



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at <http://www.giac.org/registration/gsec>

GIAC Security Essentials Certification (GSEC)
Version 1.4b
Option2

Security Vulnerability Assessment Tools

By: Amir Emamjomeh

June 10th, 2004

© SANS Institute 2005, Author retains full rights.

Contents

Introduction.....	3
Pros and Cons.....	4
Comparison.....	6
Architecture.....	9
Installation.....	10
Conclusion.....	11
Definitions.....	12
More Tools.....	12
References.....	13
Disclaimer.....	13

© SANS Institute 2005, Author retains full rights.

Introduction

Security scanners assess network infrastructure vulnerability; most scan different flavors of OSs, applications, and databases (UNIX, Windows, Cisco OS, MAC OS, HPUX, LINUX, NOVEL Netware, Wireless). Security scanners identify security problems that could allow a malicious user to gain access to your computer systems. There are security tools that can perform intrusion detection, historical tracking, and forensic analysis. However, this paper focuses on security scanners.

There are many security scanners on the market; each has different features and capabilities. The two commercial tools addressed here are Internet Security Scanner (ISS) version 7.0 from Internet Security Systems and Enterprise FoundScan 3.5 (FS) from FoundStone Technology.

ISS and Found Scan both provide vulnerability assessment of the following:

- network infrastructure
- hardware
- software
- firmware
- firewalls (most versions)
- routers
- switches
- applications

© SANS Institute 2005, Author retains full rights.

Pros and Cons

The following section briefly lists the pros and cons of both ISS and FS. For more details, see [Comparison on p.6](#).

Internet Security Scanner

pros

- easy-to-use GUI
- minimal learning curve for Graphic User interface
- up-to-date vulnerability checks
- no database administration required
- uses MSDE—a stripped-down version of SQL Server without license costs
- reports in PDF, GUI, html, and rtf format
- detailed checks per registry, Denial of Service, Windows Patches, Trojans
- excellent knowledge base for researching vulnerabilities
- MAC address identification on canned discovery reports
- informative online help
- multiple hosts discovery policies.
- added functionality for troubleshooting during host discovery
- SANS top 20 policies

cons

- wireless scanning only scalable with additional modules (exist as defaults in FS)
- no GUI with database
- reports must be downloaded through SQL scripts
- third party tool and SQL scripting required for custom reports
- cryptic-based vulnerability checks are not intuitive
- learning curve required for ISS checks and usage
- no automatic express update functionality

FoundScan Security Scanner

Pros

- nice GUI, and HTML reporting
- thorough explanations of each vulnerability
- good upper management reports
- wireless module included in default installation
- application and rogue application detection
- no learning curve for FS vulnerability checks
- informative online help
- useful HTML output with network map, IP address location and charts per breakdown per IP address, OS type
- Detailed Denial of Service Scanning
- history and vulnerability tracking
- help desk and assigning ticket capability
- automatic express update functionality
- scans are easily scheduled and set as active or inactive
- SANS top 20 policies

cons

- difficult to extract information from reports
- lengthy HTML reports
- scan engine is very different than Web portal; both tools require learning curve
- training is required for full tool usage
- Database Administration functions are required for maintaining the MS SQL database (additional overhead).
- knowledge of SQL Database and SQL scripting necessary to create custom reports
- IP addresses have to be exactly in sequence as license permits
- host discovery information is buried in database
- FS checks are not as detailed as ISS
- cumbersome extraction of MAC addresses buried either in reports or in database
- no search capability when finding vulnerability while creating policies
- scans logs do not give enough information for troubleshooting

Comparison

ISS is a detailed OS scanning tool that detects Windows registry issues and vulnerabilities. FS checks are less detailed and more high-level. Both ISS and FS have almost the same vulnerability checks and wireless scanning capabilities. With ISS, however, you have to use definitions not available in the default installation. FS has a default module policy geared toward wireless scanning, and general UNIX vulnerabilities are more toward SUN Solaris and Windows. ISS identifies and checks each flavor of UNIX operating systems in detail. ISS has greater checks for backdoors and Trojans. FS has almost the same checks but is limited on backdoors, NFS, RPC, and a limited number of other flavors of UNIX.

There is a minimal learning curve required to start using ISS 7.0. Policy templates and formats are all in xml format.

ISS 7.0 uses a stripped-down version of SQL Server for workstation called MSDE. MSDE is free SQL Server you can download and use without licensing requirements and costs. There is no GUI for MSDE database. You must install a third party tool to obtain preferred data from the MSDE database. If you require more data output than what the canned reports provide, then you must use other tools or hire an SQL developer for your special needs, unless you prefer to learn SQL.

A tool that ISS provides for extraction of data from ISS 7.0 without SQL custom scripting is called Site Protector. Information extraction is a benefit because this tool uses the ISS logs to extract any relevant data and information.

FS is more complex and requires a longer learning curve. FS can be configured as a two and three tiered architecture enterprise-scanning tool. FS was designed to provide security assessment with enterprise architecture in mind. The GUI is somewhat complex to use due to built-in enterprise features.

Like ISS, FS has canned templates and policies that you can use to scan your network. FS policy creation is well laid-out and easy to use due to its extensive library and intuitive vulnerability descriptions.

FS has good detailed canned reports with colorful GUI charts that show your vulnerabilities to upper-level management. Charts are good for upper management but not good enough for administrators who have the responsibility and tasks of applying patches and remediation.

With FS you can create user accounts for each administrator on your staff. This a excellent feature that can be used for administrators who are responsible for various systems. Another great feature is FS history tracking. History tracking is a great and excellent tool for tracking remediation done by your administrators.

Two Security Vulnerability Assessment Tools

FS policies are organized in different modules including web, UNIX, Trojans, Windows, wireless, intrusive and non-intrusive.

ISS and FS use their own numbering schema for assigning a number to their vulnerability. There is a common vulnerability number assigned by the organizations called CVE. However, not all vulnerabilities that are found under each tool have an assigned CVE numbers. There are numerous vulnerabilities in both tools that do not have a CVE, but only their proprietary assigned numbers.

There are many checks in FS that correspond to those in ISS. The ratio of checks between both tools can be categorized as one to one, one to two, one to many, many to one, many to two, and many to many.

The number of checks in ISS is approximately 1300. FS checks are close to 1200, which include a wireless scanning module. Under ISS, the wireless module is an add-on that requires an extra definitions file. Nevertheless, if you remove the wireless module for FS you cut 30% of your vulnerability scanning definitions.

Both tools use GUI and have command line capability. ISS has a simple GUI and lacks the features of FS, but it is sufficient and extremely powerful. FS uses a much more complex GUI with features that include GUI scheduling, and network mapping that is a feature that ISS lacks. FS and ISS complement each other with their colorful high-level charts, detailed HTML reporting. FS can add extra users, view and generate reports, and helpdesk ticket functionality. FS is an enterprise tool, but the GUI is more time-consuming to learn. FS offer many features for the money, but if you are a busy IT security professional, you will not have enough time to use all its features.

Both tools require MS MSDE SQL database. With ISS, you need a workstation with appropriate RAM and hard drive. Under FS, you can use FoundScan Pro with MSDE same as ISS, but this type of scanning tool is mostly used for small to medium size organizations. Under FS Enterprise you need to install and configure a standalone MS SQL Server dedicated for scanning, a workstation for an FS engine as recommended by the vendor, and a dedicated IIS web server. In addition, you need to install a few more extra plug-in that you must download before installing the vendor-provided software.

In ISS, help files are easy to find. They provide lots of information on remediation and URLs that help you download patches. Also under Windows, ISS menus there is a catalog that lists all new vulnerabilities per vendor assigned numbers, the related OS vulnerability, explanation of the vulnerability, CVE number validation, URL links to available patch download and assessment centers. A CVE number is a number assigned to vulnerability. <http://www.cve.mitre.org>

FS help files are in scan output and while enabling vulnerability checks, you can highlight each check, which gives information regarding a particular vulnerability. FS

Two Security Vulnerability Assessment Tools

does not have the same help features as ISS does, but unlike ISS, FS has other advantages like plain English and easy- to-understand vulnerability checks. ISS has a good canned reporting capability for line technicians, administrators, and corporate management. You can view the reports online before generating them into PDF, html or rtf format. Using the FS default installation, reports can only be generated in html.

In ISS, you have to use SQL scripts to generate reports. The current version of ISS uses MSDE SQL Server for workstation. Unless you download or purchase a third party tool to generate general custom reports you must use canned ISS reports. One of the advantages in creating custom reports is that in a organization with more than 500+ IP addresses and many vulnerabilities, reports can be large—thousands of pages. Each Vulnerabilities can take up to two pages. Custom reporting is required for your, management and the administrators who are responsible for remediation.

Several useful features in FS reports include the following:

- network map
- detailed breakdown of vulnerability per IP addresses
- DNS
- MAC
- NETBIOS name

If you have full access to a SQL database you can also download required data in CSV format. The only draw back is that needed information for the administrators is buried deep in various html reports. Administrators, which need to use this information, must spend a lot of time learning and digging through various web pages in order to extract this information.

When configuring FS you should consider learning database operations or hiring a database administrator to tune and administer your database. As stated before FS Enterprise requires a separate Microsoft SQL Server for capturing scan information. ISS on the other hand uses MSDE, which does not require database maintenance.

<http://www.microsoft.com/windowsserver2003/default.msp>

MSDE and MDAC plug-ins can be located from ISS or Microsoft websites.

<http://search.microsoft.com/search/results.aspx?st=b&na=88&View=en-us&qu=MSDE>

Architecture

Per vendor recommendation the minimum requirement for large scans are as follows: “For ISS installation is Pentium 4 with 1GHz or faster with 512MB of RAM or greater for the scanning machine. But for small to medium organization a Pentium II 600 256MB RAM, and 300MB hard drive”.

http://documents.iss.net/literature/InternetScanner/IS_SR_7.0.pdf

In my experience, the minimum configuration is sufficient to run scans in a small to medium size organizations and a Pentium 4 with 1GHz and 512MB RAM for medium to large size organizations with heterogeneous network is sufficient. Of course, greater the amounts of RAM the more scanning power. For more information regarding ISS, you can check out the vendor or follow the URL.

The minimum recommended vendor configuration for FS Enterprise is as follows: “For the two tier architecture system, one Web Server with Dual Pentium III, 733MHz or higher with 1GB RAM, second system is FS database Dual Pentium III 733Mhz or higher 1GB RAM with 2GB partition, both dedicated system. For three-tier architecture, the scanning engine is running on the similar systems with 1GB RAM. The SQL server memory needs to be 450MB to 1GB RAM. The above information can be found on vendor’s web site at <http://www.foundstone.com>, products, and minimum system requirements”.

© SANS Institute 2005, Author retains full rights.

Installation

ISS

It is highly recommended to backup your system before proceeding with installation. Before downloading ISS itself, download and install Microsoft MSDE and MDAC plug-in for Windows 2000 Workstation. Sometimes these updates do not install properly. In case of an issue; perform the following:

1. Uninstall all updates.
2. Reboot.
3. Install each update and reboot before installing the next plug-in
4. Install the application
5. Install all appropriate express updates (XPU)
6. In case express updates did not installed properly. Uninstall all express updates, reboot, and install each updates ten at a time.
7. Test your work by starting ISS and looking at general tab for any error.
8. For advance troubleshooting, refer to customer service.

FoundScan

With FoundScan, there are three separate installations.

1. Install a full version of MS SQL Server on a dedicated system with all available patches from Microsoft.
2. Install MSDE for workstation on a separate system.
3. Install FS engine separate system.
4. Install IIS Web Server on a separate system for better performance.
5. Point the FS engine to MS SQL Server.
6. Tune MS SQL database for better performance.
7. For advance troubleshooting, contact the vendor.

With FS engine, you can run your scans from the console. To use the full capability, install a dedicated Windows web server running IIS processes so you can run the web interface for FS.

With web server installation, you can start your scans from PCs at different locations. Of course, you will need to harden all your servers with Microsoft security patches. One drawback, the web portal and the console GUI are not alike. After you have installed both, spend a few days mastering each tool. FS has many features in its GUI, both on the engine and on the web portal. An information security administrator or manager in fire-fighting mode may find it impossible to use the numerous FS functions.

Conclusion

Both FS and ISS are some of the best tools on the market. Each tool has its own advantages and disadvantages. Neither tool gives you the reporting structure that may be demanded from upper management.

Both tools can be used for confirmation and validation assessment of your LAN, WAN, and remediation of your organization vulnerabilities. The use of each tool will give your organization a greater power in detecting and plugging holes in your organizations network and info-structure.

Both vendors complement each other with their excellent knowledge base and customer service. They are excellent source for searching vulnerabilities and remediation as well as application troubleshooting. FS and ISS customer service are excellent source of information. They are, professional, knowledgeable and can answer complex questions. Additional resources are available in each of the vendor knowledgebase.

ISS XForce database – <http://xforce.iss.net/xforce/search.php>

FS Knowledgebase – <http://support.founstone.com>

I really cannot recommend which one tool over than the other. Both tools are one of the best tools available on the market. Every IT security manager uses a different style in detection, assessment and remediation. FS and ISS both complement each other in strength and weaknesses. In conclusion, you have to decide which tool is best meet your organization needs.

© SANS Institute 2005. All rights reserved.

Definitions

backdoor	Undocumented way of access to a program
CSV	Comma-Separated Value, used for database import and export
CVE	Common Vulnerability and Exposure
GUI	Graphical User Interface
HPUX	HP UNIX
HTML	Hypertext Markup Language
LAN	Local Area Network
MS	Microsoft
NFS	Network File System
PDF	Portable Document Format used by Acrobat Reader
RPC	Remote Procedure Call
RTF	Rich Text Format
Security Administrator	A person designated for remediation vulnerabilities
Trojan	Programs devised by hackers to detect activities on PC
vulnerability remediation	patching or fixing system vulnerabilities
WAN	Wide Area Network
XML	Extensible Markup Language

More Tools

The following are commercially available scanning tools:

- Retina from eEye Digital Security - <http://www.eeye.com/html/products/index.html>
- Internet Security Scanner from ISS - http://www.iss.net/products_services/products.php
- FoundScan from Found Stone - <http://www.foundstone.com>
- Cyber Cop from Network Associates - http://www.networkassociates.com/us/products/enterprise_productlist.htm
- Net Recon from Symantec - <http://enterprisesecurity.symantec.com/content/productlink.cfm>
- Saint from Saint Corporation - http://www.saintcorporation.com/products/saint_engine.html

The following are some of open source security scanners:

- SARA - <http://www-arc.com/sara/>
- Nessus Security Scanner - <http://www.nessus.org>

References

- Internet Security System - <http://www.iss.net>
- Common Vulnerability Exposure - <http://www.cve.mitre.org>
- ISS XForce database – <http://xforce.iss.net/xforce/search.php>
- FoundStone knowledgebase – <http://support.foundstone.com>
- MSDE Download –
<http://search.microsoft.com/search/results.aspx?st=b&na=88&view=en-us&qu=MSDE>
- Microsoft Windows SQL Server –
<http://www.microsoft.com/windowsserver2003/default.msp>
- ISS installation requirements –
http://documents.iss.net/literature/InternetScanner/IS_SR_7.0.pdf

Disclaimer

The content of this paper which, is based merely on opinion, consists of information about two security tools and their features based on experience.

© SANS Institute 2005, Author retains full rights.

Upcoming Training

Click Here to
{Get CERTIFIED!}



SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event