Global Information Assurance Certification Paper

Stop being a victim of IIS

James Mignacca
Version 1.4b Option 1

One of the most important aspects of all computer services is that of security. In the past, Internet Information Services (IIS) has been one of the most unsecured web servers on the Internet ("fly by day consulting, inc."). Although IIS has been exposed to intruders and hackers in the past, Microsoft has been doing a good job of creating hot fixes as soon as vulnerabilities are found. Hot fixes are patches written by developers at Microsoft in order to secure problems that have been found after the operating systems have been released (Rosato). Although improvements have been made through Microsoft, one must consider how vulnerabilities are identified. Despite the flaws in the system, Microsoft is the most well known platform due to its high popularity among companies. There are many ways that one can attempt to ward off hackers, or at least slow down his or her attempt to gain access to valuable information on a system. First of all, an understanding of how a hacker takes advantage of system vulnerabilities will be explored. As an administrator, it is important to promptly discover where vulnerabilities lie in the computer network so that actions can be taken quickly in order to avoid being taken advantage of. This is the importance of hot fix checkers, logging, and auditing. There are, however, structural changes that can be made to the specific computer system that can help in securing the IIS. Generally, these steps are simple and easy to implement. The basis of the steps in securing IIS is to strip the system, so as to reduce the number of possible entry points in which the hacker could access the system. The specific applications necessary to execute these security measures are outlined below, point by point so that anyone could put them into place. As well, there are other ways that one can try to slow down the hacker if he or she is able to gain access to the system. These roadblocks are intended as a secondary defense to slow down the hacker and are by no means recommended as exclusive measures to secure IIS. Keeping your servers updated with the latest patches is the best way to prevent this vulnerability ("UCB Windows 2000 Resource Center").

Hacking IIS

There are many different ways in which hackers can gain access to an IIS platform. Some of the most common ways include buffer overflow, source code revelation attacks, and file system traversal exploits. Buffer overflow is usually an unchecked buffer input data. Consequently, this allows the hacker the opportunity to launch malicious code or commands to be run on the remote computer. A hacker may also gain access to an IIS platform by performing source code revelation attacks. Code revelation attacks have the potential to occur when the attacker can view the source code of the web page or scripts embedded on the server. This kind of exploitation can occur through a bug in IIS or due to bad programming. One problem is that when intruders gain access to a copy of the code, they may be able to obtain passwords and other critical information in the Active Server Page (ASP). For example, if a web developer puts the administrator password in the code to launch a script, then the hacker could find the password and gain access to the network. If an attacker can get his or her hands on the code, then he or she will have access to the administrator password, which ultimately gives the hacker access to the machine. At this point the intruder is that much closer to taking over the web server (Scambray and McClure, Pg 240 -243). In order to avoid this problem with ASP, server side tags should be used in the code. Another way to protect against source code revelation attacks is to remove all Internet Server Application Programming Interfaces (ISAPI) (Scambray and McClure, p.216). This is done by accessing the administrator tools folder and clicking on Internet Information Services, then right clicking the virtual web that is being used and then going to properties. Click → WWW services → Edit → Click the Home Directory tab → Configuration. Finally, click the extension and click the remove button at the bottom of the screen, “remove unused script mappings” (“IIS 5.0 Baseline Security Checklist”). File system traversal is the ability for hackers to move around within a web page, thus possibly allowing him or her access to the box. There are many different types of file system traversal, the most common being Unicode. The problem with Unicode is that it seems to decode the code in the wrong instance in IIS. This allows a hacker to use “dot-dot-slash” in the URL of the web page, which could allow the hacker to gain access to the system files. (Scambray and McClure, p. 208-217). In order to prevent this, one should make sure that the patches on the IIS server are up to date (“UCB Windows 2000 Resource Center”). Further steps, which are listed below, will help to be proactive in this vulnerability.

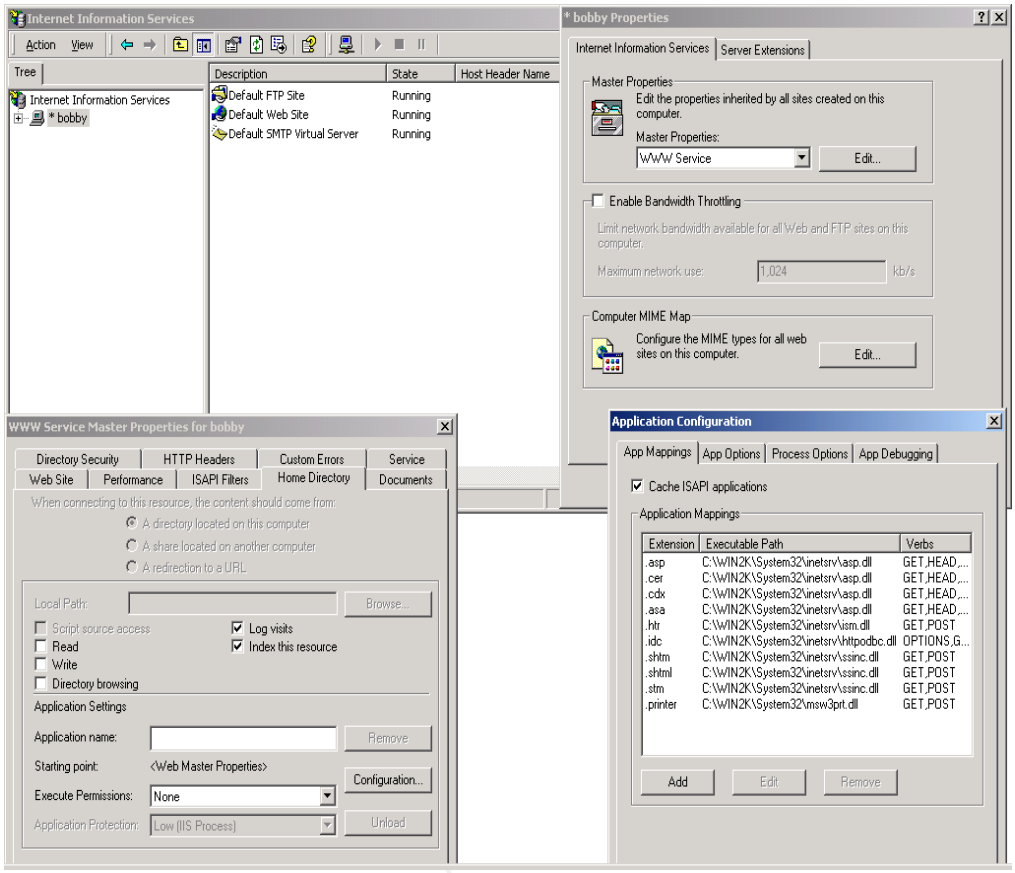

Figure 1: Properties of IIS (Scambray and McClure, p.215-216)

Exploits of IIS

An exploit is a well-known vulnerability that allows a hacker to gain access to the system. Some of the most well known exploits will be discussed in the section.

Superfluous Decoding exploit

This exploit was founded by Christine Gordon (CA-2001-12). It allows hackers to execute commands "CMD.EXE" on the web server. This occurs when IIS decodes data twice and IIS utilizes the results of the second decoding, which then opens the box up for the hacker to execute commands on the box. The solution for this exploit is patching. The following link is the patch that will fix this exploit for Microsoft IIS: ("Cert Coordination Center"- CERT® Advisory CA-2001-12).

Unicode Exploit

The problem which Unicode exploits is that Microsoft installs the Unicode extensions by default, so you might not be using them but still be a threat to this vulnerability. Unicode exploit will assign a unique number for each character of data inputted, but IIS will not allow English language character to be recognized

by the web server. Therefore, the hacker simply has to input a deformed URL on the web server. For example, http://hackedwebserver/..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\ is an arbitrary command. It should launch the command line utility therefore allowing one to gain access to the server. (Scambray and McClure, p. 222-227)

Viruses targeted at IIS

Code Red

Code Red is one of the most famous and perhaps most dangerous worm ever released on the Internet. Code Red was released on the Internet on July 19, 2000 and was estimated to infect over 250 thousand servers, but could have potentially infected up to six million servers had they not been patched. The estimated bill for cleanup was approximately 2.4 billion dollars. The Code worked by attacking servers through port eighty. The worm was designed to randomly try to connect to servers in an IP range. Once Code Red had detected a possible host to infect, it would apply an HTTP GET request to do a buffer overflow. More information can be found in the CERT advisory CA-2001-13. ("CVE"). The reason why Code Red spread so rapidly was due to its ability to self-propagate from host to host. It is believed that Code Red was developed and released in China and one interesting effect of Code Red seemed to only deface WebPages that had the English version of Microsoft IIS and the non English versions of IIS would stay in stealth mode. It would say something like, HELLO! Welcome to http://www.worm.com! Hacked by Chinese! This would only be kept in memory and not written to hard disk, so a simple reboot would clean this off. The deform of a web page would reset after 10 days unless it was infected again.

Some signs of Code Red infection could be a lack of performance, an increase in network activity and if the following appears in the logs: /default.ida?nnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnn%u9090 Code Red chooses its victims IP addresses by sequentially picking a range of IP addresses, but would always begin at the IP address where it started from. Therefore the worm could potentially attack a server more than once ("eEye digital Security", "Cert Coordination Center"- CERT® Advisory CA-2001-19, "News Factor Networks").

Code Blue

There have been many copycats of Code Red, and Code Blue is believed to be one of them. This is not a great threat to the Internet since most servers should have been patched from the Code Red exploit. ISP (internet service providers) are now doing scans to detect servers that are not patched for these vulnerabilities and would even cancel their Internet connection if the system administrator does not keep the server patched on a regular basis. There are,

however, some differences between Code Red and Code Blue. One would be that Code Blue works as a dll and runs from an exe file and not a memory resident worm like Code Red ("Der Keiler"). This makes detecting Code Blue much easier. One interesting part about Code Blue is that it intentionally deletes the IMAPI extension to prevent other hackers from using this vulnerability against that server. The effects of Code Blue are much like Code Red - lack of performance and instability of the server, which is due to ping floods. A ping flood is a large number of ICMP requests from a host or multiple hosts.

Steps to securing IIS

Minimal Operations

When attempting to secure IIS one should be sure to run only the minimal amount of operations and disable all services that are not necessary for running the web server. With this in mind one should first uninstall any programs that are not needed (Scambray and McClure, p.205-267). This can be done by using Microsoft's add and remove software in the control panel. The only operations that should remain are the bare bones, which are necessary to make the web server operate. One should also uninstall any protocols that are not needed in the network neighborhood. Finally, all ISAPI extensions should be removed, being careful to reinstall only the ones needed (Scambray and McClure, p. 205-267). Removing all unnecessary extensions will help prevent buffer overflow and source code revelation, as well as many other sources of vulnerability. Next, one should rename or remove any command line utilities on the web server. (Scambray and McClure, p. 205-267). The purpose of this process is to guard against any command line attacks against the server so that if a hacker does gain access there is one less opportunity for the hacker to compromise the server. At this point the intruder is unable to launch command line attacks against the server. Lastly, since you don't need NetBIOS over TCP, this should also be disabled (Scambray and McClure, p. 205-267). This process will fight against hackers who are trying to use adapter status commands, which may reveal users who are currently logged onto the server.

Access Control List

The next step in securing the IIS is to create an access control list (ACL). ACLs are data structures that are associated with users and determine the permission and privileges of that user. By default, ACLs are set to full access for everyone. By creating ACLs for all executables on the web server the hacker cannot gain access by using other accounts, such as guest. In order to set up ACLs in Windows the following commands should be performed (which may be carried out from any command line utility). Once in the command line the following syntax would be entered: *Cacls %system%*.exe /T /G system:F*

administrator:F. "Cacls" being the utility used by Microsoft. This command now sets all access for executables and administrator groups in the system root to full. This action will override any other permissions that were previously set on the system; at this time hackers will have a greater difficulty accessing the system. In creating ACL one is limiting the number of accounts that have full access to the system; the less accounts that are active, the less chance the hacker will have to invade the system ("IIS 5.0 Baseline Security Checklist").

Delete and Rename

Another step, more specifically related to securing the operating system, is used to limit the damage done by a hacker who has gained access to the server. The step is to delete any default virtual directories that are not currently being used. After this process it is also recommended that some files be renamed, more specifically, notepad.exe, explorer.exe and CMD.exe. All of the files that should be renamed are found in c:\winnt\system32. Notepad, for example, should be renamed in order to deter any hackers that are trying to use any utilities on the remote server. Other recommendations of utilities that should be deleted are any sample IIS templates. For example, IIS sample (c:\inetpub\iissamples), IIS documentation (c:\winnt\help\iishelp) and Data Access (c:\program files\common\files\system\msadc). The process of deleting and renaming files is an additive feature to help improve security against hackers (Scambray and McClure, p.205-267).

Password Complexity

Password complexity is an important component in securing the system. A password should be one that cannot be randomly guessed by an attacker or other intruders. It is also important to ensure that it is difficult enough so that it could not be detected by a dictionary attack. A dictionary attack is a software program that will randomly attempt to discover a password by using multiple combinations of characters in order to crack the password. A password should comply with the following rules:

- The users name, in full or any part, should not be integrated into the password
- The password should contain symbols as well as letter characters
- The password should be a length of at least six characters
- The password should be changed on a regular basis

These rules can all be enforced by a password policy to ensure that all members of the domain follow the same criteria in order to guarantee compliance (Scambray and McClure, p.205-267).

Steps to throw off the Hacker

The next step in securing IIS is done in attempt to slow down the efforts of the hacker by removing all expected default configurations. The intruder will expect a vanilla platform: one that conforms to the standardized settings of the Microsoft platform. By renaming the ".inc" file to ".asp", one could successfully throw off the hacker; the best way to accomplish this task is to use the search tool. (Scambray and McClure, p.205-267).

Another idea that would increase security is to download Microsoft's template. This is a security template that will disable delete and set ACLS for whatever Microsoft recommends. Another task that is recommended by Microsoft to secure IIS is to disable parent paths. Parent paths are used by web developers to navigate to pages that are further embedded in the directory structure. By disabling the parent paths, one is preventing the hacker from using a parent path notation (i.e."../") to move around the web site. To disable the parent paths, one would follow the subsequent commands: Start→ Settings → Control Panel → Administrator Tools and double click Internet Service Manager. Next, one would right click the virtual web to be changed and then click Properties. Finally, continue to Home Directory → Configuration → App Options and then unclick enable parent paths. An additional point of interest to keep in mind is that some changes to the web page code will have to be made so that, with respect to navigation, all pages point back to the root page.

For further instruction, the following screen shot displays some primary roles necessary to accomplish disabling of the parent paths. This display only identifies some of the steps involved in the procedure.

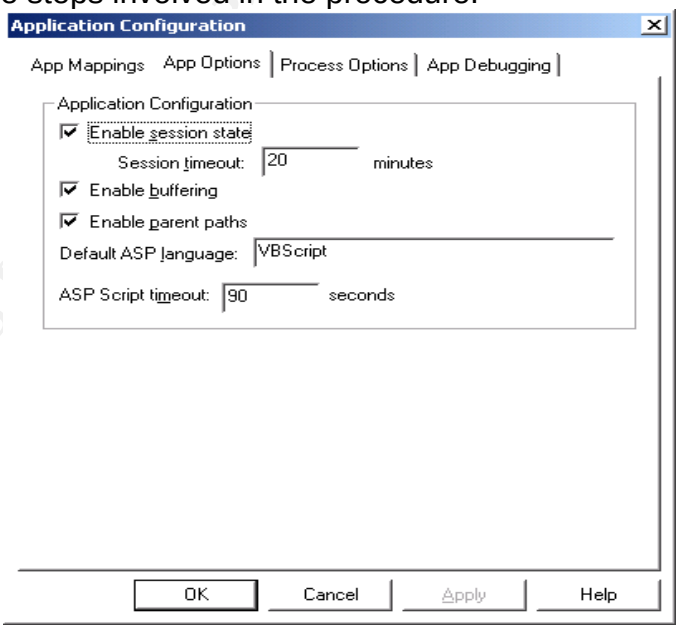

Figure 2: Disabling Parent Paths

Security Tools

Security tools are used in conjunction with IIS to access the vulnerabilities and to make the administrator more aware of them. This operation is used before and after securing IIS and as a routine operation to ensure continued safety. The route to using IIS security tools begins by setting up Install Exception Monitor to help pinpoint any IIS problems. A useful option that this tool can provide is to start the server/IIS service if an error on the server is discovered. This is helpful because one can look up the vulnerability and possibly update the specific patches, if that is the case. Another useful feature of the Install Exception Monitor program is that one can setup the software to email the administrator when an error is found. An illustration of this program is provided below.

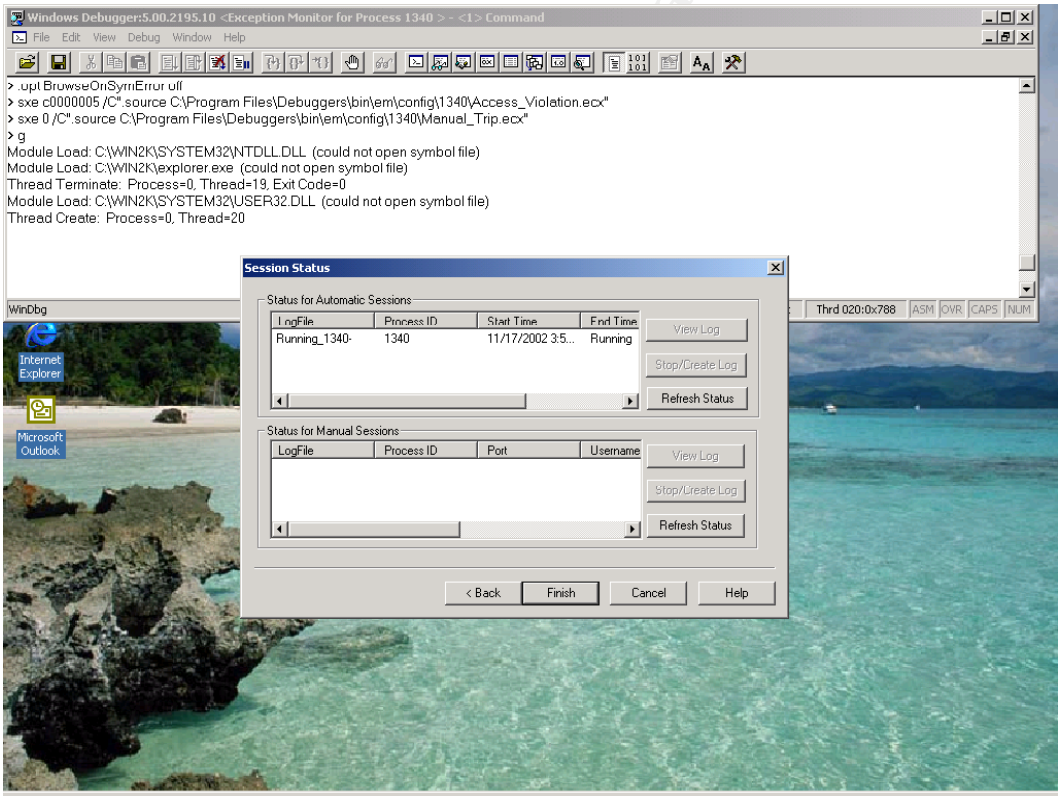

Figure 3: Install Exception Monitor program

Another security tool offered specifically by Microsoft is a utility called Microsoft hot fix checker ("Hotfix Checker"). This tool will take a snap shot of current patches running on the server and reference it against Microsoft's database. Another tool, such as Blat, can then be used to email out the results on an on going basis. Blat is an email utility, which can send the report of the

server's security status to the systems administrators ("Blat for Windows"). An example of a command line you can script with is: blat patchesreults.txt –t recipient@domain.com -s "Patch Status" –server xx.xx.xx.xx –f recipient sent from. Patchresults.txt is the file that sends the email out to the administrator regarding the results. The wildcard –t, represents the recipient of the email, which in this case is recipient@domain.com. The notation -s controls the subject line and is the heading or what is referred to as "Patch Status". The next wildcard used in this example is server, which is needed to direct the email to Simple Mail Transfer Protocol (SMTP), which then transfers the information to the recipient. The last notation in the example of a command line that can be put into a script is to specify the location where the email is derived from. The previous example is used to have patch results emailed to a specified recipient as to the vulnerabilities of the system.

An additional security tool that checks systems for specific vulnerabilities is the Stealth Scan. This tool tests the web server for known vulnerabilities. Stealth has an existing database of over 19,000 vulnerabilities to audit against. The tool is very simple to use, as the only input needed is an IP address. With this information the utility will scan the host. After the stealth scan is complete it will provide a concise and easily interpreted report of its findings. This is an essential tool for all system administrators in order to cut down on the unidentified vulnerabilities ("N-Stealth").

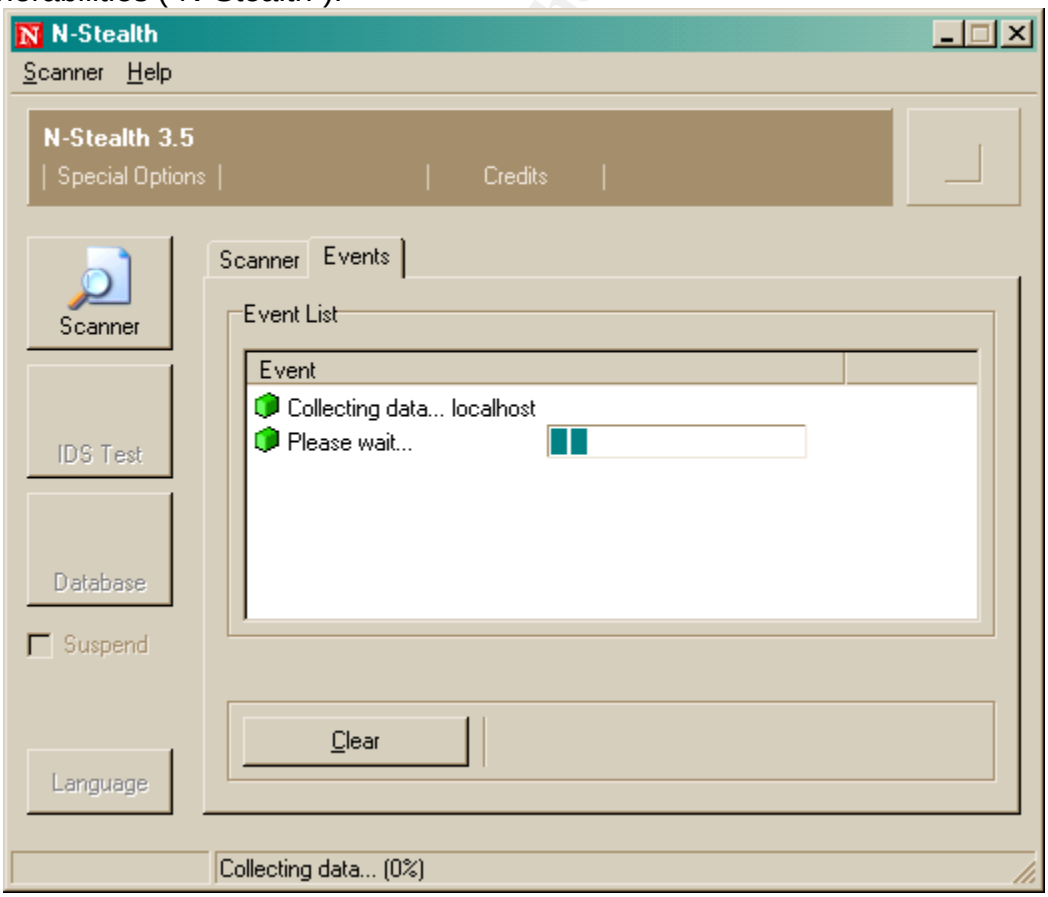

Figure 4: N-Stealth

Whisker is a scanning tool used to look for web server vulnerabilities that can be used to run against multiple servers at any given time. It is a command line utility that is fairly robust and can be configured to run different scans. Whisker is a Perl-based tool and needs Perl setup on a computer before it will work. This tool is complex but valuable because it is fairly flexible due to its ability to use custom scripts.

Another useful tool is a port scanner. There are many types of port scanners available in the industry, such as Nmap and Super scan. Nmap is a very powerful tool that can do many things other than port scanning. Nmap can also perform stealth, finger, and SynAck scans. Nmap was originally a command line utility that ran in a Unix platform. There is now a Windows version that has GUI interfaces for easy use, but also allows for command line interface for the advanced user. Nmap is a well-known tool that thousands of people download every day and is also the winner of the "Information Security Product of the year" by Code talker Digest and Info World ("Nmap").

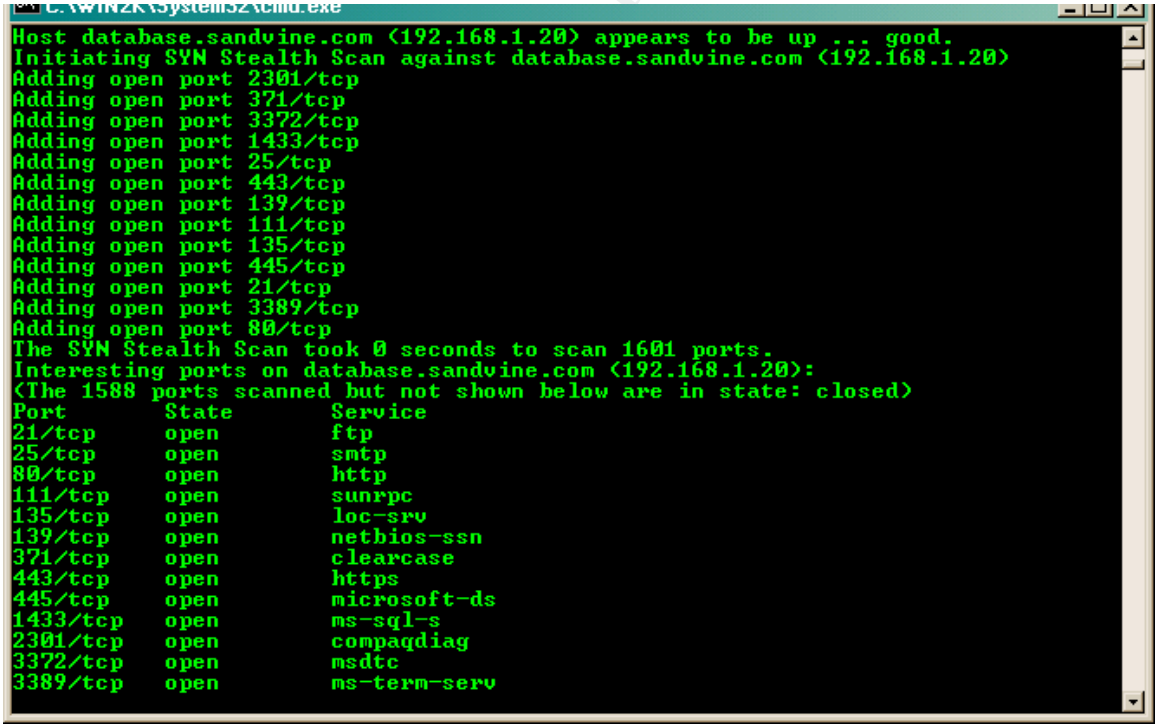

Figure 5: CMD.EXE

Super Scan is a simple tool that only performs port scans, but does its job efficiently. It lists all of the hosts within an IP range and lists all of the open ports on each host. Super Scan is supposed to be faster than other software due to the fact that it is multi-threaded ("Super Scan 3.0"). It must be noted that this tool will not work if the host has Internet Control Message Protocol (ICMP) disabled.

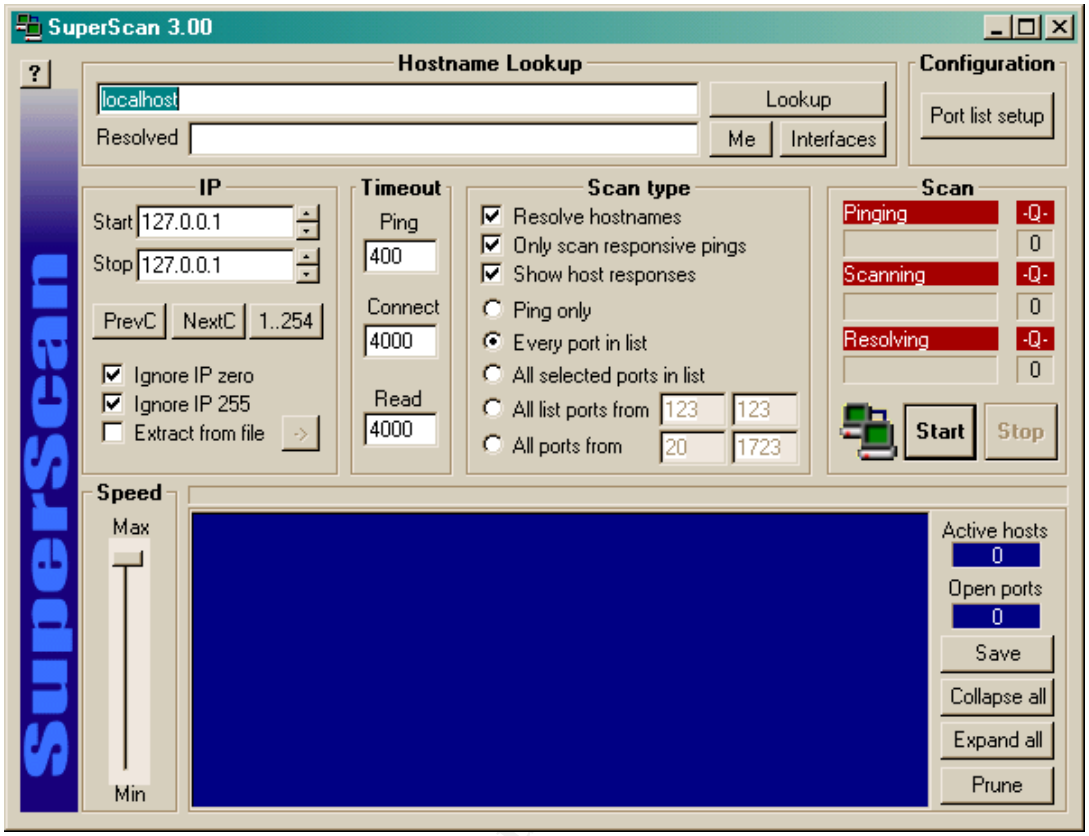

Figure 6:SuperScan 3.00

Archilles is an HTTP/SSL proxy tool that works as a local host against a remote host. This is a tool that runs as a client on a local computer and intercepts the remote computer's data path. In order for this to work one must set up the client computer to use a proxy connection. To perform this, the following steps should be taken: In the web browser, click on Tools → Internet Options → click on the connections tab and Lan settings option. Next check the box that says, "Use a proxy server". Now Archilles has to be set up for intercept mode. Once the start button is clicked Archillies will start to collect the data from the web server. The data will not be sent forward until the user clicks the send button. This gives a hacker the opportunity to modify the packets sent to the client and possibly do a "man in the middle" attack, or even give up valuable information that can be used later on (Scambray and McClure p.205-267).

Cygwin is a tool that acts as an emulator and allows users to use Unix command lines on a windows box. This tool will allow programmers to write Win32 console that makes use of Windows API extensions. Cygwin is a powerful tool and allows hackers to create bash scripts on the fly. You will notice in the snap shot below that UNIX commands are working and this was done on a Windows 2000 machine ("Cygwin").

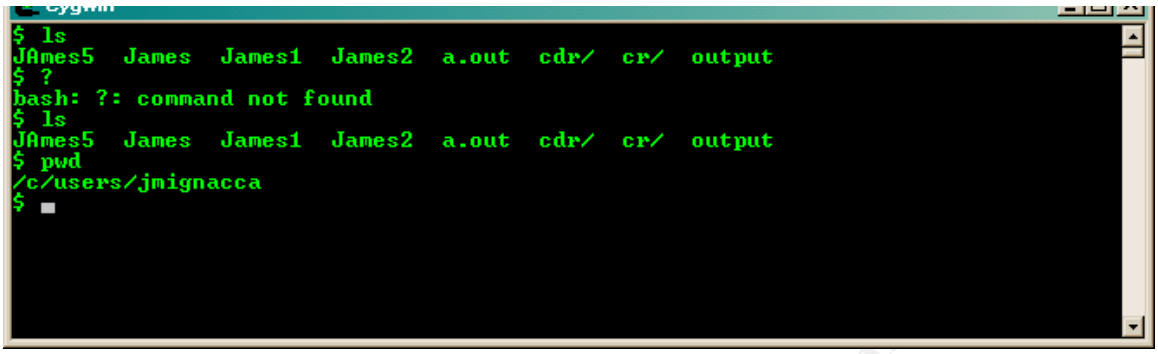

Figure 7: Cygwin

IIS Tracer is a good tool used to help monitor what IIS is doing and what people are doing to it. This tool is effective because it runs on the fly, therefore one could react to an attack as it is happening. IIS Tracer will also do logging; it can log headers and all incoming and outgoing information. This tool is very adaptable as it supports, .asp, .cfm, .cgi, .dll, and .exe files. The following snapshot is what you would see ("IIS Tracer ISAPI monitoring tool").

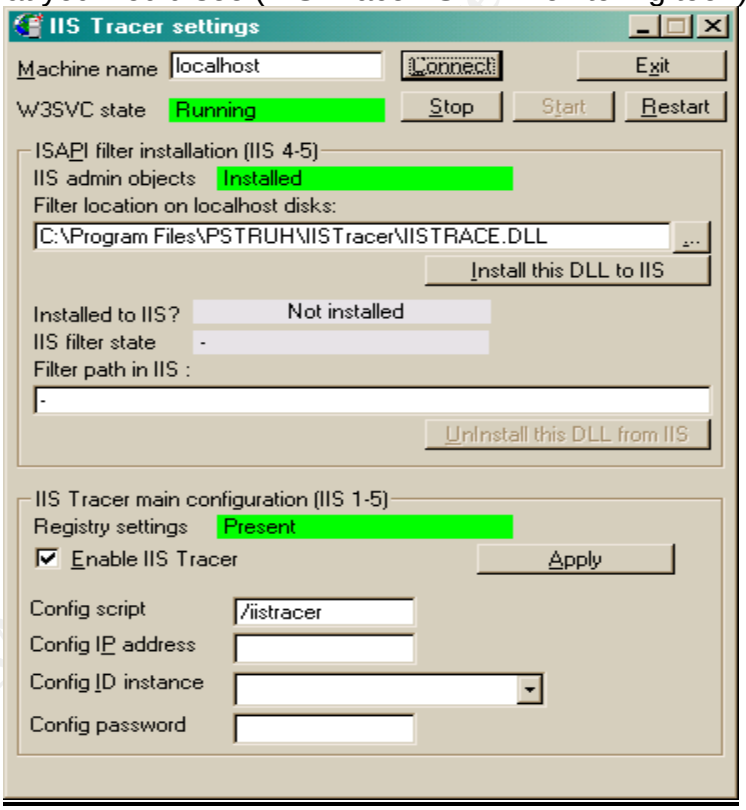

Figure 8: IIS Tracer

IIS Lockdown

Microsoft has provided a tool to automatically lock down IIS. These tools will walk you through and ask specific questions about your web server. One should be sure to test the web server after. These tools could tack some functionality that is needed on that specific web server. URL Scan is a tool that is installed as a part of IIS Lockdown. URL scan acts as a filter for ISAPI extensions and when properly configured can be a great means of defense against hackers ("IIS 5.0 Baseline Security Checklist").

File system

File system is the platform from which applications such as IIS are built on. Its importance in securing IIS is that it locks down the security of the operating system and its files. This would be necessary to implement if the hacker gets too close to the server because it could stop the hacker from making any additional progress. In order to lock down the security, one must be sure to use New Technology File System (NTFS) as opposed to Fat Allocation Table (FAT). New Technology File System was first designed in the late 1980's at which time it was released with Windows NT. The most important difference between NTFS and FAT is that NTFS supports Access control lists (ACLs). Another downfall of FAT is that it does not provide built-in security. NTFS does this and also fights against file corruption and provides data reliability. Some other benefits of NTFS are that it allocates more disk space than FAT, it is more reliable, and it can be migrated with other file systems. If one already has existing platforms containing FAT, then it can be upgraded using Convert.exe. This can be performed by typing convert.exe into the command line or by clicking the start menu and then run ("WinBook Tech Article"). By doing this no data will be lost. It is suggested that different volumes are set up so that the operating system can go onto one volume and the webroot onto another. This guards against file system traversal exploits. A hacker will not be able to jump volumes, therefore the hacker would not be able to get to the operating system where he or she could do more damage (Scambray and McClure, p.220-237).

Denial of Service

A Denial of Service (DOS) attack occurs when the TCP protocol is flooded or altered beyond the limitations of the protocol, therefore either stopping the use of that resource or reducing its performance or denies anyone access to that machine ("Internet Security Systems" - DoS). For example, ping of death, which is when so many packets are targeted at the victim's machine that it saturates the TCP protocol.

A Syn flood is a form of Denial of Service that occurs when a hacker sends more TCP connections then the host machine can handle and once the table of connections fills up, no more connections will be allowed to access the host machine ("Internet Security Systems" – Syn flood). This consequently denies all other occupants' access to the server. In order to prevent Syn floods, a registry on the server with IIS can be changed. To do so, one must first run regedt32 under the start command and then enter the run menu. Next, type in the command HKEY_LOCAL_MACHINE, which will bring up a Windows utility that will allow for one to edit the registry. In order to do this, look under the directory labeled System\CurrentControlsSet\Services\Tcpip\Parameters. On the menu bar click Edit → Add Value; it then gives a choice to add Value Name: SynAttackProtect and Data Type: Reg_DWORD. After selecting OK it will then ask for a data value. Enter the numeral 2 and decimal for the Radix. Finally, click OK and close the registry editor ("UCB Windows 2000 Resource Center"). This process will successfully change the registry on the server to avoid syn floods due to invaders. There are many other ways to perform DOS attacks. One way is to simply use up all of the CPU resources, which could possibly cause a crash. A less common DOS attack is to simply use up hard drive space to the point that the computer cannot operate any longer, thus causing the server to crash; this is common with FTP servers. Another way is to send mass quantities of mail to a server so that it is unable to handle the data. DOS attacks can be used for other resources such as, printers, routers, switches and even tape-drives.

Security Topology

A further way to increase security is to put the public web on the private Network Interface Card (NIC) on the firewall and disable any inbound traffic from the web server, making sure that the database is local on the web server. This way if the web server does become compromised, then the hacker will not be able to get onto the corporate network. Next, create a script program that would push updates to the web server using secure shell (SSH) to connect to the

server. The web server will now be isolated on the private network and will not be linked into the corporate network. Again, this is done to increase security and decrease the chances of being invaded by hackers. Refer to figure 4 for further explanation.

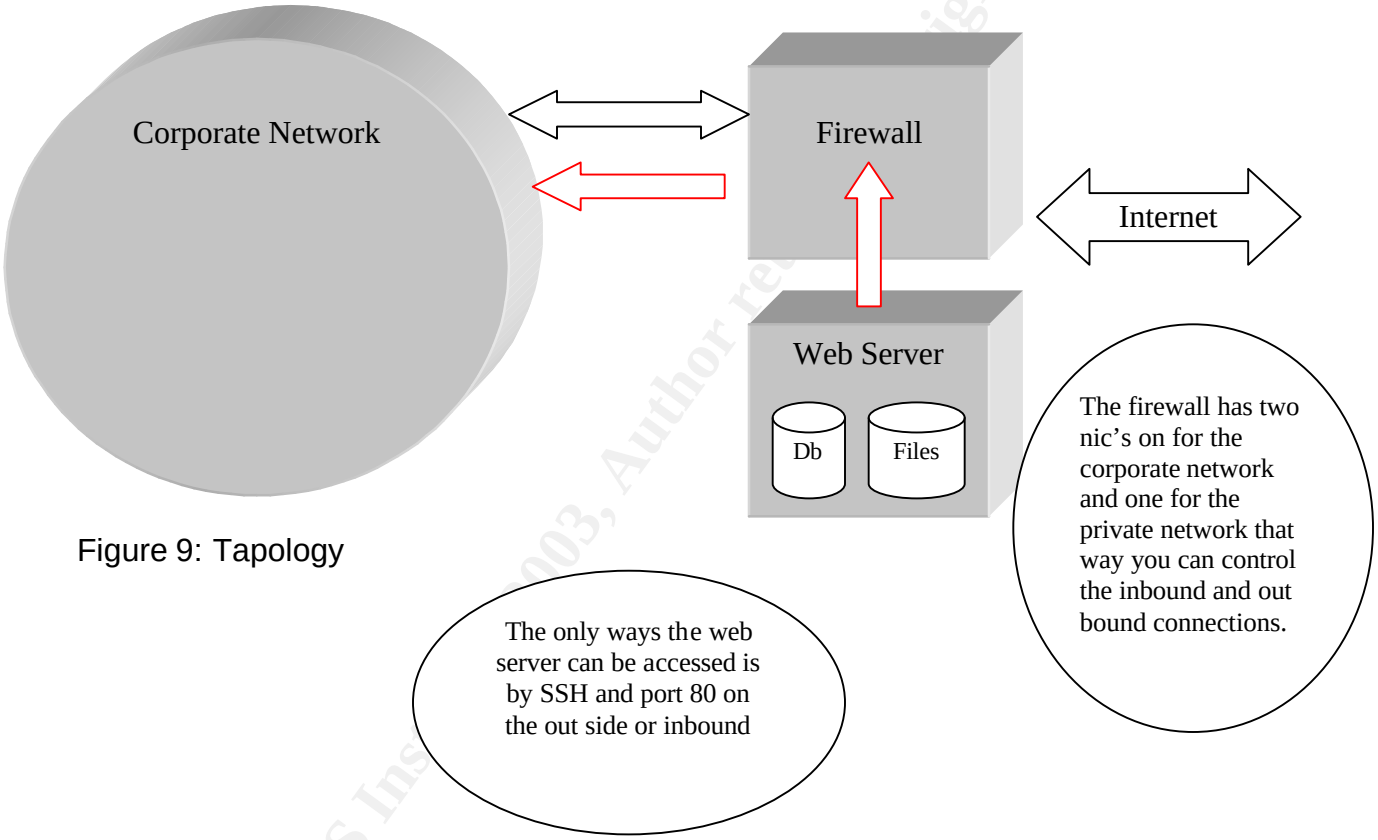

Figure 9: Tapology

Logging and Auditing

Logging is one of the most essential parts of security on a web server. It will help one find out if the system has been hacked and what damage to look for. It could also help to stop an attack. One thing to remember about logging is that it is only as good as the administrator who is using it, which means that the log has to be checked regularly. To turn logging on in IIS, do the following: Start → Settings → Control Panel, go into the Administrator Tools folder and click

Internet Information Services. Right click the Web Site tab and click Enable Logging check box. Now select W3C Extended Log File Format. Click the Extended Properties tab and select an item to log. It is a good idea to at least log Client IP, User Name: auditing, so as to have a better knowledge of what is happening on the server. Using the event log could be very useful information when trying to investigate a possible intrusion on a web server. Keep in mind that the logs will not give a clear answer as to what happened, but using them all together and piecing all the information together will help to get one step closer to finding out the damage the intruder has done on the web server ("UCB Windows 2000 Resource Center").

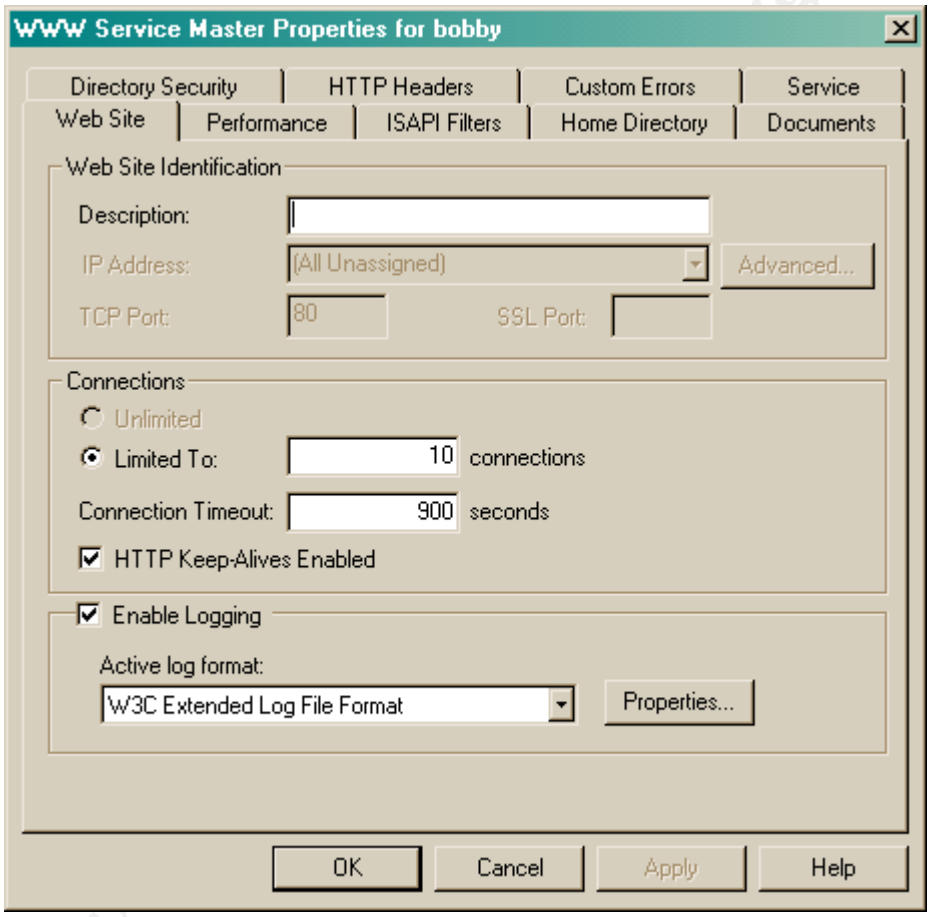

Figure 10: WWW Service Properties

Overall, there are many techniques that can be used to ensure better security in order to protect against hackers. The steps to securing IIS and the tools that can deter the hacker are only precautionary methods. As a security expert, his or her job is to think like a hacker. The expert must attempt to stay one step ahead of the game, always thinking of what a hacker would do when trying to invade a website. Although it may be unrealistic to implement all steps and programs recommended, the most important precaution that can and should be taken to prevent against hackers is to stay up to date with the patches. This is the best measure against being hacked because the vulnerabilities are

immediately detected and can be dealt with as they occur. A good example is the famous Kevin Mitnick who was a hacker in late 80's and early 90's. Kevin was released from jail and started up a security company. Kevin's web site was hacked twice to known vulnerabilities and this was caused by not patching an IIS web server ("BBC News"). Due to the overwhelming use of the Internet for leisure and business, security issues are going to continue to grow. As technology changes so will the vulnerabilities of the systems and the hackers who are trying to overtake them. One can only hope to detect the vulnerabilities one way or another before the hacker has completely overtaken the system.

References

Arif, Moe and Thomas P. Braun. "Securing Microsoft IIS". 25 July 2001. URL: http://www.cit.cornell.edu/computer/security/iis/#insecure (6 Feb 2003).

"BBC News". Prominent hacker Mitnick hacked. 11 Feb 2003. URL: http://news.bbc.co.uk/2/hi/technology/2750433.stm (4 March 2003).

"Blat for Windows". 12 Dec 2001. URL: http://www.interlog.com/~tcharron/blat.html (8 Feb 2003).

"Cert Coordination Center". CERT® Advisory CA-2001-12 Superfluous Decoding Vulnerability in IIS. 15 May 2001. URL: http://www.cert.org/advisories/CA-2001-12.html (10 Feb 2003).

"Cert Coordination Center". CERT® Advisory CA-2001-19 "Code Red" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL. URL: http://www.cert.org/advisories/CA-2001-19.html (10 Feb 2003).

"CVE". Common Vulnerabilities and Exposures. URL: (http://www.cve.mitre.org/cve/downloads/full-cve.html) (10 Feb 2003).

"Cygwin". URL: http://www.cygwin.com/ (10 Feb 2003).

Daily, Sean. "Curing ASP-Run Executable Problems in IIS 5.0". 22184. Oct 2001. URL: http://www.win2000mag.net/Articles/Index.cfm (6 Nov 2002).

"Der Keiler". ISS Alert: Code Blue Worm. URL: http://www.der-keiler.de/Mailing-Lists/ISS/2001-09/0007.html (10 Feb 2003).

"eEye digital Security". Welcome to Security. URL: http://www.eeye.com/html/Research/Advisories/AL20010717.html (10 Feb 2003).

"Explanation of Regsvr32 Usage and Error messages". Microsoft Product Support Services. 249873. 11 Oct 2002. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;249873? (28 Nov 2002).

"fly by day consulting, inc.". URL: http://www.cavu.com/news.html (6 Feb 2003).

"Hotfix Checker". Microsoft Knowledge Base Article – 814906. 21 Jan 2003. URL: http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B814906 (8 Feb 2003).

"IIS 5.0 Baseline Security Checklist". 2002. URL: http://www.microsoft.com/technet/security/tools/chklist/iis5cl.asp (12 Nov 2002).

"IIS Tracer ISAPI monitoring tool". URL: http://www.pstruh.cz/help/iistrace/default.htm (20 Nov 2002)

"Insecure". Information Security News: Hacking IIS -- how sweet it is 10 Aug 2001. URL: http://lists.insecure.org/isn/2001/Aug/0067.html (10 Feb 2003).

"Internet Security Systems". DoS. URL: http://www.iss.net/security_center/advice/Exploits/DoS/default.htm (8 Jan 2003).

"Internet Security Systems". Syn flood. URL: http://www.iss.net/security_center/advice/Exploits/TCP/SYN_flood/default.htm (5 Jan 2002).

"News Factor Network". 'Code Blue' Worm Strikes in China, May Migrate. URL: http://www.newsfactor.com/perl/story/13405.html (10 Feb 2003).

"Nmap". Insecure. 22 Feb 2003. URL: http://www.insecure.org/nmap/ (2 March 2003).

"N-Stealth". N-Stalker. 2002. URL: http://www.nstalker.com/nstealth/ndetail.php (19 Nov 2002).

Rosato, Rick. "Best Practices for Applying Service Packs, Hot Fixes and Security Patches". Microsoft TechNet. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bestprac/bpsp.asp (8 Feb 2003).

Scambray, Joel and Stuart McClure. Hacking Exposed Windows 2000: Network Security Secrets and Solutions. New York: McGraw-Hill, 2001. 205-267.

Scambray, Joel and Stuart McClure. "Protecting IIS systems requires hiding your Web-script source code from prying eyes". Info World. URL: http://archive.infoworld.com/articles/op/xml/00/10/30/001030opswatch.xml Feb 2003).

Shaw, James. "12 Oct: What does 'Disallowed Parent Path' mean?". Cover Your ASP. 2002. URL: http://coveryourasp.com/Snippet.asp (19 Nov 2002).

Spencer, Ken. "Solving IIS Application Problems". 7753. Jan 2000. URL: http://www.winnetmag.com/Articles/Index.cfm (17 Nov 2002).

"Super Scan 3.0". Web Attack. 22 Dec 2000. URL: http://www.webattack.com/get/superscan.shtml (10 Feb 2003).

"The Register". Hacking IIS -- how sweet it is. Nov 08 2001 URL: http://www.theregister.co.uk/content/4/20960.html (10 Feb 2003).

"UCB Windows 2000 Resource Center". Information Technology Services. 26 Nov 2001. URL: http://www.colorado.edu/its/Windows2000/adminguide/iis5secguidelines.html (6 Nov 2002).

"WinBook Tech Article". WBTA09000117. URL: http://www.winbookcorp.com/_technote/WBTA09000117.htm (10 Feb 2003).

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
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 Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS