Global Information Assurance Certification Paper

Title: Research Guide to Web Resources at Microsoft.com and applying this to patching Internet Information Server

This document tries to cover various web resources of Microsoft Products such as Windows 2000, Internet Explorer and Microsoft Internet Information Server. The first section is a guide to information on the microsoft.com website. The second section goes further into patching and basis security information on Microsoft Internet Information Server and lists other resources for securing IIS. The last section discusses a vulnerability scanning tool such as ISS Internet Scanner and the relevant IIS vulnerability checks.

I want this to be guide on exploring Microsoft.com wealth of information and also want to apply this information to recent Security problems such as the Nimda worm and the appropriate fixes which involve patching Internet Explorer and Internet Information Server. I also try to emphasize good security practices such as understanding the applications, reading the security bulletins and researching various topics thoroughly. Don't just install a patch!

Section 1: Microsoft Web Resources

This section shows how to use the Microsoft Web pages to look for security relevant information. This isn't a comprehensive guide but describes the more useful sections on microsoft.com. The more useful main sections are Microsoft Windows Family Home Pages, Microsoft TechNet Pages, and Microsoft Developers Network (MSDN). Other useful places for research are further down in the web hierarchy are Microsoft Security Bulletin Pages and Knowledgebase Articles.

The starting main home page is http://www.microsoft.com and the other pages are links from this page. In the main home page are most of the links to the pages described above. Microsoft has a large amount of useful information on its site. The information on the site is sometimes but not always cross-referenced many ways. For example, I don't know of a good path to get to the Security Bulletin pages from the main page. Other links that I won't go into further detail are the links for other Microsoft Product Families of Office, Servers, and Developer Tools. The Office links cover products such as Microsoft Word and Excel and the Servers cover products such as Microsoft SQL. I won't go into further detail because this coverage of the Windows Product Families link will cover similar information such a white papers and patching contained under the other sections.

Microsoft Web Resources: Microsoft Windows Family Home Page content

Microsoft Windows Family Home Pages is under the "Product Family" "Windows" link or http://microsoft.com/windows/default.asp. These pages have product information on Microsoft Windows Operating Systems such as Windows 95, 98, NT, 2000, Me and XP. Some of these operating systems are server versions. This section of Microsoft.com has lots of white papers on design, security, patches, etc. I will give examples of a couple different places to get information.

To download Microsoft Service Pack 2 for Windows 2000, select the "Windows Product" "Family" link under Microsoft.com. After the "Microsoft Windows" page loads, select the "Windows 2000" main link. After the "Windows 2000" page loads, select the "Windows

2000 Professional" link. After the "Windows 2000 Professional" page loads, there is a highlights section where there is a "Download Service Pack 2" link. There is a lot of information to read on these download pages and one needs a fast Internet connection to download a service pack.(Ref 1)

This service pack is very important but not required because it upgrades Windows 2000 but also upgrades the native Internet Explorer version 5 to disable the following vulnerability "Incorrect MIME Header Can Cause IE to Execute E-mail Attachment", Microsoft Security Bulletin (MS01-020). This security bulletin deals with infected emails from either a web server or sent email and this email can infect a users machine. Nimda is a well-known exploit of this vulnerability so patching Internet Explorer is a high priority. Of course, these instructions are only valid for the Internet Explorer that came with Windows 2000 and not for any other versions of Internet Explorer on Windows 2000. To patch other versions of Internet Explorer, one should look at the Internet Explorer information page that is the Internet Explorer link under the Microsoft Windows Family Home Pages and look for the "Download" "Internet Explorer 5.x" sub link.(Ref. 2)

Another section of interest under Windows Product Family is some of the technical papers. Under Microsoft.com, select the "Product Family" "Windows" link. After the Microsoft Windows page loads, select the "Windows 2000 Server" main link. After the "Windows 2000 Server" pages loads, select the "Technical Resources" link. When the Windows 2000 "Technical Resources" Page loads, there are many links but select the "Administration" link. I arbitrarily selected the Administration link but this illustrates some of the information on Windows 2000. On this page alone, there are many sections, but a good one to note is the "Security Services" section. Now if you're interested in understanding winlogon, and this paper is very technical, read the following paper: "The Essentials of Replacing MSGINA.DLL".

Microsoft Web Resources: Microsoft TechNet content
Microsoft TechNet Pages is under the Information for IT Professionals link from the microsoft.com page or http://microsoft.com/technet/. These pages are valuable resources for IT Professionals such as system administrators. These pages contains Security Bulletins, Knowledgebase articles, Downloads, etc.

The Security Bulletins are a box on the right side of the TechNet main page. In the Security Bulletins section, click on the more... link to get more information on security bulletins. This will bring the "Security Bulletins Search Page". These pages are very useful to fix vulnerabilities found in Microsoft Products. This page can search for appropriate Security Bulletins by Product and Service Pack. For example, select Product "Internet Explorer 5.0" and Service Pack "All". This search will come up with 17 Microsoft Security Bulletins. Now under March 2001, click on "MS01-020: Incorrect MIME Header Can Cause IE to Execute E-mail Attachment" link. This is the actual security bulletin that we talked about earlier that is exploited by the Nimda worm. (Ref. 2,10)

Now lets delve deeper into Microsoft Security Bulletin MS01-020 at http://microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-

020.asp. There are multiple sections to this bulletin. There is a summary section, technical details section, frequently asked questions section, a patch availability section (download information), and an additional information and other information section. The technical details go into details of the vulnerability; the Frequently Asked Questions cover various useful details such as the scope of products with this vulnerability, i.e. Internet Explorer 5.x, 5.5 and 6.x. And the patch availability section discusses how to get and apply the patch. Also read the Additional Information section because this gives important information on when the patch will be included in present or future Internet Explorer service pack. This patch is included in Internet Explorer 5.01 service pack 2. But if this was a new vulnerability, this might be the only fix available. Notice that in the patch availability link
http://www.microsoft.com/windows/ie/download/critical/Q290108/default.asp there is an associated knowlegebase article Q290108. I will discuss this in the next section. (Ref. 2)

The Knowledgebase Articles is another resource in the TechNet Pages. One can either put in a search string in the Main Search Text Window that searches the TechNet Pages or one can use the Knowledgebase link to refine the search. Knowledgebase articles are the actual bug report for Microsoft products. They have the form Q######, where ###### is a number such as Q290108 as seen above. These knowledgebase articles give more details on the actual bug. In the TechNet search window (near the upper left hand of the window), type Q290108 to find the knowledgebase article. The search pulls up many articles but select the article titled "Incorrect MIME Header Can Cause Internet Explorer to Run E-mail Attachment (Q290108)". This article talks about vulnerability and its relation to the many different versions of Internet Explorer. And this knowledgebase articles mentions which library gets updated. This library information can be very useful when installing multiple patches. For this patch, the Shdocvw.dll is updated. (Ref. 3)

Click on the Downloads link to load the TechNet Downloads page. The Download page has numerous links to download various Windows applications. There are there major sections (links) "IT Downloads", "Microsoft Download Center", and "Service Packs". Click on the "IT Downloads" link and note that some of the downloaded applications are for Windows, Office and Server. Now click on the "Windows 2000 Downloads" and we get a page with various subcategories such as "Windows 2000 service packs", "Tools and Utilities for Windows 2000" or "Recommended Updates for Windows 2000". Now click on the "Tools and Utilities for Windows 2000" link to get to the next page. Now click on "Windows 2000 Resource Kit Tools" to get a list of available free tools. (Ref. 4,5)

Microsoft Web Resources: Microsoft Security content
The Microsoft Security Pages isn't a link from the main pages but is at http://microsoft.com/security/ and cross links security documents from all over microsoft.com web site.

Under this page are links for IT Professionals to the "TechNet Security Site", "Security Bulletins", "Tool & Checklists", etc. The TechNet Security Site and Security Bulletins were already discussed in the TechNet content section. The "Tool & Checklists" section has useful security checklists and one can now click on the "Tool & Checklists" link and

we will get a TechNet page that has a section on "Security Tools" and a section on "Security Checklists". One of the checklist that I would like to download is "IIS 5.0 Baseline Security Checklist", click on this link. This document covers some of the first steps in securing a default installation of IIS. (Ref. 6)

Microsoft Web Resources: Microsoft Developers Network content
Microsoft Developers Network (MSDN) is under the Information for Developers or http://msdn.microsoft.com/. This part of Microsoft web site is for Application Programmers and has very detailed programming information. Much of the material in this section of microsoft.com is for system and application programmers.

Now lets look for some Component Object Model (COM) information. COM is very important component architecture in the Microsoft Application Programming (and has been extended by DCOM and COM+). Object Link and Embedding (OLE), ActiveX (Internet-enabled components), and DirectX are APIs based on COM. From the MSDN home page, click on "MSDN Library" link in the left frame. This brings us to the MSDN library, a treasure trove of information on the Microsoft Windows Programming environment. The left frame represents the "Table of Contents" of the site and the + can be clicked on to expand the contents. In the left frame, click on the + for "Component Development" to expand the tree hierarchy, then click on the + for "Component Object Model (General)", then click on the + for "SDK Documentation", then click on the + for "COM Fundamentals", then click on the + for "Guide" and then click on "The Component Object Model" (not the +), and this article can be viewed in the right frame. This is a good starting point for someone that wants to understand the COM model. (Ref. 7,8)

Section 2: Microsoft Internet Information Server version 4.0 patching
Now that we have seen some of the information and resources available at microsoft.com, this part will show how to use the resources and patch Microsoft Internet Information Server 4.0. But I want to emphasize understanding some of the Internet Information Server version 4.0, which is a component of Windows NT 4.0 Option Pack. In the default installation of Option Pack, other components such as Microsoft Transaction Server, Ftp server, sendmail server, Index Server, IIS samples and FrontPage 98 Server Extensions are also installed. Nntp is not installed by default. I am only going to cover the details of patching Microsoft IIS and will only cover these components lightly.

Lets go to the Microsoft Security Bulletins Search page that was explained earlier, you could either click on the links detailed in the earlier section or click directly on the following link:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/current.asp
Now look through the list of patches and notice that "MS01-044: 15 August 2001 Cumulative Patch for IIS" looks promising, so click on the link. Microsoft has improved the IIS patches and its content significantly this year. One big improvement started with patch MS01-026 is an IIS cumulative patch. Prior to this patch, many patches were needed. The details in the patches have increased. The technical details section explains the vulnerabilities patched and the corresponding CVE/CAN bulletin. The frequently

asked questions are the answer to some of the more prevalent questions. Some of the questions associated with MS01-044 are "What machines should this patch be applied to? ", "What are the new security vulnerabilities addressed by the patch?" and "What's the scope of the first vulnerability? ". There is a patch download section. There is additional information about this patch section. MS01-044 Additional Information details the Installation Platform, states that these patches will be included with Windows 2000 Service Pack 3, and a caveats section. (Ref. 9)

So can we just apply the patch and be done with it. NO!!! One must read the patch, and understand the components in the Windows NT 4.0 Option Pack. I want to point out some important points that are described in the patch notes. The first point directly from the "Additional Information about this patch" Caveats section as follows: "The fixes for four vulnerabilities affecting IIS 4.0 servers are not included in the patch, because they require administrative action rather than a software change. Administrators should ensure that in addition to applying this patch, they also have taken the administrative action discussed in the following bulletins..." Now notice that if we blindly installed the patch and left, we still might have some gaping security holes! Now reinforcing a second point, further reading of the Caveats section: "The patch does not include fixes for vulnerabilities involving non-IIS products like Front Page Server Extensions and Index Server, even though these products are closely associated with IIS and typically installed on IIS servers..." A second set of security holes would have been left open if we just blindly applied a patch and left. (Ref. 9)

So in addition to applying the patch, we fix the administrative actions as specified in the caveats section by upgrading or removing Microsoft Data Access Components according to MS99-025, removing the IISSamples directory as in MS99-013. And either uninstall or add the patches to the following components: FrontPage 98 Server Extensions, and Index Server. Disable the ftp service, and sendmail service if not needed.

FrontPage 98 Server Extensions can be upgraded at the following Microsoft site.
Microsoft FrontPage Server Extensions 2002 for Windows
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnservext/html/fpse02win.asp

Microsoft Security Bulletin MS01-025 patches Index Server
Index Server Search Function Contains Unchecked Buffer
Note: MS01-033 an Index Server Patch is included in MS01-044 due to the severity of the vulnerability with respect to IIS.

Nimda can attack web servers so are we safe from Nimda. Lets look up some Nimda vulnerability information. In the TechNet search, enter Nimda into the text box. The following item looks a like a good search candidate, "Information on the Nimda Worm" at http://www.microsoft.com/TechNet/security/topics/Nimda.asp.
It says that MS01-044 protects from the Nimda on servers so we are safe from Nimda on the IIS web server. (Ref. 10)

Section 3: Verification
One way to test if there are any IIS vulnerabilities are on the network is to use a scanning tool. Internet Security Systems Internet Scanner, and Network Associates PGP CyberCop Scanner are network vulnerability scanning tools. Nessus is an open source vulnerability scanning tool. Further information is at the vendors' web site. Vulnerability scanning can be a complete security report by itself. Internet Scanner has a lot of online information on its security checks. Nessus has the security check as open source so one can actually look at what the check is doing.

http://www.nessus.org
http://www.iss.net
http://www.nai.com

Summary:
I tried to give an overall feel to the Microsoft web site as a resource for security professionals and to try to correlate a wide variety of information that is necessary for the Windows security professional. I picked a few of the more useful microsoft.com pages. But I tried to have an overall agenda. First I started with a Microsoft Bulletin on Internet Explorer but correlated the information with the Nimda worm. Later I went into the details of patching IIS and also related this to the Nimda worm and the importance of reading security bulletins. I wanted to show the depth of knowledge at Microsoft.com by finding in-depth programming articles on COM, and show the various downloads for security tools or checklists such as "5.0 Baseline Security Checklist". In fact, I found a few new things just by writing this article. I want to spend more time at the MSDN COM SDK section.

References:
1. Windows 2000 Service Pack 2 Market Bulletin
http://microsoft.com/windows2000/server/evaluation/news/bulletins/sp2.asp

2. Microsoft Security Bulletin (MS01-020)
http://www.microsoft.com/technet/treeview/default.asp?
url=/technet/security/bulletin/MS01-020.asp

3. Microsoft Knowldege Base Article Q290108
Incorrect MIME Header Can Cause Internet Explorer to Run E-mail Attachment
http://support.microsoft.com/support/kb/articles/Q290/1/08.ASP

4. Technet Security Tools and Checklists
http://www.microsoft.com/technet/treeview/default.asp?
url=/technet/security/tools/tools.asp

5. Technet Download Section
http://microsoft.com/technet/treeview/default.asp?url=/technet/downloads/Default.asp

6. IIS 5.0 Baseline Security Checklist

http://www.microsoft.com/technet/treeview/default.asp?
url=/technet/security/tools/iis5cl.asp

7. MSDN Library
http://msdn.microsoft.com/library/

8. Microsoft Platform SDK, Component Object Model
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/com/comportal_
3qn9.asp?frame=true&hidetoc=true

9. Microsoft Security Bulletin MS01-044 Cumulative Patch for IIS
http://www.microsoft.com/technet/treeview/default.asp?
url=/technet/security/bulletin/MS01-044.asp

10. Information on the "Nimda" Worm
http://www.microsoft.com/technet/treeview/default.asp?
url=/TechNet/security/topics/Nimda.asp

Last Updated: June 25th, 2017

Upcoming Training

SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS San Diego SEC401	San Diego, CA	Aug 21, 2017 - Aug 26, 2017	Community SANS
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor