

Close the door on hackers. Your Weapon: Sunbelt Network Security Inspector.

You can't close the door if you don't know which ones are open. Find security holes fast with Sunbelt Software's Network Security Inspector (SNSI). SNSI delivers what system, network, and security administrators need in a vulnerability assessment scanner: a low-cost, quick-install, fast-results security scanner with a top quality vulnerability database and prioritized reports that show you how to fix security holes fast. Proactively protect your systems and networks with a world-class scanner that detects a broad range of vulnerabilities in a number of system platforms and Microsoft® applications.

Easy to use interface and fast deployment

SNSI's quick and easy install gets you up and running in a matter of minutes. With its simple point-and-click graphical interface, you can start scanning for vulnerabilities and obtain information rapidly on the security status of your networks. Setting up policy-based scans is simple and easy with the policy set-up wizard. You have the ability to set up custom scan groups by IP range, vulnerabilities, machines, or any combination thereof.

Completely customizable, administrators can choose any combination of multiple tabs or single windows for policies, groups, and reports. Documents can be rearranged into groups by splitting a group of tabs either vertically or horizontally and documents can be freely moved from one group to another, providing side-by-side comparisons of different policies and scan results.

New scanning engine for faster scan times

The new scanning engine now runs as a service to provide considerably faster scanning times and accuracy. SNSI's engine continues to utilize a top-rated vulnerability database for its scanning. The database contains over 4000 vulnerability audits with wide support across Windows, POSIX and

infrastructure devices. Vulnerability audits include security configurations, OS and application vulnerabilities, null passwords, patch-level related vulnerabilities, known hacking tools, malware, common worms, and P2P software checks.

SNSI uses the latest MITRE Common Vulnerabilities and Exposures (CVE) list of computer vulnerabilities and contains the latest SANS/FBI top 20 vulnerability list. It also uses the latest CERT, CIAC, Microsoft, and FedCIRC (Department of Homeland Security) advisories.



Policy-based scanning and scheduled scans

You can now schedule scans, allowing vulnerability scanning to occur during low traffic times and automatically set this schedule to reoccur on a daily, weekly or monthly basis. SNSI uses an advanced policy-based approach to configuring scans.

Policies are configured once and contain all of the configuration information required to perform a scan. The target discovery options available in the policies allow administrators to dynamically determine which targets will be scanned based on their network status at the time of the scan. Scans can be run "on demand" by an administrator, or can be scheduled using a variety of scheduling options to occur automatically such as monthly auditing of all machines.

Supports multi-platform and IP-based scanning

In addition to Windows, SNSI provides vulnerability assessment support for systems running Sun Solaris, HP-UX, Red Hat, Mandriva and SUSE Linux, Cisco routers, and HP printers. You have the ability to scan by single IP address, range of addresses or entire subnet.





File version scanning

Through definitions, SNSI now offers file version scanning to scan for the latest versions of files, by setting a range of versions for specified file types. This improves scanning times by reducing the scan parameters and eliminates scanning for vulnerabilities that were corrected in previous software patches.

Port and service scanning

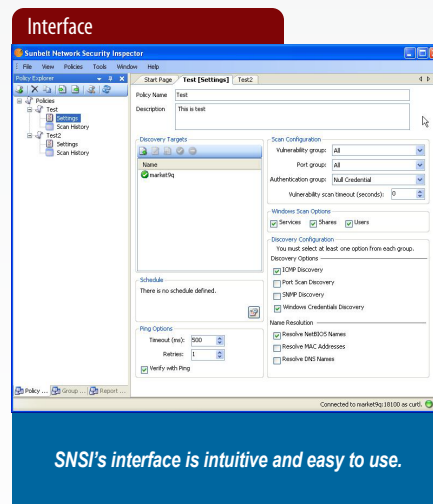
Scan for open ports and active Windows services running on any target machine. A list of open ports provide information on what protocols may be running on discovered open ports, including HTTP, FTP, and P2P software. For service scanning, SNSI determines what Windows services are running and labels them as “known” or “unknown” based on SNSI’s known list of services.

IP and vulnerability searching

SNSI organizes scans according to policies. In the policy settings, you can configure the scan based on the type of search, vulnerabilities and ports, as well as the range of machines to scan. There are a number of options to choose from to customize the scan. You can schedule scans for each policy. You can also use the wizard to configure a new policy, stepping through the various settings to ensure key settings are not missed.

Licensed per Administrator - not IP

High cost is often a major factor in not being able to purchase a quality scanner. SNSI gives you the ability to implement a high quality security scanner at a price point that fits within tight budgets. And, you can scan IPs or machines as many times as you would like for one low price. SNSI is the exception to the rule “you get what you pay for”—with SNSI, you’re getting commercial-grade vulnerability scanning at a price to fit your budget.



SNSI's interface is intuitive and easy to use.

Prioritized vulnerability reports

SNSI provides vulnerability reports that display scanning results in an understandable and usable format. You can customize reports for management and technical personnel that include comprehensive details for selected machines or entire domains.

Available reports range from high level summaries to detailed vulnerability descriptions that include:

- Executive Summary
- Listing by Target
- Listing by Vulnerability
- Scan Summary
- Top 20
- Vulnerabilities by Target
- Vulnerability Details

Configurable vulnerability testing

You have the ability to create a “Quick Scan” for one machine or an entire domain by selecting only those attributes required, or create a “Deep Scan” for an in-depth assessment of your entire network. You can create your own custom vulnerability scans or use SNSI’s predefined scans such as “high risk” or the “SANS top 20”.

Close the door on hackers

Find out how easy and affordable world-class vulnerability scanning can be! Visit www.sunbeltsoftware.com for more information on SNSI.

Technical Specifications

Sunbelt Network Security Inspector Version 2.0

Minimum System Requirements:

- 20GB free disk space
- 512 MB RAM (recommend 2 GB)
- Monitor display resolution of 1024 x 768
- Windows XP Professional SP2
- Windows Server 2003 SP1

Types of Systems Scanned for Vulnerabilities:

Cisco / IOS, CatOS, PIX
 HP / HP-UX 10.x and later
 HP / Tru64 4.0F and later
 Linux / Fedora (6.7)
 Linux / Mandriva (7.0, 7.1)
 Linux / Red Hat (Enterprise 2.1, 3, 4, 5)
 Linux / SuSE Open/Enterprise (9, 10.0, 10.1, 10.2, 10.3)
 Mac OS X
 OpenBSD 3.8 and later

Printers / HP Networked
 Sun Solaris / 2.5 and later
 Windows 2000
 Windows 2003
 Windows 2008
 Windows XP
 Windows XP Embedded
 Windows Vista



Features are subject to change without notice. All products mentioned are trademarks or registered trademarks of their respective companies. Copyright © 2004-2009 Sunbelt Software, Inc.

snsidatasheet February 2009