Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

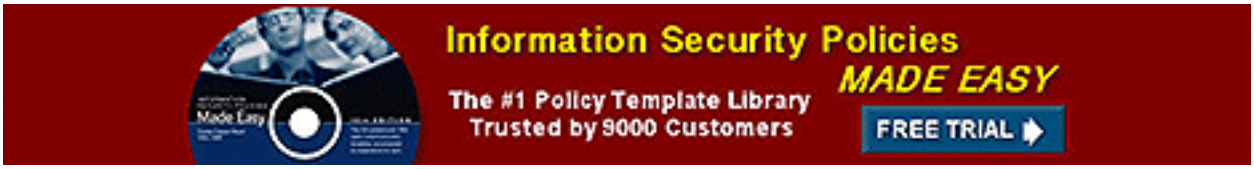
This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Systems Security Management: Small Business Style

So you've got a handful of Microsoft(R) Windows servers and another few handfuls of Microsoft(R) Windows workstations. Security management and administration should not be all that difficult ... right?" Unfortunately, that was only one of many hats I had to wear on a weekly, often daily basis. Most small businesses simply do not have the resources for even one full-time employee dedicated to Information Systems; however, I had landed that position. Four servers and thirty workstations can be a bit much without a good p...

Copyright SANS Institute
Author Retains Full Rights

AD



Systems Security Management: Small Business Style

By Nathaniel L. Dean

GSEC CERTIFICATION
Case Study version 1.4b
February 2, 2003

© SANS Institute 2003, Author retains full rights

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

Table of Contents

Introduction....3
Identifying the Tasks....3
The Perimeter....3
The Firewall....3
Dial-up Access....4
Wireless Handhelds....4
AntiVirus/AntiSPAM....4
Managing Updates....6
Deeper: Analysis & Prevention....8
Summary....10
Citations....11

© SANS Institute 2003, Author retains full rights

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

Introduction

"So you've got a handful of Microsoft® Windows servers and another few handfuls of Microsoft® Windows workstations. Security management and administration should not be all that difficult … right?" Unfortunately, that was only one of many hats I had to wear on a weekly, often daily basis. Most small businesses simply do not have the resources for even one full-time employee dedicated to Information Systems; however, I had landed that position. Four servers and thirty workstations can be a bit much without a good plan and the right tools to aid in the execution. The most basic assumptions that can be made are that humans are human and systems, being ultimately designed and built by humans, will indeed contain flaws. And then, of course, there's entropy… Thus began my journey to circumvent humans and their systems in the most centralized and simplified methods possible … all the while, of course, defying my own humanity!

Identifying the Tasks

This environment had fortunately been kept relatively current and Microsoft®-centric: Windows 2000 Server & Professional, Exchange Server 2000, SQL Server 2000, and some Windows XP Professional. Nonetheless, every element requires regular patching and updating for remediation of faults, performance issues, virus signatures, etc. Initial system and application configurations are never quite sufficient; thus, ongoing analysis cannot be ignored. And last, or perhaps first, perimeter defenses needed to be more than just a Network Address Translation (NAT)/Port Address Translation (PAT) gateway. "Although not primarily a security feature, NAT hides internal IP addresses from public view."[1] Yet, hiding behind a door does little good when your enemy knows your there and has the keys.

The Perimeter

A couple of principles provide initial guidance here. All pathways in and out of the network should incorporate more than just a gateway. Additionally, if a resource cannot be accessed securely from beyond the perimeter, then it simply should not be; security should trump accessibility unless business continuity and/or commerce are significantly disrupted in the mitigation of a relatively minor risk.

The Firewall

Whereas a properly configured NAT/PAT, application gateway, or stateful firewall can provide significant protection, with limited resources, monitoring and analysis are unlikely to be anything more than sporadic. The decision was made to contract for a monitored/managed service from SecureWorks® who provides what they refer to as Four-Dimensional℠ security, addressing the elements of time, technology, process and people.

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

SecureWorks® deploys one piece of Customer Premise Equipment (CPE), the iSensor, which contains their proprietary, hardened OS. Ingress/egress rules, port forwarding, services, alerting and reporting are all accessible via the SecureHub, a secure web-based interface. The iSensor is additionally configured to block a specified list of attachments, acting as a pre-filter to protect the corporate eMail server and lighten the load on the anti-virus server. Ultimately, the iSensor is a second-generation IPS (intrusion prevention system) residing at the perimeter, intelligently blocking malicious traffic while allowing all else to flow through.[2] More than a couple of times I have called to inquire about a specific threat to find that at the least they were already aware and had even been involved in the identification of the threat. Threats of all types have been prevented from ever entering the private network including Klez, Code Red, Nimda, and on down the list to the SQL Slammer. Summary reports are currently auto-generated on a daily basis but can be requested at other intervals. Any alerts that are classified as 'severity 3' generate an eMail to those within the escalation matrix. Additionally, custom reporting on and searching of both incident history and configuration activity can be done via the SecureHub. For all the iSensor does, its throughput is rated at up to 60Mbps.

Dial-up Access

There was a small bank of modems providing dial-up access to the corporate LAN. These modems connected directly to a server that contained sensitive data. Yet, no monitoring or logging of their usage was done. The decision was made to terminate use of direct dial-up access in favor of whatever Internet access each remote user may have. Additionally, a corporate nationwide Internet dial-up account was established. Once connected to the Internet, the users could then access corporate resources via approved methods such as Terminal Services, SSL, and PPTP. POP, IMAP and all other protocols and/or methods of access that employ clear-text authentication were disallowed and blocked at the iSensor.

Wireless Handhelds

A number of users had adopted the use of Palm or Windows CE based handhelds and had experimented with their associated wireless services. Upon review of the real needs and available solutions, a Blackberry Enterprise Server (BES) from Research in Motion® was deployed. In order to allow for secure, wireless communication, Blackberry employs Triple-DES encryption of all traffic flowing between each handheld and the BES. Also, each handheld device can be set to require password authentication for direct access along with lock-out following a selected period of inactivity. The password is stored on the handheld as an SHA-1 encrypted hash.[3] While its use cannot currently be enforced, that feature is forthcoming.

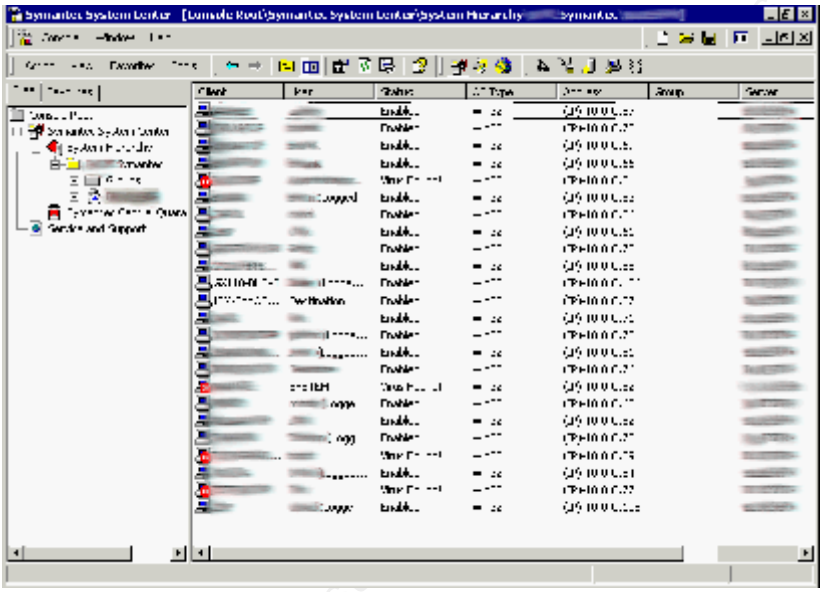
AntiVirus/AntiSPAM

Although most new computers include at least limited antivirus protection, most users are not diligent to maintain nor knowledgeable enough to properly

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

configure the software. Basic user awareness and education is paramount, however difficult it may be to accomplish.[4] There will eventually arise a situation in which an educated user can at least exercise due restraint or caution and perhaps save untold fiscal and/or intellectual damage.

The pursuit of a solution that would prove both effective and simple both to implement and maintain culminated in the selection of Symantec AntiVirus™ Corporate Edition. Deployment, updates, configuration, and control for all servers and clients are accomplished from a single console. The quarantine and alert management systems are also integrated into the console. Symantec AntiVirus™/Filtering (SAVF) for Microsoft® Exchange was implemented at the Exchange server. This provides an additional layer prior to the client real-time scanner and, most importantly, prevents infection and possible corruption of the Exchange Information Stores.



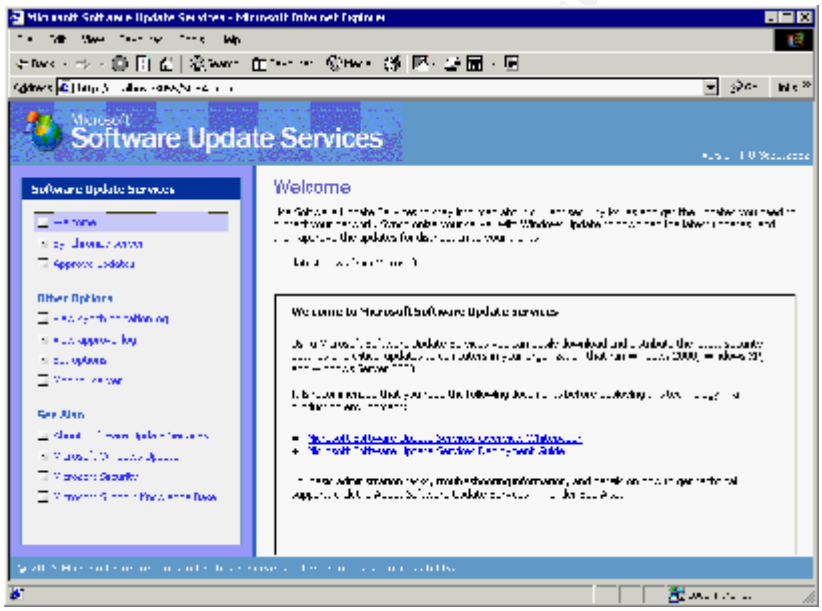
As the name implies, SAVF incorporates message filtering – actually, extensive filtering. Through its web-based interface, the filtering modules can be configured to block, quarantine, delete, or simply report on message and attachment size, subject, source, content, context and scoring/weighting. While the filters are effective, a modest amount of SPAM/Unsolicited Commercial Email (UCE) must still be handled manually be each individual user. As with most SPAM filters, some wanted messages are also blocked, but can be released from the Quarantine server. In spite of its configurability, SAVF works mostly from the principal of denying unwanted/unauthorized eMail (blacklist style) rather than allowing wanted/authorized eMail (whitelist style.) Just as this principal would prove to be most flawed for the design of a firewall, it is equally as flawed in the management of electronic messaging. The frustration with SPAM and blacklist/filtering software has driven many to predict the demise of the Internet as a tool for communication.[5] Hence, it is most likely that some form of hybrid white/blacklist server will eventually be implemented.

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

Managing Updates

A combination of factors (sloppy coding, careless configuration, number of Internet users, ignorance/prowess of Internet users, etc.) over the past decade has led to what today is often a cacophony of announcements identifying the next bug or exploited flaw. Although no platform or environment is immune to this, the market dominance of Microsoft® Windows has granted it the position of market leader in over-exposure.[6] Subsequently, patch upon patch is released to correct not only these 'critical' issues but also more isolated issues relating to performance, interoperability, and such.

In order to help users keep up with the volume of updates and to help them better understand what needed to be updated, Microsoft® began developing online sites to automate the analysis and updating of a user's computer. Today, there exists both Windows Update (http://windowsupdate.microsoft.com) for their OS and Office Update (http://office.microsoft.com/productupdates) for their productivity suite. Both of these update sites have evolved quite nicely such that a diligent, knowledgeable user (no, that's not always an oxymoron) can manage the necessary updates for their individual computer. But alas, I had a bit more than a user or two with which to deal, let alone the aforementioned oxymoron. Before long, the process in my environment was deteriorating into haphazardness.



Microsoft® eventually released Software Update Services (SUS). SUS is an IIS based application that serves as a corporate local distribution point for Windows clients configured with the Automatic Updates client. I implemented the group policy template included with SUS to point all corporate clients to the SUS server and to control the deployment schedule. I configured SUS to query for and retrieve all of the updates available from Windows Update. I was then able to select which updates to approve for deployment at the next scheduled cycle.

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

This process decreases the Internet bandwidth consumed for update downloads, and of course benefits Microsoft® by decreasing the load on their update distribution servers. SUS SP1 was just released and provides the following enhancements:

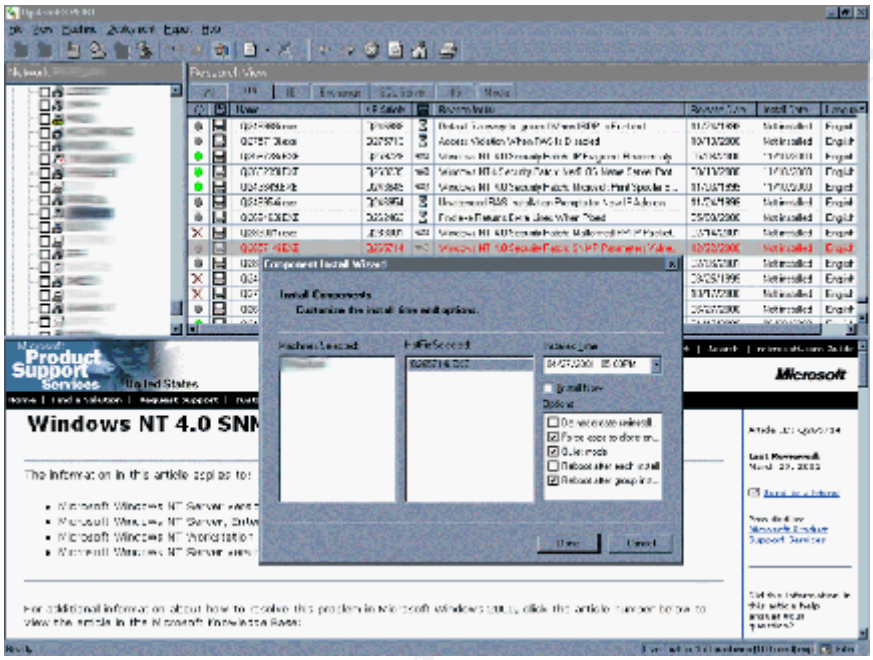
- Ability to run on Windows 2000 domain controllers and Small Business Server
- Better integration with IIS Lockdown
- Details links of software update packages
- Installation under the default IIS web sites
- Increased proxy server time out
- New software catalog files

In addition to the list above, there is better deployment control. Should a client system happen to be shutdown prior to a scheduled deployment, when the client does restart and the Automatic Updates service restarts, after a specified timeout, the updates can be applied (rather than delaying until the next scheduled update cycle) and a warning will be displayed for the logged on user five minutes prior to any required reboot. However, for all that SUS does, it only deals with client OS's that are Windows 2000 or newer; and it only manages updates normally available via Windows Update.

The search for a more complete process led to the evaluation of a few products including those from Gravity Storm, Shavlik and the one which I implemented – that being UpdateExpert from St. Bernard Software. Each product has continued to improve since my original evaluation. UpdateExpert enables remote analysis, "Querying," of all Microsoft® Windows NT based OS's. A "Query" is the equivalent of parsing the Windows Registry to identify that which has been installed. This process is rather fast, generating the least amount of overhead on the target system yet can yield unreliable data. Sometimes installed updates can be overwritten by each other or perhaps by the installation of another application. Thus, there is "Validation", which ensures the correct installation of each update. When "Validation" is selected, UpdateExpert warns of the extra resources required to complete the process. The data generated by a "Query" is compared against a database that is maintained by St. Bernard Software. The local copy of the database is automatically updated by subscription over the Internet into UpdateExpert. The database covers not only the OS, but also Internet Explorer, Exchange, SQL Server, Windows Media, MDAC, Outlook, and Office. The types of updates not only include those publicly available, but also those which may be relevant to my research yet require a phone call to in order to specifically request and obtain. Nicely enough, I was also able to build custom packages and have them made available for deployment in addition to those in the UpdateExpert database. Once acquired, any update that is not normally downloadable directly from the console, can be added to repository of updates by right-clicking on the relevant research item in the console and selecting "Locate." Through the console, each update I wanted to use was downloaded to the central repository.

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

Deployment of updates encompasses all necessary "chaining" of packages, timing of installation, reboots, and real-time status of each package deployed to each client during the process. While the forced reboot of a client can be specified, I found that that was normally only an issue where I had not executed a reboot process across all the clients prior to update deployment. One of the most likely ways to have an update go awry is to allow it to execute when the system has not been rebooted in a few days or when the user remained logged in, but locked the system – this led to a policy requiring users logout rather than lockout after hours.



The UpdateExpert console presents a unified 3-pane view of all computers (managed and unmanaged), the relevant updates for each, and the web page(s) detailing the update information and availability. To complete the product, St Bernard includes the ability to set deployment policies of required updates and to generate nicely formatted reports from system "Queries."

Deeper: Analysis & Prevention

Even with all of the updates and perimeter security being actively managed, there still remains the issue of elemental system configuration details. I needed to manage all the details about which I knew, along with the ones that had evaded my radar. Microsoft® provides the Security Configuration Management (SCM) console, along with a set of templates that can be used for both for initial configuration and later review/auditing. SCM templates can be deployed via Group Policy for Windows 2000 domains, but SCM does not provide much in the way of reporting. Beyond that, there is a wealth of information available via toolsets, whitepapers, checklists, and guides – some of the most thorough being made available by the NSA at http://www.nsa.gov/snac/index.html. Yet for this environment, automation and expedience were very critical. What is the status of

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

each system? Has anything changed since the last analysis? What remediation can be done? Can I perhaps prevent future, as of yet unknown, threats?

A search of the available toolsets pointed me to Harris® Corporation, a resource which was new to me at the time. In the late 1800's, the Harris brothers began turning their tinkering into a business. This firm has withstood the times, merging, evolving, and adapting whenever necessary. Today, Harris® Corporation is a global electronic communications company. The area of specialty that caught my attention was their Security Threat Avoidance Technology (STAT®) http://www.STATOnline.Harris.com. The STAT® products are broken out into two areas of focus: Vulnerability Management and Behavior Based Intrusion Prevention.

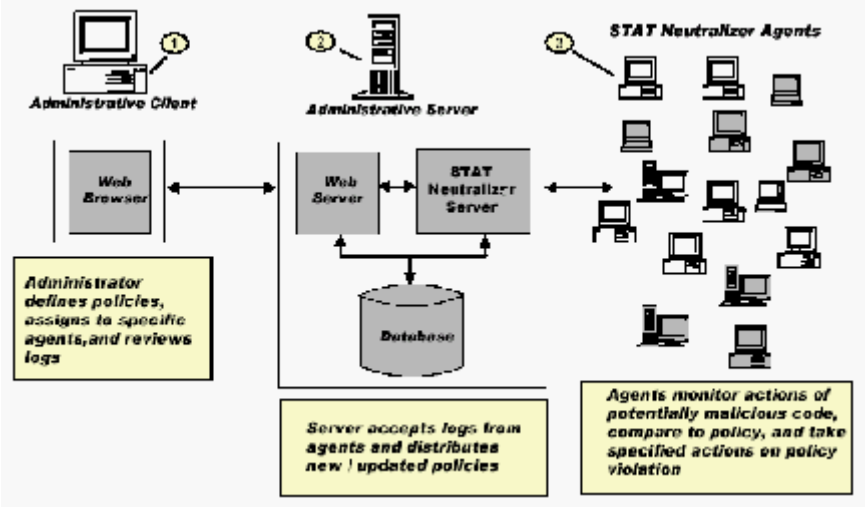
From the Vulnerability Management side, I selected STAT® Scanner. More elaborate analysis, reporting and integration of third-party tools are available via STAT® Analyzer and Console; yet those items are more relevant to an enterprise environment that is also likely to be less homogenous. There are literally thousands of vulnerabilities in the STAT® Scanner database against which each scanned system is evaluated. Monthly updates to the database are made available for download to subscribers. It was of great significance that I could work with the threats that imposed specific risk to my systems. Many of the vulnerabilities can be remedied via the AutoFix feature available in the console. From within the console, most of the OS tools that would normally be used for manual remediation or investigation, are available on the toolbar. Target systems include Windows 95 through Windows XP, Red Hat® and Mandrake® Linux, and Sun® Solaris Unix … even routers and network printers. Protocols include TCP/IP, NetBEUI, and Novell® IPX/SPX. Systems can be scanned by name, address, or range. Scanning can be initiated via the console or the CLI (command line interface) thus allowing for automation and scripting. Scan results can be reviewed immediately in the console, stored for later review, or emailed. When reviewing the scan results in the console, each vulnerability identified is categorized and described in detail along with the solution for remediation. Also included are links to information resources on the Internet wherever possible. References are identified from CVE® (Common Vulnerabilities and Exposures), SecurityFocus®, the Microsoft® KnowledgeBase, and each related vendor site. The CVE® dictionary has proven to be useful in providing additional reference pointers to research information. There are more than ten different types and levels of reporting by default. I was able to generate very detailed reports for my use in establishing baseline status and evaluating remediation, while providing more executive level reports for communicating progress and goal completion to management.

Behavior blocking is a category of security tool that has come into its own over the past couple of years. Prevention of undesirable system activity can be related to antivirus software, in such that fingerprinting (comparison of objects against a database of known offenders) and heuristics (analysis of a programs

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

overall logic and structure in order to assess its likelihood of malicious intent) are used to block programmatic behavior from causing potential damage.[7] However, neither fingerprinting nor heuristics have been able to adequately cope with the rapid and dynamic spread of new and/or modified viruses and trojans via networked systems. Thus, again, why allow what shouldn't be? Define permissible behavior and prevent all else. Ultimately, this is a most effective solution in choking off the rampant spread of known and unknown viruses, trojans, and the like – whether used to supplement traditional antivirus products or perhaps eventually in replacement of such.[8]

Quite a few companies have products offered in this area, including Aladdin, Finjan, and Tiny Software, to name a few. Since my experience with Harris Corporation was already favorable, I proceeded with their STAT® Neutralizer and found it to be a superb product. The agents, currently available for Windows NT 4.0 and 2000 (Linux and Solaris are forthcoming), act in accordance with the policy established by the server. Policy customization and deployment is accomplished via a web-based administrative console. Policy is enforced from the kernel level up and takes into account action and context. As with other blocking technologies, there are false positives that must be corrected, but the central policy management does help ease that process.



Summary

Indeed, this journey has no end. Yet, the tools available today have evolved so far beyond their humble beginnings. Today, most every process that encompasses security management is available in a secure remote method or tool. The savings in time and energy, let alone the confident awareness of security issues, for me and for the rest of the company, add up to a significant ROI. This small business, fortunately, was willing to acknowledge the threats and evaluate the risks to their establishment. Thus, appropriate resources were allocated and I was able to assemble a toolset worthy of the tasks.

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

Citations

1 Cisco® Systems Inc. "Perimeter Security." http://www.cisco.com/warp/public/732/net_foundation/perimeter_security.html (1-Feb-03)
2 DeShon, Markus, PhD. "Intrusion Prevention versus Intrusion Detection." http://www.secureworks.net/techResourceCenter/fullTechArticle.php?article=IpsVsIds (1-Feb-03)
3 Danielson, Jeff. "Wireless Security: Blackberry by Research In Motion." (18-Feb-2002) http://www.sans.org/rr/pdas/blackberry.php (1-Feb-03)
4 DiVittorio, Terry. "Security Within the Organization: Everyone Has a Role." http://www.eds.com/thought/so_securityorg.shtml (1-Feb-03)
5 Berlind, David. "Why spam could destroy the Internet." (14-Nov-2002) http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2897473,00.html (1-Feb-03)
6 Ulfelder, Steve. "Practical Patch Management." (21-Oct-2002) http://www.nwfusion.com/supp/security2/patch.html (1-Feb-03)
7 Nachenberg, Karrie. "Behavior Blocking: The Next Step in Anti-Virus Protection." (19-Mar-2002) http://online.securityfocus.com/infocus/1557 (1-Feb-03)
8 Conry-Murray, Andrew. "Product Focus: Behavior-Blocking Stops Unknown Malicious Code." (5-Jun-2002) http://www.networkmagazine.com/article/printableArticle?doc_id=NMG20020603S0009 (1-Feb-03)

© SANS Institute 2003, Author retains full rights.

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

Last Updated: September 5th, 2015

Upcoming SANS Training

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

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
Security Leadership Summit & Training	Dallas, TXUS	Dec 03, 2015 - Dec 10, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced