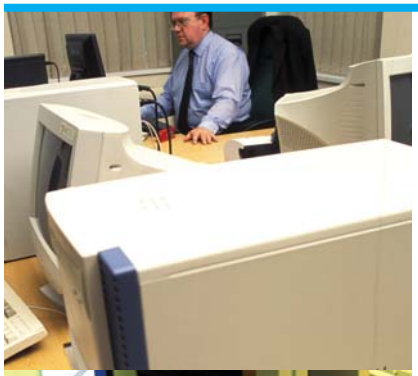
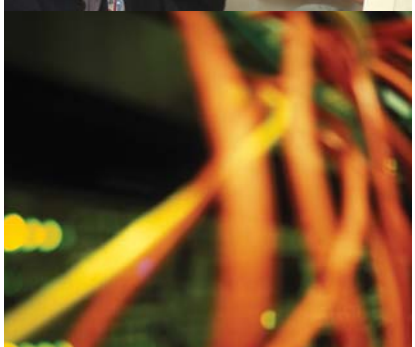
VULNERABILITY ASSESSMENT
TECHNOLOGY REPORT

ISS Internet Scanner





OCTOBER 2006

WEST COAST LABS
www.westcoastlabs.org

CONTENTS

ISS Internet Scanner

Internet Security Systems, 6303 Barfield Road, Atlanta, GA 30328,
USA Phone: +1-404-236-2700

Test Environment and Network 3

Test Reports and Assessments 4

Checkmark Certification – Standard and Premium 5

Vulnerabilities 6

West Coast Labs Vulnerabilities Classification 7

The Product 8

Developments in the Internet Scanner Technology 9

Test Report 10

Test Results 17

West Coast Labs Conclusion 18

Security Features Buyers Guide 19

West Coast Labs, William Knox House, Britannic Way, Llandarcy,
Swansea, SA10 6EL, UK. Tel : +44 1792 324000, Fax : +44 1792 324001.
www.westcoastlabs.org

TEST ENVIRONMENT AND NETWORK

For this Technology Report, West Coast Labs engineers created a network infrastructure similar to that found in most corporate IT environments. Each solution entered into this Technology Report was required to perform vulnerability tests against this network.

The network used by WCL consisted of between 20 and 30 distinct hosts, and included routers, managed switches, network servers, client machines, and printers. Included within the available services were web servers, mail servers, file and database servers. Customized web applications, designed by engineers at West Coast Labs and containing common scripting errors, were installed on servers across the network.

A variety of Operating Systems were used on the network, on different hardware platforms. A number of virtual hosts were also included. In building the network, some of the machines and services were installed with default settings. Various levels of patching were applied across the range of Operating Systems. In addition, a number of common mis-configurations were made in setting up and deploying particular services. Every host on the test network was imaged prior to testing, and restored to the original state before each round of testing for the individual solutions.

The test network was protected by a router, and ACLs were set to restrict access to the test network to and from IP addresses specified by the participating vendor, if appropriate. If the solution under test needed no Internet connectivity then the router was configured to block all access to and from the Internet for the period of test.

The test network was available to each solution for a 48 hour period.

TEST REPORTS AND ASSESSMENTS

WCL have assessed the individual vulnerability assessment reports from each solution on the following basis, with Vulnerabilities on the target network classified under 4 headings:

Critical vulnerabilities – those that allow an attacker with minimal knowledge or skill to compromise the integrity of the network: this may include gaining control of a server or network device, gaining illegitimate access to network resources or disrupting normal network operations.

Severe vulnerabilities – those that allow illegitimate access to, or control over, network resources, but that require considerable knowledge or skill on the part of the attacker.

Non-critical vulnerabilities – those that allow attackers to gain access to specific information stored on the network, including security settings. This could result in potential misuse of network resources. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on hosts, directory browsing, disclosure of filtering rules and security mechanisms.

Information leaks – these allow attackers to collect sensitive information about the network and the hosts (open ports, services, precise version of software installed etc.)

The performance of each solution under test was evaluated on the following criteria:

- The ease of deployment of the solution
- The number of vulnerabilities correctly identified in each class
- The completeness of the report, including identification of any network changes made
- The clarity of presentation of the findings

CHECKMARK CERTIFICATION

Soilutions under test in this Technology Report are eligible for the Checkmark Vulnerability Assessment certification.

In order to achieve the Standard Checkmark Certification for Vulnerability Assessment the candidate solution must identify at a minimum 100% of the Critical Vulnerabilities and 75% of the Serious Vulnerabilities.

However, those developers identifying 100% of the Critical Vulnerabilities and a minimum 90% of the Serious Vulnerabilities will be awarded the Premium Checkmark Certification for Vulnerability Assessment.

www.check-mark.com

VULNERABILITIES

To ensure that the test network mirrored that found in many businesses, a variety of operating systems, on different hardware platforms, were included. A Windows domain was set up using a Windows 2003 Server and a mix of workstations running Windows XP and Windows 2000 Professional. Some Sun Servers running various Solaris distributions provided web services and file storage, assorted Linux boxes were included running Debian and RedHat distributions, and a host running BeOS completed the mix.

Some of the servers were installed with default settings and varying levels of patching were applied: some hosts were patched fully up to date while others had been left out of the process. Also, a number of common mis-configurations were made in setting up servers, and deploying particular services. For example, Windows servers were configured with open network shares, ftp servers with anonymous write access, smtp servers configured as open proxies. These are configuration errors that can have profound effects on network security but can easily be implemented by a hard-pressed administrator as a “temporary” quick fix to a connectivity problem.

The Windows 2003 Domain Controller hosted an UltraVNC server using a weak password, the DNS server itself was configured to be compatible with pre-2000 machines. Also installed on the PDC was IIS version 5.0 running default services. Alongside the Primary Domain Controller, a mail server was configured running Microsoft Exchange 2000, and this server also had an instance of UltraVNC running alongside popular game servers with known vulnerabilities.

One of the client machines was host to a vulnerable .ASP script written in-house by WCL engineers. This had a number of common programming errors in it allowing a user to bypass security measures using a number of different techniques.

A bank of Linux machines running a variety of Linux flavors and distributions completed the list of servers. The Linux systems were host to an array of services including FTP, sendmail, apache, and samba. Each of these was mis-configured with common errors, for example anonymous ftp access with write permissions and publicly writeable samba shares.

Each of the user client workstations were patched to different levels using official Microsoft Service Packs, historical patches and Windows Update. These machines then had different applications installed, ranging from popular game servers and UltraVNC through to IIS 5.0 and remote admin. Some machines were included in the Windows Domain. Back Orifice was installed on one machine on an unusual port.

The test network thus consisted of a series of machines with differing hardware specifications, operating systems, patch levels, and software installations, and multiple vulnerabilities. This Technology Report also saw the inclusion of common vulnerabilities found in software from leading vendors used worldwide along with those on the SANS Top 20.

WEST COAST LABS VULNERABILITIES CLASSIFICATION

As a basis of the test program, West Coast Labs engineers built a series of known vulnerabilities in the network on which each of the solutions was installed. To mimic those vulnerabilities found in many corporate IT environments, the risk level of these varied between Critical, Serious, and Minimal.

As part of the scope of testing and certification, particular attention was paid to how each of the products detected and classified those vulnerabilities deemed by West Coast Labs to be of either Critical or Serious risk.

So that the performance of each product can be clearly understood, this report contains some examples of the types of vulnerability listed as Critical and Serious.

CRITICAL VULNERABILITIES

- MS-Blaster patches not installed on servers
- FTP server with anonymous, writeable access
- Publicly available file shares using NetBIOS and Samba
- Blank Administrator passwords
- Back Orifice installations
- Open SMTP relays
- Completely unpatched operating systems (base installs)
- Base install of Windows Media Player 9 with no security patches
- Sun Solaris RPC vulnerabilities

SERIOUS VULNERABILITIES

- Partially patched operating systems to known levels
- Default or weak passwords
- VNC servers
- Popular game servers with known vulnerabilities
- FTP servers with non-writeable anonymous access
- Web sites with back-end scripting vulnerabilities
- Instant Messaging clients
- Virtual office software
- Microsoft Desktop Remote Access

The classification of the above vulnerabilities is based on information provided by external sources including the SANS Top 20, Bugtraq, and other well known vulnerability lists and sites.

THE PRODUCT

INTERNET SCANNER FROM ISS

ISS SAYS ABOUT INTERNET SCANNER...

The Internet Scanner vulnerability assessment application provides the foundation for effective network security for your small, medium or enterprise-sized business. Internet Scanner minimizes your risk by identifying the security holes, or vulnerabilities, in your network so you can protect them before an attack occurs.

http://www.iss.net/products/Internet_Scanner/product_main_page.html

ISS SAYS ABOUT THE INTERNET SCANNER BUSINESS BENEFITS...

Internet Scanner improves your network security, lowers business risk, increases up time and productivity, decreases cost of ownership and frees up time for security administrators to focus on vulnerability correction and security strategy issues. Internet Scanner can identify more over 1,300 networked devices, perform automated vulnerability scans of your assets and report on results. By assessing the security of networked systems and prioritizing remediation tasks, Internet Scanner allows businesses to address high-risk vulnerabilities before they are exploited in an attack. Furthermore, Internet Scanner is a highly scalable solution for both small to enterprise-sized installations.

ISS SAYS ABOUT THE INTERNET SCANNER TECHNICAL BENEFITS...

Internet Scanner provides:

- Unlimited asset identification,
- Robust asset management tools,
- Dynamic check assignment for speed and accuracy,
- A common policy editor for control and quick scan configuration,
- Real-time display options,
- The most extensive vulnerability catalog in the world, and updates from ISS' world-renown X-Force security team,
- Automatic vulnerability content updates,
- Remote scanning behind firewalls and in distant geographies, and
- Integration with SiteProtector for ease of management, reporting and analysis

DEVELOPMENTS IN THE INTERNET SCANNER TECHNOLOGY

AS STATED BY ISS...

Internet Scanner 7.0 contains the following new features and enhancements:

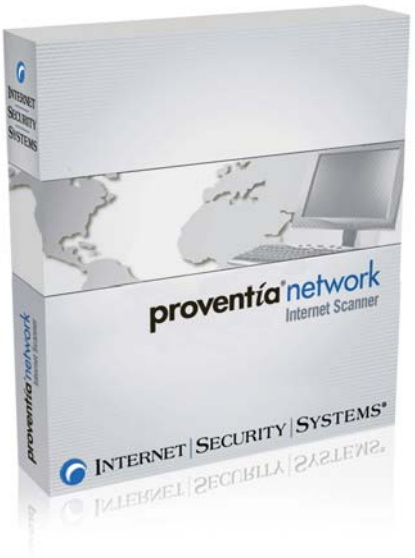
- Unlimited Discovery capability with valid license
- SiteProtector™ and SiteProtector's SecurityFusion™ support
- Enhanced scanning engine
- Enhance policy editor and scanning policies
- Host List Generator
- Enhanced command line interface (CLI)
- Simplified licensing mechanism
- Support for Microsoft Windows XP
- MSDE database support
- X-Force™ Catastrophic Risk Index scanning policy

http://www.iss.net/support/documentation/docs.php?product=7&family=9

TEST REPORT

INTRODUCTION

InternetScanner 7.0 is a software-based application that is deployed on a server within a network, and has no client based components. System requirements for this product are relatively low allowing the user more freedom in machine selection. This means that InternetScanner is potentially less of a drain on perhaps stretched hardware resources. That it does not require the latest technology, however, does not impact on its scanning ability.



The product was installed on an SMB environment created by engineers at West Coast Labs; this environment contained multiple vulnerabilities associated with this type of network and hosted an array of common applications and services.

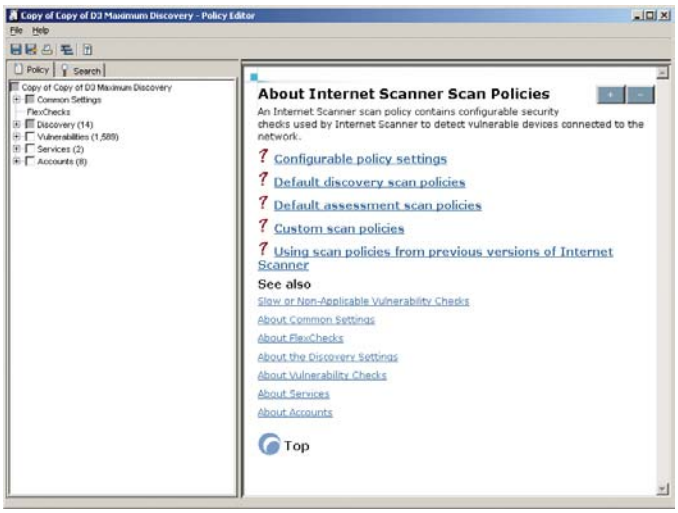
TEST REPORT

INSTALLATION AND CONFIGURATION

West Coast Labs Engineers installed InternetScanner on a Dell Optiplex 170L desktop. The installation method is very straightforward and allowed for a quick installation with no difficulties. During installation, InternetScanner performs a series of checks on the host computer to determine if it meets the system requirements. The progress of these checks is displayed on-screen and alerts the user should anything not meet the minimum requirements.

Once the installation is complete the user can begin the progress of configuring the solution to meet their individual needs. An Administrator may immediately begin changing options relating directly to the scanning methods, without the need to set up or configure any special users.

The setup of scans with InternetScanner is made simple via a well-constructed setup process. The user must first select from a large range of scan types or Policies, including the aptly named "kitchen sink" policy. This list contains many default Policies pre-installed by ISS and helps to further decrease the time between installation and the first set of vulnerability scans. The default policies include individual scans to check for the detection of specific vulnerabilities related to a variety of appliances such as Web Servers, Routers, and Switches.



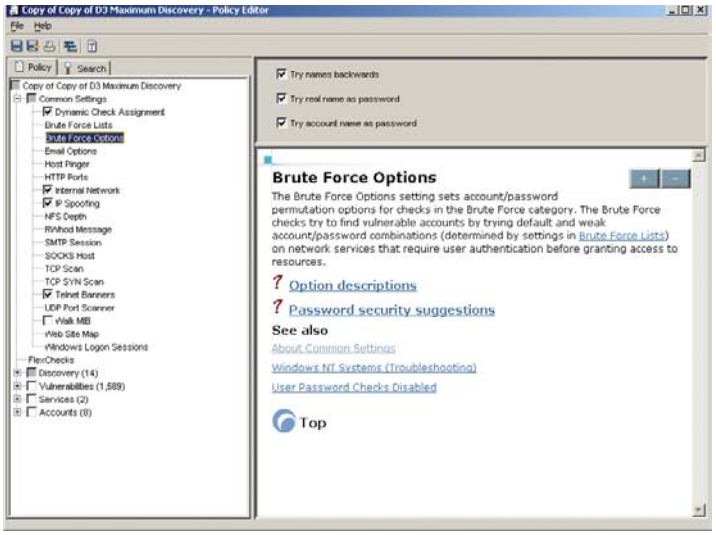
The list also hosts policies designed to search for vulnerabilities entered into the SANS top 20 list, along with four policies relating to the level of discovery required ranging from light to maximum. With the number of default policies available a perhaps already burdened Administrator or network team is not then required to spend time creating policies before the protection offered by InternetScanner can be utilized.

Should, however, the user wish to create a customized policy to best fit the needs of their network, then they can do this by simply selecting the option Derive New Policy. This presents the user with a new window, from which they are free to select from a number of options relating to the way in which the network is scanned. Included in these options is the ability to enable scanning for individual vulnerabilities, along with definitions of which services InternetScanner should try to detect.

TEST REPORT

Selecting the tab for Common Settings, the user is presented with an extensive list of options. From this point the user can control the way in which the target network is to be scanned, using options relating to fields such as Brute Force checks, web server mapping, and defining which ports are to be targeted across the network. Each of these settings is clearly labelled and described for the user, ensuring that the product is easy to use.

The Discovery and Services options relate to the method with which InternetScanner should look for running services and applications. If a corporation is happy that the target hosts are free from third party software then only a simple check is needed, while more cautious Administrators may use InternetScanner to thoroughly search each host.



When selecting from the expansive list of vulnerabilities, InternetScanner displays one of three icons depending on the severity of the vulnerability: red and green arrows for high and low risk, with a yellow square for medium risk. The Administrator may then decide whether to include the specific vulnerability in the scan based of this simple and effective risk assessment.

Should the Administrator require further information about any of the liabilities present in the organisation, simply clicking on the name of the entry displays the platforms that are at risk from the vulnerability along with a description and remedial advice. Below this advice, InternetScanner provides the user with links to related articles on the Internet from sites such as BugTraq and ISS' own X-Force. This information allows the user to make an informed decision about which vulnerabilities should be included in any scans.

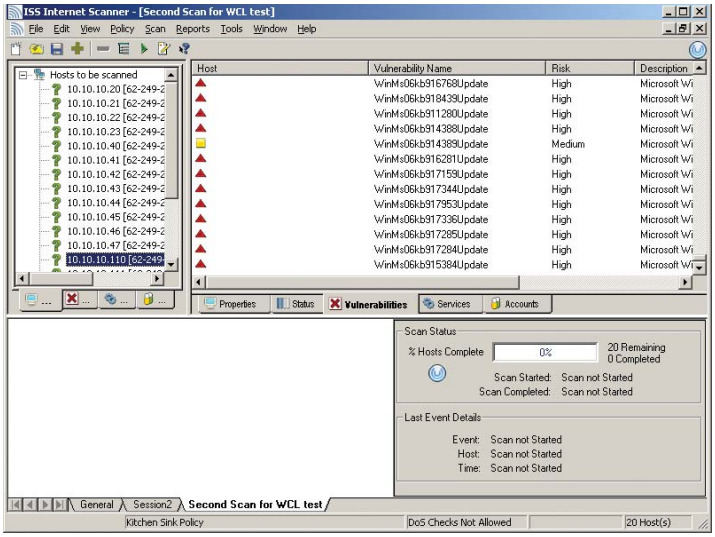
Also included within this setup screen is a help section that provides clear and concise descriptions of the options available.

When the user is happy with the options selected and the policy has been saved, the user is then asked to specify the target IP addresses. These can be entered in one of two ways - first, the target addresses can be entered manually as either individual addresses or as address ranges. While this first option may suit a smaller company, for larger companies containing possibly tens of thousands of addresses or hosts it could mean considerable time is taken up entering this data. To counter this, InternetScanner can read a list of addresses from either a .csv or .hst file.

TEST REPORT

It is in the area of customization and flexibility that InternetScanner excels owing largely to the number of options, or scan types, available. Due to this adaptability there can be a noticeable difference in the amount of time required to complete different scans. For example, one simple scan across a network can take less than an hour to collate results whilst a further, deeper, scan can easily take several hours to finish. This variety of scanning types and durations gives more freedom to a busy administrator who wants either to regularly monitor weaknesses in the network with a series of daily quick scans, or to run more exhaustive scans over a weekend or holiday period.

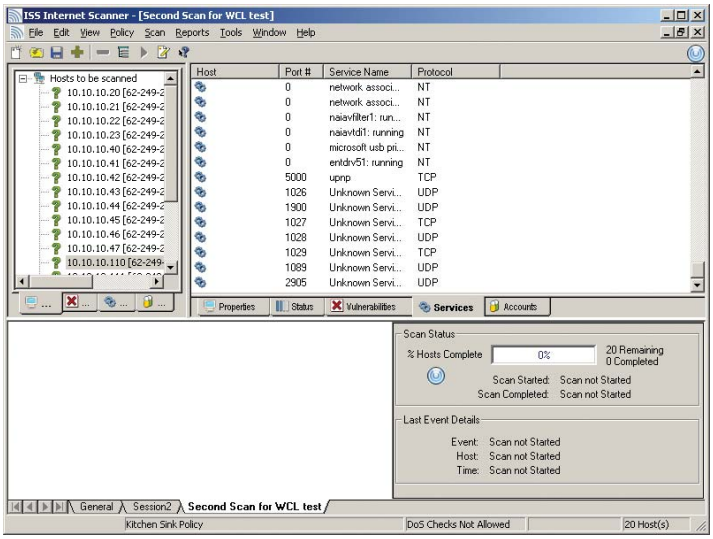
THE MAIN INTERFACE AND SCANNING



Once a scan has been created, the user enters a Session screen, and it is from here that they may access options relating to reporting, monitoring and detection - the Session screen acts as the point of control for the Administrator. Running along the top of the Session screen are a further series of options allowing for the addition of further IP addresses, report generation, and the commencement of scans.

Upon starting the scan, the Scan Status screen begins to update the list of hosts, defined earlier by the user, in real time. There are three main areas of the Sessions screen that relate to the currently running scan: the main area displays the list of IP addresses to be scanned, listed individually instead of in the ranges in which they may have been entered. Alongside the IP addresses are initially blank fields for information such as the Operating System, MAC Address, Domain and NetBIOS names - the InternetScanner engine fills in these fields as the scan continues, ensuring that the user is continuously aware of the progress of each scan.

TEST REPORT



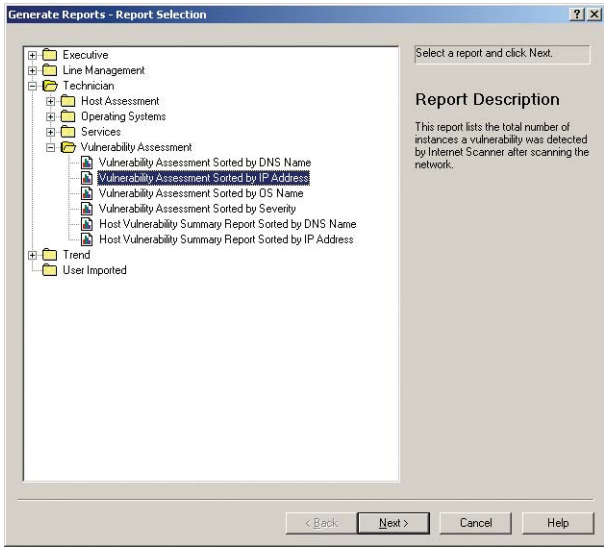
The second of the two remaining areas is split into Scan Status and Last Event Details. The former displays information such as the percentage progress of the scan, the number of appliances yet to be scanned along with the number of those completed, and the time the scan was started. Next to this is a blank field for the estimated time to completion of the scan. The latter half of this area displays the name of any system events, the host on which the event occurred, and the time the event occurred. The third and final area in the Scan Status screen is a system event screen that displays the date and time of the event along with a further, more detailed description of the event itself.

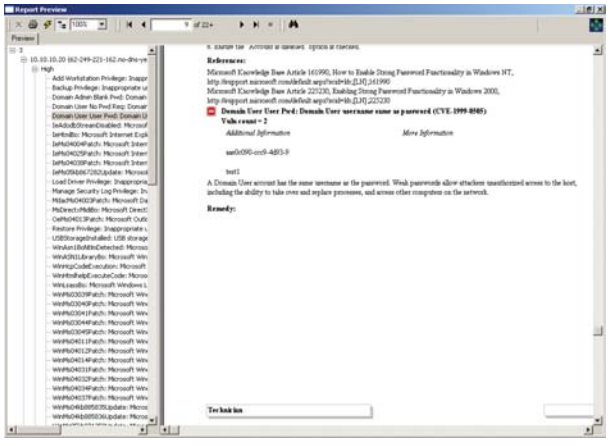
When the scan is complete the user can then use the options described earlier to save the session for later review. A user may then re-open a session at any point and can choose to either re-run the scan, view the data gathered the last time it was run, or to generate a report for the session.

TEST REPORT

REPORTS

Reporting with InternetScanner provides detailed insight into all detected vulnerabilities including remediation advice. The reports can be created to suit a number of different audiences ranging from the executive summary level to a more detailed technical output. Further to this, reports may be exported into a variety of common formats including PDF and HTML. These reports also include information regarding the operating system, installed applications, and the aforementioned recommended remediation steps.





Generating the reports based on an Executive Overview template, InternetScanner provides the user with a simple one page report showing the number of vulnerabilities and how many are classified as either high, medium, or low risk. This vulnerability count is also displayed as a chart which helps to demonstrate and compare the number of vulnerabilities detected. Information relating to the session, such as time, date, and number of hosts, is displayed near the top of the report.

However selecting to generate a report based on one of the technical templates, aimed at security teams or Network Administrators, significantly increases both the page count and the level of detail contained within. This increased level of data includes detailed remediation advice, information about the offending application or service, and information regarding the affected operating system.

TEST REPORT

When viewing the technical reports a list of IP addresses of the machines detected during scanning are displayed as a list onm the left hand side of the report. Clicking on these addresses presents the Administrator with the vulnerabilities grouped into categories of high, middle, and low risk. Selecting one of these categories the displays a further list of every relative vulnerability detected on the targeted host.

From this point the Administrator can view the above-mentioned remedial advice. This is in the forms of a set of clear and easy to follow instructions, allowing the Administrator to quickly mitigate the potential threat created by the discovered vulnerability. The ability of InternetScanner to sort the vulnerabilities by risk level also helps prioritise those vulnerabilities that pose the greatest risk.

TEST RESULTS

InternetScanner system requirements are very low, and due to this engineers at West Coast Labs were able to install the software on a standard Dell desktop machine. While a standard machine was of a high enough specification for an SMB size network, a larger company should consider installing InternetScanner on a high-end server for optimum performance.

Set up and configuration of the solution was straightforward and there were no problems encountered when either creating or running scans. An Administrator looking to create a series of highly customized scans would welcome the large number of individual options.

While some degree of digging is required to get to the information contained with the reports, InternetScanner provides a good level of information and very well presented and detailed remediation advice.

InternetScanner successfully detected 100% of the Critical vulnerabilities and over 90% of the Serious vulnerabilities on the West Coast Labs test network. The Internet Scanner software has been awarded the Premium Checkmark Certification for Vulnerability Assessment.

WEST COAST LABS CONCLUSION

InternetScanner 7.0 from Internet Security Systems is a highly scalable software-based security solution, providing a fast scan engine with an impressive number of options. The level of detail included within the reports equips any Administrator or network security team with the information required to secure an IT infrastructure.

InternetScanner goes a long way towards securing a company against threats posed by today's IT world. This is helped by an intuitive and quick update process that enables InternetScanner to constantly check for the most recent vulnerabilities.

SECURITY FEATURES BUYERS GUIDE

AS STATED BY ISS...

Internet Scanner has scanned more electronic assets and identified more vulnerabilities at more companies in the past 10 years than any other vulnerability scanning product.

In fact, 19 of the world's 20 largest financial institutions rely on Internet Scanner for vulnerability assessment and management.

KEY FEATURES

UNLIMITED ASSET IDENTIFICATION

Internet Scanner helps you keep an accurate inventory of the electronic assets connected to your network. It identifies more than 1,300 types of devices using Transmission Control Protocol (TCP) stack fingerprinting and an integrated NMAP asset database. User-defined extensions can be added to the database to enable custom asset identification.

DYNAMIC CHECK ASSIGNMENT

Internet Scanner's intelligent scanning agent increases scanning speed and accuracy by identifying the operating systems (OS) of target hosts, and then automatically running OS-specific checks to find vulnerabilities.

COMMON POLICY EDITOR

Internet Scanner's easy-to-use Common Policy Editor gives you complete control of your scanning policies and the power to write custom checks. 20 predefined policies, including the SANS Top 20 and X-Force Catastrophic Risk Index policies, allow you to quickly configure scans for your organization.

REAL-TIME DISPLAY

Internet Scanner's real-time display options enable you to review scan results and monitor scans in progress to quickly identify vulnerabilities and vulnerable hosts.

VULNERABILITY CATALOG

The Internet Scanner vulnerability catalog delivers in-depth information on vulnerabilities, including root causes, detailed descriptions and remediation steps. The catalog is produced by ISS' world-renown X-Force security research and development team.

COMPREHENSIVE REPORTING

Internet Scanner delivers a large selection of reports that enable quick and easy information sharing across all levels of your organization. The more than 70 pre-defined reports include:

- Executive reports
- Line management reports
- Technician reports
- Trend reports
- Operating system reports

SECURITY FEATURES BUYERS GUIDE

CENTRALIZED VULNERABILITY MANAGEMENT FEATURES

Manage Internet Scanner agents with the SiteProtector management system for centralized vulnerability management.

ENTERPRISE-CLASS SCALABILITY

When managed using SiteProtector, hundreds of Internet Scanner agents deliver enterprise-wide vulnerability management for even the largest organizations.

REMOTE SCANNING

SiteProtector controls and operates scanning agents located in remote geographies and behind firewalls.

ENTERPRISE REPORTING

SiteProtector enables true multi-scanner/multi-scan enterprise correlation, aggregation and reporting. Management reports deliver concise information, while detailed operational reports assist technicians with vulnerability remediation. In addition, SiteProtector allows you to group information assets according to your enterprise layout and produce reports using that structure.

AUTOMATIC SECURITY CONTENT UPDATES

Using SiteProtector, updated security content can be applied automatically so that your vulnerability management system is continuously improving.

COMMAND SCHEDULER

The feature-rich SiteProtector command scheduler enables you to run scans, generate reports and update vulnerability information automatically.

ASSET MANAGEMENT

SiteProtector performs automatic, passive discovery of information assets, identifying new assets as they are added to your network. You can also import your company's assets from the active directory structure, import assets from external databases, and group assets easily.

REAL-TIME DISPLAY

SiteProtector's real-time, flexible display options allow you to monitor vulnerability information at the macro level down to the micro level, with the ability to create custom analysis views that can be saved and shared with other users. The FastAnalysis feature delivers guided analysis, offering answers to the most common-context sensitive questions with a single click.

SECURITY FEATURES BUYERS GUIDE

USER ADMINISTRATION

SiteProtector allows you to manage user accounts and roles easily, including group-based user access control

REQUIREMENTS

PROCESSOR

Recommended: 2.4 GHz Dual XEON Processor

Minimum: 1.2 GHz Intel Pentium III

MEMORY

Recommended: 1 GB

Minimum: 512 MB

HARD DISK

315 MB for installation from CD-ROM

345 MB for installation from file

OTHER REQUIREMENTS:

Free hard disk space: 300 MB

NTFS partition required

Sufficient disk space for session log files

OPERATING SYSTEM

The following operating systems are officially supported:

Windows 2000 Professional with SP4

Windows Server 2003 Standard SP1

Windows XP Professional with SP1a

DATABASE

Standard installation:

MSDE is automatically installed if it is not already present.

Microsoft Data Access Components (MDAC) 2.8 is included with the MSDE install.

RAM requirements include:

128 MB of RAM (Windows XP)

64 MB of RAM (Windows 2000)

32 MB of RAM for all other operating systems

Sensor-only installation:

MSDE is not required.

THIRD-PARTY SOFTWARE

Included:

MDAC 2.8

Sun Java 2 Runtime Environment (J2RE), Standard Edition, Version 1.4.x

Not included - needed for console only:

Microsoft Internet Explorer 5.5 or later to run HTML Help

Adobe Acrobat Reader 4.x or later to view PDF files