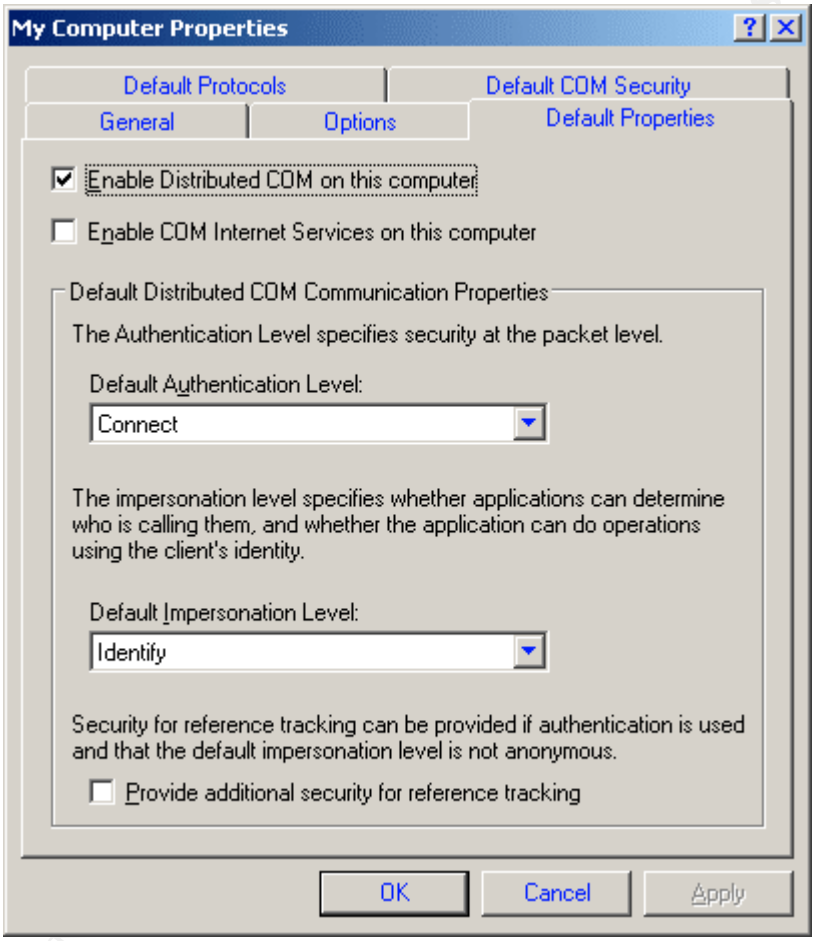

Figure 6

The security settings for DCOM are influenced by the needs of the applications installed by the Administrator. Launch permissions are a little too open by default, and should have IWAM, IUSR, and Interactive removed. Configuration permissions are more tightly configured, with Administrators and System having full control, and virtually everyone else granted read (Power Users, Users, etc., not the 'everyone' group).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Logging

Logging should be enabled on all web sites on the server. By default, the log is created and stored in the \Windows\System32\Logfiles directory. The log can be moved to the data drive containing web site files, and secured with NTFS permissions, but it is safe from modification by anyone other than the Administrators group in its default location. Log files can be analyzed with tools such as the extremely powerful command-line utility, Log Parser 2.1, available in the free IIS6 Resource Kit. With Log Parser 2.1, explicit strings can be queried for, locating entries of attempted attacks. There are also GUI log parsers available; however, they primarily focus on site usage statistics.

Web Site Permissions

When a new web site is created, the 'allow anonymous access' option is enabled. To create a web, extranet, or intranet site that requires authentication, this should be disabled. It can also be disabled or enabled through the 'properties' of the web site, on the Directory Security tab.

Three different forms of security reside on the Directory Security tab: Authentication, IP Address/Host name filtering, and Certificates. 'Authentication and access control' can be edited to force credentials to be entered to gain access to the web site. Basic Authentication should be used in conjunction with encryption; otherwise, passwords are transmitted in clear text.

Ideally, basic authentication is used over Secure Sockets Layer (SSL). IIS6 supports SSL v3.0 and Transport Layer Security v1.0, which should replace SSL in the near future (Dierks, Rescorla). SSL can encrypt using a session-key of up to 128-bit. Once a SSL session has begun, all traffic traversing the tunnel is encrypted. Typically, access to extranets and intranets is controlled through authentication; however, an Administrator can also require credentials to access specific areas of a publicly accessible web site.

Finally, using IP Address/Host name filtering, an Administrator can explicitly deny access to her web site to a single or group of computers, or by domain name. IIS6 has many methods to help Administrators keep their web servers secure, but ultimately, all environments are different. Even though initial lab testing is conducted in most cases, production servers should only "go-live" after thoroughly testing the settings Administrators put into place.

Manual Tweaks

While security templates provide a nice springboard for locking a first server down, it is the Administrator's touch through manual configuration that solidifies a server's defenses. After a machine of a specific type and function has been secured, a custom template can be exported, which can be used to apply standardized settings to a group of computers. Care must be taken, however, when testing new settings, that the master template remains accurately updated. Using the SCA tool, an Administrator can make manual changes throughout the

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

system, and save them in a working security database. Once all policies have been defined, the result can be applied to the system, and a copy of the settings exported in the form of a security template.

Services

As mentioned previously in this document, Win2K3 is installed with a plethora of services. Many of them are disabled or set to manually start by default; nevertheless, there are several that remain enabled which are not needed in a corporate-application server role. Windows Management Instrumentation (WMI) can be used to enumerate the services installed on a system, gleaning such information as a service's status, description, start mode, and start name (Appendix A). The services running after application of the member baseline and IIS security templates include:

Computer Browser
Cryptographic Services
DHCP Client
DNS Client
Event Log
COM+ Event System
HTTP SSL
IIS Admin Service
Server
Workstation
TCP/IP NetBIOS Helper
Windows Installer
Network Connections
Network Location Awareness
NT LM Security Support Provider
Plug and Play
IPSEC Services
Protected Storage
Remote Registry
Remote Procedure Call (RPC)
Remote Administrator Service
Security Accounts Manager
System Event Notification
Terminal Services
Windows Time
World Wide Web Publishing Service
Windows Management Instrumentation
Automatic Updates

* Third party remote control software

Armed with the output from the WMI script, open the SCA tool, navigate to the System Services console tree, and start disabling undesired services. The lab machine used for this paper will have the following services disabled:

DHCP Client –
The name of the service is self-explanatory. As most servers have IP addresses statically assigned, they do not need to function as DHCP clients.

COM+ Event System –
This service is a dependency of System Event Notification

System Event Notification –
It notifies subscribers of the COM+ Event System when system events occur.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Windows Time –
Production servers require some type of service/application to help them keep the correct time. If a third-party program is used, disable Windows Time.

Windows Installer –
Manages Windows Installer (msi) packages.

Network Location Awareness –
This service is used by ICS and the ICF to store network configuration.

Automatic Updates –
Automatically updating production servers without proper testing is not wise.

Plug and Play* –
It enables the system to dynamically detect changes in hardware configuration.
*Note, the system will complain when trying to enter the properties sheet of a service from the services control manager, but it succeeds.

In some circumstances, it may be possible to also disable the Network Connections, TCP/IP NetBIOS Helper, and IPSEC Services. After making the desired changes in the SCA, 'save' them to the database, and 'configure' the changes. Next, reboot the machine, and finally, reanalyze the security settings after it comes up.

In addition to the existence of environments where this configuration of running services is too strict, there are circumstances where it could be tightened more. Personal attention is required by the Administrator to get the perfect mix of security and functionality in their situation.

Registry
Although registry permissions are not defined in the security database with the member baseline and IIS server templates applied, Microsoft tightened it down well out-of-the-box. Default permissions of the primary registry hives are:

Local_Machine
Administrators – Full Control; Everyone – Read; Restricted – Read; System – Full Control

Users
Administrators – Full Control; Everyone – Read; Restricted – Read; System – Full Control

Root
Administrators – Full Control; System – Full Control; Creator Owner – Special (virtually full control on subkeys); Power User - Special (virtually full control on subkeys)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

If the default settings need to be modified, there are three methods available: SCA/Registries console tree; Regedt32.exe, a GUI tool; Reg.exe, from the command-line. The reg.exe utility can be used to script and automate registry management.

Registry permissions are inheritable from the parent hives. Within the properties dialogue of a primary hive in the SCA\registries console tree, the properties sheet offers the option to 'Propagate inheritable permissions to all subkeys' This allows the Administrator to define a top-level policy, and enforce it throughout the hive's children.

Accounts

A commonly known tactic for securing well-known accounts, such as, Administrator, is to rename them. The Administrator and Guest accounts can be renamed from within the Security Options console tree. Double-click the corresponding setting to define their policies in the security database.

This strategy works best when additional methods are put in place to protect against anonymous account enumeration. A setting under the Security Options console tree stops 'anonymous enumeration of SAM accounts and shares'. Another similar setting prevents enumeration of SAM accounts exclusively. The previous two settings in the local security policy correlate to a registry value called RestrictAnonymous. Configuring RestrictAnonymous too tightly can have dire consequences on functionality and communications, so ensure that ample testing has been completed prior to modifying it. Allowing anonymous connections and enumeration can yield a great deal of information with the right tools.

Finally, Account Policies should be configured according to the institution's corporate security policy, or equivalent. Since account policies vary greatly between environments, Win2K3 installs with a minimal configuration. At the minimum, Administrators are encouraged to configure password complexity requirements, and the account lockout settings. After all desired modifications have been made, 'save' the new policies in the security database, and 'configure' to apply them to the system.

File System

As with its predecessors, the Win2K3 file system is hierarchal. Using inheritance of permissions, an Administrator can create baseline settings at the root of a partition, e.g. C or D, and 'propagate them throughout sub directories and files.' Alternatively, permissions can be specified down to the file level, although the 'allow inheritable permissions …' in the properties/security check box must be cleared first. When this option is exercised, a dialogue box gives the Administrator the opportunity to copy the current security settings, allowing her to modify current settings, instead of having to come up with them from scratch.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

By default, the permissions settings are fairly strict, with Administrators and System granted full control, and Users, read. The infamous Everyone group only has read on the \Documents and Settings directory, where profiles are stored. For most environments, the default permissions should suffice.

Current Security Vulnerabilities

At the time of writing, Win2K3 suffers from several vulnerabilities. There are work-arounds or patches for each, however, so practice diligence in keeping the server updated.

Cumulative Patch for Internet Explorer (822925)
http://www.microsoft.com/windows/ie/downloads/critical/822925s/default.asp

Buffer Overrun in RPC Interface Could Allow Code Execution (823980)
http://www.microsoft.com/downloads/details.aspx?FamilyId=F8E0FF3A-9F4C-4061-9009-3A212458E92E&displaylang=en

Buffer Overrun in RPCSS Service Could Allow Code Execution (824146)
http://www.microsoft.com/downloads/details.aspx?FamilyId=51184D09-4F7E-4F7B-87A4-C208E9BA4787&displaylang=en

Flaw in NetBIOS Could Lead to Information Disclosure (824105)
http://www.microsoft.com/downloads/details.aspx?FamilyId=A59CC2AC-F182-4CD5-ACE7-3D4C2E3F1326&displaylang=en

Unchecked Buffer in DirectX Could Enable System Compromise (819696)
http://www.microsoft.com/downloads/details.aspx?FamilyId=A5156FF8-1812-4DB4-9175-BF9CA370279D&displaylang=en

Buffer Overrun in HTML Converter Could Allow Code Execution (823559)
http://www.microsoft.com/downloads/details.aspx?FamilyId=1C9914AB-25F8-462E-ADC0-5AC6BD0116DE&displaylang=en

Additionally, there is an issue with two of third-party network drivers Microsoft ships with Win2k3. It stems from an earlier security advisory reported by @Stake, concerning the padding of Ethernet frames with previously transmitted data, instead of null bytes (Arkin, Anderson). Chris Paget, a security researcher with NGSSoftware, discovered third-party network device drivers that are vulnerable to a similar issue, specifically regarding Win2K3 (Paget).

Finally, as if Administrators didn't already know attempting to manage IIS with the web-based Remote Administration tool was bad news, it is vulnerable to several attacks (Carames, Martinez).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Conclusion

Compiling recommendations accumulated from Microsoft documentation, knowledgeable Internet resources, and experience, the collection of tasks in this document greatly reduce a server's attack surface area, and provides an Administrator with a solid foundation on which to devise their custom solution. It requires more than a simple whitepaper to fully understand the power and security available to Administrators with the Win2K3/IIS6 offering. Microsoft has clearly undergone a change in focus, and is no longer allowing user's desire of functionality to outweigh the importance of security.

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Bibliography

Arkin, Ofir, and Josh Anderson. "Etherleak: Ethernet Frame Padding Information Leakage". 6 Jan. 2003
URL: http://www.atstake.com/research/advisories/2003/a010603-1.txt (17 Sep. 2003)

Carames, Hugo Vazquez, and Toni Cortes Martinez. "IIS 6.0 Web Admin Multiple vulnerabilities". URL: http://www.infohacking.com/INFOHACKING_RESEARCH/Our_Advisories/iis6/index.html

Cox, Phil. "Hardening Windows 2000". Version 1.0. 30 March 2001.
URL: http://www.systemexperts.com/tutors/HardenW2K101.pdf (17 Sep. 2003)

Dierks, Tim, and Eric Rescorla. "The TLS Protocol Version 1.1". June 2003.
URL: http://www.ietf.org/internet-drafts/draft-ietf-tls-rfc2246-bis-05.txt (17 Sep. 2003)

First Base Technologies. "Windows 2000 Server Security Standards".
17 Jan. 2003. URL: http://www.fbtechies.co.uk/Downloads/W2KServerSec.pdf (17 Sep. 2003)

Honeynet Project. "Know Your Enemy: Statistics". 22 July 2001.
URL: http://project.honeynet.org/papers/stats/ (17 Sep. 2003)

Microsoft Corp. "IIS 6.0 Core Components". IIS 6.0 Architecture. URL:
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/standard/arc_core.asp (17 Sep. 2003)

---. "Threats and Countermeasures Guide". 24 April 2003.
URL: http://go.microsoft.com/fwlink/?LinkId=15160 (17 Sep. 2003)

---. "Windows Server 2003 Delivers Higher Level of Security Without Compromising Functionality". 23 Jan. 2003 URL:
http://www.microsoft.com/presspass/press/2003/Jan03/01-23SecurityInnovationsPR.asp (17 Sep. 2003)

---. "Windows Server 2003 Security Guide". 14 August 2003.
URL: http://go.microsoft.com/fwlink/?LinkId=14846 (17 Sep. 2003)

Paget, Chris. "Etherleak information leak in Windows Server 2003 drivers".
9 June 2003. URL: http://www.nextgenss.com/advisories/etherleak-2003.txt (17 Sep. 2003)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Appendix A

Here's a simple script to enumerate the services on Win2K3. It was used to keep track of their state throughout the installation / hardening process.

```
'=====================================================================
'WorkFile: EnumServiceStateStartMode.vbs
'Created:  3 September 2003
'Modified: 3 September 2003
'Author: Joey Peloquin
'Description: Enumerates the services installed on a system (local),
'their state at script run-time and their start-mode.
'=====================================================================
OPTION EXPLICIT

Dim oFSO, oWSH, oLogFile, oInputFile
Dim ServiceSet, Service

Set oWSH = CreateObject("Wscript.Shell")
Set oFSO = CreateObject("Scripting.FileSystemObject")
Set oLogFile = oFSO.OpenTextFile("output.log", 8, True)

' Main
Trace "-----------------------------------------------------------------"
Trace "Service Enumeration has Begun: " & Date & " -- " & Time
Trace "-----------------------------------------------------------------"
Set ServiceSet = GetObject("winmgmts:{impersonationLevel=impersonate}") _
.ExecQuery("select * from Win32_Service")

For each Service in ServiceSet
        Trace Service.DisplayName & vbNewline & "status: " & Service.State & _
        vbTab & "start mode: " & Service.StartMode & vbNewline & _
        Service.Description & vbNewline & _
        "-------------------------------------------------------"
Next

Trace "-----------------------------------------------------------------"
Trace "Script Completed at: " & Time
Trace "-----------------------------------------------------------------"

oWSH.Run "notepad.exe output.log"
Set oLogFile = Nothing
Set oFSO = Nothing
Set oWSH = Nothing
Wscript.Quit

'*********************************************************************
' Function and Sub definitions below
'*********************************************************************
' Logging
Sub Trace(LogInfo)
        oLogFile.WriteLine LogInfo
End Sub
```

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Acknowledgements
I would like to thank my wife for her patience and understanding, and helping me find the motivation to press-on… to continue learning.

Also, Simon Dove, he encouraged me to learn VBS and WMI scripting, and shared a few techniques along the way.

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 20th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced