
# Running a Default Vulnerability Scan

## A Step-by-Step Guide

www.saintcorporation.com

## Examine. Expose. Exploit.

*Welcome to SAINT!* Congratulations on a smart choice by selecting SAINT's integrated vulnerability assessment and penetration testing tool (SAINTexploit™). With SAINT, you can examine your network for vulnerabilities, identify exposed resources, and safely exploit them. The SAINT product suite offers you a complete solution to evaluate the threats to your network and help you determine if your current security investments are preventing attacks.

The following is a step-by-step guide to running a default SAINT vulnerability scan.

## Download SAINT

1. Go to *http://www.saintcorporation.com/*
2. Select the "Customer Login" button located in the top right corner
3. Enter your customer login and password
4. Under *My Software Downloads*, choose SAINT+SAINTexploit, and click on *Continue*
5. Choose the platform: Linux, Solaris, FreeBSD, Mac, Ubuntu, or Red Hat
6. Accept the license agreement
7. Save the file in the directory where you want to install SAINT
   *Example:* /root or /usr/local/src



## Install SAINT

*These instructions apply if you chose the platform "Linux". For other platforms, follow the instructions shown on the download page*

1. Unzip the downloaded file: `gunzip saintexploit-install-x.x.gz` (`x.x` is the version number).
   *Note:* The downloaded file is gzipped. If your browser dropped the `.gz` extension from the filename, rename it so it ends in `.gz`.
2. Set the execution mode on the file: `chmod a+x saint-exploit-install-x.x`
3. Install SAINT by entering: `./saintexploit-install-x.x`
4. Accept the license agreement
5. Enter the saint directory: `cd saint-x.x`

The README file (`more README`) contains information that you should know before using SAINT, such as the startup procedure and the recommended utilities which will automatically be used by SAINT if they are installed:

- Nmap and Xprobe2 – advanced host type detection capabilities.
- Samba – Helps with Windows file system checks and SMB file sharing checks

- OpenSSL – Enables scanning of SSL Web servers
- OpenSSH – Local Linux checks and SSH password checks

## Generate a Key

The key specifies the licensed targets.

- Log on using your customer ID:
  *http://www.saintcorporation.com*
- Choose *New Key*
- Enter your IP address range
  *Tip:* SAINT's "Discovery" scan level is useful for determining your target IP addresses
- Click on *Verify Key*, then *Generate Key*
- Leave the browser open

## Configure the Key

Once SAINT is installed, use SAINT by following these steps:

- `./saint` (or double-click icon).
  *Note:* SAINT should always be run as "root"
- Choose *Configure SAINT Key* from the pull-down menu
- Cut and paste your key into SAINT® (include #Begin Key and #End Key)
- Click on *Save SAINT* Key
- If you see a Password Disclosure warning, click on *Reload*



## Start the Scan

First, always be certain that you have permission to scan any hosts.
*Note:* You will need PERL v5.0 or above to get SAINT running properly.

Choose *Scan* to select the target host(s), scan level, and firewall support, and to start the scan.

1. Enter the IP address of a target host in the first set of boxes, and click the *Add* button
2. Choose *Vulnerability* under the *Scanning Level* tab
3. Leave *Exhaustive* and *Full Port Scan* checked, and *Extreme* unchecked
4. Choose *No Firewall Support* under the *Other Options* tab (*Note:* Review the *Other Options* before starting the scan to ensure the firewall support mode is correct, i.e., Ping, TCP Sweep, etc.)
5. If the target's authentication credentials are known, enter them under the *Authentication* tab
6. Choose *Scan Now* to begin scanning

### SAINT Control Panel

While running a scan, SAINT opens a control panel with various options –

*Note:* you may need to disable your browser's popup blocker.

- Pause and Resume the scan – finishes all probes in progress and then waits for Resume
- Stop the scan – Interrupts the scan and can only be recovered by going back to *Scan*
- The progress bar shows the ratio of completed probes for each phase. A typical scan has three or four phases.

### SAINT Status Updates

SAINT tells you the name, target, flags, and maximum time for each probe. The maximum time tells how long SAINT allows a probe to run before assuming it is hung and killing the process. The probe name is the name of an executable file in the bin directory. The same information you see on the screen is logged in *status_file*.

You can view results in progress in a separate *SAINT Data* pane below the status updates.

## SAINT Probes

SAINT's vulnerability checks are divided into probes. Each probe launches a set of "attacks" designed to detect vulnerabilities in a certain service, or of a certain type. Examples include FTP vulnerabilities, Sendmail vulnerabilities, and distributed denial-of-service. All probes are found in *bin/*.saint*.



**Core probes** are probes that run against every target you specify. **Conditional probes** are probes that run against a target only if a condition is met. The results of a core probe cause conditional probes to run.

A typical probe sequence would be as follows –

1. tcpscan probe runs (a core probe) and detects an open finger port
2. finger probe runs (a conditional probe) and detects accounts "foo" and "bar"
3. login probe runs (another conditional probe) and tries to guess password to "foo" and password to "bar"

## Data Analysis

The four main categories found in SAINT's Data Analysis section are reports, vulnerabilities, host information, and trust. The categories differ in that each will emphasize and display different portions of the scan data.

To analyze the scan results, click on the link to *Reporting and Analysis*. (Alternatively, you could go back to the previous screen and choose *Data.)* The Data page provides links to create reports or to view vulnerability or host information in a variety of views.

## Severity Levels

### Critical Problems

Critical problems could allow an attacker to gain unauthorized access to files, execute commands, or create a denial-of- service. Such problems could include guessable passwords, buffer overflows, unrestricted file sharing, etc.
*Example* – host1.domain.com: Exports /export/home to everyone

### Areas of Concern

Areas of concern are problems which do not allow an attacker to gain direct, unauthorized access, but do allow the following:

- Access to information on network or host configuration (e.g., FTP bounce, finger information)
- Privilege elevation
- Use as an intermediary (e.g., cross-site scripting)
- Susceptibility to malicious content (e.g., vulnerable browsers)

*Example* – host2.domain.com: Excessive finger information

### Potential Problems

These are conditions which may or may not be vulnerabilities, depending on the version or configuration. Further investigation is usually required on the part of the administrator. SAINT cannot always tell whether or not a vulnerability is present. These should **not** be interpreted as "low" severity, since a potential problem could be critical if it exists. This is also where false positives would appear.

*Example* – host3.domain.com: Possible buffer overflow in rpc.statd

### Services

This indicates that a network service is running or open, and is reported for informational purposes. This does not indicate a vulnerability.

*Example* – host4.domain.com: Offers FTP

## Vulnerabilities

Vulnerabilities are further subdivided into more specific severity levels. Click on a severity level to see all the vulnerabilities detected at that level. For each vulnerability, the host name, vulnerability description, and CVE name (if applicable) are shown. Each field is hyperlinked to further information.

The *Exploit* link means there is a corresponding exploit available in SAINTexploit, SAINT's penetration test tool. Simply click the link to run the exploit.

### Confirmed vs. Inferred Vulnerabilities

 A checkmark on the icon means that the vulnerability is confirmed. Confirmed vulnerabilities are determined by definitive test, for example successful password guess or read access to a file on the target.

The inferred vulnerability icon does not contain a checkmark. Inferred vulnerabilities are determined by known information, for example service banners or software version numbers. Inferred vulnerabilities are not necessarily false positives; they are detected through the use of a different methodology.

## Host Information

You can click on a host name to get the following host-specific information:

- Scan time
- Scan level
- Operating system type, if known
- Netbios name, if known
- MAC address, if known
- Subnet (first three octets of IP address)
- List of services running
- List of vulnerabilities detected



All host information is hyperlinked to further information. You can click on a service to see a list of hosts running that service, or go back and click on the system type to see a list of hosts which are of the same type.

## Vulnerability Tutorials

Click on a vulnerability to bring up a tutorial or knowledge base for that vulnerability. Tutorials are divided into the following six sections:

1. **Impact** – The potential consequences of the vulnerability
2. **Background** – Any general information which might be useful to help you understand the problem.
3. **The Problem** – Specific information about the cause of the vulnerability, how it could be exploited, and what platforms or versions could be affected.
4. **Resolution** – Instructions on how to fix the vulnerability, with links to any necessary patches or upgrades.
5. **More Information** – Links to advisories, mailing list postings, and any other resources which provide additional information.
6. **Technical Details** – Port number or service name and network data or test method, if available.

Exit SAINT by closing the browser.