



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 Windows 2000

Microsoft's server products have a history of security issues. Microsoft releases Service Packs and hotfixes on a regular basis. Service Packs are compilations of patched files that have been thoroughly tested by Microsoft. Hotfixes are intermediate patches released between Service Packs and are not thoroughly tested, but fix a bug or vulnerability deemed important enough to be fixed in the interim. Since Service Pack 6a, which was released in May 1999, there have been 27 Security related Hotfixes released for NT 4.0. ...

Copyright SANS Institute
Author Retains Full Rights

AD

JOIN THE WORLD'S LARGEST
OPEN THREAT
EXCHANGE

500,000
Malware Samples Analyzed per Day

ALIEN VAULT

JOIN NOW ►

SANS Practical

**By Scott Hoppe
Exodus Communications, Inc.**

Securing Windows 2000

© SANS Institute 2003, Author retains full rights

Contents:

Disclaimer:.....3
Importance:.....4
Assumptions:.....4
Hotfix Best Practices:.....6
Tools:.....6
 Microsoft Security Notification Service.....7
 HFCHECK.....7
 QFECHECK.....10
 Patchwork.....12
 Windows Update.....14
Conclusion:.....20
Resources:.....21

© SANS Institute 2003, Author retains full rights

Disclaimer:

All efforts have been made to ensure the accuracy and completeness of the information contained in this document. However, discovery of new software revisions, new or revised fixes, and new or revised vendor documentation may, at any time, make portions of this document invalid in terms of its applicability in a computing environment. Before using the tools described below or installing any hotfixes in a production environment test it on a non-production, test machine.

© SANS Institute 2003, Author retains full rights.

Hotfix Management for Windows 2000 running IIS5

Microsoft's server products have a history of security issues. Microsoft releases Service Packs and hotfixes on a regular basis. Service Packs are compilations of patched files that have been thoroughly tested by Microsoft. Hotfixes are intermediate patches released between Service Packs and are not thoroughly tested, but fix a bug or vulnerability deemed important enough to be fixed in the interim. Since Service Pack 6a, which was released in May 1999, there have been 27 Security related Hotfixes released for NT 4.0. After Service Pack 1 was released for Windows 2000 in July 2000, there have been 29 Security related hotfixes released as of March 16, 2001. Are all of these important? How does an administrator wade through and track all of these hotfixes? This document will explain how to manage hotfixes on a Windows 2000 server running IIS 5 on the Internet. There will be five sections to this document: Importance, Assumptions, Hotfix practices, Tools, Installing Hotfixes, and Resources.

Importance:

A Windows 2000 server with a default install of IIS5.0 and Service Pack 1 leaves several holes open. Even in the network described in the assumptions section below, this server would be vulnerable. By carefully crafting URLs, a malicious person could read, write, delete, or execute any file on the system, or cause the server to become unusable by running the CPU utilization to 100%. The abuses range from digital graffiti to theft of credit card information from the on-line databases. If the server being administrated is an e-commerce or e-banking site, abuse of these vulnerabilities (especially if it became public knowledge) could dramatically impact the image of the site.

Assumptions:

In order to keep the focus of this document somewhat manageable, the system to be secured will have the following setup:

The server will sit on a DMZ network (See figure 1), traffic from the internal and external network will be limited to HTTP, HTTPS, and FTP traffic only. The number of hotfixes needed to secure a server configured in this manner is drastically reduced, because the network vulnerabilities from traffic other than the type listed above is removed. Many firewalls are setup to allow all traffic from the internal network to the DMZ. If this is the case, ALL security hotfixes should be applied, because there are numerous vulnerabilities with the file and print services that Windows 2000 provides.

Anti-Virus software is an important part of any server deployment. It is not the focus of this document, but is mentioned because it such an important item. This software is crucial for an FTP server that allows uploads.

Since most administrators are on a tight time and money budget, any tools used will be either freely downloadable or come with Windows 2000 and run on a Windows 2000 Server. Vulnerability Scanners would be a very helpful tool for keeping vulnerabilities minimized, but they cost a great deal of money (ISS), only run under Unix (Nessus), and are generally very complicated for the average administrator to setup and maintain. Unfortunately, the only way to be sure the vulnerability has been fixed is to test it. Currently, there is no better way to test that known vulnerabilities have been fixed than by using vulnerability scanners.

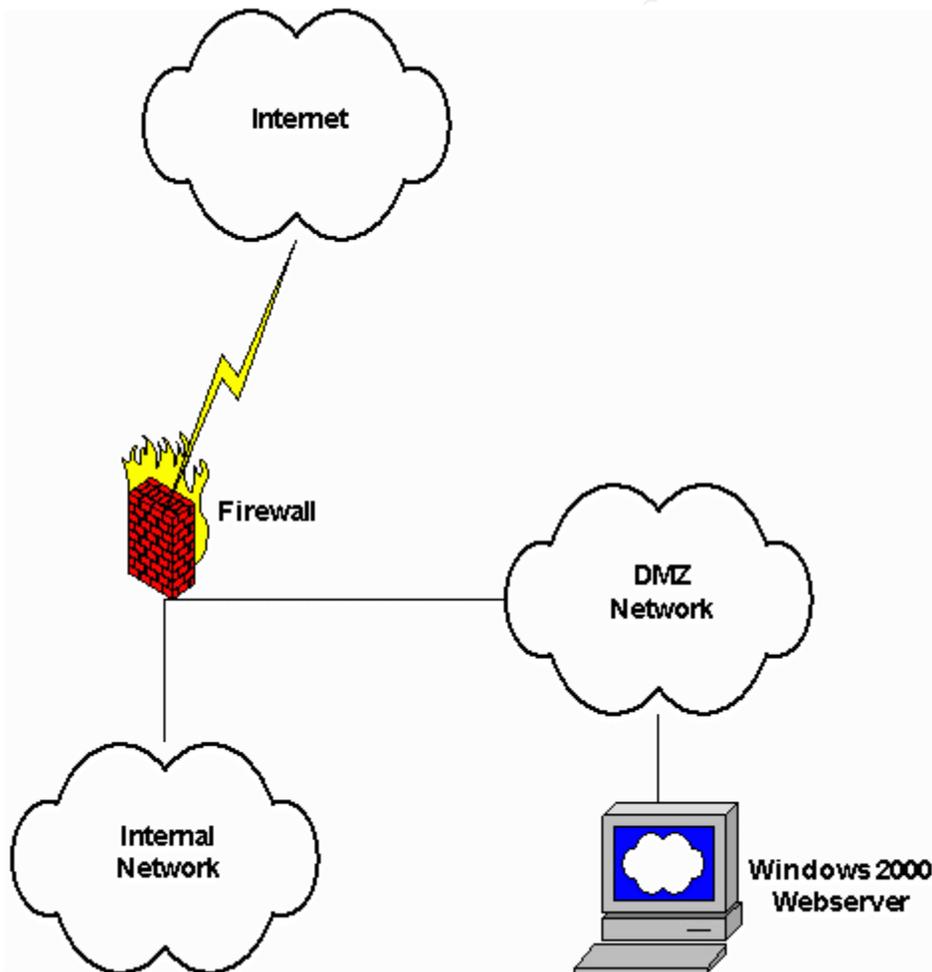


Figure 1

Hotfix Best Practices:

When installing a new server, the latest service pack and all security related hotfixes should be applied. For details, see the Windows 2000 download webpage:

<http://www.microsoft.com/windows2000/downloads/default.asp>

There is no reason not to have all of the security fixes on a brand new install. If an application doesn't work with a particular hotfix, there should be time to get the application fixed before the server goes live. A hotfix could be backed out if it has a known issue with an application, but that is not recommended.

For a webserver already in production, all hotfixes should be tested on a non-production server BEFORE deploying on the production website. A good, reliable, tested backup of the server should be done BEFORE adding any hotfixes. Microsoft's hotfixes are not regression tested as thoroughly as their Service Packs, so they may cause incompatibilities with production applications and sometimes have trouble with hardware. In either case, the application would be unavailable for a period of time while the hotfixes were being backed out or the server being re-installed or restored from tape.

Once the desired hotfixes have been downloaded, they should be installed in date order (i.e. the date they were released by Microsoft). It is probably best to download them into directories that let the administrator know the hotfix date, so that future updates can use the existing downloads without a lot of confusion as to which hotfix is which.

To install a hotfix, simply run the .exe file. The following command line arguments are available:

- m = unattended install (this is not recommended)
- y = uninstall the hotfix.
- z = do not reboot after applying the hotfix.
- q = quiet install, no user interaction.

When any software is installed or updated, or files copied from the Windows 2000 CD, the latest Service Pack and all hotfixes to that point should be reapplied. Installing software can replace patched files with previous versions of those files and leave a vulnerability open that the administrator had already closed. This is another reason for keeping a local copy of the hotfixes and naming them appropriately.

When installing a group of hotfixes, Microsoft recommends rebooting between each hotfix. This can make the process take a lot of time, so be sure that the window of downtime allowed for the hotfixing process is large enough to accommodate several reboots.

Tools:

There are a few tools for determining which hotfixes are critical to the running of an IIS server with the configuration outlined above. Microsoft Security Notification Service,

HFCHECK, QFECHECK, Patchwork, and Windows Update are the products or services that will be discussed. The notification service is an automated information outlet. The others are software or web based programs that will scan your system and compare the files or registry with the tools' own database to determine if your system has the right patch level of critical files. If the system is not sufficiently patched, some of the tools will produce URLs to the required hotfixes so that the administrator can download and install them. Running the tools again will verify that the files have been installed. The tools can be automated so that the administrator will be notified when new vulnerabilities and hotfixes to close them are available.

Microsoft Security Notification Service

The Microsoft Security Notification Service (<http://www.microsoft.com/technet/security/notify.asp>) is a free e-mail notification service that Microsoft uses to send information to subscribers about the security of Microsoft products. Anyone can subscribe or unsubscribe to the service at any time. The service provides information to subscribers that they can use to inform and protect themselves from malicious attacks. The Microsoft security team investigates issues reported directly to Microsoft, as well as issues discussed in certain popular security newsgroups. When bulletins are published, they'll contain information on what the issue is, what products it affects-if any, how to protect yourself against, what Microsoft plans to do to fix the problem, and links to other sources of information on the issues.

HFCHECK

HFCHECK is a tool from Microsoft that can be used to check a Windows 2000 system for IIS related hotfixes. From the Microsoft Website (<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=24168>): "The HFCheck tool allows IIS5.0 administrators to ensure that their servers are up to date on all security patches. The tool can be run continuously or periodically, against the local machine or a remote one, using either a database on the Microsoft web site or a locally-hosted copy. When the tool finds a patch that hasn't been installed, it can display or dialogue or write a warning to the event log." From the documentation file: "HFCHECK.WSF consults an XML file list – either hosted on the Microsoft site or downloaded to the local machine – for the list of hotfixes available for IIS, then compares this list to the hotfixes installed on the local system. If a hotfix is missing, the tool calls the Notify function in NOTIFY.JS. The current implementation of Notify reports an error on the command-line and writes a warning message to the Application Eventlog, but it is possible to customize it to perform other actions such as stopping the server or sending an e-mail to the administrator. The Notify function is in a separate file (NOTIFY.JS), so that you can easily rewrite the Notify function for your own needs."

Download the tool from the URL above, run HFCINST.EXE and unpack into a new directory. You should have the following files in your new directory:

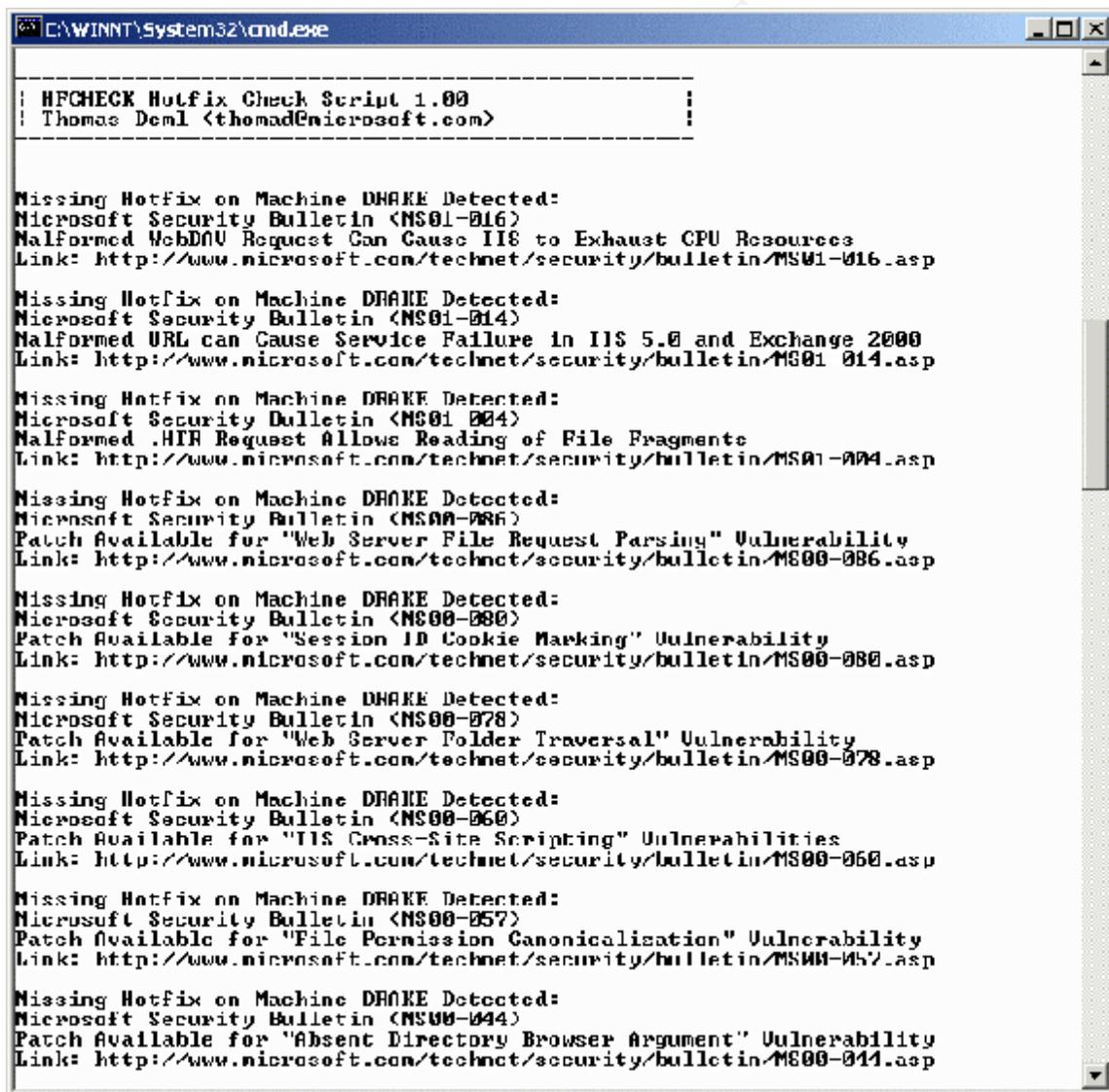
- EULA.txt – Microsoft's License Agreement
- HFCheck.doc – the instructions
- Hfcheck.wsf – the script file for reporting the hotfixes
- Notify.js – a script file for alerting

In order to use the files, the default windows scripting host may need to be changed to cscript. To do this, run the following on a command-line: *cscript //H:cscript*
You should get the following output:

```
Microsoft (R) Windows Script Host Version 5.1 for Windows  
Copyright (C) Microsoft Corporation 1996-1999. All rights reserved.
```

The default script host is now set to "cscript.exe".

HFCHECK can now be run from a command-line – change directory to where you installed the files and run: *hfcheck.wsf*
The output for a machine that hasn't been hotfixed after Service Pack 1 will look similar to Figure 2.



```
-----  
| HFCHECK Hotfix Check Script 1.00 |  
| Thomas DeMl <thomad@microsoft.com> |  
-----  
  
Missing Hotfix on Machine DRAKE Detected:  
Microsoft Security Bulletin <MS01-016>  
Malformed WebDNU Request Can Cause IIS to Exhaust CPU Resources  
Link: http://www.microsoft.com/technet/security/bulletin/MS01-016.asp  
  
Missing Hotfix on Machine DRAKE Detected:  
Microsoft Security Bulletin <MS01-014>  
Malformed URL can Cause Service Failure in IIS 5.0 and Exchange 2000  
Link: http://www.microsoft.com/technet/security/bulletin/MS01-014.asp  
  
Missing Hotfix on Machine DRAKE Detected:  
Microsoft Security Bulletin <MS01-004>  
Malformed .HTA Request Allows Reading of File Fragments  
Link: http://www.microsoft.com/technet/security/bulletin/MS01-004.asp  
  
Missing Hotfix on Machine DRAKE Detected:  
Microsoft Security Bulletin <MS00-086>  
Patch Available for "Web Server File Request Parsing" Vulnerability  
Link: http://www.microsoft.com/technet/security/bulletin/MS00-086.asp  
  
Missing Hotfix on Machine DRAKE Detected:  
Microsoft Security Bulletin <MS00-080>  
Patch Available for "Session ID Cookie Marking" Vulnerability  
Link: http://www.microsoft.com/technet/security/bulletin/MS00-080.asp  
  
Missing Hotfix on Machine DRAKE Detected:  
Microsoft Security Bulletin <MS00-078>  
Patch Available for "Web Server Folder Traversal" Vulnerability  
Link: http://www.microsoft.com/technet/security/bulletin/MS00-078.asp  
  
Missing Hotfix on Machine DRAKE Detected:  
Microsoft Security Bulletin <MS00-060>  
Patch Available for "IIS Cross-Site Scripting" Vulnerabilities  
Link: http://www.microsoft.com/technet/security/bulletin/MS00-060.asp  
  
Missing Hotfix on Machine DRAKE Detected:  
Microsoft Security Bulletin <MS00-057>  
Patch Available for "File Permission Canonicalization" Vulnerability  
Link: http://www.microsoft.com/technet/security/bulletin/MS00-057.asp  
  
Missing Hotfix on Machine DRAKE Detected:  
Microsoft Security Bulletin <MS00-044>  
Patch Available for "Absent Directory Browser Argument" Vulnerability  
Link: http://www.microsoft.com/technet/security/bulletin/MS00-044.asp
```

Figure 2

Take a look in the Application Event Log. There should be entries similar to Figure 3 and Figure 4. Figure 3 shows that the application event log entries are given 'Warning' priority and are entered by 'WSH' – the Windows Scripting Host. Figure 4 shows the detail from one of these entries. The detail names the vulnerability, gives a short description of the vulnerability, and gives a URL to the security bulletin that describes the vulnerability in detail and how to workaroud, fix, or hotfix the problem.

Warning	3/15/2001	3:53:12 PM	WSH	None	2	N/A	DRAKE
Warning	3/15/2001	3:53:12 PM	WSH	None	2	N/A	DRAKE
Warning	3/15/2001	3:53:12 PM	WSH	None	2	N/A	DRAKE
Warning	3/15/2001	3:53:12 PM	WSH	None	2	N/A	DRAKE

Figure 3

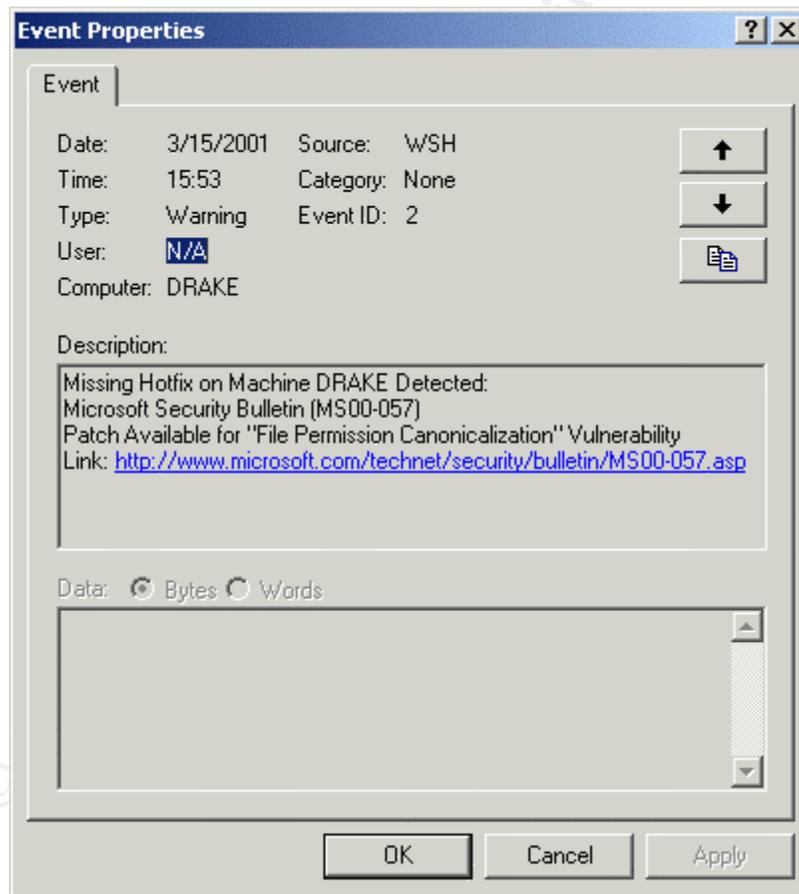


Figure 4

Interestingly, the subroutine that writes to the event log (Notify.js) can be modified so that it can do anything a javascript can do – send an email, send a page, or send an SNMP

trap, for example. The documentation for HFCHECK gives the following code example to get Notify.js to send an email:

```
Set objMsg = CreateObject("CDONTS.NewMail")
'Set the properties of the Message
objMsg.From = "HotfixNotification@YourCompany.com"
objMsg.To = "Administrators@YourCompany.com"
objMsg.Subject = "Missing Hotfix Detected!"
objMsg.Body = "Microsoft Security Bulletin _
(" + sBulletin + ") " + sTitle + " Link:
_http://www.microsoft.com" + sLink
objMsg.Send
```

The last step for using HFCHECK is automation. The scheduled tasks system can be used to run HFCHECK on a periodic basis so that an administrator will be automatically alerted in the event a new hotfix has been posted since the Windows 2000 server was last updated. The user the task is scheduled to run under will need permissions to execute the HFCHECK script and any command-line utilities or scripts that Notify.js is setup to run.

QFECHECK

QFECHECK is a command-line tool from Microsoft (see <http://www.microsoft.com/technet/support/kb.asp?ID=282784>) that gives administrators increased ability to track and verify installed Windows 2000 hotfixes. The tool lists the installed hotfixes on a system by Microsoft Knowledge Base article 'Q' number. This allows an administrator to install and verify the appropriate set of fixes before using a valuable support incident and potentially experiencing unplanned down time. The tool can create logs with the hotfix information for each computer and the logs can be scanned to verify constancy across an organization. According to Microsoft: "There are rare situations in which, because of a network problem, a problem with the update itself, or a subsequent update that improperly overwrites a previous fix, updates could be damaged or removed in error. This tool ensures that not only have the fixes been installed, but that they are current on the computer."

When QFECHECK is run, it identifies two main issues: hotfix files that are current but not considered valid by the installed catalogs, and files that have been hotfixed but the installed file is not current. QFECHECK compares the registry information at **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates** and reports an error if it does not match the current version of the file. It also verifies that the file information for hotfixed files is valid in the Windows File Protection (WFP) system. The possibility exists for WFP to roll back a hotfix if this happens, and basically uninstall a hotfix, re-opening a vulnerability an administrator thought closed.

Download QFECHECK from

<http://www.microsoft.com/downbads/release.asp?ReleaseID=27333>. Run the file – it installs like a hotfix, but does not require a reboot. From a command line, run QFECHECK.EXE. Output for a system that doesn't have any problems should be similar to Figure 5.

```
C:\WINNT\System32\cmd.exe
C:\>qfcheck /?
QFCHCK [ /l[:location] /u /q /? ]
  /l          Log output to machinename.log in current directory
  location    Use specified location to store the log file
  /u          Verbose output
  /q          Quiet mode
  /?         This help

C:\>qfcheck /u

Windows 2000 Hotfix Validation Report for \\GALACTICA
Report Date: 3/17/2001 3:49pm

Current Service Pack Level: Service Pack 1

Hotfixes Identified:
Q259524: Current on system.
Q277007: Current on system.
Q280838: Current on system.
Q287030: Current on system.
Q282784: Current on system.

C:\>_
```

Figure 5

In the following case, hotfix Q272743 is installed, but the binary is not current:
Windows 2000 Hotfix Validation Report for \\WinAdvSrv
Report Date: 1/11/2001 9:30pm

Current Service Pack Level: Service Pack 1

Hotfixes Identified:
Q267866: Current on system.
Q272743: This hotfix should be reinstalled.

The following files are incorrect for this hotfix:
C:\WINNT\SYSTEM32\TELNET.EXE
C:\WINNT\SYSTEM32\DLLCACHE\TELNET.EXE

In the following case, hotfix Q272743 is installed, the binary is current, but the system catalog is incorrect:

Windows 2000 Hotfix Validation Report for \\WinAdvSrv
Report Date: 1/11/2001 9:24pm

Current Service Pack Level: Service Pack 1

Hotfixes Identified:
Q267866: Current on system.
Q272743: This hotfix should be reinstalled.

The following files are not valid in the system catalog:
C:\WINNT\SYSTEM32\TELNET.EXE
C:\WINNT\SYSTEM32\DLLCACHE\TELNET.EXE

If the second error type is encountered (incorrect system catalog), see Microsoft Knowledge Base Article Q281787 (<http://support.microsoft.com/support/kb/articles/Q281/7/67.ASP>) for information on resolving the problem.

QFECHECK should be run after any hotfix is installed to verify that the hotfix was installed correctly, and that the WFP will not accidentally uninstall the hotfix in the future.

Patchwork

Patchwork, written by Steve Gibson, is a software tool that automates the process of finding the vulnerabilities and identifying needed patches. Its purpose is to assist companies that have not secured their systems to do so quickly. Patchwork does two things:

- 1) Rapidly scans the system's mass storage for evidence of files known to be used by hackers for system intrusion and also files implicated in the specific intrusions researched by the FBI.
- 2) Analyze the Windows server for the presence of the specific vulnerabilities known to have been exploited by the Russian hackers.

This tool is not a comprehensive patch verification tool. It will, however, verify that specific vulnerabilities known to have been used by hackers have been patched or give information on how to patch them. Information describing the attacks that this tool protects against can be found from a March 8, 2001 news article on the SANS website at: <http://www.sans.org/newlook/alerts/NTE-bank.htm>. “More than 40 victims located in 20 states have been identified and notified in ongoing investigations in 14 Federal Bureau of Investigation Field Offices and 7 United States Secret Service Field Offices. Once the hackers gain access, they download proprietary information, customer databases, and credit card information.”

Download Patchwork from <http://grc.com/pw/patchwork.htm>. Verify that the tool downloaded has not been tampered with by following the instructions at: <http://grc.com/pw/patchsig.htm>. Once the tool has been downloaded and verified to be authentic, simply double-click on the file to run it. Output should be similar to Figure 6 if the system has not been patched. If the system is vulnerable, go ahead and click ‘Scan FileSystem’ to see if it has been compromised by the specific hacks related in the news article. Once the scan is finished, click on the ‘Findings’ tab. It should look like Figure 6a.



Figure 6

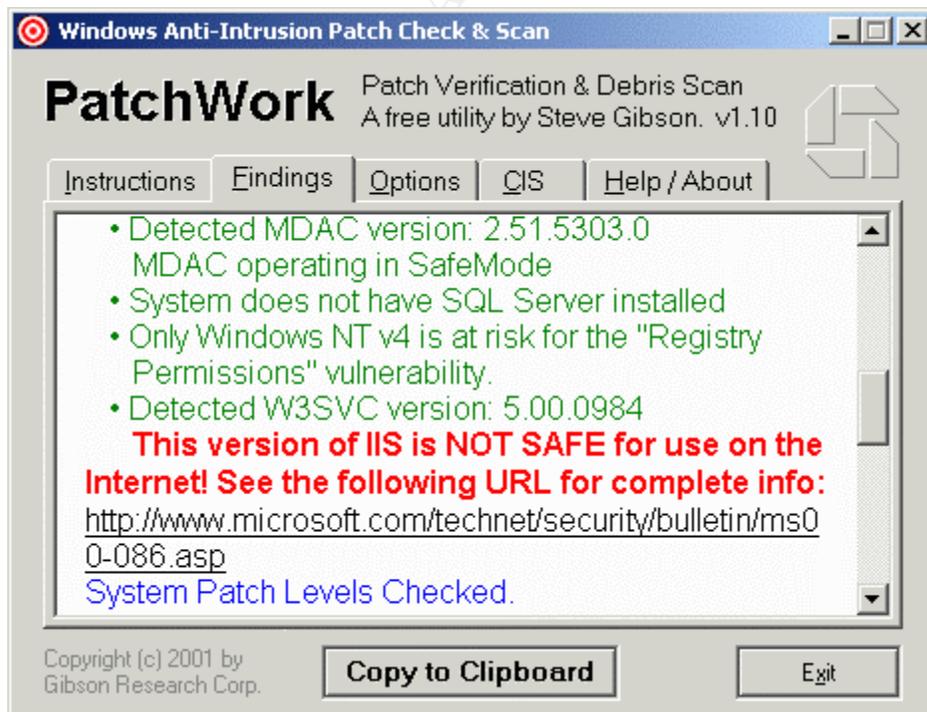


Figure 6a

Patchwork reports the version of IIS currently being used, the status of that version – safe or unsafe – and a URL to the hotfix on Microsoft’s website if it is found to be unsafe. If the system has been compromised, the tool will also report how to disinfect the system.

This tool can also be configured to run at system startup. Go to the ‘Options’ tab, as in Figure 7. The drive letters to be scanned can be checked, and the tool can be configured to popup for a number of seconds to show an administrator that the system is ‘OK’. If there is a problem, it will popup and alert the administrator about a patch or an intrusion.

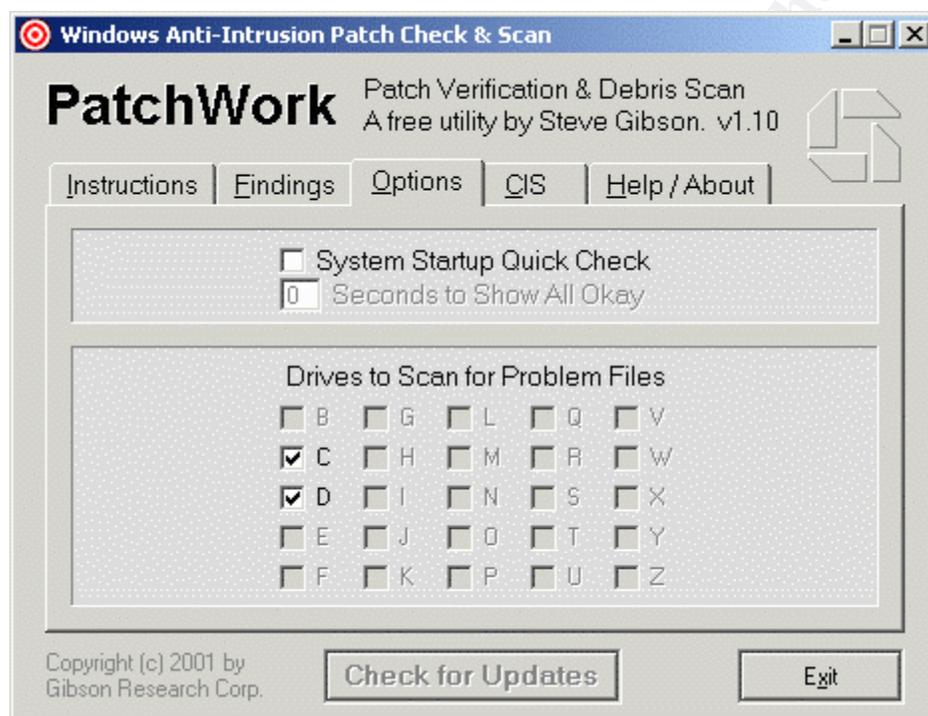


Figure 7

Windows Update

Windows Update (<http://windowsupdate.microsoft.com/>) is a website that Microsoft touts as an “online extension of Windows that helps you get the most out of your computer”. By default, there is a web link in the Start Menu of Windows 2000 called ‘Windows Update’ that points to the Product Updates section of the Windows Update website. This link is created in the Start Menu whenever Windows 2000 is installed. If this is the first time the computer has connected to this website, a Security Warning popup will ask whether the Active-X control should be allowed to execute – click ‘Yes’.

The Product Updates section of Windows Update runs an Active-X control (See Figure 8) that scans the computer connected to the site and compares what it finds to the latest levels of file versions in its database. New product enhancements such as system files, device drivers, service packs, critical updates, and new Windows features are

recommended based on what is needed for the specific computer connecting to the site (See Figure 9). The software this website updates is mainly for Internet Explorer and the associated programs (examples: MSN Messenger Service, DirectPlay, Direct X, Netmeeting, Media Player, Microsoft's Virtual Machine, etc.). It will alert you if you do not have the latest Service Pack or latest Internet Explorer installed, but does not alert you to operating system hotfixes. The Critical Updates it fixes are usually exploits specific to Internet Explorer.



Figure 8

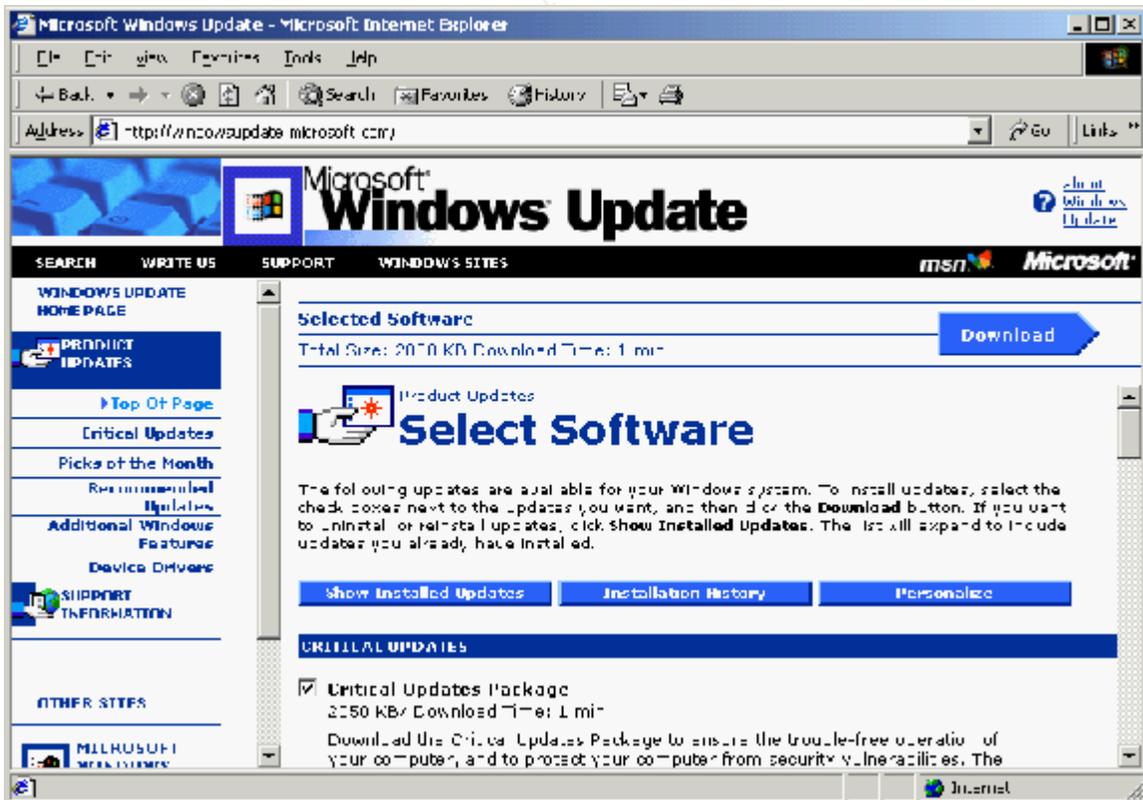


Figure 9

An error about Active-X may pop up when trying to connect to the Product Updates section. This message is displayed when the security setting in Internet Explorer is set to High. For the Windows Update site to work properly, Microsoft's Windows Update FAQ recommends changing the browser's security settings for the Internet zone to Medium or lower. To do so, click the Tools menu, then click Internet Options. Select the Security tab and then click on Internet. A more secure way to fix this would be to add the Windows Update website to trusted sites, instead of lowering the security for the Internet zone. On the same tab mentioned above, select Trusted Sites, then click Sites. Uncheck the box by "Require server verification (https:) for all sites in this zone", type in the full URL for windows update (<http://windowsupdate.microsoft.com>) in the "Add this website to the zone:" box, and click "Add".

According to Microsoft, no information about the scanned computer is sent to the website or to Microsoft. The Active-X control scans the computer and compares what it finds to an internal database. The check is done locally to ensure privacy and data integrity.

Critical updates are always listed at the top of the Product Updates section. The critical updates are selected by default, and presented as a package. Individual critical updates can be viewed and selected by clicking the Show Individual Updates '+' button. For Windows 2000 running Service Pack 1 and Internet Explorer 5.5 SP1, there are three critical updates as of March 17, 2001. The first from November 22, 2000 addresses security issues in Internet Explorer dealing with "Browser Print Template", "File Upload via Form", and "Frame Domain Verification". The second from December 20, 2000 fixes the "Indexing Service File Enumeration" vulnerability with Indexing Service 3.0. The third update from January 30, 2001 fixes the "VM File Reading" security vulnerability in Microsoft Virtual Machine.

Currently installed updates can be viewed by selecting the "Show Installed Updates" button. It will present a list of what is installed, and in some cases allow uninstallation.

Internet Explorer and the latest service pack can be downloaded from this page, but will require that only Internet Explorer or the service pack be installed at that time (i.e. no other updates can be downloaded and installed at the same time). These files have their own separate download and installation process. When packages are selected, the download size and approximate download time are displayed under the 'Selected Software' heading at the top of the page. Once the desired packages have been selected, click on the 'Download' button. A checklist confirms the selected packages and redisplay the size and approximate time to download the files. It might be wise to select the 'View Instructions' button at this point to verify whether there are any special procedures needed to install the files selected.

Before continuing, be advised that the process will want to reboot the computer once it is finished.

Select the 'Start Download' button. A EULA popup similar to Figure 9a appears to ask if you agree to Microsoft's terms. Click Yes. Another window will popup displaying the download and install progress. Once the process is finished, the browser should display a success message (See Figure 9b) and a popup will ask to reboot the computer (See Figure 9c).

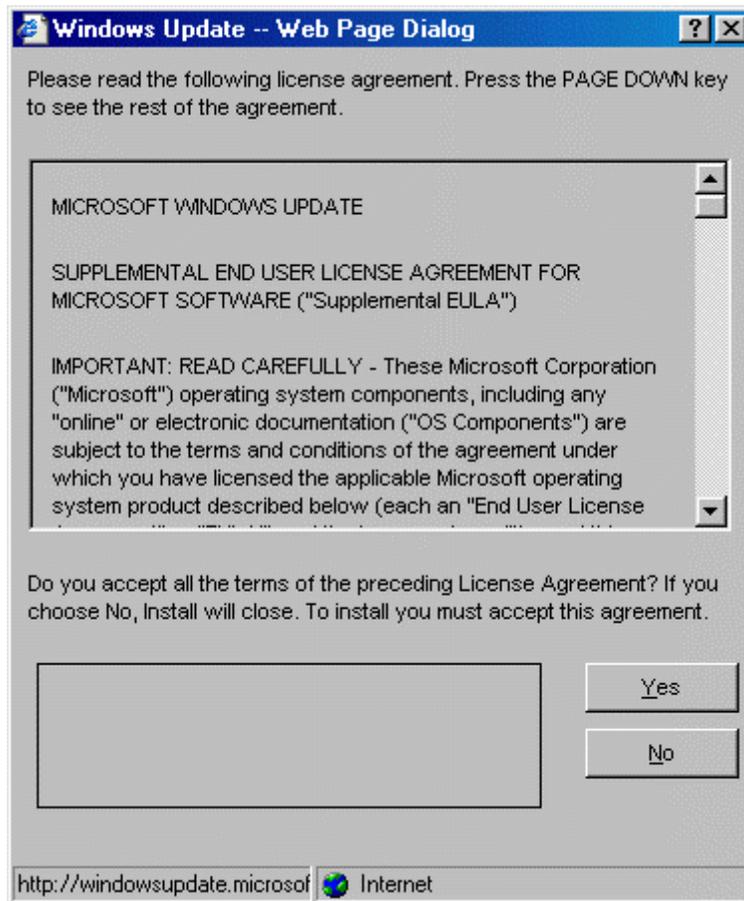


Figure 9a

© SANS

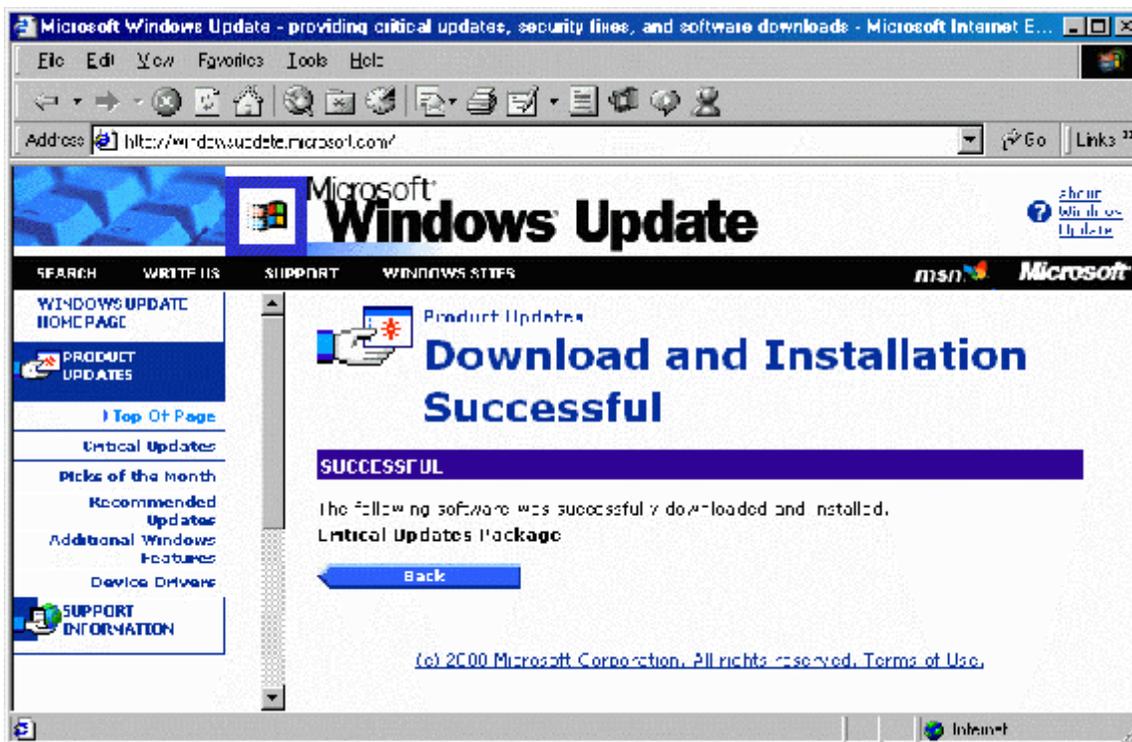


Figure 9b



Figure 9c

Why would an administrator be interested in patching Internet Explorer on the webserver itself? Generally, Internet Explorer should not be used on the console of a webserver. Unfortunately, it often can't be avoided. To download the latest patches, device drivers, find a problem in the Microsoft Support database (<http://support.microsoft.com/>), etc. the browser on the webserver does get used. It is important to make sure malicious code won't make it to the server just because of an unpatched browser.

Getting information on these Critical Updates can be automated using the Critical Update Notification package. One of the items on the Product Updates page, if it is not installed already, should be Windows Critical Update Notification (Version 3.0 at this writing). It is a small download - about 54 KB. When installed, it creates a scheduled task called Windows Critical Update Notification that runs an executable (WUCRTUPD.EXE) on a

periodic basis. This file does a similar task to clicking on the Product Updates link on the Windows update website, and provides a popup window in the event there is a new patch available. The popup window (See Figure 10) allows you to click 'Notify Me Later', in which case the popup will come back in 24 hours, or 'View Critical Updates'. If 'View Critical Updates' is clicked, Internet Explorer is executed and connects to the Product Updates section of the Windows Update website.

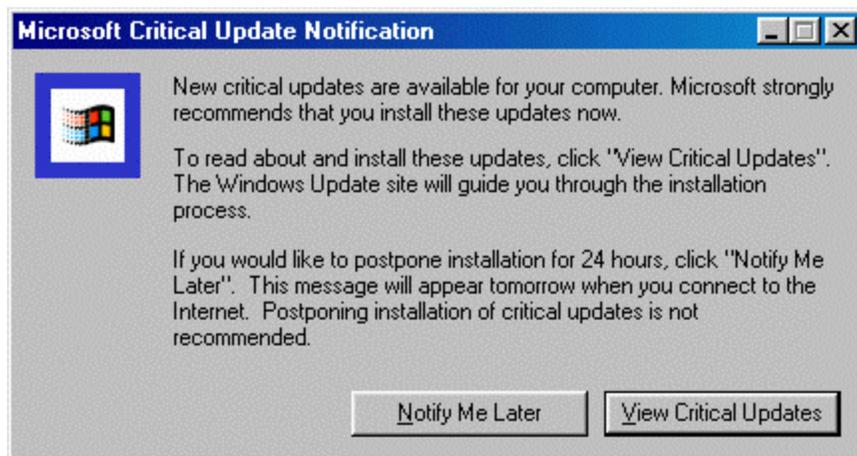


Figure 10

© SANS Institute 2003, Author

Conclusion:

Running a publicly available webserver can be a daunting task. Besides having to deal with the day-to-day maintenance of file rights, login permissions, content, file space, backup, throughput, etc. an administrator has to deal with patches for operating system vulnerabilities. Just having the latest service pack in a Microsoft environment is not enough. Fortunately, there are freely available tools that make this task less daunting. Microsoft Security Notification Service, HFCHECK, QFECHECK, Patchwork, and Windows Update are helpful tools for the administrator on a tight time and money budget to help stay on top of these problems.

© SANS Institute 2003, Author retains full rights.

Resources:

'Windows NT Server Downloads' Microsoft website
<http://www.microsoft.com/NTServer/all/downloads.asp>

'Windows 2000 Downloads' Microsoft website
<http://www.microsoft.com/windows2000/downloads/default.asp>

'Microsoft Security Notification Service' Microsoft website
<http://www.microsoft.com/technet/security/notify.asp>

'Microsoft Technet Online Support' Microsoft website
<http://support.microsoft.com/servicedesks/technet/default.asp?fr=0&sd=tech>

'Securing Windows 2000 running IIS5' Alan McClelland
http://www.sans.org/y2k/practical/Alan_McClelland_GCNT.doc

'Alert: Large Criminal Hacker Attack on Windows NTE-Banking and E-Commerce Sites' SANS website
<http://www.sans.org/newlook/alerts/NTE-bank.htm>

'Patchwork – Windows NT Security Checker' Patchwork website
<http://grc.com/pw/patchwork.htm>

© SANS Institute 2003. Author retains full rights.



Upcoming SANS Training

[Click Here for a full list of all Upcoming SANS Events by Location](#)

SANS Northern Virginia - McLean 2016	McLean, VAUS	Feb 15, 2016 - Feb 20, 2016	Live Event
SANS Munich Winter 2016	Munich, DE	Feb 15, 2016 - Feb 20, 2016	Live Event
ICS Security Summit & Training - Orlando	Orlando, FLUS	Feb 16, 2016 - Feb 23, 2016	Live Event
SANS Southern California - Anaheim 2016	Anaheim, CAUS	Feb 22, 2016 - Feb 27, 2016	Live Event
SANS Secure India 2016	Bangalore, IN	Feb 22, 2016 - Mar 05, 2016	Live Event
RSA Conference 2016	San Francisco, CAUS	Feb 28, 2016 - Feb 29, 2016	Live Event
SANS London Spring 2016	London, GB	Feb 29, 2016 - Mar 05, 2016	Live Event
SANS Philadelphia 2016	Philadelphia, PAUS	Feb 29, 2016 - Mar 05, 2016	Live Event
SANS Abu Dhabi 2016	Abu Dhabi, AE	Mar 05, 2016 - Mar 10, 2016	Live Event
SANS 2016	Orlando, FLUS	Mar 12, 2016 - Mar 21, 2016	Live Event
ICS410 Dubai 2016	Dubai, AE	Mar 13, 2016 - Mar 17, 2016	Live Event
SANS Secure Singapore 2016	Singapore, SG	Mar 28, 2016 - Apr 09, 2016	Live Event
SANS Secure Europe 2016	Amsterdam, NL	Apr 04, 2016 - Apr 16, 2016	Live Event
SANS Northern Virginia - Reston 2016	Reston, VAUS	Apr 04, 2016 - Apr 09, 2016	Live Event
SANS Atlanta 2016	Atlanta, GAUS	Apr 04, 2016 - Apr 09, 2016	Live Event
Threat Hunting and Incident Response Summit	New Orleans, LAUS	Apr 12, 2016 - Apr 19, 2016	Live Event
ICS Amsterdam 2016	Amsterdam, NL	Apr 18, 2016 - Apr 23, 2016	Live Event
SANS Secure Canberra 2016	Canberra, AU	Apr 18, 2016 - Apr 23, 2016	Live Event
SANS Pen Test Austin	Austin, TXUS	Apr 18, 2016 - Apr 23, 2016	Live Event
SANS Copenhagen 2016	Copenhagen, DK	Apr 25, 2016 - Apr 30, 2016	Live Event
SANS Security West 2016	San Diego, CAUS	Apr 29, 2016 - May 06, 2016	Live Event
SANS Baltimore Spring 2016	Baltimore, MDUS	May 09, 2016 - May 14, 2016	Live Event
SANS Houston 2016	Houston, TXUS	May 09, 2016 - May 14, 2016	Live Event
SANS Stockholm 2016	Stockholm, SE	May 09, 2016 - May 14, 2016	Live Event
SANS Prague 2016	Prague, CZ	May 09, 2016 - May 14, 2016	Live Event
SANS Secure Japan 2016	OnlineJP	Feb 15, 2016 - Feb 20, 2016	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced