SAINT®

Examine. Expose. Exploit.

Vulnerability Scanning | Penetration Testing

"... the interface is excellent"
— Jason, General Dynamics

"The [SAINT] software you have created is one of the best I have ever used and the commitment by your support team to constantly improve is outstanding."
— Chris, IT Security Specialist
U.S. Dept. of HHS, AHRQ

"I just wanted to let you know we are performing training tests using our new SAINTbox and LOVE it. Great job on design, intuitiveness, ease of use, and performance."
— David, Entercomp Consulting

PCI Security Standards Council™
APPROVED SCANNING VENDOR

SC MAGAZINE

Vulnerability Scanning

and integrated

Penetration Testing

Extreme Network Security

www.saintcorporation.com

SAINT® Vulnerability Scanning

SAINT® at a Glance

- Frequent automatic updates
- Scans anything with an IP address running TCP/IP protocols
- Customizable scanning options including SANS/FBI Top 20
- Online documentation and tutorials
- Includes links to patches and new versions of software to eliminate the detected vulnerabilities
- Runs in remote mode
- Add your own vulnerability checks and exploits
- Dynamic reporting capability allows you to drill down to get more information about the vulnerability and how to correct it
- Includes and correlates industry cross references such as CVE, CVSS, IAVA, OSVDB, BID and more
- Scans IPv4 or IPv6 addresses
- Control panel allows you to stop, pause, and resume scans; and to view results in progress while the scan runs
- Certified CVE-compatible by MITRE

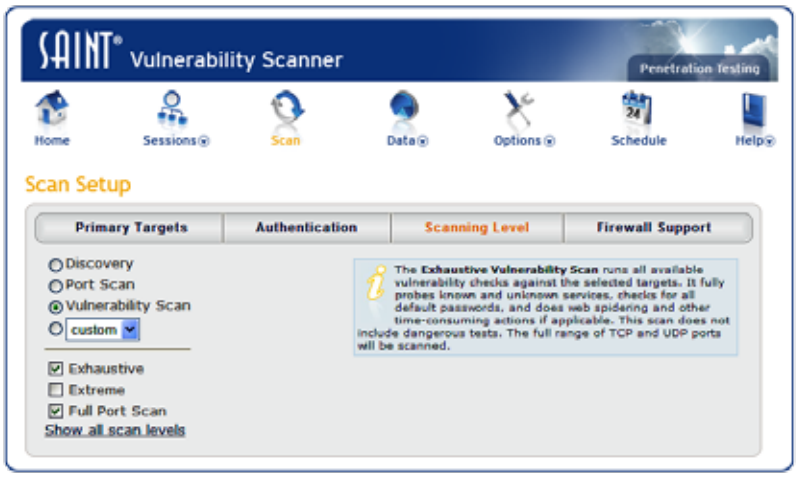
Proactive Network Security

SAINT® scans your network to detect anything that could allow an attacker to gain unauthorized access, create a denial-of-service, or gain sensitive information about your network. Every live system on your network is screened for TCP and UDP services. For each service it finds running, it launches a set of probes designed to detect known vulnerabilities.

In addition to detecting vulnerabilities, SAINT® gives you the ability to fix weaknesses in your network security before they can be exploited by intruders. SAINT® provides vulnerability information and links so you can download patches or new versions of the software that will eliminate the detected vulnerabilities.

SAINT® is available three ways:

- Software (download from www.saintcorporation.com)
- SAINTbox™ pre-configured appliance
- WebSAINT® online service



SAINT's interface is easy to use

Enterprise-wide Vulnerability Scanning with SAINTmanager™

Manage and schedule SAINT® scans across your enterprise with the SAINTmanager™ remote management console. This centralized management and reporting capability lets a single vulnerability assessment team see the overall security posture of the entire enterprise. It reduces the length of time for enterprise-wide vulnerability scanning and keeps a centralized schedule of all scans to be run. It is easy to install and maintain; typically taking 10-15 minutes.

The centralized trouble ticketing system allows automatic assignment and easy tracking of vulnerability remediation. SSL encryption ensures that scan results are secure as they travel across the network.

SAINTexploit™ Penetration Testing

Integrated Scans and Exploits

SAINTexploit™ goes beyond simply detecting vulnerabilities to safely exploiting them. The first integrated vulnerability scanner and penetration testing tool, SAINTexploit™ is part of the complete solution SAINT offers to evaluate the threats and vulnerabilities to your network.

Examine. Expose. Exploit.

This fully automated product examines potentially vulnerable services discovered by SAINT, exposes points where an attacker could breach the network, and exploits the vulnerability to prove its existence without a doubt. The file browsing, screen capture, and command execution capabilities resulting from a successful exploit provide undeniable evidence of a network vulnerability.

Exploit tools provide extra penetration testing capability

System Requirements

- Unix/Linux platform – Linux, Solaris, FreeBSD, or Mac OS X
- Disk Space/memory
  - 64 MB to run
  - Up to 70 MB for additional packages (e.g., PERL, Web browser)
  - Additional space for optional packages (e.g., Samba, NMAP, OpenSSL, OpenSSH)
  - At least 256 MB of RAM
- Essential Software
  - PERL 5.004 or above
  - Web browser (e.g., Internet Explorer, Firefox, Mozilla)

SAINTexploit™ at a Glance

- Exploits vulnerabilities found by the SAINT® vulnerability scanner
- Proves the existence of critical vulnerabilities
- Features seamless integration with SAINT's graphical user interface
- Boasts an extensive, multi-platform exploit library
- Includes remote, local, and client exploits
- Provides automatic penetration testing
- Runs individual exploits on demand
- Includes Web site emulator and e-mail forgery tool with built-in design templates.
- Includes IPv4 and IPv6 exploits
- Features exploit tunneling that allows you to run penetration tests from an exploited target.
- Exploit tools provide extra penetration testing capabilities (see screen capture).

SAINTbox™ Appliances

Automatic Updates

New threats to your networks can emerge in an instant. Every time SAINT® runs a scan, SAINTexpress® checks the SAINT® Web server for updates. If updates are present, SAINTexpress® installs them and SAINT® continues to run as usual. Updates are released every two weeks, or sooner for a critical vulnerability announcement.

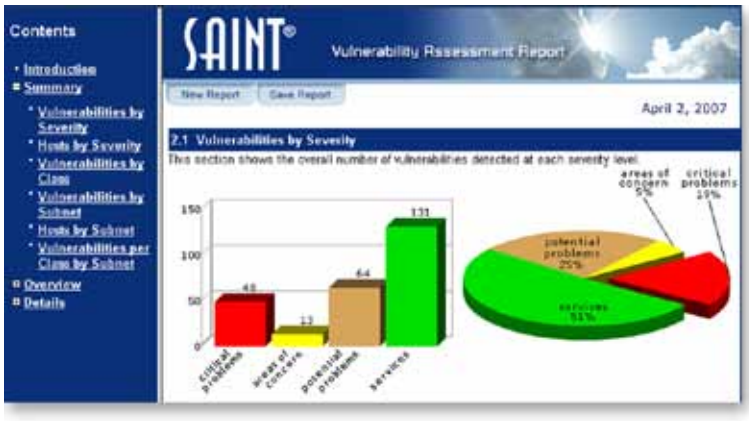
SAINT® Custom Reports

SAINTwriter® software allows you to easily design and generate custom vulnerability assessment reports complete with charts, tables, and graphs. Extensive configuration options allow you to pinpoint the information needed and present it in formats appropriate to your audience. SAINTwriter® offers several pre-configured reports that can be easily customized. Reports are exportable and can be saved in HTML, PDF, XML, text, and CSV formats.

In order to evaluate the effectiveness of your remediation program, SAINTwriter® offers a trend analysis report that provides you with a long-term perspective of your security program's improvements and weaknesses.

Reports at a Glance

- Numerous standard reports ranging from executive summary to technical detail.
- Each report has configurable options. The customized formats can be saved for future use.
- Colorful graphs and tables help you quickly identify problem areas.
- Trend analysis report option allows you to quantitatively analyze your remediation program.
- PCI compliance reports allow you to see at a glance whether your network is compliant with PCI security standards.
- CVSS option allows you to report CVSS base scores and vectors.
- Reports can be easily exported to other applications like spreadsheets, word processors, and databases.



SAINTmanager™ Overview page

SAINT Corporation

SAINT Corporation is a global leader in network security. Our customers include high-level government agencies, top colleges and universities, and major financial institutions. Our mission is to make network security easy and affordable.

Corporate Office: 4720 Montgomery Lane, Suite 800, Bethesda, MD 20814-3444
Phone: (301) 656-0521 or toll-free: (800) 596-2006
sales@saintcorporation.com **www.saintcorporation.com**

July 2009

PCI Security Standards Council
APPROVED SCANNING VENDOR

CVE COMPATIBLE
cve.mitre.org