

# SAINT<sup>®</sup>

## Integrated Vulnerability Assessment and Penetration Testing

### Customer Quotes

"... 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, HHS

"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 perfor-  
mance." – David, Entercomp



**NIST SCAP Validated**

### SAINT Editions

#### SAINT<sup>®</sup> Professional

A complete illustration of both internal and external threats. Offered as downloadable software or a pre-configured appliance, this option includes vulnerability scanning, penetration testing, web application scanning, along with full customization of both the configuration and report sections. SAINTscanner™ + SAINTexploit® technology is included with the SAINTwriter® report generator.

#### SAINT<sup>®</sup> Enterprise

The ideal choice that includes all of the functionality above plus the SAINTmanager® vulnerability management console. Organizations that select this option typically want to take advantage of the centralized GUI for communicating to multiple scanner instances, granular access controls, dashboard view of scanners, trouble tickets, security trending, and more.

#### Software as a Service (Cloud) Editions –

##### WebSAINT<sup>®</sup>

A great way to get started performing basic vulnerability assessments on external targets. Permits unlimited scanning, scheduling, and numerous canned security reports.

##### WebSAINT PRO<sup>®</sup>

Excellent for practitioners that need the full power of SAINT as a SaaS based model focusing on external targets. Functionality includes vulnerability scanning, penetration testing, web application scanning, along with full customization of both the configuration and report sections.

# SAINT<sup>®</sup> Vulnerability Scanning

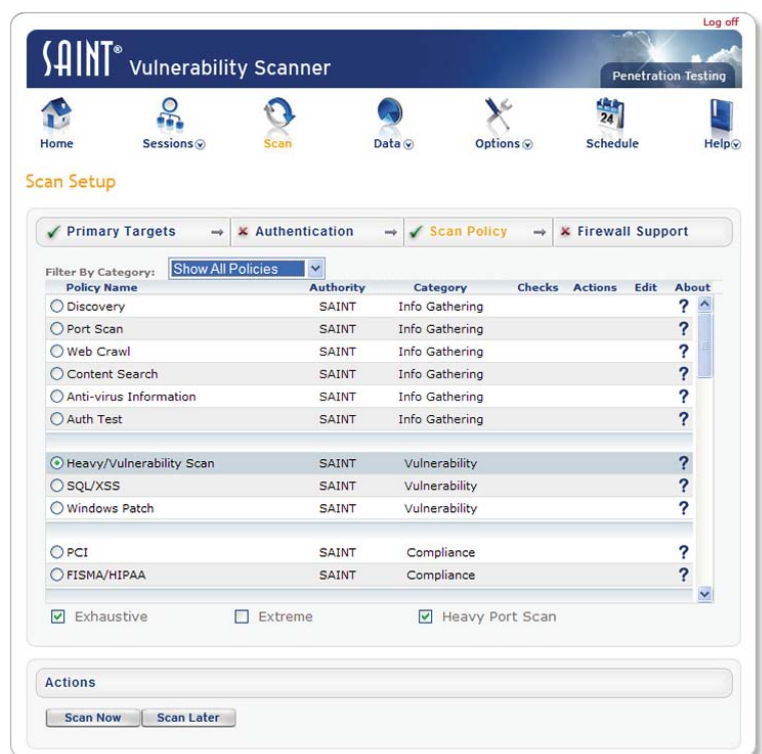
## SAINTscanner at a Glance

- SAINT software can be downloaded, comes on a preloaded appliance, or as a SaaS model.
- Performs authenticated and unauthenticated vulnerability scans for operating systems, databases, Web applications, and network devices
- Frequent automatic updates
- USGCB and FDCC configuration auditing
- Online documentation and tutorials
- Shows you how to fix the vulnerabilities, and where to begin remediation efforts—with the exploitable vulnerabilities
- Runs in remote mode
- Add your own custom vulnerability checks and exploits
- Correlates industry standard identifiers such as CVE, OSVDB, BID, IAVA, OVAL, the presence of exploits, CVSS score, and vendor ID
- Shows you if the network is compliant with PCI security standards; SAINT is a Payment Card Industry (PCI) Approved Scanning Vendor
- SCAP validation by NIST

## Proactive Network Security

The SAINTscanner scans your network to detect anything that could allow an attacker to gain unauthorized access, create a denial-of-service, or gain sensitive information. SAINTscanner offers heterogeneous scanning that identifies vulnerabilities across operating systems, desktop applications, network devices, Web applications, databases, and more.

In addition to detecting vulnerabilities, SAINTscanner 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's interface is easy to use*

## SAINT Corporation

SAINT customers include high-level government agencies, top colleges and universities, and major financial institutions. Industries and governments all over the world use SAINT products and services to manage IT security risk and compliance.

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

[www.saintcorporation.com](http://www.saintcorporation.com)

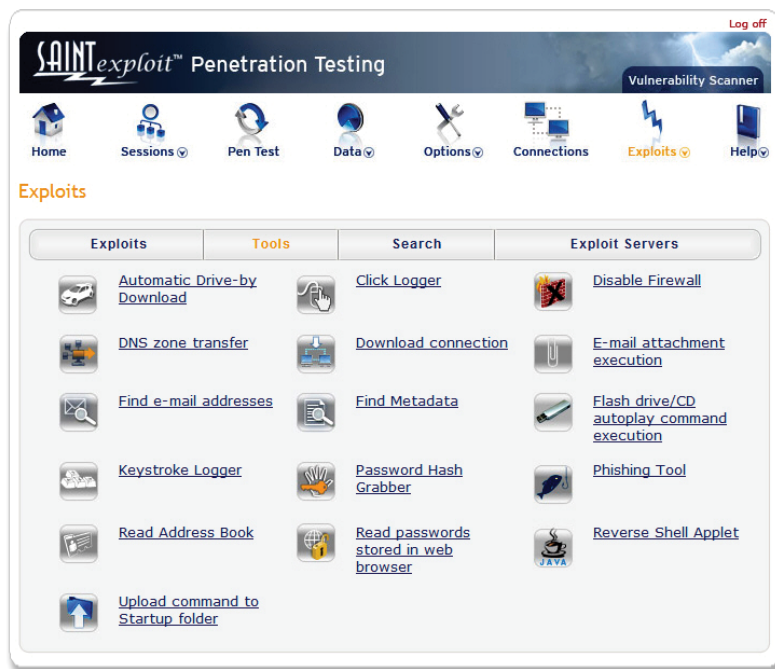
# SAINTexploit<sup>®</sup> Penetration Testing

## Integrated Scans and Exploits

SAINTexploit goes beyond simply detecting vulnerabilities to safely exploiting them.

### Examine. Expose. Exploit.

This fully automated product examines potentially vulnerable services discovered by the SAINTscanner, exposes points where an attacker could breach the network, and exploits the vulnerability to prove its existence. 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

- Linux, Unix, or Mac OS X platform
- Disk Space/memory
  - 100 MB to run
  - Additional space for optional packages (e.g., Samba, NMAP, OpenSSL, OpenSSH)
  - 2 GB of RAM is recommended
- Essential Software
  - PERL 5.004 or above
  - Web browser (e.g., Internet Explorer, Firefox, Safari)

## SAINTexploit at a Glance

- Exploits vulnerabilities found by SAINTscanner proving the existence of critical vulnerabilities.
- Features seamless integration with the SAINTscanner graphical user interface
- Exploit tools provide extra penetration testing capabilities
- Includes social engineering tools such as phishing and flash drive autoplay
- 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

## SAINT Appliances



Portable

Mini w/LCD

Rack Mountable

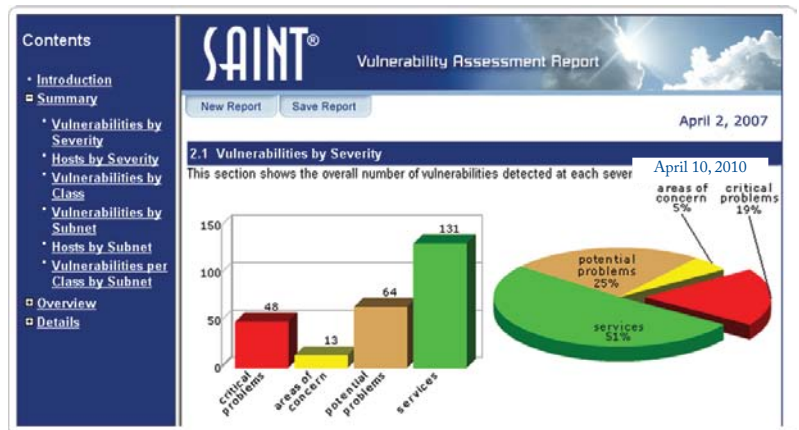
USB Flash Drive

The **SAINTmanager**® browser-based console provides the ability to centrally manage an entire network of SAINTscanners located around the globe from a single interface. This provides the following benefits:

- **Quicker enterprise-wide vulnerability scanning**, regardless of organization size.
- **Distributed architecture** that supports as many remote SAINTscanners as needed.
- **Delegation of responsibilities** to other department owners for assigning administration roles such as scanning, tickets, reporting, etc.
- **Remote access** for administration from any Internet connection and a browser.
- **Centralized default and custom reporting** of threats and risks of the organization.
- **Dashboard with trending analysis** illustrating if security posture is improving over time.
- **SSL encryption** ensures that scan results are secure as they travel across the network between the management console and all nodes.



SAINTmanager® Overview page



**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.

- **Numerous standard reports** ranging from executive summary to technical detail.
- **Multiple format selections** such as HTML, PDF, CSV, XML, plain text and tab separated.
- Each report has **configurable options**. The customized formats can be saved for future use. Brand reports with your own logo.
- **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.
- **Correlation of vulnerability cross references** such as CVE, CVSS, OVAL, CPE, IAVA, OSVDB, BID, Microsoft IDs, vendor IDs, exploit available, and many more.
- Reports can be **easily exported** to other applications like spreadsheets, word processors, and databases.