

August 2005

Vulnerability Assessment Technology Report

Internet Security Systems – Internet Scanner



Contents

Test Specifications	3
Vulnerabilities	4
The Product	5
Test Report	8
Test Results	12
West Coast Labs Conclusion	13
Security Features Buyers Guide	14
Appendix	15



Test Specifications

The aim of this Technology Report is to evaluate solutions in the field of Vulnerability Assessment. Participants in the report may include online services, appliances and software tools.

Test Environment

Participants in the technology report were invited to provide a vulnerability assessment of a heterogeneous network, together with proposals and recommendations for remediation. The network set up by West Coast Labs for evaluation of solutions comprised 24 distinct hosts, including routers, managed switches, network servers and client machines.

Web applications were installed on relevant servers. A variety of Operating Systems were used on the network, on different hardware platforms. A small number of virtual hosts were included.

In building the network, some of the servers were installed with default settings. Various levels of patching were applied. In addition a number of common misconfigurations were made in setting up the servers, and in deploying particular services.

Every host on the test network was imaged, and restored to its start state before each round of testing for individual solutions.

The test network was protected by a router. ACLs were set on the router to restrict access to the test network from IP addresses specified by the participating vendor, if appropriate. Where the solution under test was an appliance or software solution then the router was configured to block all access from the internet for the period of test.

The test network was available to each solution for 2 days. The final report, containing the results of the Vulnerability Assessment and any recommendations are addressed in the Test Results that follow.

Appliances were provided to WCL in the default shipping state. WCL engineers configured appliances in accordance with documentation provided. Software solutions state the desired specification and OS of the hardware on which the software is to be installed. WCL engineers installed and configured software in accordance with documentation provided.

All participating solutions were provided together with documentation supplied to a normal user.

Test Specifications

WCL evaluation of the Vulnerability Assessment Report

Vulnerabilities on the target network were 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.)

Each report was assessed on:

- 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
- The clarity of advice on remediation

WCL also comments on the level of technical knowledge required to understand and act on the information contained in the final report.

Participants in the Technology Report will be eligible for the Checkmark certification for Vulnerability Assessment.

In order to achieve the **Standard Checkmark Certification**, 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. All solutions must also provide accurate advice on mitigating the risks posed by the vulnerabilities.

Vulnerabilities

So that the test network would mirror that found in many businesses, a variety of operating systems, on different hardware platforms, were included. A Windows domain was set up with three servers and a mix of workstations running Windows XP and Windows 2000 professional. Some Sun Servers running Solaris 2.8 provided web services and file storage, assorted Linux boxes running Mandrake and RedHat distributions, and a Mac 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 misconfigurations 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.

On the Windows 2000 PDC we installed TightVNC as a service without tunnelling through SSH, SQLServer with a blank SA password, Active Directory, and IIS 5.0 with the demo applications. The BDC had Exchange 2000 and Active Directory installed. DNS was provided by the remaining Windows 2003 server. DNS was configured to allow zone transfers. In addition, IIS5.0 was installed with demo applications, and a vulnerable web application that was specially crafted in-house.

The server was also running Unreal Tournament GOTY edition (version 436) along with the UT web interface running on an unusual high port. There were user shares available on the wwwroot and ftproot directories and a world-writable FTP server. One of the Sun Blade servers had a Virtual Learning Environment (VLE) installed. The VLE had a default admin username and password as well as being installed with an old version and vulnerable version of Apache. Vulnerabilities included SSH access, Apache installations, Samba and a writable FTP directory.

Each of the “user” workstations was patched to a different level using official Microsoft Service Packs, historical patches and Windows Update. These machines then had different applications installed, ranging from Unreal Tournament client and TightVNC through to IIS 5.0 and remote admin. Some machines were included in the Windows Domain. Back Orifice was installed on one machine on a high end port.

An HP printer was added with default settings and open to administrative access via telnet and HTTP, a Cisco router configured with default settings, default username/password and open web admintool and an Apple Mac Power G3 running OS 8.6. If changes were made to the default settings, over all these devices passwords were set to be blank or easily guessable. Our test network thus consisted of a series of machines with differing hardware specifications, operating systems, patch levels, and software installations, and multiple vulnerabilities.

The Product

ISS presents the Internet Scanner vulnerability assessment application as providing the foundation for effective network security for corporate businesses. ISS claims that Internet Scanner minimizes risk by identifying the security holes, or vulnerabilities in networks so security managers can protect them before an attack occurs.

ISS also claims that Internet Scanner can identify more than 1,300 types of networked devices on a network, including desktops, servers, routers/switches, firewalls, security devices and application routers.

Internet Scanner can analyze the configurations, patch levels, operating systems and installed applications to find vulnerabilities that could be exploited by hackers trying to gain unauthorized access.

Internet Security Systems say...about the product.

Internet Scanner is an Enterprise Class vulnerability management system managed by the SiteProtector Enterprise Security Platform. SiteProtector combines scanning with Pre-emptive Protection Technologies to provide a VirtualPatch(tm) safeguard for over 1,500 vulnerabilities.

www.iss.net

Internet Security Systems say...about the Internet Scanner Business Benefits.

- Internet Scanner protects against the loss of customer data, preserves the availability of IT applications, and stops the malicious alteration of information.
- Internet Scanner identifies the computers, servers, routers, and other electronic assets on your corporate network and identifies the vulnerabilities on those assets which could lead to compromise.
- Preserves network uptime by scanning systems to identifying worms, backdoors, network attacks, and many other system vulnerabilities.
- Enables the communication of security status to the enterprise through executive and operational, business-unit oriented reports and reduces analysis cost burden through real-time correlation with security alerts.

www.iss.net

The Product

Internet Security Systems say...about the Internet Scanner Technical Benefits.

Internet Scanner is designed to serve large enterprise-class organizations.

- The product has unlimited discovery scanning for fast, efficient and effective network asset discovery. Dynamic Check Assignment - Probes a device, determines the OS and automatically executes appropriate checks, eliminating false positives, while optimizing scan performance.
- It also features Multi-Tiered Enterprise Security Platform Architecture (ESP) – Internet Scanner integrates into the ESP architecture providing vulnerability management in a common management system supporting over 25 types of security devices including; Intrusion Prevention, Desktop & Server Protection, and Integrated Security devices.

www.iss.net

Test Report

Internet Security Systems, Inc. (ISS) supplied West Coast Labs with a copy of the Internet Scanner Service Pack 2 software as a single zip file containing the executable, a readme document, an Installation Guide, and a User Guide. They requested that we installed the software as a Scanner Agent only on an appropriate machine and then they performed the scan from offsite using a tunnel into our network via that device and provided us with the reports at the end of the process.

The minimum specifications for installing and running the software are not too high – a Pentium III 1.2 GHz processor with 512Mb RAM which is more than reasonable. In terms of software environment, Internet Scanner can be installed on Windows 2000 Professional Service Pack 4, Windows XP Professional Service Pack 1a or Windows 2003 Server. The software must be installed on an NTFS partition.

ISS configured this scan to mimic a centralised administrator reviewing security at a remote branch office. This is a service that they can offer to perform if a company prefers outsourcing the scans to a third party.

Installation

Test Engineers installed the software on a Dell Poweredge 1750 with 1GB RAM running Windows 2003 Server.

The Install Shield based installation was very straightforward and caused no problems at all. There is the option to unpack the install files to a temporary location or to copy them to a specified location, and then keep them after the installation has completed. The installation then unpacks these files and then runs through a fairly standard set up procedure that should be familiar to anyone who has installed Windows software before.

The first screen on the run through is the license agreement, then there is the choice of doing a standard installation, Sensor Only or Custom. There are several checks at this point to ensure that the correct filesystem type is in place, and that the hardware requirements are met. Each of these checks will throw up a warning if minimum requirements are not found. If there is a critical error, for example trying to install on a FAT32 partition, the installation will exit. Finally there is a summation of the parameters and a final chance to exit the installation.

It is worth noting that choosing the Sensor Only option, as we did for this test, does not add any options into the Program Files menu on Windows except for a Vulnerability Catalog in the form of a Windows help file. This is because it is intended to be remotely managed.

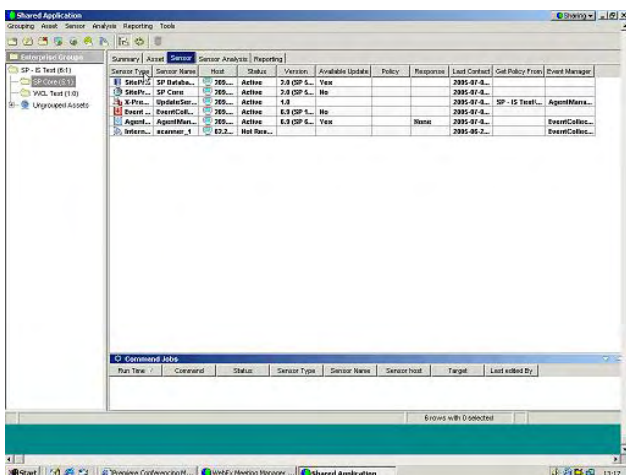
Test Report

The Main Interface and Scanning

Although we did not perform the scans or generate the reports ourselves, ISS demonstrated the software in use to us. From this we could see that the central administration of both the scanning and reporting functions is performed from the main SiteProtector application.

Assets may be added in one of several ways – they may be added manually, imported through integration with Active Directory, or, as was the case with the scan performed against our test network, discovered via the results of a scan.

Once the assets have been identified, an Administrator has discretionary control over grouping the devices to best suit the existing business structure, and can then perform scans against distinct groups. Scheduling is also possible, so that scans may be run at set intervals without manual intervention.



The application delivers a range of predefined policies for the scans in order to start the user off as quickly as possible. These can, of course, be customised quite easily and any proprietary scan policies and settings can be stored for later use. Users may be defined within the application with differing privilege levels giving them different rights and access to policies.

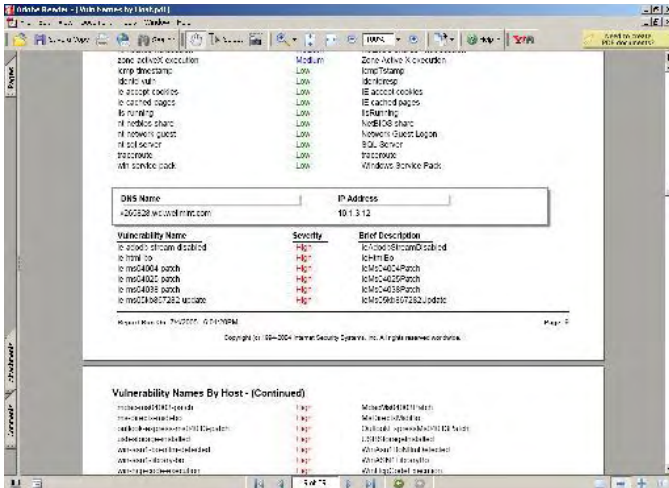
This is a useful delegation tool whereby named contacts may have responsibility for discrete parts of the network, and would be especially useful in the context of an enterprise level large scale

deployment. It is worth noting that specific ports on any intervening firewalls need to be opened for communication between the scanner host and the management station.

An Administrator is also able to set benchmarks, so that any changes in the status of the security profile can be readily monitored. There is also a rather useful ability to specify exceptions either by host, by vulnerability, or for a specific vulnerability on a specific host. For example, business critical services running on servers that have already been scanned can be excluded so that an engineer does not decide to patch the device at an inappropriate time.

Another feature worth mentioning is the ability to incorporate Vulnerability Assessment results with other components of the SiteProtector infrastructure. This enables impressive real time correlations between perceived network activity and previously identified vulnerabilities, allowing the Administrator to focus precisely on threats that relate to the actual risk profile of the network.

Test Report



The level of description available for each resolution was impressive, with step by step guides available to mitigate these risks at source where this was possible. These will act as a useful reference guide for the engineers tasked with problem resolution.

All reports categorise the vulnerabilities according to their severity level. This is set to be consistent with ISS' X-Force Research and Development Team's ratings.

Test Results

The results we received were well defined, and the ability to generate different levels of reports will be appreciated by both the management and the engineers of any company.

The speed of the scan and the quality of the remediation advice, with attendant walkthroughs for the majority of the problems should also be noted. These make it possible for any company to very rapidly mitigate against possible intrusions or threats.

Internet Scanner 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

ISS Internet Scanner is an impressive answer to the many problems faced by any network Administrator.

As a scalable solution, Internet Scanner has the ability to go from SMB level to Enterprise level effortlessly and the ability to install a remotely managed scanner only solution in remote offices mitigates against any users with physical access to the machine changing parameters without the knowledge of the central administrator.

ISS Internet Scanner can be recommended on several levels as it goes a long way towards the process of making a network safer.



CUSTOM TESTED

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

Security Features Guide

As Stated by ISS

1. Identifies more than 1,500 vulnerabilities
2. Identifies over 1,300 various types of electronic assets (desktops servers, routers, etc.)
3. Supported by X-Force(tm), ISS' R&D team credited with discovering 55% of high risk vulnerabilities
4. OS specific scanning (Dynamic Check Assignment) improves performance & accuracy
5. 20 default scanning policies
6. Unlimited Discovery, enabling asset discovery for your entire enterprise
7. Central policy manager allows policies to be shared amongst users
8. 74+ Default out-of-the-box reports
9. Real-time display of scan status
10. Remediation (fix) information provided on screen and within reports
11. Integration with ISS' SiteProtector management system
12. Scan Scheduling allows automation of recurring scans
13. Group oriented scanning using user-defined asset groups
14. Multi-scanner capable
15. Multi-tiered architecture
16. Active Directory Integration
17. User based access privileges restricts visibility to allowed groups per user
18. Multiple user-roles restricts actions allows per user
19. Automatic Asset grouping against user defined criteria (OS, DNS name)
20. X-Press Updates provide security intelligence updates
21. 17 Default Analysis Views
22. Unlimited number of custom vulnerability analysis views
23. FastAnalysis provides one click analysis navigation
24. Advanced correlation power by ISS' Security Fusion module
25. Failover Ready
26. Data Backup and purging capable
27. Pause live scan and resume later

http://documents.iss.net/literature/InternetScanner/InternetScanner_datasheet.pdf

Appendix

Vulnerability Assessment Premium Level Certification



Within the framework of the testing carried out in this Technology Report, those developers identifying 100% of the Critical Vulnerabilities and a minimum 90% of the Serious Vulnerabilities are awarded the *Premium Checkmark Certification* for Vulnerability Assessment.

<http://westcoastlabs.org/cm-briefingdocs.asp>