



**INTERNET**  
**SECURITY**  
**SYSTEMS™**

**Internet Scanner® 7.0**  
**Frequently Asked Questions**  
*April 2003*

Internet Security Systems'™ (ISS) Internet Scanner® application provides automated detection and analysis assessment of vulnerabilities on servers, desktops, and other network devices. Internet Scanner helps organizations proactively protect their information assets by discovering the vulnerabilities that expose them to compromise.

### 1. What is Internet Scanner?

Internet Scanner provides automated assessment and analysis for vulnerabilities on network-connected devices. With Internet Scanner, network and security administrators can assess the security of their servers, desktops, and other networked devices for vulnerability to the latest information security threats.

### 2. What are the benefits of Internet Scanner?

Internet Scanner benefits organizations of all sizes in any industry:

- **Minimize business risk** – Secures critical assets to prevent compromise that may result in loss of availability, integrity or confidentiality of networks and critical business systems.
- **Proactive protection** – Identifies and assesses the security posture of networked systems for prioritization of remediation tasks so that high-risk vulnerabilities are addressed quickly.
- **Low cost of ownership** – Mitigates resource constraints and maximizes the organization's security investment. Ease-of-use features and the advantages of a supported and extensively tested commercial product provide a cost-effective method for risk reduction.
- **Scalable** – Multiple policy options, built-in security intelligence, and customizable scan parameters offer flexibility for any size network. Parallel scanning features enable the execution of multiple and diverse scans checking for and reporting common vulnerabilities in devices across the enterprise and maximizing Internet Scanner's return on investment.

### 3. How can Internet Scanner save time and effort?

Internet Scanner saves organizations time and effort and improves the return on their information security investment through its many ease-of-use features, built-in security intelligence, and integration with ISS' Dynamic Threat Protection Platform.

- **Ease of use** – Internet Scanner automates a wide range of vulnerability assessment tasks, from configuring scans to communicating results.
- **Security intelligence** – From X-Force™ security content to predefined scanning policies and extensive end-user documentation, Internet Scanner puts industry-leading information security expertise in the hands of its users.
- **ISS protection platform integration** – Internet Security Systems unique Dynamic Threat Protection platform permits users to achieve improved security with lower cost of ownership by leveraging the integration and interaction of the full range of ISS solutions.

### 4. What new features are available in Internet Scanner 7.0?

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

For more information about these features, please consult the Internet Scanner 7.0 product documentation at <http://www.iss.net/support/documentation/docs.php?product=7&family=9>.

**5. How can Internet Scanner 7.0's unlimited Discovery help protect my organization's information assets?**

Discovery is a critical component of the vulnerability assessment process, allowing organizations to find and identify information assets and determine their relative importance. Particularly vital is the discovery of unknown, and often unpatched, web servers and other assets that often represent the most likely avenue of attack, whether from an automated blended threat or a meticulous, knowledgeable attacker. Internet Scanner 7.0's unlimited Discovery capability permits organizations to use Internet Scanner to discover assets on their network without being constrained by their licensed device count, and then use the Host List Generator or SiteProtector's robust sorting and filtering features to quickly and easily create groups of hosts for targeted vulnerability assessment scans. Unlimited Discovery represents a significant cost savings and allows users to employ Internet Scanner for asset discovery and vulnerability assessment, streamlining processes and reducing overall cost of ownership.

**6. How does Dynamic Check Assignment work?**

When the Dynamic Check Assignment option is enabled in an Internet Scanner policy, the application will perform an operating system (OS) identification on the target hosts to determine the type of operating system being scanned. If the host has a Windows-type OS, Internet Scanner will run only enabled Windows-related checks against that host. If the host operating system is a Unix flavor (for example, Linux, Solaris, FreeBSD, etc.), Internet Scanner will run only enabled Unix-flavored checks against that host. If the host operating system is neither of these (e.g., "unknown", Cisco IOS, etc.), all enabled checks in the policy will be run against that host.

**7. Does Internet Scanner include predefined scanning policies?**

Yes, Internet Scanner 7.0 includes a variety of predefined policies designed to simplify the challenges of starting and progressing in network vulnerability assessment.

- Discovery policies permit users to identify the devices on their networks without being constrained by their licensed device count.
- Level 3-5 policies – including policies tailored to web servers, desktops, and routers – enable users to start by focusing on critical vulnerabilities and gradually increase the depth of their assessments as they progress through the assessment cycle.

The SANS Top 20 policy provides industry-standard benchmark against which users can assess the relative security of their information assets.

**8. How often is Internet Scanner updated?**

Timely inclusion of emerging security information is critical to protecting network hosts. For that reason, Internet Scanner provides regular X-Press Updates™ containing new tests. Critically important new checks are released more quickly if the danger level is high.

**9. What is the X-Force™?**

Internet Security Systems' *X-Force*™ organization is a leading research and development group dedicated to discovering vulnerabilities and design weaknesses that potentially open operating systems and applications to attack or misuse. This process includes both active research of products and technologies and ongoing surveillance within the hacking underground. Relevant discoveries are released in the form of alerts and advisories, and are delivered within product enhancements for Internet Security Systems' enterprise prevention and protection platform, in order to protect Internet Security Systems' customers, critical infrastructure and the Internet at large.

**10. Can Internet Scanner help me communicate vulnerability information within my organization?**

Internet Scanner includes multi-level vulnerability reports designed to facilitate the communication of information about vulnerabilities and vulnerability status to different levels of an organization. Internet Scanner's selection of predefined reports provides different levels of reporting for different audiences, from technical detail for security experts to high-level

graph reports for executive summaries. Clear graphical reports allow users to quickly determine security status of their network, while detailed fix information speeds remediation. Reports are also exportable to multiple formats for easy distribution. This reporting system helps organizations save time and money by accelerating the auditing and enforcement process.

**11. Can Internet Scanner be used for enterprise-level vulnerability assessment?**

Yes, Internet Scanner offers a complete solution for enterprise-level vulnerability assessment, whether used alone or with SiteProtector, centralized security management for enterprise security. Internet Scanner's robust scanning engine and flexible discovery licensing help users perform vulnerability assessment over environments of any size.

**12. What is SiteProtector? What additional capabilities can SiteProtector offer?**

RealSecure® SiteProtector provides scalable, centralized security management for enterprise security, extending the capabilities of Internet Scanner by offering:

- SecurityFusion's correlation analysis engine uses X-Force security intelligence to automate incident recognition and management through real-time correlation of attacks and vulnerabilities.
- Powerful information analysis tools such as Advance Analysis and configurable views and filters. Event prioritization and correlation create real-time attack and misuse tracking. Powerful filters screen for event exceptions and false alerts, while incident creation options help users track vulnerabilities and remediation status.
- Remote command and control, data consolidation, and increased automation, permit enterprises to extend the scope of their vulnerability assessment programs without the need for additional resources.

For additional information about SiteProtector, please see the Internet Security Systems' Internet site at [http://www.iss.net/products\\_services/enterprise\\_protection/rssite\\_protector/](http://www.iss.net/products_services/enterprise_protection/rssite_protector/).

**13. Does Internet Scanner support distributed scanning?**

Yes, distributed scanning – including remote command and control, data consolidation, and centralized reporting – are all available when operating Internet Scanner via SiteProtector.

**14. Why is vulnerability assessment important?**

Vulnerability assessment is critical to the strategy of “defense-in-depth.” Regular vulnerability assessment permits organizations to:

- Identify information assets in their environment.
- Determine their value to the organization and their appropriate protection level.
- Assess the security posture of assets, and of the network as a whole.
- Protect critical systems through the placement of protection agents or through remediation.
- Improve the efficiency and return on investment of perimeter protection systems through the SecurityFusion module.

**15. I already have perimeter defenses protecting my network. Why do I need Internet Scanner?**

Although firewalls, intrusion detection systems, and other perimeter security systems are important security components, regular vulnerability assessment of devices on an organization's internal and Internet-facing networks is essential to a true “defense in depth” security strategy. Regular vulnerability assessment is critical to helping protect information assets from today's “blended threats,” which are capable of entering a network via email, HTTP traffic, or other means not normally blocked by firewalls. Security organizations around the world use Internet Scanner to complement their perimeter defenses, protecting their vital information assets at all levels.

SiteProtector's™ SecurityFusion™ module now makes it possible for users to leverage their vulnerability information for automated analysis of intrusion detection traffic, reducing false

alarms and improving prioritization of high-risk events. With SecurityFusion, regular vulnerability assessment allows Internet Scanner to strengthen perimeter defenses and reduce the overall cost of ownership for information security.

#### **16. Is it necessary to scan my entire network?**

There are many different ways to compromise a network. Scanning the entire network provides a definitive understanding of all available devices and services, and renders a road map of the potential exposure. For example, low-value computers (e.g. desktop workstations) can be compromised with any of a large number of "back door" programs like NetBus or BackOrifice. These systems can then be used to attack more important computers, such as database servers. Regular scanning of desktop computers helps protect important assets.

A critical first step in the assessment process is the discovery and inventory of devices on your network, in order to identify critical business assets. Internet Scanner 7.0's unlimited Discovery capability makes it possible for organizations to cost-effectively use Internet Scanner for the full vulnerability assessment cycle.

Scanning your entire network also allows you to recognize even greater benefits from the SecurityFusion correlation module. The more devices included in the correlation analysis, the more effectively the SecurityFusion module can determine the status of attacks against the network and help you prioritize your response.

#### **17. Can Internet Scanner assess devices from inside and outside a network?**

Internet Scanner can be used alone or with SiteProtector to assess devices from inside and outside a network. Scanning from both perspectives is vital to obtaining a comprehensive view of your network's vulnerability posture. SiteProtector's support for distributed vulnerability scanning dramatically simplifies this process by allowing users to run Internet Scanner agents from multiple locations inside and outside the network, then centralizing the vulnerability data from all scanning agents for a consolidated view of host and network vulnerabilities.

When scanning a firewall, you should attempt to reach at least one address on the opposite side of the firewall in order to test both the firewall itself and traffic it allows through. Assuming Internet Scanner can penetrate the firewall from the outside, it will simulate an attack on all devices authorized with an IP address defined in the key. Inside the firewall, scans identify vulnerabilities on network devices behind the firewall. Internal scans are especially important since over 60% of all security breaches occur from inside a corporate network.

#### **18. What are the Denial of Service checks in Internet Scanner?**

Checks in Internet Scanner's Denial of Service (DoS) category include checks for DoS vulnerabilities, as well as checks that, through their operation, have the potential – however slight – to disrupt a host or service. For example, the OpenSSLMasterKeyBo check attempts to detect vulnerability to a buffer overflow attack using a weakened version of the attack, and is included in the DoS category because there remains the small possibility that it will cause a disruption in the Web server service.

Checks in the Denial of Service category should not bring down the whole network, but they can disrupt certain services and/or machines. Some of the Denial of Service checks may affect network devices such as routers that are in the path of the scan. For example, the UDP bomb tests can "panic" an unpatched SunOS machine, causing it to reboot. Ping Bomb can instantly reboot a Linux box. When running DoS category check, users should verify the target host and understand the effect of the check.

No Denial of Service category checks are enabled by default in any of Internet Scanner's predefined scanning policies.

**19. Is it possible to migrate from Internet Scanner 7.0 beta to the release version of 7.0?**

No, it is not possible to migrate from beta to production versions of Internet Scanner 7.0. Beta users who wish to install the release version of Internet Scanner 7.0 must uninstall the beta before proceeding with the installation of version 7.0. In addition, there is no means to roll back from version 7.0 beta to version 6.2.1.

**20. Internet Scanner only performs its scans from a Windows operating system, but is it capable of assessing non-Windows devices?**

Internet Scanner has the ability to scan any network device with an IP address. This includes routers, printers, PC's, firewalls, workstations, etc. For this reason, ISS recommends generating a host list so the scanner does not scan devices that do not require this service or are out of bounds of an administrator's zone of authority.

**21. Does Internet Scanner 7.0 support Windows Server?**

No, Internet Scanner 7.0 is not supported for installation or operation on Windows Server. Support for this platform is under consideration by Internet Security Systems for a future version of Internet Scanner.

**22. Does Internet Security Systems offer professional services to help users get started with Internet Scanner and vulnerability assessment?**

Yes, X-Force Professional Security Services provides rapid, cost-effective security optimization and protection with minimal impact on normal staff operations. ISS deploys the technology as well as customizes and integrates the solution for an organization's unique environment.

**23. Are training classes available for Internet Scanner?**

Internet Security Systems' X-Force Education offers multi-day courses in Internet Scanner that cover topics from scanning principles and installation to advanced topics. For information regarding Internet Scanner classes, please visit us online at <http://education.iss.net/namerica.php>.

**24. How do I obtain Internet Scanner for evaluation purposes?**

Internet Scanner can be downloaded for evaluation from the Internet Security Systems public Internet site at <http://www.iss.net/downloads/>. It can be run without a license in loopback mode for evaluation of basic scanning and reporting capabilities, or with an evaluation license for a complete assessment of Internet Scanner's features and functionality. Evaluation licenses can be obtained by contacting an authorized reseller or [sales@iss.net](mailto:sales@iss.net).

**About Internet Security Systems (ISS)**

Founded in 1994, Internet Security Systems (ISS) (Nasdaq: ISSX) is a pioneer and world leader in software and services that protect corporate and personal information from an ever-changing spectrum of online threats and misuse. Internet Security Systems is headquartered in Atlanta, GA, with additional operations throughout the Americas, Asia, Australia, Europe and the Middle East. For more information, visit the Internet Security Systems Web site at [www.iss.net](http://www.iss.net) or call 888-901-7477.

*Copyright © 1994 -2003, Internet Security Systems, Inc. All rights reserved worldwide.*

*Internet Security Systems, the Internet Security Systems logo, SiteProtector, SecurityFusion, X-Force and X-Press Update are trademarks, and RealSecure and Internet Scanner registered trademarks and service marks, of Internet Security Systems, Inc. All marks are the property of their respective owners and used in an editorial context without intent of infringement. Specifications and content are subject to change without notice.*